

**UNIVERSITATEA „SAPIENTIA” DIN CLUJ-
NAPOCA**

**FACULTATEA DE ȘTIINȚE TEHNICE ȘI UMANISTE,
TÎRGU MUREȘ**

**SPECIALIZAREA TECHNOLOGII ȘI SISTEME DE
TELECOMUNICAȚII**

**Analiza traficului de rețea sub diferite sarcini de trafic
PROIECT DE DIPLOMĂ**

Absolvent:

Erszény Péter-Tibor

Coordonator științific:

Dr. ing. Hajdu Szabolcs

2024

Extras

Scopul tezei este de a proiecta diferite topologii de rețea pentru a testa debitul și capacitatea de încărcare a diferitelor tipuri și mărci de routere în condiții reale de trafic. Se va compara randamentul mai multor routere. Pentru comparație au fost selectate routere cu lățimi de bandă de linie de 100 Mbps și 1 Gbps, atât corporative, cât și casnice sau SOHO (Small Office Home Office), examinând diferența de performanță dintre fiecare router. În plus, studiul include și o comparație preț-performanță, analizând când și în ce condiții de încărcare un utilizator casnic ar considera că merită să achiziționeze un router dintr-o gamă de preț mai mare. Dispozitivele utilizate au fost TP-Link ER6120, TP-Link WR941ND, Cisco 2800 Series și ASUS RT-N18U. Pentru comparație au fost utilizate două programe diferite de testare a rețelelor: Iperf și SourcesOnOff. Iperf este cel mai utilizat program de testare a lățimii de bandă și a debitului de rețea, în timp ce SourcesOnOff generează fluxuri de date de diferite lungimi care apar într-o rețea reală pe baza parametrilor de distribuție care aproximează cel mai bine structura traficului de rețea într-o rețea reală. Parametrii hardware și software calculatoarelor utilizate pentru testare sunt identice, astfel încât acest lucru nu reprezintă un factor în generarea fluxurilor de date, în timp ce cablurile de date și conectorii sunt, de asemenea, de aceeași marcă, garantând eficiența măsurătorilor. Testarea se face prin măsurarea și compararea vitezelor de date pentru a vedea cum se comportă fiecare router în diferite condiții de rețea. În timpul măsurătorilor, mai multe calculatoare sunt conectate la același router generând continuu un trafic de date în creștere prin comutarea sistematică între diferite adrese IP și protocoale, generând un flux de date complet natural în timp ce se măsoară debitul. În paralel, traficul generat este injectat cu așa-numitele date cunoscute predefinite pentru a determina impactul unei anumite sarcini asupra unui anumit trafic de date al utilizatorului.

Cuvinte cheie: lățime de bandă, Router, TCP-UDP, Iperf, SourcesOnOff

**SAPIENTIA ERDÉLYI MAGYAR
TUDOMÁNYEGYETEM**
MAROSVÁSÁRHELYI KAR
INFOKOMMUNIKÁCIÓS HÁLÓZATOK ÉS RENDSZEREK SZAK

**Hálózati adatforgalom vizsgálata
különböző adatforgalmi terhelés
mellett**
DIPLOMADOLGOZAT

Végzős hallgató:
Ersény Péter-Tibor

Témavezető:
Dr. ing. Hajdu Szabolcs

2024

Kivonat

A dolgozat célja különböző hálózati topológiák kialakítása, amely segítségével megvizsgálható valós forgalom terhelése alatt különböző típusú és márkájú routerek átviteli sebessége, terhelési kapacitása. A dolgozatban több router átviteli sebessége kerül összehasonlításra. Az összehasonlítás során 100 Mbps-es, illetve 1 Gbps vonal sávszélességgel rendelkező routerek kerültek kiválasztásra úgy vállalati, mint otthoni vagy SOHO (Small Office Home Office) kategóriában, vizsgálva az egyes routerek közti teljesítmény különbséget. Emellett a vizsgálat kiterjed a teljesítmény összehasonlításra is keresve a választ arra, hogy egy otthoni felhasználónak mikor, milyen terhelési mutatók mellett érne meg egy magasabb árkategóriás router beszerzése. A használt eszközök a következők: TP-Link ER6120, TP-Link WR941ND, Cisco 2800 Series és ASUS RT-N18U. Az összehasonlítás során két különböző hálózat tesztelési program volt használva: az Iperf és a SourcesOnOff. Az Iperf a legelterjedtebb hálózati sávszélesség és adatátvitel tesztelő program, míg a SourcesOnOff egy valós hálózatban is fellépő különböző hosszúságú adatfolyamokat generál olyan elosztási paraméterek alapján, amelyek a legjobban megközelítik egy valós hálózatban létrejövő hálózati forgalom felépítését. A teszteléshez használt számítógépek hardver és szoftver paraméterei megegyeznek, hogy az adatfolyam generálásnál ez ne legyen befolyásoló tényező, ugyanakkor az adat kábelek és csatlakozók ugyancsak azonos gyártmányúak garantálva a mérés eredményességét. A tesztelés során az adatátviteli sebességet mérve és összehasonlítva vizsgáljuk, hogy melyik router milyen teljesítményt nyújt különböző hálózati feltételek mellett. A mérés alatt több számítógép csatlakozik ugyanazon routerre folyamatosan egy növekvő adatforgalmat generálva különböző IP cím és protokoll szisztematikus váltásával így egy teljesen természetes adatfolyamot generálva eközben az átviteli sebesség mérése zajlik. Ezzel párhuzamosan a generált forgalomban előre meghatározott ügynevezett ismert adat kerül injektálásra, amellyel meghatározható az adott terhelés hatása egy adott felhasználói adat forgalomra.

Kulcsszavak: Sávszélesség, Router, TCP-UDP, Iperf, SourcesOnOff

Abstract

The aim of this thesis is to design different network topologies to test the throughput and load capacity of different types and brands of routers under real traffic load. The throughput of several routers will be compared. Routers with 100 Mbps and 1 Gbps line bandwidths were selected for comparison, both enterprise and home or SOHO (Small Office Home Office) categories, examining the performance difference between each router. In addition, the study also includes a price-performance comparison, looking at when and under what load conditions a home user would find it reasonable to purchase a router in a higher price range. The devices used are the TP-Link ER6120, TP-Link WR941ND, Cisco 2800 Series and ASUS RT-N18U. Two different network testing programs were used in the comparison: Iperf and SourcesOnOff. Iperf is the most widely used network bandwidth and throughput tester, while SourcesOnOff generates data streams of different lengths that occur in a real network based on distribution parameters that best approximate the structure of network traffic in a real network. The hardware and software parameters of the computers used for testing are identical so that this is not a factor in the generation of the data streams, while the data cables and connectors are also of the same make, guaranteeing the effectiveness of the measurement. The testing is done by measuring and comparing data rates to see how each router performs under different network conditions. During the measurement, several computers are connected to the same router continuously generating an increasing amount of data traffic by systematically switching between different IP addresses and protocols, generating a completely natural data stream while measuring the throughput. In parallel, the generated traffic is injected with predefined so-called known data to determine the impact of a given load on a given user data traffic.

Keywords: bandwidth, Router, TCP-UDP, Iperf, SourcesOnOff

TARTALOM

1.	Bevezetés.....	8
2.	Elméleti megalapozás.....	10
2.1.	Szabványok és protokollok.....	10
2.2.	Internet	11
2.3.	OSI modell.....	12
2.4.	TCP/IP modell.....	15
2.5.	Az IP (Internet Protocol) protokoll	18
2.6.	A TCP Protokoll.....	20
2.7.	Az UDP Protokoll	22
2.8.	Útválasztó	23
2.9.	Hálózati kapcsoló	25
2.10.	DHCP	26
2.11.	Internet sebesség mérése.....	28
2.12.	NAT	29
2.13.	Cisco Packet Tracer.....	30
2.14.	Tűzfal	30
3.	A rendszer tervezése és felépítése	32
3.1.	A rendszer architektúrája.....	32
3.2.	Rendszer követelmények	34
3.2.1	Funkcionális követelmények.....	34
3.2.2	Nem funkcionális követelmények.....	34
4.	Részletes tervezés.....	35
4.1.	A hardver összetétele és konfigurációja	35
4.2.	A mérés menete.....	36
4.2.1	Iperf	36
4.2.2	Iperf hibája	38
4.2.3	SourcesOnOff.....	39
4.3.	Mérési eredmények	40
4.3.1	TP-LINK TL-WR941ND mérési eredményei.....	40
4.3.2	Cisco 2800 mérési eredményei.....	43
4.3.3	ASUS RT-N18U mérési eredményei	45
4.3.4	TP-LINK TL-ER6120 mérési eredményei.....	47
4.4.	Terhelés közbeni mérési eredmények.....	50
4.5.	Router szűrő funkció implementálása	53

4.6.	Tűzfal beiktatása a rendszerbe.....	56
5.	Összegzés.....	59
6.	Ábrajegyzék	60
7.	Hivatkozások.....	61

1. BEVEZETÉS

Az embernek mindig is megvolt az igénye, hogy kommunikáljon embertársaival, a beszédkésztséget már nagyon rég használjuk a mindennapokban, alap és természetes dolognak tartjuk. Ahogy az emberiség fejlődött az évek során, úgy fejlődött a kommunikációs stratégia is. Jött az írás, olvasás, majd a levél, mint hosszabb távolságok áthidalására feltalált eszköz. A levél kézbesítése egy lassú folyamat. Ezt szerették volna kiküszöbölni, felgyorsítani, ennek hatására megjelentek olyan technológiák, amelyek ezt a fajta igényünket próbálták kielégíteni. A technológia lassan fejlődik, és ez a fejlődés hozza magával a kommunikációs eszközök fejlődését is. Megjelennek a távírók, amiknek az átviteli sebessége a profi távírársoknál akár 50-60 szó/ perc volt, melyekkel már sokkal nagyobb távolságot lehetett áthidalni sokkal rövidebb idő alatt (fénysebességgel). Az első a Bell által 1846-ban feltalált telefon. [1] Ezt a fajta fejlődést követte a telefon hálózatok kialakítása, ami behálózta az egész világot, ezzel lehetővé téve a gyors információcserét a világ minden táján. Az analóg telefonok hosszú éveken és évtizedeken át szolgálták az embereket, mígnem megjelent az igény az egyszerű telefonhálózatok digitalizálására (ISDN), annak jobb S/N (Signal to Noise Ratio) aránya és jobb minősége miatt. Az ISDN átviteli sebesség maximuma 64kbps volt. A digitális telefon megszületése után jelent meg a digitális adat továbbítás az adott hálózaton keresztül: xDSL (Digital Subscriber Line). A DSL technológia már az átviteli sebességet is megnövelte, aminek maximuma 2Mbps alap ADSL (Asymmetric DSL) átvitel esetén, és 24Mbps ADSL2 átvitel esetén. A 60-as években az Amerikai Védelmi Minisztérium által kifejlesztésre került az ARPANET, ami az internet legelső változata volt. Az ARPANET számítógépeket kötött össze, több amerikai egyetem között. Az ARPANET már használt kezdetleges útválasztást, és itt jelent meg a csomagkapcsolás első változata is. Az ARPANET projektet követte a ma is használatos internet. Az internet fejlődése és fejlesztése mind a mai napig töretlen. A gyorsabb adat átvitel, a nagyobb frekvencia, a kábelek tökéletesítése, a protokollok finom hangolása mind hozzájárult ahhoz az internethez, amit a mai napig használunk. Az egyre nagyobb adatmennyiség áramlása miatt, az interneten egyszerre keresztülvihető adat mennyiségének is növekednie kellett, főleg az élő műsorszórás miatt, aminek az átviteli sebessége nagy, a videó minőségétől függően. A ma használt internet sebessége elérheti az akár 10Gbps-ot is. Ennek a technológiának az eléréséhez sok ember ötlete és találékonysága járult hozzá.

A dolgozat témája az adat átviteli sebességre fókuszál, különböző hálózati topológiákban. A megvalósítás során több router adatátviteli sebessége került összehasonlításra, különböző hálózati terhelés mellett. A cél valós képet kapni a különböző kategóriájú és árfekvésű routerek átviteli sebességéről. Egy 100Mbps-os vállalati router, illetve egy otthoni felhasználásra szánt router, valamint egy 1Gbps vállalati, ugyancsak egy otthoni felhasználásra szánt router került összehasonlításra adott sebesség kategóriában. A dedikált routerek összehasonlítása mellett, még egy router funkciókkal rendelkező szoftverben implementált tűzfal mérés is a dolgozat tárgyát képezi. A dolgozat célja az azonos átviteli sebességet biztosító routerek összehasonlítása nyers, illetve szaggatott adatfolyamok esetén. A mérési eredmények összevetése a gyártó által megadott paraméterekkel történik.

2. ELMÉLETI MEGALAPOZÁS

2.1. Szabványok és protokollok

A szabványok és protokollok kiemelkedően fontosak a számítástechnikában és a hálózati kommunikáció területén. Ezek a normák meghatározzák hogyan kell működniük az egyes komponenseknek és rendszereknek ahhoz, hogy kompatibilisek legyenek, és kommunikálni tudjanak egymással. „A szabványok azt definiálják, ami az együttműködéshez (interoperability) kell: se többet se kevesebbet” (Tannenbaum & Wetherall, 2013, old.: 174). A szabványok lényegében meghatározzák azokat a minimális követelményeket, amelyeket az eszközöknek és rendszereknek tudniuk kell ahhoz, hogy gond nélkül kommunikálni tudjanak egymással. A szabványok pontosan meghatározzák az ilyen együttműködéshez szükséges alapvető feltételeket, mint az adatok formátumát, az adatközlés módját, és más technikai részleteket. Ezekre a szabványokra azért van szükség, hogy a különböző gyártóktól származó eszközök és rendszerek összekapcsolódhassanak, és együttműködhessenek anélkül, hogy mélyrehatóbban ismerni kellene a másik rendszer belső felépítését és működését. A szabványok segítenek az iparág fejlődésében. Ezáltal a felhasználók számára nagyobb választékot és rugalmasságot biztosítanak, miközben garantálják a különböző rendszerek és eszközök zökkenőmentes együttműködését.

A szabványokat két csoportra lehet osztani, „de facto” és „de jure”. A „de facto” szabványok olyan szabványok, amelyek a gyakorlatban alakultak ki, és váltak elfogadottá anélkül, hogy valamilyen szabványügyi szervezet állt volna a szabvány létrejötte mögött. Ezeket a szabványokat a piaci erők, az iparági szokások tették széles körben elfogadottá és így alakultak ki. A „de facto” szabványok jellemzően azáltal váltak elfogadottá, hogy sokan használják, mivel rendelkeznek egy előnyös tulajdonsággal, vagy könnyebb implementációs előnyökkel. A „de facto” szabványok jelentősége, hogy gyakran sokkal jobban és gyorsabban kielégítik a piac igényeit, mint a „de jure” szabványok. „De facto” szabványok például az MP3 (MPEG Layer 3) formátum a WAV (Waveform Audio File Format) alternatívájaként indult az internetes zenei terjesztésben, majd felváltotta azt. Ma már a legtöbb zenelejátszó média támogatja. Egy másik ilyen szabvány az Ethernet, magas megbízhatósága és könnyű telepítése miatt vált a helyi hálózatok közkedvelt szabványává.

A „de jure” szabványok olyan hivatalos szabványok, amelyeket szabványügyi hivatalok hoztak létre és fejlesztettek ki a hivatalos eljárások mentén. Ezek a szabványok jól dokumentált és rögzített dokumentumok, melyek teljes mértékben megmagyarázzák a szabvány használatát az adott területen. A „de jure” szabványok létrejöttéért egy vagy több szabványügyi szervezet munkája szükséges, legyen az államközi vagy önkéntes szervezet. A legismertebb szabványosítási szervezetek közé tartozik az ISO (International Standard Organization), az ITU (International Telecommunication Union), az IETF (Internet Engineering Task Force) vagy az IEEE (Institute of Electrical and Electronics Engineers), vagy más iparági vagy regionális szervezetek. Ezek a szabványok gyakran hivatkozási pontot jelentenek a termékek, szolgáltatások vagy folyamatok minőségének és megfelelőségének mérésében és értékelésében. „De jure” szabvány például az IEEE 802.11, amely a vezeték nélküli hálózatok kialakításához és működtetéséhez szükséges szabványt írja le, amit az IEEE fejlesztett ki és írt le, ezzel meghatározva a Wi-Fi technológiát. Egy másik példa az ISO 18000, ami az RFID (Radio-Frequency Identification) technológiát írja le, ami egy fontos szerepet tölt be az azonosítás és nyomkövetés terén. [2]

A protokoll szabályok összessége, amely az adatok formázására és feldolgozására vonatkozik. A protokoll a számítógépes hálózatokban az úgynevezett „közös nyelv”, melynek segítségével tudnak a számítógépek kommunikálni egymással. Ahhoz, hogy egy protokoll működhessen, mind a két félnek ismernie kell a protokollt a sikeres kommunikáció érdekében. Ez nagyban hasonlít ahhoz, mikor két teljesen más anyanyelvet beszélő ember, tegyük fel, hogy egy német és egy japán ajkú ember ahhoz, hogy egymással kommunikálni tudjanak, az angolt, mint közös nyelvet használják, feltételezve, hogy mind a ketten ismerik azt, tudnak beszélgetni. Ebben a példában a protokoll az angol nyelv. [2] Ilyen protokollra számos példát lehet keresni az internet világában, mint a TCP, UDP protokollok, melyekről a későbbiekben még szó lesz. [3]

2.2. Internet

Az „internet” egy globális hálózat, amely különböző számítógépeket és hálózati eszközöket kapcsol össze szerte a világon. Az internet lehetővé teszi az adatok cseréjét, a kommunikációt, az információhoz való hozzáférést és az online tartalmak megosztását.

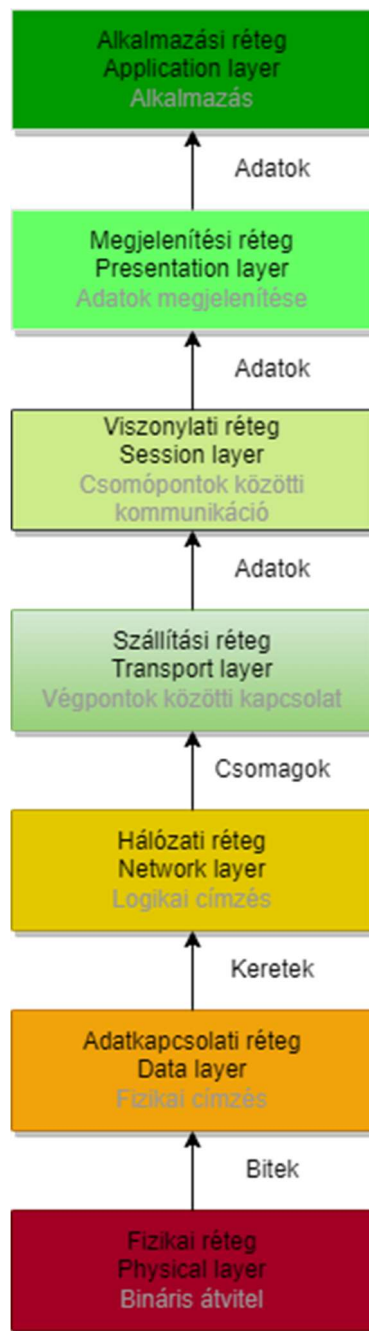
Az internet a következő fő jellemzőkkel rendelkezik:

1. Globális elérhetőség: Az internet egy világméretű hálózat, amelyen keresztül a felhasználók a világ bármely részén könnyen elérhetik az információkat és a szolgáltatásokat.
2. Számítógépek és eszközök hálózata: Az interneten keresztül számítógépek, okostelefonok, táblagépek, szerverek és más hálózati eszközök kapcsolódnak egymáshoz.
3. Protokollok és szabványok: Az internet működését különböző protokollok és szabványok szabályozzák, például a TCP/IP (Transmission Control Protocol/Internet Protocol), amely az adatátvitelt és az adatok csomagolását kezeli.
4. Weboldalak és alkalmazások: Az interneten található weboldalak, alkalmazások, szolgáltatások és tartalmak sokféle témában érhetők el, beleértve az információkeresést, a közösségi médiát, az online vásárlást, az oktatást és még sok más.
5. Elektronikus levelezés: Az internet lehetővé teszi az elektronikus levelezést (e-mail), amely egy gyors és hatékony kommunikációs eszköz.
6. Online kapcsolatok: Az internet lehetővé teszi az emberek számára, hogy online kapcsolatba lépjenek másokkal, például közösségi média platformokon vagy online csevegőszolgáltatásokon keresztül.

Az internet elindítása és fejlesztése a múlt század közepén kezdődött, és azóta folyamatosan bővül és fejlődik. A közös szabványok és protokollok révén, az internet összekapcsolja a világ számítógépes rendszereit és eszközeit, létrehozva a digitális információs és kommunikációs kor egyik kulcsfontosságú alapját. [4]

2.3. OSI modell

Az OSI (Open System Interconnection) modell egy ISO alapján szabványosított különböző rétegeket használó hivatkozási modell.



ábra 1

OSI modell 7 rétege

Az OSI modellnek 7 különálló rétege van, 5 felosztási elvet követve:

1. A rétegek különböző absztrakciós szinteket képviselnek
2. Minden réteg jól definiált feladatot hajt végre

3. A rétegek feladatának definiálásakor a nemzetközileg szabványosított protokollokat kell figyelembe vennie
4. A rétegek határait úgy kell meghatározni, hogy a rétegek közötti információcsere minimális legyen
5. A rétegek számának elég nagynek kell lennie ahhoz, hogy eltérő feladatok ne kerüljenek szükségtelenül ugyanabba a rétegbe, viszont elég kicsinek kell lennie ahhoz, hogy az architektúra ne váljon kezelhetetlenné.

Az OSI modell 7 réteget úgy szabványok, mint protokollok alkotják. Minden egyes rétegnek megvan a maga protokollja, ami szerint meg tud történni a kommunikáció. [2]
Röviden részletezni fogom a 7 réteg tulajdonságát.

Az OSI modell első rétege a fizikai réteg (Physical Layer) dolgozik a hardverhez legközelebb, mivel a bitek fizikai átvitelével, az átviteli közeggel foglalkozik. Meghatározza a fizikai közeg jellemzőit, mint az elektromos jellemzők, vagy a fényimpulzusok. Az adatok átvitele történhet fizikai kábeleken, mint a sodrott érpár, koaxiális kábel, vagy történhet vezeték nélkül is, mint rádióhullámos átvitel. Főbb protokolljai: DSL (Digital Subscriber Line), 802.11.

Az adatkapcsolati réteg (Data Link Layer), mint a modell második rétege, fő feladata biztosítani, hogy az adatok a megfelelőképpen megérkezzenek a közegen keresztül egyik eszközről a másikra, a megfelelő sorrend biztosítása az átvitel során. Kezeli az adatok össze és kicsomagolását. A két legfőbb protokollja ennek a rétegnek a MAC és az LLC. Még megemlíthető a 802.11 vagy az Ethernet protokollok.

A harmadik. réteg a hálózati réteg (Network Layer), feladata a csomagok eljuttatása a forrástól a célállomásra. A réteg meghatározza és kijelöli az útvonalat, az összeköttetést, megadott kritériumok szerint, feladata az optimális út kiválasztása. Másik feladata az egyszerre történő túl sok adat által okozott torlódások megakadályozása és/vagy kezelése. IGP (Interior Gateway Protocol), ICMP (Internet Control Message Protocol), IP (Internet Protocol), csak néhány az ehhez a réteghez tartozó protokollokból.

A szállítási réteg (Transport Layer) az OSI modell következő rétege, mely feladata a hosztok közötti adatátvitel. Fontos része a címezések kezelése, forrás cél összeköttetések meghatározása, és annak felügyelete. Mivel a forrás és a célállomás gyakran nagy távolságra vannak egymástól, ezért a küldeni kívánt adat több

csomóponton is át kell menjen. A réteg másik feladata ennek kezelése és annak a megvalósítása, hogy a két hoszt csak egy pont-pont összeköttetésnek lássa az adatküldést. Az ehhez a réteghez tartozó protokollok az UDP (User Datagram Protocol), TCP (Transmission Control Protocol), SSL (Secure Socket Layer).

A következő réteg az úgynevezett viszony réteg (session layer), szokás még együttműködési rétegnek is nevezni, mely fenntartja a kapcsolatot a két hoszt között, illetve lebontja a kapcsolatot mikor az már nem használatos. Beiktat ellenőrző pontokat, hogy ne kelljen a meghibásodott adatokat teljesen az elejétől újra küldeni, hanem csak a meghibásodás előtti ponttól. A réteg másik nagyon fontos feladata minden adatcsomag és berendezés szinkronban tartása. Néhány fontosabb protokoll, ami ebben a rétegben található: TCP, SIP (Session Initiation Protocol), RTP (Real Time Transport Protocol).

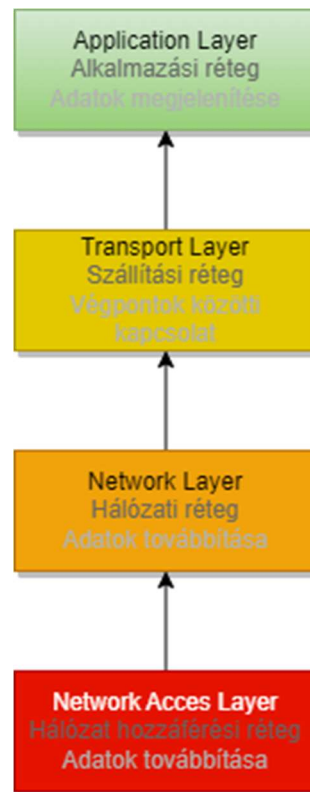
A hatodik réteg a megjelenítési réteg (presentation layer), feladata a bitek által küldött adatcsomagok lefordítását szükséges kódkonverzió, mint például az ASCII (American Standard Code for Information Interchange) vagy más formátumra. Egységes absztrakt adat struktúrákat alakít ki és kezeli azokat. Feladata közé tartozik az adatok tömörítése a kisebb méret elérése, és így könnyebb kezelhetőség miatt, például videóbeszélgetés során. A fontos adatok titkosítása is ebben a rétegben valósul meg. Főbb protokolljai: HTML (HyperText Markup Language), MPEG (Moving Picture Experts Group), JPEG (Joint Photographic Experts Group) stb.

Az OSI modell utolsó rétege az alkalmazási réteg (Application layer), a felhasználóhoz ez a réteg áll a legközelebb, mivel a végfelhasználó az ezen réteg által nyújtott szolgáltatást látja. A megjelenítési réteg egy interfészt biztosít a mögöttes hálózat és felhasználó között. A réteg több protokollt is támogat, mint FTP (File Transfer Protocol) vagy a HTTP (HyperText Transfer Protocol), mely lekéri a weboldal adatait, és megjeleníti azokat egy web böngésző segítségével. [5]

2.4. TCP/IP modell

A TCP/IP modell megvalósulásának egyik fő oka, hogy a hálózat terjeszkedésével a régebbi protokollok nem, vagy csak alig tudtak működni az új technológiákkal, mint a műholdas vagy rádiós kommunikáció. A modellt úgy alkották meg, hogy minden

szempontból lehetővé tegye a hálózatok zökkenőmentes összekapcsolását. [6] Ennek kiküszöbölésére jött létre egy új modell, amit a két legfőbb protokollról neveztek el, amit elsőként Cerf és Kahn [1974] definiált. A másik fő szempont, amit a modellel alkottak meg az az, hogy ha a végpontok közötti kapcsolat megvan, akkor egy alhálózat meghibásodása ne tudja tönkre tenni a teljes kapcsolatot. [2] [7]



ábra 2

TCP/IP modell 4 rétege

A TCP/IP protokollcsomagnak több kulcsfontosságú szolgáltatása van a hálózati kommunikációja során. Néhány ezek közül:

1. **Logikai címzés:** A TCP/IP protokollcsomag lehetővé teszi a logikai címzést azáltal, hogy minden eszköznek a hálózatban egyedi, úgynevezett IP címet rendel hozzá. Az IP címnek az azonosításban és kommunikációban van fontos szerepe
2. **Útválasztás:** A TCP/IP protokollcsomag lehetővé teszi az útválasztást, vagyis az adatok továbbítását a hálózaton belül egy adott útvonalat kijelölve, és azt használva
3. **Névfeloldás:** A TCP/IP protokollcsomag lehetővé teszi a névfeloldást, ami az IP címeket az emberek által könnyebben megjegyezhető formára alakítsa át és fordítva, például a DNS (Domain Name System) segítségével.

4. Hibakezelés és folyamatszabályozás: A TCP/IP protokollcsomag biztosítja a megfelelő hibakezelést és folyamatszabályozást a hálózaton belül, amely így egy megbízhatóbb hálózatot eredményez.
5. Az alkalmazások támogatása: A TCP/IP protokollcsomag lehetővé teszi számos alkalmazás használatát a hálózaton, mint például az email küldése és fogadása, böngészés, fájlmegosztás, videó folyam sugárzása, valamint más alkalmazások, amelyek hatékony és megbízható adatátvitelt tesznek lehetővé.

A TCP/IP modell tervezésének kulcsfontosságú előnyei közé tartozik:

- Univerzalitás: A TCP/IP protokollokat az interneten és a legtöbb hálózati környezetben használják, így a modell egyetemes elfogadottságot élvez.
- Szabványosítás: A modell segít létrehozni és fenntartani szabványokat a hálózati kommunikációhoz, amelyek segítik az interoperabilitást különböző eszközök és rendszerek között.
- Rugalmas skálázhatóság: A négy réteg modellje lehetővé teszi az egyszerűsített fejlesztést, bővítést és konfigurációt a hálózati rendszerek számára.

A TCP/IP modell legelső rétege a hálózat hozzáférési réteg (Network Access Layer) lehetővé teszi az adatok továbbítását egyik hosttól a másik felé. Mivel a TCP/IP modell megalkotásánál a fő szempont a különböző átviteli közegek és protokollok használata volt, ezért ez a réteg képes kezelni úgy a vezetékes, mint a vezeték nélküli protokollokon alapuló átviteli technikákat. Más szóval ez a réteg független bármilyen konkrét hálózati átviteli technológiától.

A modell második rétege, a hálózati réteg (Network Layer) hasonló feladatokat lát el, mint az OSI modell hálózati rétege. Feladata az adatok eljuttatása, azok kezelése, mivel az adatok a kezdeti sorrendtől eltérően is megérkezhetnek, a réteg feladata ezen adatok sorba rendezése. A réteg másik feladata az adatok csomagolása és a különböző elválasztási funkciók ellátása. Az ebben a rétegben használt legfontosabb protokollok az IP (lásd később), az ARP (Address Resolution Protocol), mely felelős az internet rétegben lévő hardver címek feltérképezésében. Az ICMP protokoll diagnosztikai funkciókat lát el, például mikor egy csomag nem érkezik meg, a protokoll észleli a hibát és diagnosztizálja a hiba okát.

A szállítási réteg (Transport Layer) felelős a hosztok közötti párbeszéd megvalósítására, az adatok eljuttatásáért a forrástól a célállomás felé. Az ebben a rétegben használt két legfontosabb protokoll a TCP és az UDP, melyek segítenek az adatok eljuttatásában. A TCP egy az egyhez kapcsolatot hoz létre, figyeli az adatsomagokat, az esetleges adat meghibásodásokat kezeli és/vagy javítja azokat. Ezzel szemben az UDP protokoll egy az egyhez, vagy egy a többhöz kapcsolatot alakít ki, az adatsomagok elküldése után nem követi végig az adat útját a forrástól a célig.

A TCP/IP protokoll utolsó rétege az alkalmazási réteg (Application Layer), mely feladata az adatok kezelése és megjelenítése a végfelhasználó számára. Biztosítja a többi réteghez való hozzáférést. Főbb protokolljai a HTTP, FTP, DNS stb.. [7]

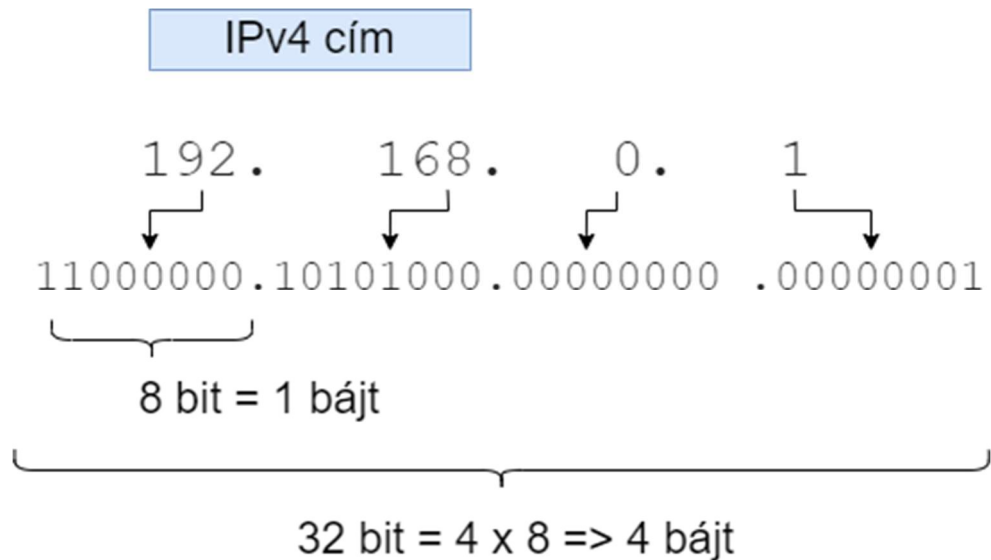
2.5. Az IP (Internet Protocol) protokoll

Az „IP protokoll” vagy az „Internet Protocol” egy olyan protokoll, amely a hálózatokban történő adatátvitelért felelős. Az IP egy alapvető eleme a TCP/IP hálózati modellnek, és az interneten és más hálózatokban a leggyakrabban használt protokoll.

Az IP protokoll fő feladata a csomagok (packets) címezése és továbbítása a hálózaton keresztül. Az IP címkék segítségével azonosítja az adatok forrását és célját. Az IP címek hierarchikus rendszert alkotnak, amelyek segítik az útvonal választási folyamatot.

Az IP protokollnak két verziója van:

IPv4 (Internet Protocol version 4): Ez a régebbi verzió, amely négy bájtos (32 bites) IP címeket használ. Az IPv4 címek például 192.168.0.1 formátumban jelennek meg. Az IPv4 címtartomány korlátozott, és az aktív hosztok számának gyors növekedése miatt a rendelkezésre álló IP címek száma kimerült.

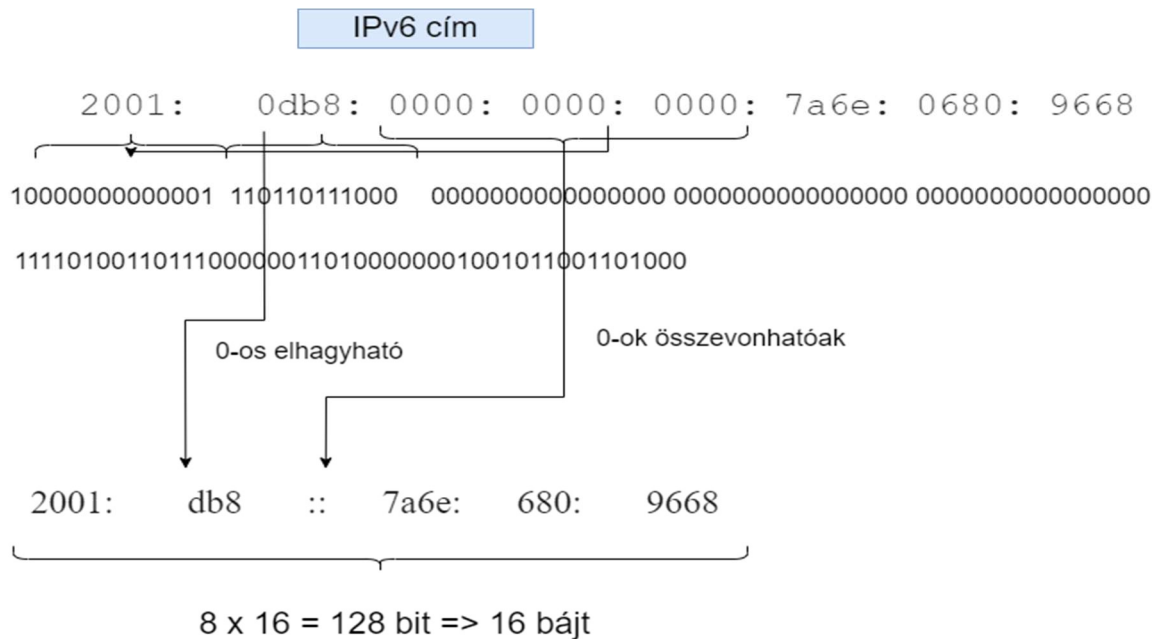


ábra 3

IPv4 képzése

IPv6 (Internet Protocol version 6): Az IPv6 a következő generációs IP protokoll, amely 128 bites IP címeket használ. Ez jelentősen megnöveli a használható címek számát, így a kiosztható címek tartománya kielégíti a világban használt eszközöket. Az IPv6 címek például:

2001:0db8:0000:0000: 0000:7a6e: 0680:9668 formátumban jelennek meg.



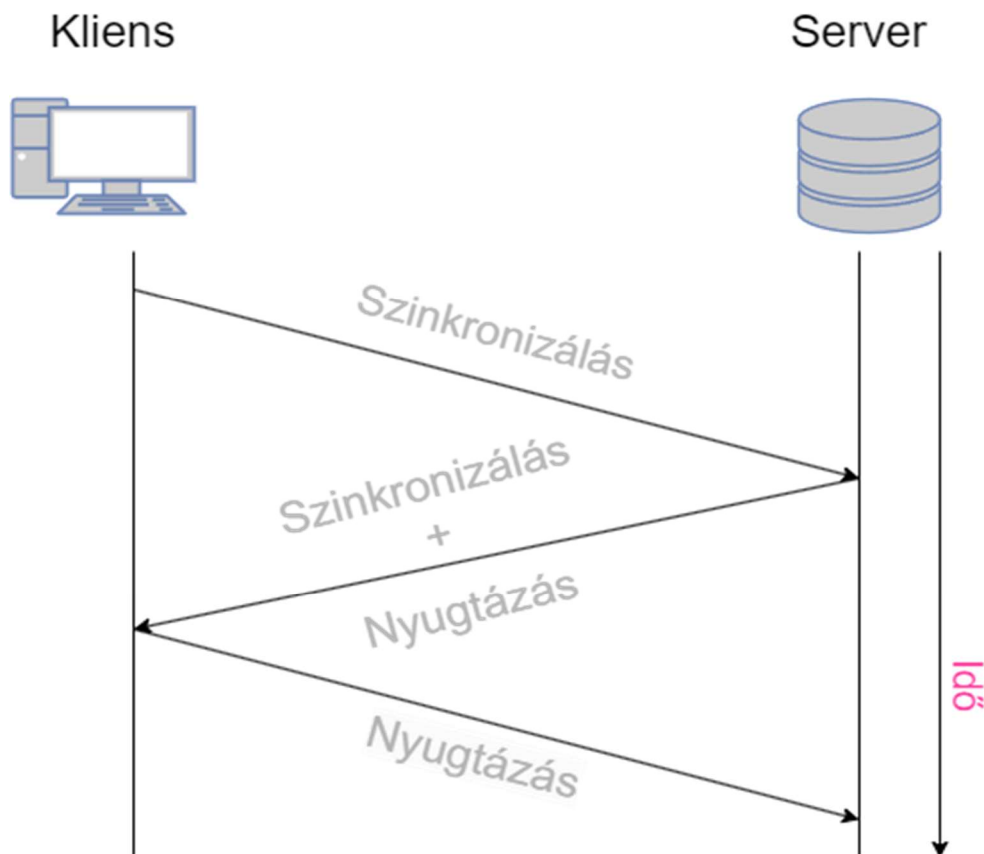
ábra 4

IPv6 képzése

Az IP protokoll együttműködik más protokollokkal a TCP/IP hálózati modellben. Például az IP és a TCP (Transmission Control Protocol) együttműködik a megbízható adatátvitelért, míg az IP és az UDP (User Datagram Protocol) a gyors, viszont nem megbízható adatátvitelért felelős. [6]

2.6. A TCP Protokoll

A TCP (Transmission Control Protocol) egy megbízható kapcsolatorientált protokoll, amelyet a TCP/IP hálózati modell transzport rétegében használnak az adatok megbízható továbbítására. A TCP a számítógépek közötti adatkommunikáció egyik alapvető építőköve, az interneten és más hálózatokon általánosan alkalmazott. A protokoll figyeli az adatok áramlását a hálózaton, és az esetleges hibákat kijavítja vagy újra küldi, monitorizálja az adatok megérkezési sorrendjét, és ha szükséges akkor újra rendezi azokat. [6] [8]



ábra 5
TCP kapcsolat felépítése

Amikor egy feladó (client) TCP kapcsolatot szeretne kezdeményezni egy fogadóval (server) akkor egy három irányú kézfogás (three-way handshake) mechanizmus fog lefolyni a két hoszt között. A három irányú kézfogás az ábra 5-ön látható.

- Első lépésben a feladó egy szinkronizációs üzenetet küld a fogadónak, ami egy egyedi érték, ezzel jelezve a szerver fele, hogy kapcsolatot szeretne kezdeményezni.
- Második lépésben a fogadó egy szinkronizációs és nyugtázó (synchronization + acknowledgment) üzenettel válaszol, amely egy szinkronizációs értéknek eggyel megnövelt értékéből és egy nyugtázó számértékből áll.
- Harmadik lépésben a feladó válaszol egy nyugtázó érték eggyel nagyobb számával. A kapcsolat felépítése ennél a lépésnél lezárul, a kapcsolat ilyenkor sikeresen felépült és az adatküldés megindulhat a két hoszt között. [9]

A TCP protokoll fő jellemzői:

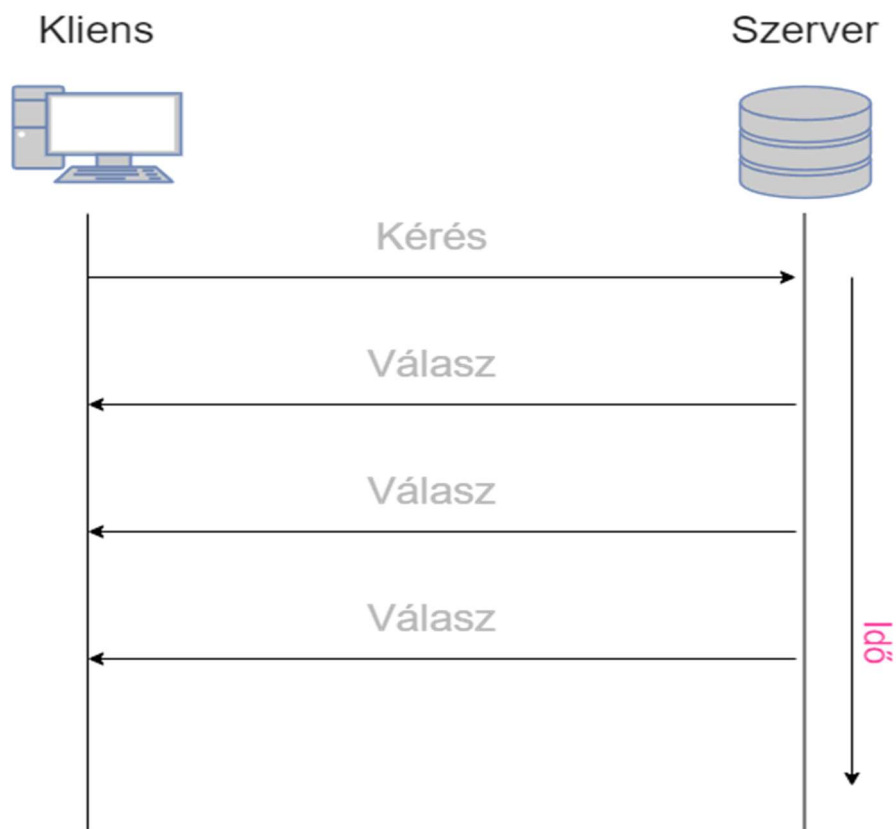
1. Megbízhatóság: A TCP megbízható adatátvitelt biztosít. Ez azt jelenti, hogy az adatokat az egyik végponttól a másikig megbízhatóan és sorrendben továbbítja, gondoskodik arról, hogy az adatok a célpontnál egységesen hibátlanul megérkezzenek.
2. Kapcsolatorientált: A TCP kapcsolatot hoz létre a kommunikáló felek között mielőtt adatokat küldenének. Ez a kapcsolat biztosítja a megbízható adatátvitelt és mindkét fél szinkronban tartja az adatforgalmat.
3. Áramlásszabályozás: A TCP áramlásszabályozást alkalmaz, amely szabályozza a küldő és a fogadó oldal közötti adatátvitelt, és csökkenti a túlzott terhelést vagy adatvesztést a hálózaton.
4. Kézbetétési visszaigazolások: A TCP visszaigazolásokat küld az adatok érkezéséről. Ha az adatok nem érkeznek meg vagy hibásak, a TCP újra küldi azokat.
5. A TCP és az IP (Internet Protocol) együtt alkotja a TCP/IP protokollcsaládot, amely a legtöbb modern hálózati kommunikáció alapját képezi, beleértve az interneten történő adatátvitelt is. A név utal a két fő protokollra, melyet használ. A TCP protokoll az átvitelért, míg az IP az adatok csomagolásáért és továbbításáért felel.

A TCP protokoll folyamatos ellenőrzései miatt késleltetések lépnek fel, ezért ez a protokollt olyankor használják, mikor az a lényeg, hogy az adat biztonságosan és

bithiba nélkül megérkezzen. Ilyen alkalmazás például a fájl átvitel FTP protokollt használva, vagy az e-mail küldése, de számos adatbázis is ezt a protokollt használja az adatok továbbítására.

2.7. Az UDP Protokoll

Az UDP (User Datagram Protocol) egy másik szállítási réteg protokollja a TCP/IP hálózati modellben. Az UDP kevésbé komplex, ugyanakkor nem megbízható, mint a TCP, de a gyorsabb és könnyebb használata miatt használják. Míg a TCP célja a megbízható adatátvitel és a kapcsolatfenntartás, az UDP a gyors és hatékony adatátvitelt preferálja anélkül, hogy megbizonyosodna az adatok sorrendjéről vagy épségéről. Amikor a feladó (Client) UDP kapcsolatot szeretne létesíteni a fogadó (Server) féllal, akkor nincsen más dolga, csak egy kérés (Request) üzenetet küldeni. A fogadó fogadja az üzenetet és folyamatosan küldi a választ (Response) a feladónak anélkül, hogy bármi mást is tenne az adatokkal, lásd ábra 6. A TCP protokollal ellentétben nem követi nyomon az adat útját.



ábra 6
UDP kapcsolat felépítése

Az UDP protokoll fő jellemzői:

1. Nem kapcsolatorientált: Az UDP nem hoz létre kapcsolatot a kommunikáló felek között, mielőtt adatokat küldene. Ez azt jelenti, hogy nem biztosítja az adatok megérkezését, mint a TCP.
2. Nincs kézbesítési visszaigazolás: Az UDP nem küld visszaigazolásokat az adatok sikeres kézbesítéséről. Ha az adatok elvesznek vagy sérülnek, az UDP nem próbálja meg újra küldeni őket.
3. Nincs áramlásszabályozás: Az UDP nem tartalmaz áramlásszabályozási mechanizmust, így nincs olyan funkció, amely megfékezi az adatküldést, ha a fogadó oldal túlterhelt.
4. Gyors és könnyű: Az UDP kevesebb protokollinformációt tartalmaz a fejlécében, ami csökkenti az adatátviteli késleltetést és a hálózati terhelést.

Az UDP-t olyan alkalmazások használják, amelyeknél a gyorsaság fontosabb, mint a megbízhatóság. Példák közé tartozik a hang- és videóközvetítés, a játékokhoz használt adatkommunikáció, a DNS (Domain Name System) kérések stb.. [6] [8]

2.8. Útválasztó

Az útválasztó továbbiakban router egy hálózati eszköz, amely az adatcsomagok útját irányítja a különböző hálózatok között. A router egy eszköz, ami összekapcsol kettő vagy több csomag kapcsolt hálózatot vagy alhálózatot. A routerek az OSI modell harmadik rétegében (Layer 3) működnek. A szakirodalomban a routerek jelölésére az ábra 7 látható piktogramot használják. [10] A routerek lehetővé teszik az eszközök számára, hogy kommunikáljanak egymással, még akkor is, ha különböző hálózatokban vannak.



ábra 7

Router ikonja

A routerek általában két vagy több hálózati interfésszel rendelkeznek. Minden interfész egy adott hálózathoz csatlakozik. A routerek az adatsomagokat az egyik interfésztől a másikkra továbbítják, az adott célhálózat felé.

A routerek fontos szerepet játszanak az internet hálózatokban. Az interneten a routerek az adatsomagokat az internetszolgáltatók hálózatai között továbbítják. A routereknek különböző típusai léteznek, beleértve a vezetékes routereket, a vezeték nélküli routereket és a mobil routereket.

1. Vezetékes routerek

A vezetékes routerek vezetékes hálózatokhoz csatlakoznak. A vezetékes routerek általában Ethernet-kábellel csatlakoznak a számítógépekhez és más eszközökhöz.

2. Vezeték nélküli routerek

A vezeték nélküli routerek vezeték nélküli hálózatokhoz csatlakoznak. A vezeték nélküli routerek általában Wi-Fi-vel csatlakoznak a számítógépekhez és más eszközökhöz.

3. Mobil routerek

A mobil routerek mobil hálózatokhoz csatlakoznak. A mobil routerek általában mobil adatsomaggal csatlakoznak az internethez.

A routerek számos előnnyel járnak, beleértve:

- Az eszközök közötti kommunikáció lehetővé tétele különböző hálózatokon
- Az adatsomagok útjának optimalizálása
- A hálózat biztonságának javítása

A routereknek néhány hátránya is van, beleértve:

- A routerek költségesek lehetnek
- A routerek telepítése és konfigurálása bonyolult lehet
- A routerek meghibásodhatnak, ami a hálózat leállítását okozhatja

Gondoljunk a routerre úgy, mint egy légiforgalmi irányító központra. Az adatok a repülőgépek, a célállomás pedig a reptér. Minden repülőgépnek egyedi célállomása van és egyedi útvonalon halad, úgy kell minden adatsomagot a lehető leghatékonyabban a célállomásra eljuttatni. Ebben a szerepkörben a router a forgalomirányító, és ő felel azért, hogy mindenki eljusson a célállomásra anélkül, hogy elvesznének, vagy ütközések

történnének az út során. A csomagok hatékony irányításához az útválasztó egy belső útválasztási táblázatot használ, a különböző hálózati célállomások elérési útvonalainak a listáját. A router leolvassa a csomag fejlécében, hogy hova is tart, majd megkeresi az útválasztási táblázatból (routing table) a célállomáshoz vezető legjobb utat. Ezután a csomagot továbbítja a következő hálózat felé.

2.9. Hálózati kapcsoló

A hálózati kapcsoló a továbbiakban switch összekapcsolja az eszközöket egy hálózaton (gyakran helyi hálózaton, LAN) belül, és továbbítja az adatsomagokat az eszközök között. Az útválasztóval ellentétben, a kapcsoló csak a neki szánt egyetlen eszköznek (amely lehet egy másik kapcsoló, útválasztó vagy a felhasználó számítógépe) küld adatokat, több eszközből álló hálózatoknak nem. Ethernet protokoll használatával működik a helyi hálózatokban. MAC-cím (Media Access Control) alapján határozza meg, hogy hova továbbítsa a bejövő üzeneteket. A switch az OSI-modell adatátviteli rétegének második rétegében működik (Layer 2).

- **Virtual switches** – kizárólag szoftveres kapcsoló, amit szoftver környezetben belül határozzunk meg
- **Routing switches** – LAN-ok összekapcsolása. Az OSI harmadik réteg útválasztási funkcióit is ellátja, és a forgalmat a csomagokban szereplő IP cím alapján is képes továbbítani
- **Managed switches** – lehetővé teszi, hogy a switch minden egyes interfészét be lehessen állítani. Lehetővé teszi a konfigurálást és a felügyeletet
- **Unmanaged switches** – biztosítja az Ethernet eszközök számára az adatok automatikus átvitelét az automatikus megállapodás segítségével, amely meghatározza az olyan paramétereket, mint például az adatátviteli sebesség. A konfiguráció rögzített
- **Smart switches** – konfigurálható, hogy nagyobb ellenőrzést tegyenek lehetővé az adatátvitel felett, de a managed switch-hez képest több korlátozással rendelkeznek
- **Stackable switches** – olyan kapcsolók, amelyek egy hátlati interfészen keresztül csatlakoztathatók egymáshoz, hogy két vagy több fizikai kapcsolóból egyetlen logikai kapcsolót alkossanak

- **Modular switches** – kapcsolókártyákkal való bővíthetőséget tesz lehetővé két vagy több fix formátumú kártya befogadására alkalmas switch. Ez a fajta kapcsoló biztosítja a legnagyobb rugalmasságot és frissíthetőséget. [11]



ábra 8
Switch ikonja

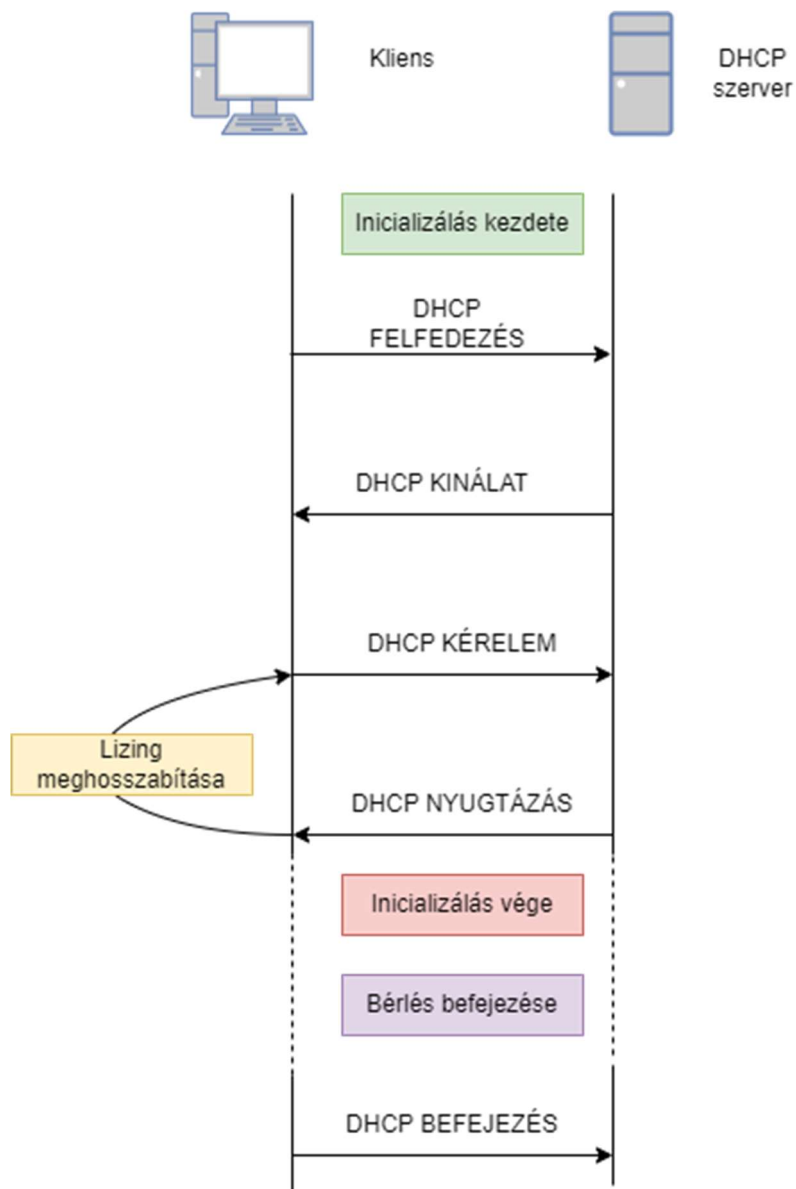
2.10. DHCP

Minden számítógép rendelkezik a hálózati kártyába épített adatkapcsolati réteggel, de IP-címmel nem. Nagy hálózatokon belül nagyon problémás minden végberendezésnek külön - külön megadni az IP-címét anélkül, hogy valami hiba csúszna bele. Erre a problémára ad megoldást a DHCP. A DHCP (Dynamic Host Configuration Protocol) egy olyan hálózati protokoll, amely az IP-hálózatokon lévő eszközök konfigurálásának automatizálását valósítja meg. DHCP alkalmazás esetén minden hálózat kell rendelkezzen egy DHCP szerverrel. A végberendezés adatszórással kér IP-címet a hálózaton belül, ezt DHCP felfedezés csomag küldésével teszi. Amikor a DHCP szerver megkapja a kérést, kioszt egy szabad IP-címet a végberendezésnek. Azért, hogy a DHCP szerver IP-cím nélkül ezt meg tudja tenni, a végberendezést az Ethernet címével, másik nevén MAC címével azonosítja, amit a DHCP felfedezés csomag tartalmaz. De mi van akkor, ha a végberendezés megszűnik? Olyankor a kiosztott IP-címmel mi történik? Ilyen esetekre találták ki a bérlet módszerét, ami annyit takar, hogy a kiosztott IP-cím egy adott időre szól. Az IP-cím lízingelése egy dinamikus folyamat, ahol a DHCP szerver egy ideiglenes IP-címet kioszt egy végberendezésnek. A lízingelési idő egy meghatározott időintervallum, amelyet a DHCP szerver állít be. Amikor a lízingelési idő közel jár a lejáráshoz, a végberendezés automatikusan megpróbálja megújítani az IP-cím lízingjét a DHCP szerverrel. A DHCP szerver ekkor eldönti, hogy további lízingidőt biztosít vagy egy új IP-címet kínál. Ha a végberendezés nem válaszol a lízingmegújítási kérésre, a DHCP szerver újra elérhetővé teheti az adott IP-címet más eszközök számára. [2]

DHCP Folyamat lépései:

1. DHCP Felfedezés (DHCP Discover): Amikor egy eszköz (pl.: számítógép, mobiltelefon) csatlakozik a hálózathoz, és nincs neki konfigurált IP-címe, a DHCP felfedezés csomagot küld a hálózaton. Ez a csomag általában a kliens egyedi azonosítóját (jellemzően a MAC címét) tartalmazza. Az üzenet üzenetközvetítés útján kerül kiküldésre. Ha a hálózatban vannak routerek, akkor azokat úgy kell konfigurálni, hogy a DHCP szerver felé továbbítsák a DHCP felfedezés csomagot.
2. DHCP Kínálat (DHCP Offer): A hálózati eszköz által küldött felfedezési csomagot a hálózati eszközökön kívül lévő DHCP szerver észleli. A DHCP szerver válaszként kínálatot (offer) küld vissza a szabad IP-címek közül, amelyeket a végberendezés használhat. Ha a DHCP nem küld vissza a kliensnek kínálat üzenetet, a leggyakoribb okok lehetnek, hogy minden rendelkezésre álló cím ki van osztva, nincs szabad IP cím, a kliens nincs támogatva.
3. DHCP Kérelem (DHCP Request): A végberendezés kiválasztja a kapott kínálatból az egyik IP-címet, majd DHCP kérelmet küld, amelyben elfogadja az ajánlatot és jelzi, hogy melyik általa kiválasztott IP címet kívánja használni. Ezt az üzenetet a teljes hálózat számára elküldi, hogy mindegyik DHCP szerver értesüljön a kiválasztott IP címről.
4. DHCP Nyugtázás (DHCP Acknowledge): A DHCP szerver megkapva a kérelmet, visszaigazolásként (acknowledge) elküldi a végberendezésnek a kiválasztott IP-címet, valamint a hálózati beállításokat. A kliens mostantól használhatja a kapott IP címet.
5. DHCP lízing meghosszabbítása (DHCP kérelem, DHCP Nyugtázás): A lízing idő lejártá előtt a kliens megkísérli meghosszabbítani. Ha a szerver elfogadja a kérést, visszaküld egy nyugtázás üzenetet. Ha a szerver nem válaszol, a kliens használhatja bérleti idő lejártáig a kapott IP címet. Mindaddig, amíg a bérlet él, a kliens és a szerver nem kell felfedezés és kínálat üzeneteket cseréljenek.
6. DHCP Befejezés (DHCP Release): A kliens befejezi a bérletet befejezés üzenet küldésével, ekkor a szerver visszahelyezi az IP címet a kiosztható címek közé.

Az ábra 9 szemlélteti a teljes adatfolyamot egy kliens és szerver között.



ábra 9
DHCP folyamat

2.11. Internet sebesség mérése

Az internet sebesség mérése egy alapvető módja az internet kapcsolat minőségének megállapítására. Amikor egy weboldal nehezen tölt be, akkor kell megvizsgálni az internet sebességét egy erre a mérésre kitalált weboldallal. Az internet kapcsolat átviteli sebessége nagyon sok tényezőtől függ, beleértve a szerver sebességét, egyszerre hányan használják az internetet, mit csinálunk, amikor használjuk az internetet stb. Elsőként a kiszolgáló feltérképezi a jelenlegi helyzetünket és a legközelebbi teszt-kiszolgálót. A teszt-kiszolgáló

egy egyszerű jelet (ping) küld a teszt kiszolgálónak és az válaszol. Az üzenet küldése és válasza között eltelt időt milliszekundumban méri le a rendszer. A ping befejezése után a letöltési fázis következik. A kiszolgáló egyszerre több kapcsolaton próbál kis mennyiségű adatot letölteni a teszt kiszolgálótól. [12]

De mennyi is a „jó internet sebesség”? A Federal Communications Commission (FCC) szerint a szélessávú internet minimum követelményei: 25Mbps-os letöltési sebesség és 3Mbps feltöltési sebesség. Az internet sebességét bit/szekundumban mérik, amin a bitek másodpercenkénti sebességét értik, így a Mbps a bit milliommód szorosa. A letöltési sebesség azt jelenti, hogy milyen gyorsan áramlik át az információ a hálózaton keresztül a számítógépre. A feltöltési sebesség méri, hogy milyen sebességgel jut át az információ a számítógépről a hálózatra. A késleltetés (latency) azt az időt jelenti, ami alatt a számítógép kapcsolatba lép az internetszolgáltatóval, és az internetszolgáltatótól visszatér a kapcsolat.

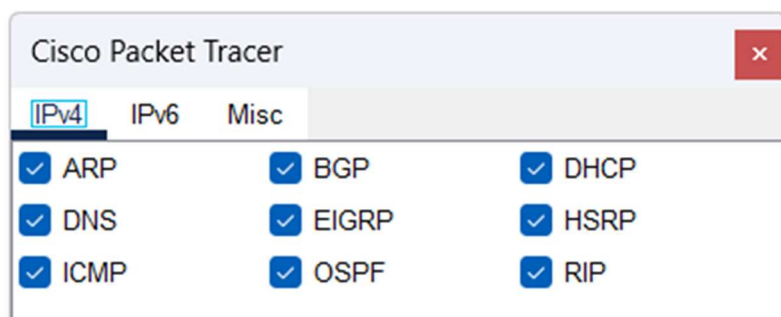
A leggyakrabban használt internetsebességet mérő oldalak a fast.com, Speedtest.net, CloudFlare. [13].

2.12. NAT

Az internetet használó eszközök száma meghaladja az IPv4 publikus címtartományban által kiosztható címek számát. Ez problémát jelent mivel az eszközök száma bővül, de a címtartomány kibővítésére nincsen lehetőség, erre a problémára kínál lehetőséget az IPv6. Az IPv6 címzés megjelenése előtt egy másik módszernek a kifejlesztésére volt szükség és ez a módszer lett a NAT (Network Address Translation). A NAT használata megengedi, hogy az alhálózatok, mint LAN hálózatok úgynevezett privát IP címeket használjanak, míg a privát hálózatokon kívül publikus IP címekkel azonosítják egymást. A privát IP címek minden alhálózatban felhasználhatók mivel nem befolyásolják a publikus globális hálózatot. Ilyen privát IP cím például az 192.168.XXX.XXX vagy az 10.XXX.XXX.XXX. Ezeket az IP címeket a router ossza ki a DHCP segítségével minden olyan eszköznek, ami az adott alhálózathoz tartozik. Az internet szolgáltató a külső hálózaton egy publikus IP címmel látja el a routert, így biztosítva az internethez való hozzáférést. Amikor az alhálózat egyik eszköze (legyen az személyi számítógép, okostelefon, okos tévé stb.), a saját lokális IP címét használja a router ezzel a NAT funkcióval átforgassa a kapott globális IP címre, és fordítva is ugyan ezt teszi.

2.13. Cisco Packet Tracer

A Cisco Packet Tracer egy olyan szoftver, amelyet a Cisco Systems fejlesztett ki, és célja a hálózati tervezés, szimuláció és gyakorlás elősegítése. A Packet Tracer lehetővé teszi diákoknak, hálózati szakembereknek és tanároknak, hogy virtuális hálózatokat hozzanak létre és működtessenek, szimulálva valós hálózati környezeteket. A Cisco Packet Tracer képes logikai és fizikai nézetben mutatni a hálózat felépítését. A logikai nézet az általunk felépített hálózat logikai felépítését, az eszközöket és az eszközök közötti felépítést mutatja meg. A fizikai nézet megmutatja a logikai hálózat fizikai megvalósítását, az üzenetek áramlását a forrástól a célállomás felé. [14] A Cisco Packet Tracer képes számos, a hálózatokban használt protokollok megvalósítására (ábra 10).



ábra 10
A Cisco Packet Tracer által támogatott protokollok

2.14. Tűzfal

A tűzfal (firewall) egy olyan biztonsági eszköz vagy szoftver, amely védelmet nyújt a számítógépes hálózatok és rendszerek számára, megakadályozva vagy ellenőrizve a nem kívánt hozzáférést és adatáramlást. A tűzfalak fontos szerepet játszanak a hálózati biztonság fenntartásában, és segítenek megelőzni a jogosulatlan hozzáférést, a rosszindulatú támadásokat és a biztonsági fenyegetések ellen. [15]

A tűzfaloknak két fő típusa létezik:

- a. Hardveres tűzfal (Hardware Firewall): A hardveres tűzfal egy olyan eszköz, amelyet a hálózati infrastruktúrába integrálnak. Ezek gyakran különálló eszközök, például tűzfalas routerek, amelyek a hálózati forgalmat ellenőrzik és szűrik. A hardveres tűzfalak fizikai eszközként működnek a hálózat és a külvilág között.

- b. Szoftveres tűzfal (Software Firewall): A szoftveres tűzfal olyan számítógépes program vagy alkalmazás, amely egy számítógépen fut és ellenőrzi, ill. szűri az átmenő adatokat.

A tűzfalak általában a következő funkciókat látják el:

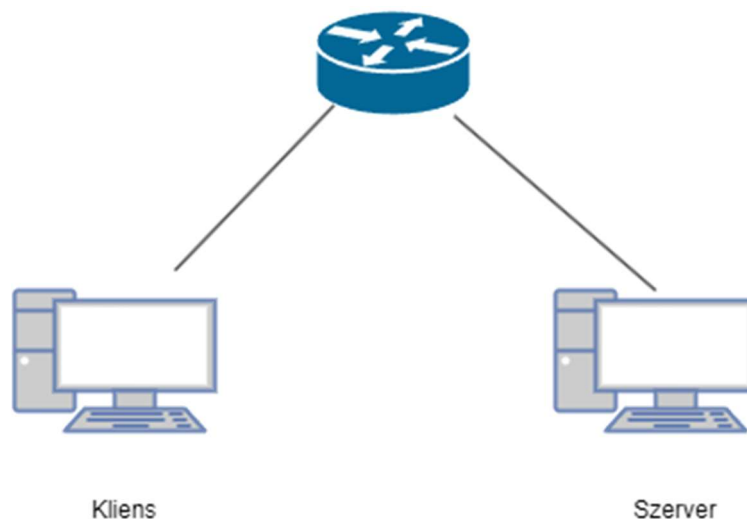
- Állapotellenőrzés (Stateful Inspection): A tűzfal figyeli az átmenő forgalmat és döntéseket hoz annak alapján, hogy milyen állapotban van az adatkapcsolat.
- Csomagszűrés (Packet Filtering): A tűzfal szűri az adatcsomagokat a megengedett és tiltott típusok szerint.
- Proxy szolgáltatások: A tűzfal proxyként működhet, ahol közvetítőként működik az átmenő forgalom és a hálózati erőforrások között.
- Hálózati cím fordítás (Network Address Translation - NAT): A tűzfal általában NAT funkciót használ, hogy elrejtse a belső hálózatok IP-címeit a külvilág elől.
- Hozzáférési vezérlés (Access Control): A tűzfal meghatározza, hogy milyen hozzáférést engedélyez vagy tilt.

A tűzfalak alkalmazásának célja a hálózati biztonság megerősítése és a jogosulatlan hozzáférés, támadások és károkozás minimalizálása. Hasonló a tűzfalak felhasználói hozzáférés-szabályozás tágabb kategóriájának egyik biztonsági eszköze. Ezeket a korlátokat jellemzően két helyen állítják fel: a hálózat dedikált számítógépein vagy magukon a felhasználói számítógépeken és más végpontokon (hosztokon).

3. A RENDSZER TERVEZÉSE ÉS FELÉPÍTÉSE

3.1. A rendszer architektúrája

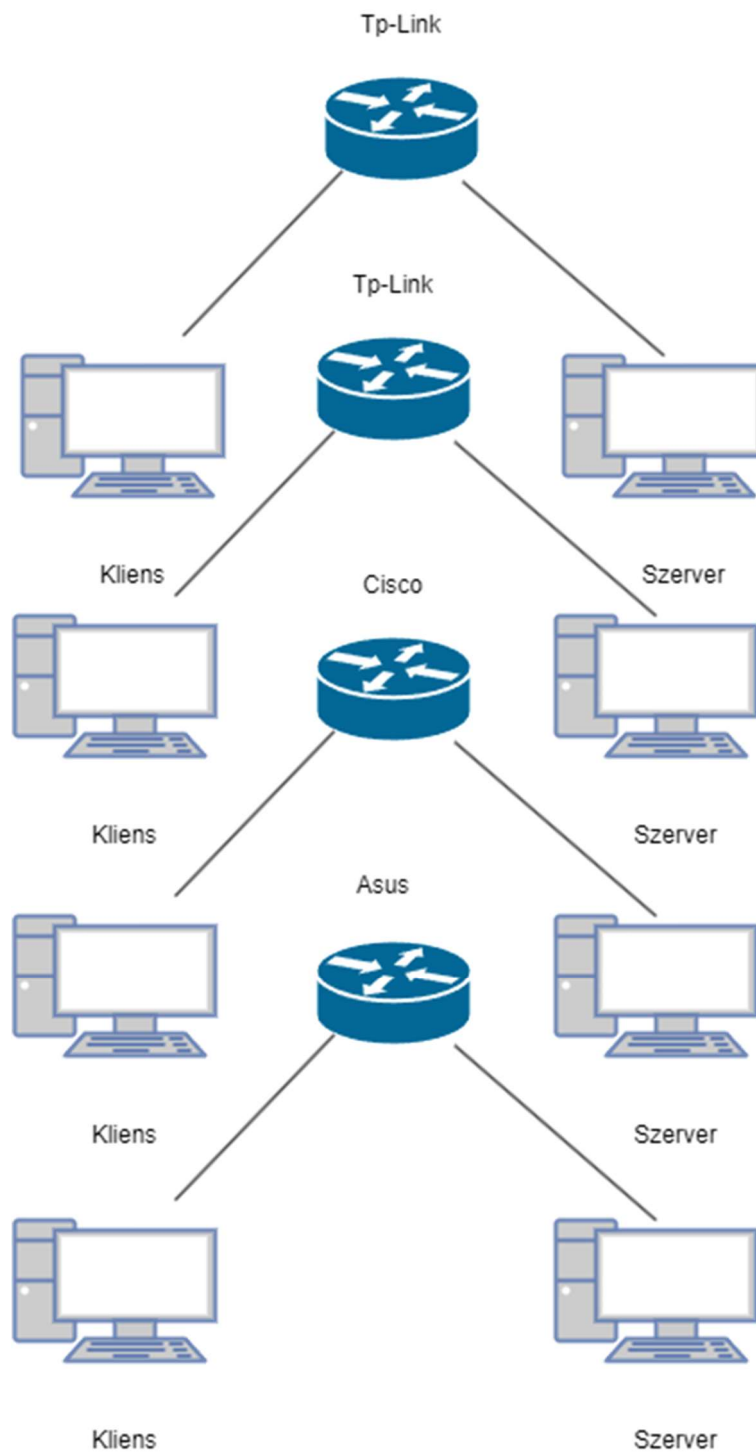
A következő ábrán (ábra 11) látható egy leegyszerűsített teszt rendszer felépítése. A rendszer összetétele egy routerből és két számítógépből áll. A két számítógép funkcióját tekintve az egyik a szerver, a másik a kliens. A router összeköttetést biztosít a két gép között, mivel ennek a routernek a teljesítményét szeretnénk mérni és elemzeni különböző adat terhelés mellett.



ábra 11

Rendszer összetétele

Mivel a routerek teljesítményének a mérése és a különböző terhelés melletti működés összehasonlítása a cél, ezért több mérő rendszer lett kialakítva. A következő ábra (ábra 12) mutatja minden teszt rendszer felépítését. A számítógépek hardver felépítése teljesen azonos, így lehet garantálni, hogy az adatfolyam generálása is megegyezzen, ellenben minden routert más és más cég gyártja, más paraméterekkel. Az összehasonlítás két darab 100Mbps átviteli sebességű és két darab 1Gbps átviteli sebességű eszköz között történik.



ábra 12
Teljes rendszer felépítése

3.2. Rendszer követelmények

3.2.1 Funkcionális követelmények

A tesztelés elvégzésére szükség van 8 darab azonos hardver architektúrával rendelkező teljes értékű számítógépre, Ubuntu Linux operációs rendszerrel. A számítógépekre fel kell legyen telepítve az *iperf3*, valamint a *sourcesonoff*, és a *vnstat* programok. A követelmények közé tartozik két darab 100Mbps adatátviteli sebességet biztosító, egy vállalati környezetben használt magas teljesítményű, valamint egy otthoni használatra szánt kisebb teljesítmény kategóriába sorolható router. Még szükséges két darab 1Gbps adat átviteli sebességet biztosító, egy nagy és egy kis teljesítményű, az otthonokban is megtalálható router. Emellé még kellenek UTP kábelek az összeköttetések megvalósítására. Szükséges egy switch, valamint egy tűzfalat futtatni képes számítógép.

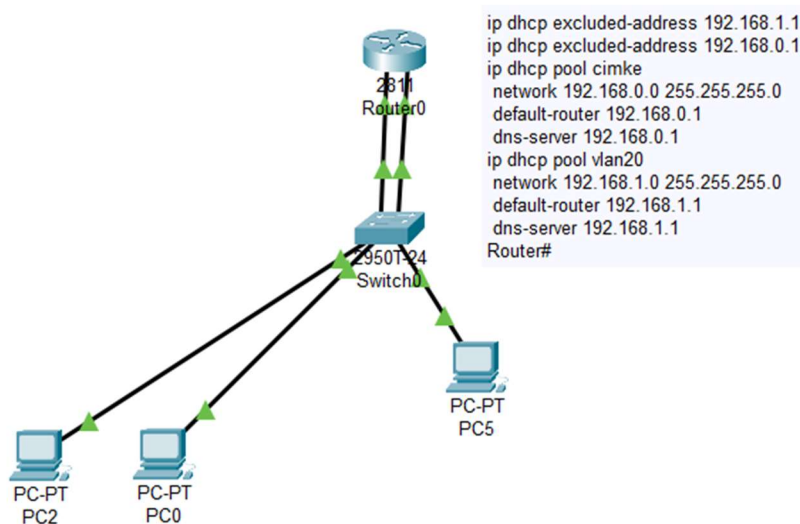
3.2.2 Nem funkcionális követelmények

Nem funkcionális követelmény egy 10Gbps átvitelt biztosító, vállalati környezetben is használt router, amivel szintén sebesség méréseket lehetne végezni.

4. RÉSZLETES TERVEZÉS

4.1. A hardver összetétele és konfigurációja

A tervezés első lépése egy szimulációs környezetben kialakított topológia volt, ahol is összeraktam egy kis hálózatot, mivel a megvalósítás kezdetét egy Cisco típusú útválasztó konfigurációjával kezdtem. A szimulációs környezet a Cisco Packet Tracer nevű program volt, mely pontosan leképezi a valóságban is használt Cisco által gyártott eszközök működését [14], pontosabban egy Cisco 2800 útválasztót.



ábra 13
Rendszer felépítése

A routernek a két interfészét két külön IP címmel láttam el, mivel ez a típusú router képes arra, hogy minden interfészét úgy állítsuk be, ahogyan csak akarjuk, ezért az egyik interfészére egy 192.168.0.1-es, míg a másikra egy 192.168.1.1-es címet adtam. Az általam használt switch szintén egy Cisco által gyártott eszköz, melyet virtuálisan két részre „vágtam”. A switch egyik részéhez a Vlan 10 volt rendelve, a másikhoz a Vlan 20, ezzel megvalósítva egy fizikai switch-en belül két virtuális és teljesen szétválasztott switch-et. A router még DHCP funkciókat is ellát, hogy ne kelljen a számítógépekben egyesével az IP címeket megadni. Ami itt megvalósítható volt, az viszont a későbbiekben még probléma lesz.

Az összehasonlításhoz még szükség volt 3 darab routerre, mivel a Cisco elméleti maximális adat átviteli sebessége 100Mbps, ezért az összehasonlítani kívánt router egy TP-LINK TL-WR941ND szintén 100Mbps sebességű, viszont alacsony árfekvésű eszköz. Ugyanakkor összehasonlításra került másik 2 router, mivel ma már a háztartásokban sok helyen megjelent a „Gigabyte Ethernet”, ezért ezek átviteli sebessége 1Gbps. Egy ASUS által gyártott alacsony árfekvésű ASUS RT-N18U és egy TP-Link által gyártott középkeletű TP-LINK TL-ER6120, mely routerek elméleti maximális sebessége 1Gbps. Mivel a hagyományos értelemben vett router, amit a mindennapokban használunk, legyen az otthoni vagy vállalati használat, magukban integrálnak switch funkciókat is, a bemeneteik ezeknek a rendszereknek általában egy vagy több WAN interfészt integrálnak, illetve általában 3, de lehet több LAN interfészt tartalmaznak. Az egyik probléma, hogy a számítógépeket nem érdemes csak a LAN portokra kötni, mivel így a router csak sima switchként működne, csupán DHCP vagy egyéb magasabb szintű router funkciókat kiszolgáló rendszer. A másik probléma, hogy az alacsony árfekvésbe tartozó routerek, mint az általam használt eszközökben, nincsen olyan funkció, amivel be lehetne állítani, melyik interfész milyen IP címmel dolgozzon. Ahhoz, hogy az adatfolyam a routeren keresztül haladjon át, a bekötés úgy van kialakítva, hogy a kliens gép a WAN interfészre van csatlakoztatva, a szerver gép a LAN interfészre van bekötve. A WAN interfészre, mint egy külső hálózatra, rá van kötve egy más tartományban lévő IP cím. A belső LAN hálózat IP címe eltér a WAN IP címétől, és egy *virtual server* nevű eljárással a külső IP címről érkező forgalom át lett forgatva a belső hálózat IP címén lévő számítógépre, így biztosítva, hogy az adat áthaladása minden esetben a routeren keresztül történjen. Mivel az IP címek át lettek forgatva, ezért ebben a megvalósításban nem alkalmaztam DHCP szervert. A számítógépek kis létszáma és az IP átforgatás miatt konkrétan meg kell adni az átirányított IP címet, ezen két kritérium miatt nem használtam ezeknél a routereknél DHCP címezést. Így épül fel a teljes rendszer, mint az ahogy az ábra 12. is mutatja.

4.2. A mérés menete

4.2.1 Iperf

Az első méréseket az Iperf3 nevű programmal végeztem el, mely TCP és UDP kapcsolat alapú méréseket is képes elvégezni. Az Iperf3 egy nyílt forráskódú szoftvereszköz, amely a hálózati teljesítmény mérésére lett létrehozva. Az Iperf3 számos

funkciót kínál a hálózati átviteli sebességének mérésére, ezért ez az egyik legajánlottabb szoftver ezeknek a méréseknek az elvégzésére. Az Iperf3 futtatása Linux terminálban történik, ahol meg lehet adni a paraméter kapcsolókat [16]. A mérést ebben a részben hét felé osztottam fel, ami 1000,800,600,400,200,100,50Mbps adatsebességre van felosztva. A parancssorba a következő parancsot kellett megadni

- szerver oldalon:

`iperf3 -s -p 30000`, ahol a `-s` egy szervert indít el, ahova lehet küldeni az adatot a `-p` kapcsoló pedig egy általam a routerben megadott port-ot nyit a kapcsolat létrehozásához.

- kliens oldalon pedig:

`iperf3 -c 192.168.33.1 -p30000 -b 1000M`, ahol `-c` jelzi, hogy kliens oldalon vagyunk, `-p` szintén a portot határozza meg, `-b` pedig a maximális bit sebességet, amit megengedünk az átvitel során, ezt az értéket változtattam a korábban megadott paraméterek szerint. UDP kapcsolat esetén annyit változik a parancssor, hogy a `-b` kapcsoló elé bekerül egy `-u` kapcsoló is, ezzel jelezve, hogy UDP átvitelt szeretnénk, alapértelmezetten TCP kapcsolatot valósít meg. Az Iperf a mérés lejárta után a következő paramétereket adja meg: lásd ábra 14., a mérési intervallumot, hogy az adott mérés mennyi időt tartott, ezt az értéket milliszekundumban, az átlagosan elküldött adat mennyiséget, az adatátvitel sebességét TCP kapcsolat esetén megjelenik a `Retr`, ami az újra elküldött csomagok számát jelenti. UDP kapcsolat esetén még megjelenik a `dzsitter` (remegés), valamint az adatvesztés százalékban kifejezve.

[ID]	Interval		Transfer	Bitrate	Retr	
[5]	0.00-10.00	sec	59.6 MBytes	50.0 Mb/s	1	sender
[5]	0.00-10.04	sec	59.6 MBytes	49.8 Mb/s		receiver

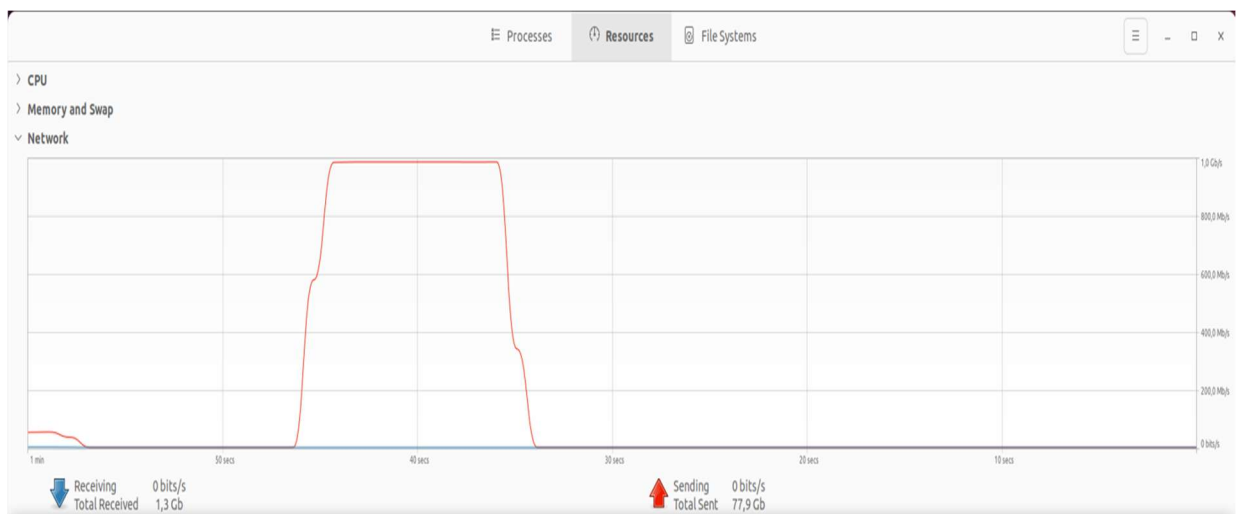
ábra 14
Iperf3 mérési eredménye TCP kapcsolat során

[ID]	Interval		Transfer	Bitrate	Jitter	Lost/Total Datagrams	
[5]	0.00-10.00	sec	954 MBytes	800 Mb/s	0.000 ms	0/690608 (0%)	sender
[5]	0.00-10.04	sec	953 MBytes	796 Mb/s	0.006 ms	742/690574 (0.11%)	receiver

ábra 15
Iperf3 mérési eredménye UDP kapcsolat során

4.2.2 Iperf hibája

Mivel az Iperf alkalmazásnak megvan az a rossz tulajdonsága, hogy hálózat tesztelés során az adatfolyam konstans ábra 16. Az alábbi képen jól látszik, hogy az Iperf futása alatt az átvitelben nincs változás. Az Iperf esetében a TCP kapcsolatok hosszúak (akár 10 másodperc), így kialakítva egy hosszú kapcsolatot a küldő és a fogadó oldal között, ami miatt hozzájárul a torlódás-szabályozáshoz és az adatút kialakulásához, ami állandó adatfolyamot hoz létre a tesztelés során. [17]. Ez a fajta adatfolyam nem tükrözi egy valós hálózaton megjelenő adatfolyamot. A valóságban azonban a hálózati forgalom gyakran változik, ami függ az adatok hosszától, a hálózat terheltségétől, a torlódásoktól. Az adatátvitel másodpercről másodpercre változhat a hálózat terheltségétől függően. Ezért az Iperf nem a legalkalmasabb egy valós hálózat tesztelésére, ami ebben a dolgozatban egy nagyon fontos aspektus, mivel a routerek átviteli képességeit valós környezetben szeretném mérni.



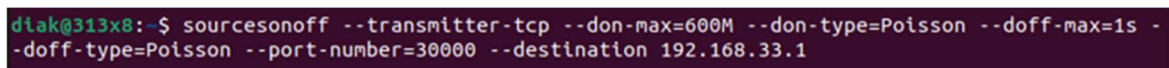
ábra 16

Iperf által megvalósított mérés

A szakirodalomban is kifejtik ezt a problémát [17], hogy az Iperf és más hálózat elemző programok nem a legjobbak erre a problémára. A szakirodalom felkínál egy lehetőséget (programot) erre, aminek a neve SourcesOnOff.

4.2.3 SourcesOnOff

A SourcesOnOff egy olyan program, amit arra fejlesztettek ki, hogy az olyan hálózati tesztelési problémákat kiküszöbölje, mint amiről az előbb szó esett. A SourcesOnOff nevű program próbálja szimulálni a valós hálózatokban történő adatfolyamot. [17] A program a megadott paraméterek között generálja le egy random eloszlás segítségével az adatfolyamot. Az általam használt adatfolyam a következő kódból tevődik össze ábra 17:



```
dlak@313x8:~$ sourcesonoff --transmitter-tcp --don-max=600M --don-type=Poisson --doff-max=1s -  
-doff-type=Poisson --port-number=30000 --destination 192.168.33.1
```

*ábra 17
Sourcesonoff kódja*

Ahol: -transmitter jelzi, hogy az átviteli protokoll UDP vagy TCP, ezt az -udp/-tcp paranccsal lehet megvalósítani, a don-max megadja a maximális adatfolyamot, ennek a paraméternek a változtatásával fogom befolyásolni az adatátviteli sebességet, a minimális adatfolyam alapértelmezetten 1kb, amit nem is változtattam meg. Az eloszlása ennek az adatnak Poisson eloszlást követ. Léteznek még más eloszlások is, de azok valamilyen oknál fogva nem működnek megfelelően. A doff- max paraméter megadja az egymás után generált állományok között eltelt időt, a doff-min alap értéke 100ms. A port megmondja melyik porton szeretném az adatot elküldeni, a destination pedig a szerver IP címét.

Szerver oldalon csak annyit kell megadni, hogy sourcesonoff --receiver-tcp vagy -udp --port-number=30000, ami megadja a portot és hogy az átvitel UDP, vagy TCP protokollt használ.

Mivel a sourcesonoff program nem képes az átviteli sebességet kiírni, ezért egy másik programot is használatba kellett vennem, aminek a neve vnstat. A vnstat kiírja az átvitt adatmennyiséget és sebességet, amivel ki lehetett számolni az adatátviteli sebességet és az elveszett adatok arányát, amit az Iperf a mérés folyamata után kiírt.



ábra 18
SourcesOnOff által megvalósított mérés

A fenti ábra 18 is látható, hogy az adatfolyam nem folyamatos és konstans. Vannak az adatfolyamban megjelenő „hegyek és völgyek”, ami azt jelenti, hogy a SourcesOnOff egy jobb adatfolyamatot generál, mint az Iperf, és a generált adat jobban hasonlít egy valós hálózatban is fellépő adatfolyamra.

4.3. Mérési eredmények

Először az Iperf által, utána pedig a SourcesOnOff által mért eredmények kerülnek bemutatásra, majd egy routerben tett forgalomkorlátozás, egy több gépes terhelés, végezetül pedig egy tűzfalas mérés lesz bemutatva. Kezdetben a mérések minden esetben olyan routereken történnek, ahol nincsen semmilyen útválasztás vagy korlátozás megadva.

4.3.1 TP-LINK TL-WR941ND mérési eredményei

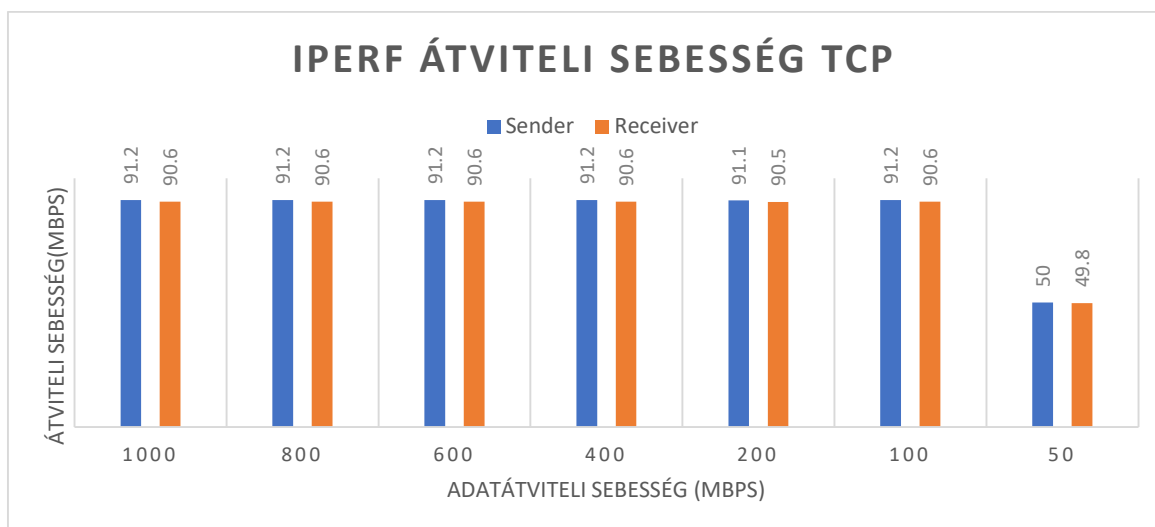
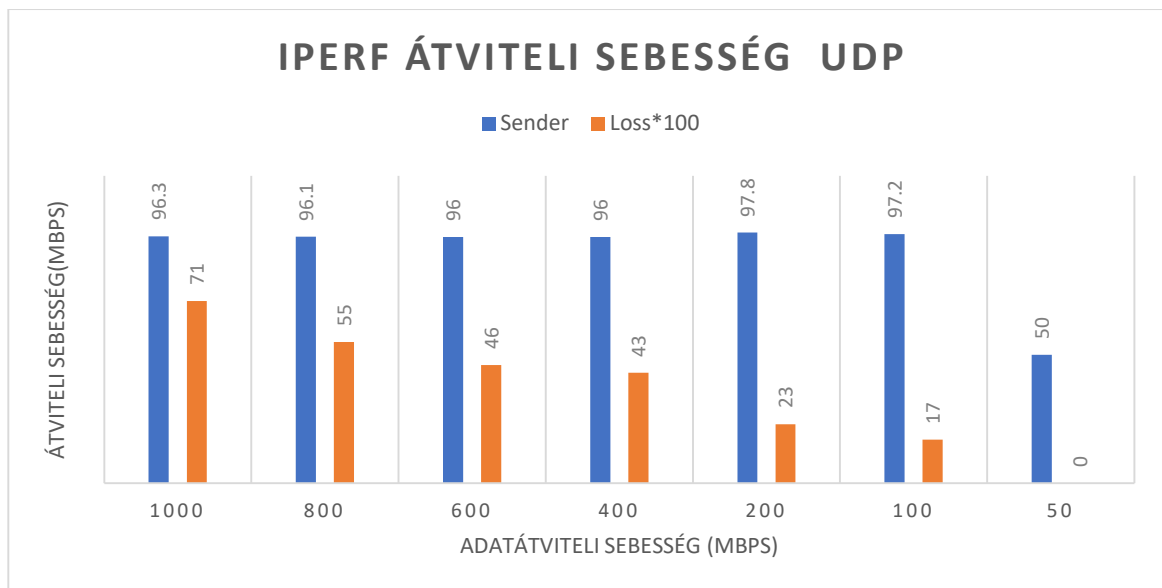


Diagramm 1
Iperf mérési eredménye TCP kapcsolat esetén



*Diagramm 2
Iperf mérési eredménye UDP kapcsolat esetén*

Nagyon jól látható, hogy a 100Mbps átviteli sebességet a router biztosítani is tudja, ez látszik, mind a Diagramm 1 mind a Diagramm 2-ből. A két diagrammról leolvasható, hogy adott átviteli sebesség mellett milyen gyorsan tudja a router átvinni az adatot. Ameddig az átviteli sebesség nem haladja meg a router tényleges sebességét, addig a maximális adatátvitel a 91-92 Mbps TCP kapcsolat esetén, míg UDP kapcsolat esetén ez az érték 96-97 Mbps. Az UDP kapcsolat során a protokoll felépítése miatt nagyobb a sebesség. A Diagramm 2 megjelenik egy másik adat, mivel itt nincsen visszaigazolás, hogy az adat megérkezett-e, ezért az adatvesztést vettem figyelembe. Mivel az adatvesztés kisebb, mint az átviteli sebesség, ezért a diagrammon nem látszana nagyon jól, így a jobb szemléltethetőségért az adatvesztést megszoroztam 100-zal. Észrevehető, amíg az adatsebesség kisebb, mint a router teoretikus maximum átviteli sebessége, addig az adatvesztés is alacsony. A 71-es adatvesztés igazából 0.71%-nak felel meg, ami nem jelentős, viszont ahogy csökken az adatátviteli sebesség, annál inkább a csomag veszteség is vele együtt csökken.

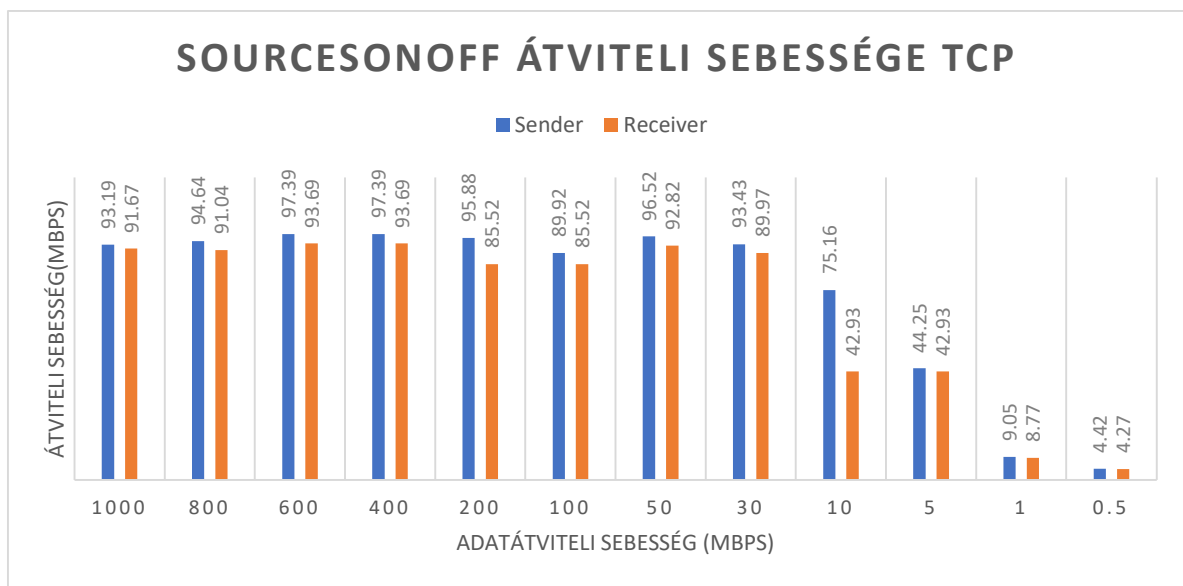


Diagramm 3
SourcesOnOff mérési eredménye TCP kapcsolat esetén

A fenti diagrammon Diagramm 3 látható, hogy a valós adattal való mérési eredmények addig nem változnak jelentősen, amíg nem érik el a router maximális átviteli sebességét. Miután ezt a küszöböt meghaladta, látszik a változás az Iperf méréshez képest. Látható, hogy az 50 Mbps átvitel alatt is megmarad a 90Mbps átviteli sebesség, mivel az adatfolyam nem konstans. Az értékeket tovább csökkentve is észrevehető, hogy az adatsebességhez képest nagyobb sávszélesség kell egy valós adatfolyam átviteléhez. Az Iperf mérésekhez képest azért van több mérés, mivel az Iperf esetében a beállított értéket folyamatosan tartja a program, itt viszont az adat adási sebességhez képest változik az átviteli sebesség.

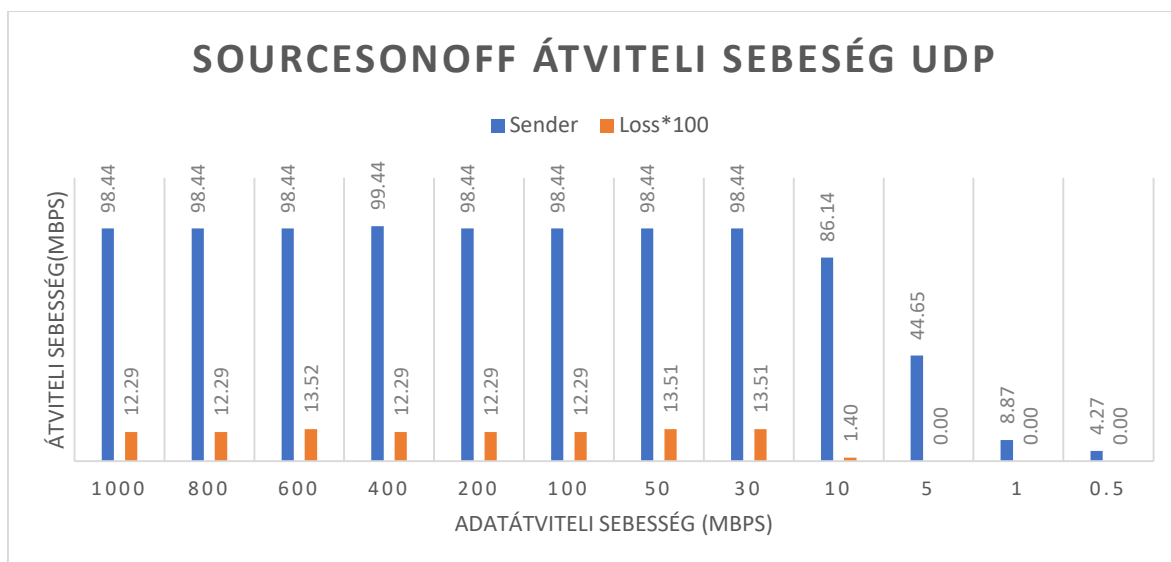


Diagramm 4
SourcesOnOff mérési eredménye UDP kapcsolat esetén

Az UDP átvitelnél nagyon hasonló eredményeket kaptam, mint az Iperf mérésnél. Ez annak köszönhető, hogy az UDP nem ellenőrzi az adatokat elküldés után. Ebben az esetben nem változnak az értékek, annak ellenére, hogy a generált adat nem konstans.

4.3.2 Cisco 2800 mérési eredményei

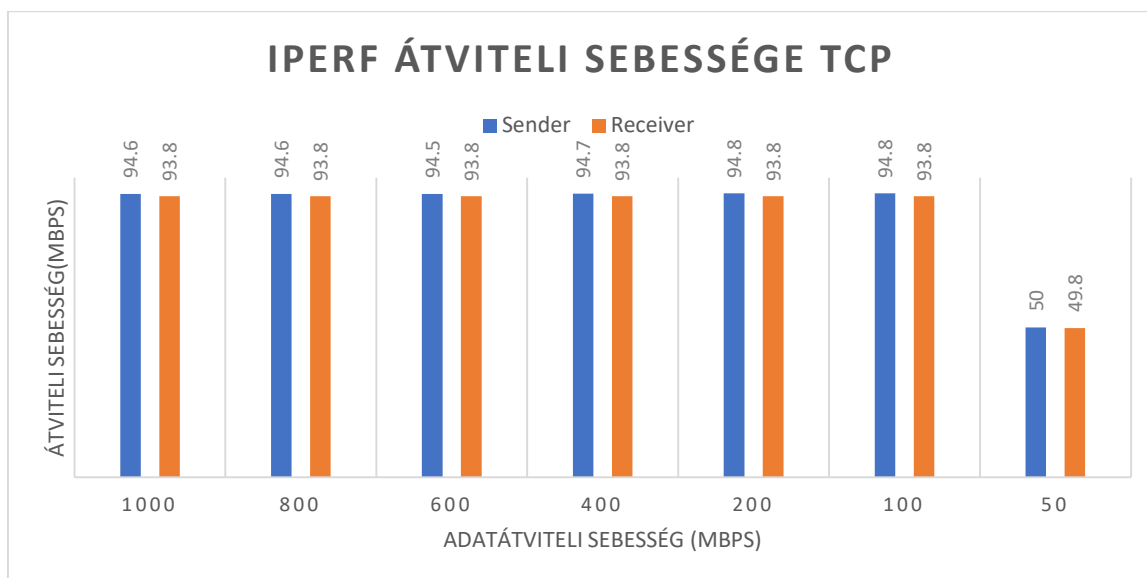


Diagramm 5
Iperf mérési eredménye TCP kapcsolat esetén

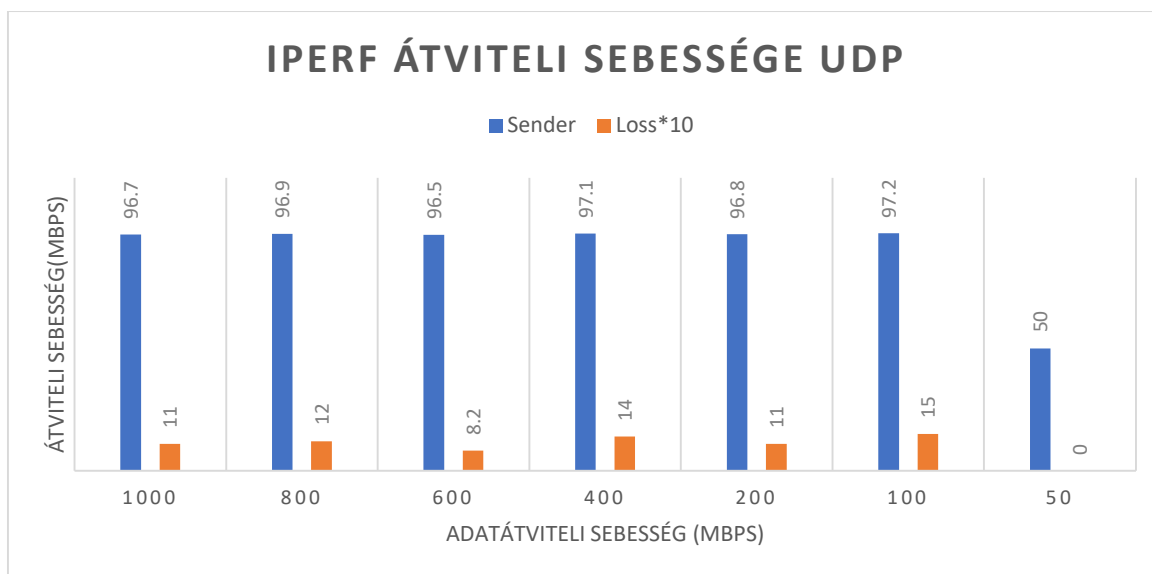


Diagramm 6
Iperf mérési eredménye UDP kapcsolat esetén

TCP átvitel esetén az ipari router számottevően nem tér el az előző router mérésekhez. Az ígért 100Mbps maximális átvitel ugyan azok a paraméterek alapján képes a 100Mbps sávszélességet tartani. A különbség az előző méréshez képest az UDP átvitelben jelentkezik, ahol ugyan is az elvesztett adatokat tekintve változik, ami kicsit rosszabb, mint az olcsó árfekvésű routerben. Nem nagy mértékben, de van különbség. Ebben a mérésben a csomagvesztést 10-zel szoroztam meg, mivel vannak nagyon kiugró esetek.

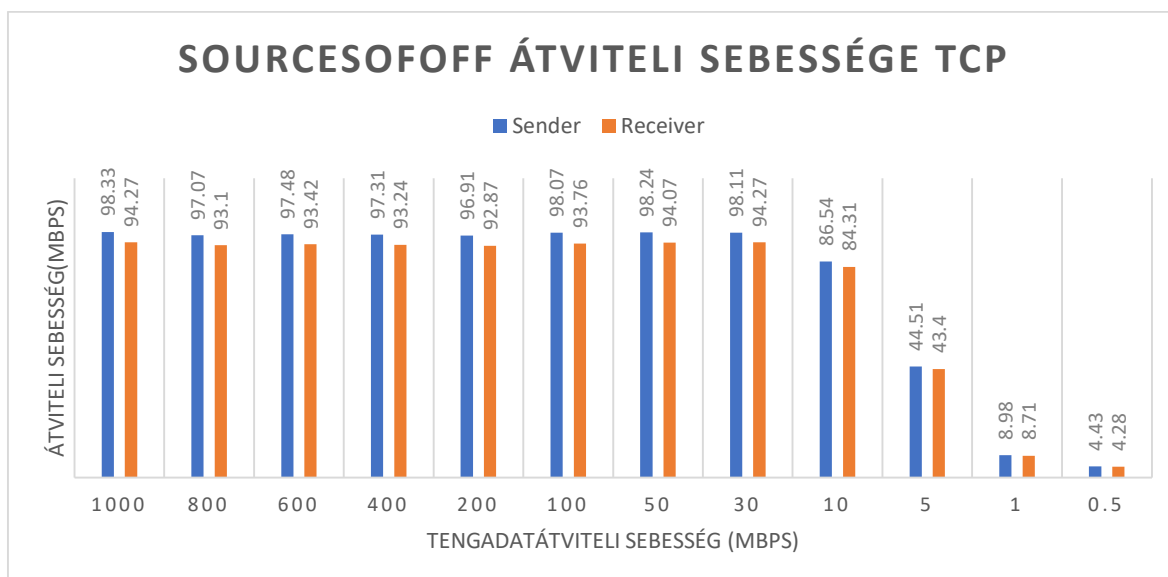


Diagramm 7
SourcesOnOff mérési eredménye TCP kapcsolat esetén

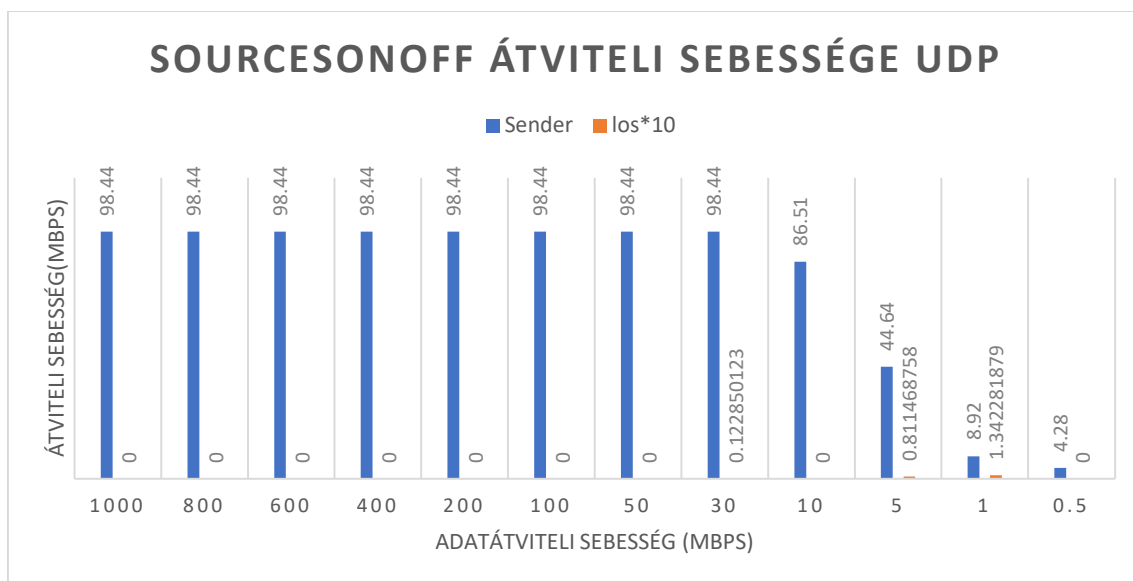


Diagramm 8
SourcesOnOff mérési eredménye UDP kapcsolat esetén

A SourcesOnOff mérés tekintetében sincsen nagyobb különbség az előző mérésekhez képest, mint TCP átvitel esetén. Itt is fellelhető, hogy gyorsabb adatátviteli sebességet igényel a TCP kapcsolat. Az UDP átvitel viszont sokkal érdekesebb mérési eredményeket eredményez, mivel az elveszett adatok tekintetében 0-ás értékek jöttek ki, ami azt jelenti az átvitel során nincsen adatvesztés.

4.3.3 ASUS RT-N18U mérési eredményei

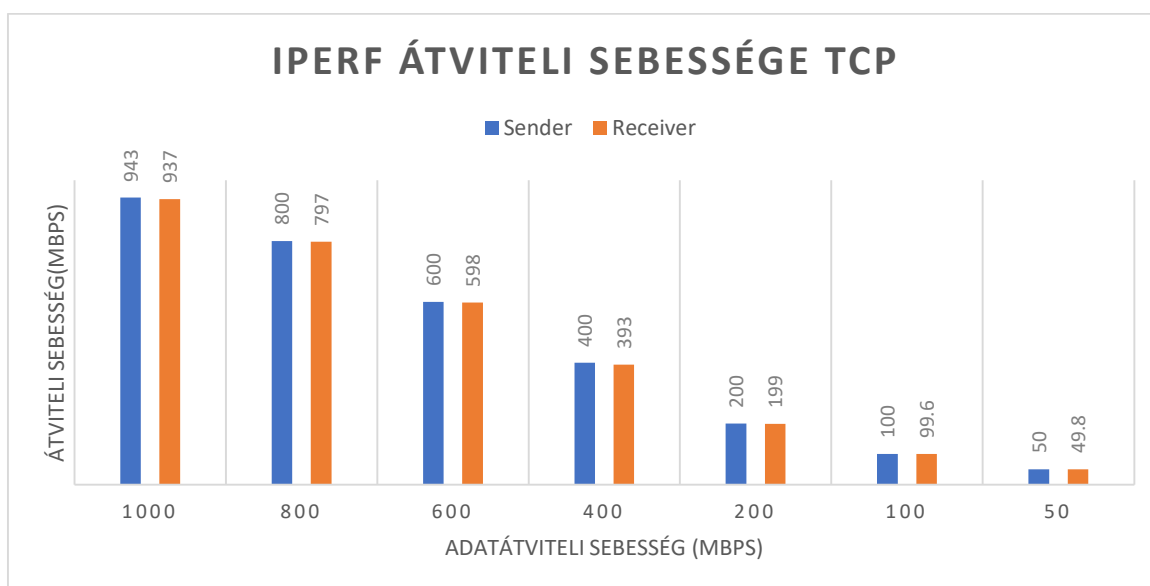


Diagramm 9
Iperf mérési eredmények TCP kapcsolat esetén

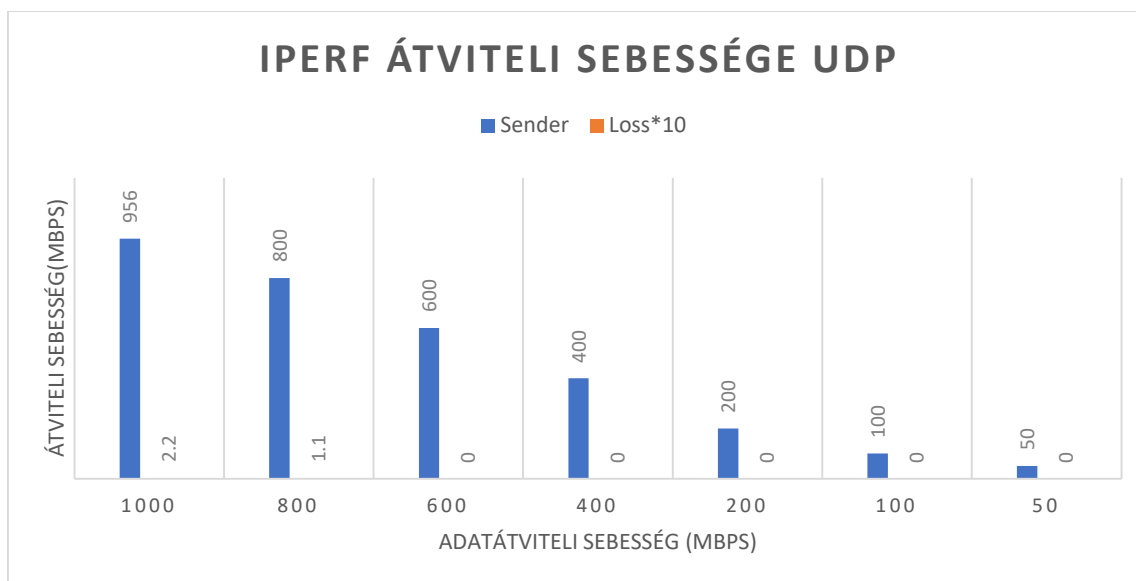


Diagramm 10
Iperf mérési eredmények UDP kapcsolat esetén

Az Asus router is képes tartani a gyártó által megadott 1Gbps átviteli sebességet. Látható, hogy az Iperf mérés nem tér el az eddigi mérési eredményektől, mindig tartja az adott átviteli sebességet. UDP kapcsolat esetén Diagramm 10 látható, hogy az elveszett adatok oszlopa szerint a routeren keresztül nem vesznek el adatok. Az előző routerekhez képes ez a router később jelent meg és erősebb, ugyan abban a belépő kategóriában ennek is tudható, hogy az adatvesztés sok helyen 0.

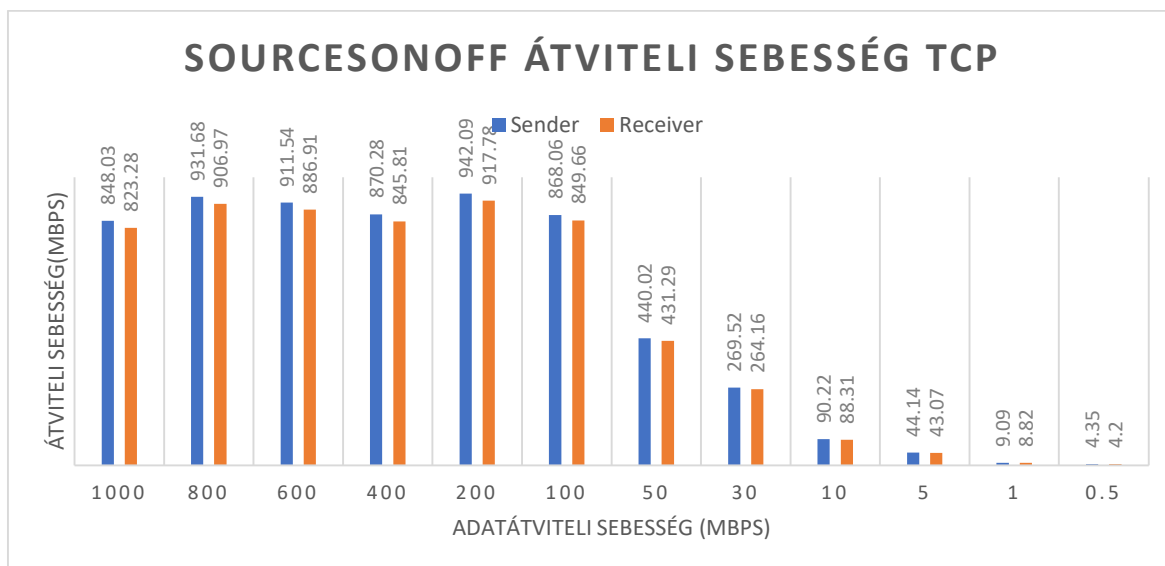


Diagramm 11
SourcesOnOff mérési eredmények TCP kapcsolat esetén

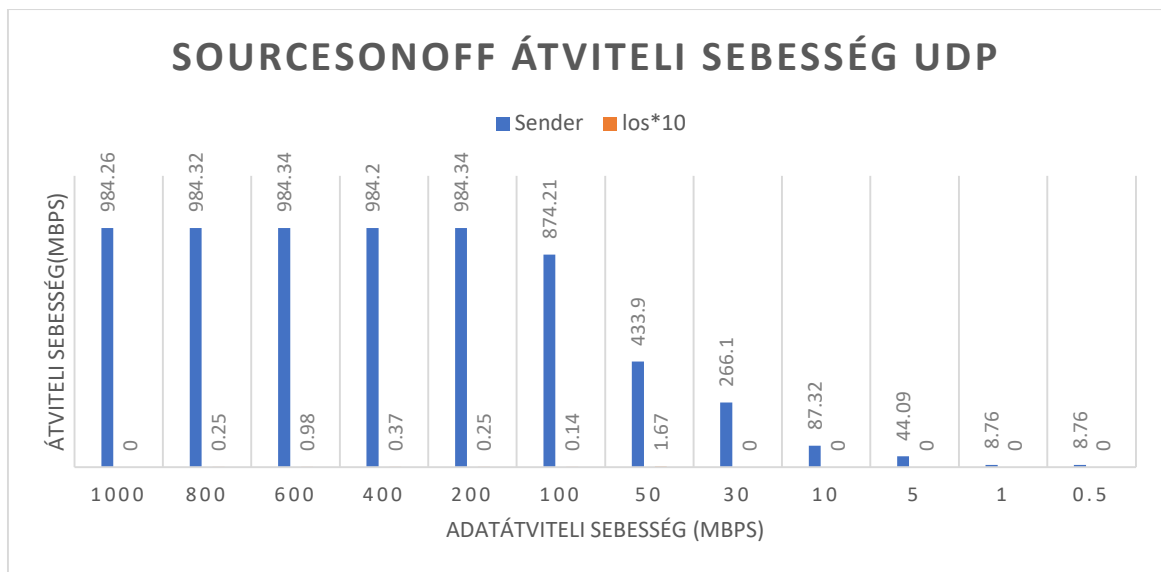


Diagramm 12
SourcesOnOff mérési eredmények UDP kapcsolat esetén

A SourcesOnOff mérési eredményei is a vártnak megfelelően alakulnak. A szaggatott adatfolyam TCP kapcsolat esetén Diagramm 11 is több sávszélességet igényel az adatméret alsóbb felében is, mint az Iperf mérés. UDP kapcsolat esetén a csomag veszteség több, mint az Iperf esetén, de nem jelentősebb az adatközlés során. Ebben az esetben is a vártnak megfelelően viselkedik a router annak ellenére, hogy a sávszélesség jóval nagyobb, mint az előző routerek esetén.

4.3.4 TP-LINK TL-ER6120 mérési eredményei

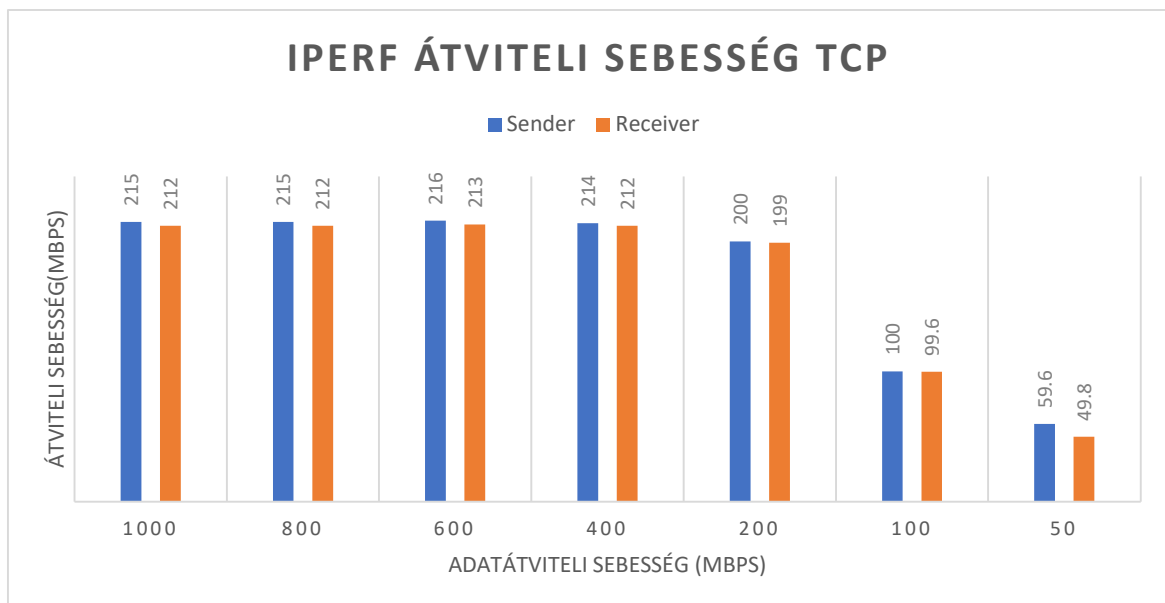
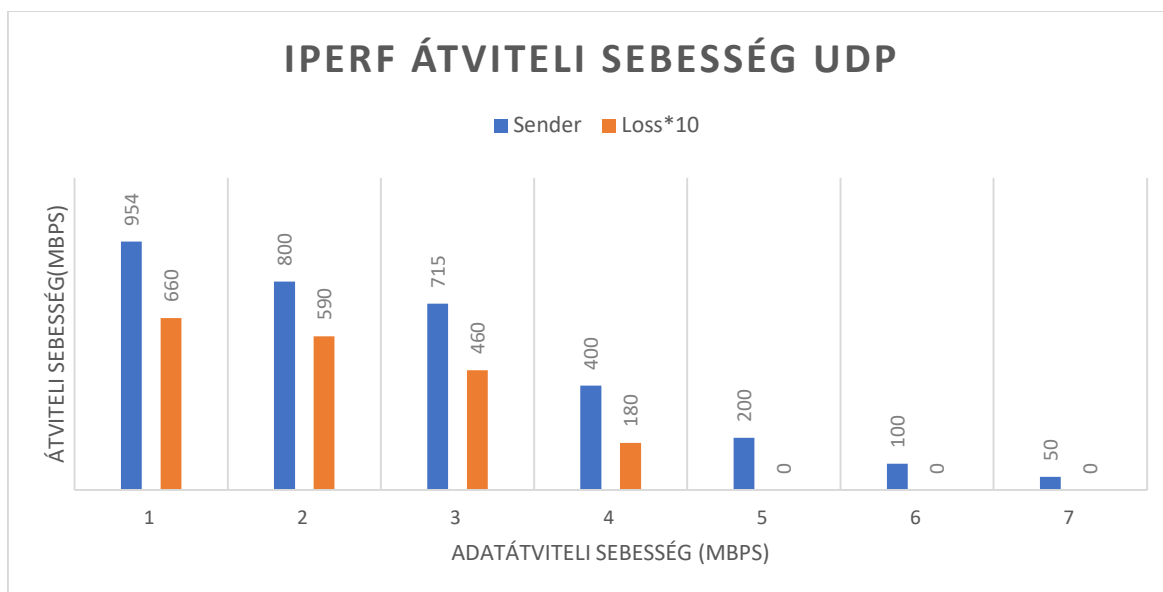


Diagramm 13
Iperf mérési eredmények TCP kapcsolat esetén



*Diagramm 14
Iperf mérési eredmények UDP kapcsolat esetén*

Az általam használt TP-LINK vállalati router átvitele a mérés során nem a várt értékeket hozta ki. A várt értékek a Diagramm 13 nem tükrözik egy 1Gbps átvitelre képes routerek sebességét. A 200Mbps tartomány fölé TCP kapcsolat esetén nem lehet nagyobb átviteli sebességet elérni, egyszerűen valami korlátozza. A hibát egy hardver probléma okozhatja. A probléma forrását próbáltam kiküszöbölni, ami sikertelen lett. A router szoftverében nincs korlátozva, minden korlátozó tényező ki van kapcsolva. A számítógépek hálózati kártyája támogatja az 1Gbps adatátviteli standardot, és a kábelek is megfelelnek ennek. A Diagramm 14-en látszik, hogy UDP kapcsolat esetén ki lehet használni a teljes sávszélességet, viszont az elvesztett adatoknál van, ahol eléri az akár 60%-ot is, ami rengeteg veszteség. A Diagramm 14 megfigyelhető, hogy a 200Mbps-os sávszélesség alatti tartományban az átvitel teljesen megtörténik. Nincsen adatvesztés, úgy működik, ahogy azt elvárnám egy ilyen kategóriájú routeren.

A Diagramm 15 és Diagramm 16 is jól szemlélteti, hogy az általam használt router nem működik megfelelően. A szaggatott adatfolyammal történő átvitel is hasonló eredményeket hoz, mint az Iperf mérés. Itt is megjelenik az a probléma, hogy a 200Mbps átvitel fölött az adatok átvitelét korlátozza a router, vagy pedig UDP kapcsolat során az adatvesztés jelentős. TCP kapcsolat esetén azért csökken ennyit a sávszélesség, mivel a TCP protokoll kijavítja a hibát minden esetben, ami sávszélességet igényel, így a probléma nem a sáv korlátozás, hanem az adatvesztésben kell keresni. Az adat a routerben valahol elvesz, ami egy rossz alkatrésznek vagy komponensnek az oka is lehet.

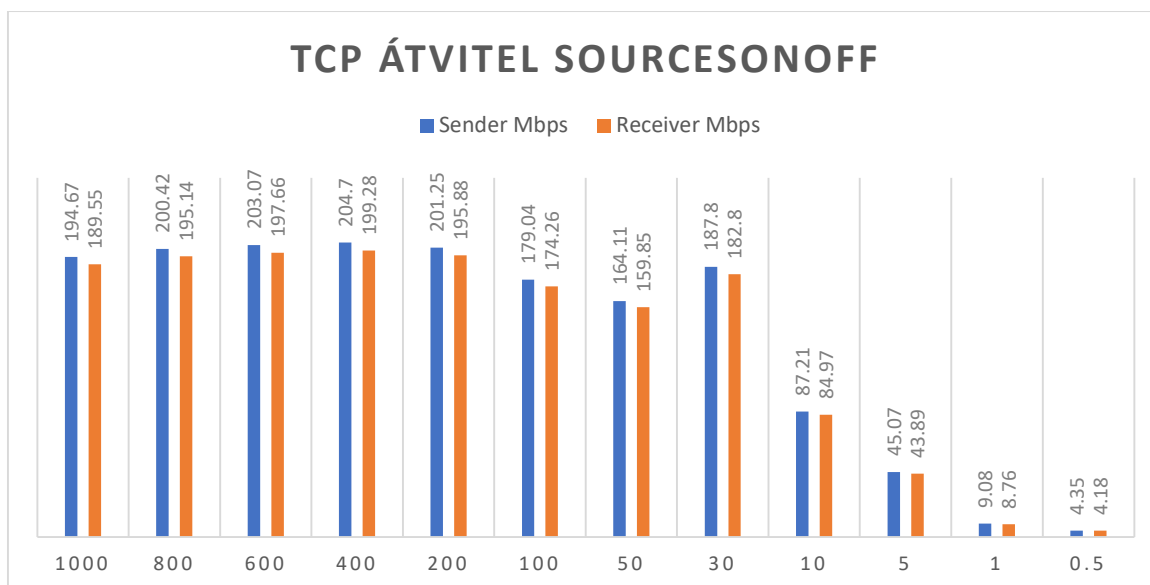


Diagramm 15
SourcesOnOff mérési eredmények TCP kapcsolat esetén

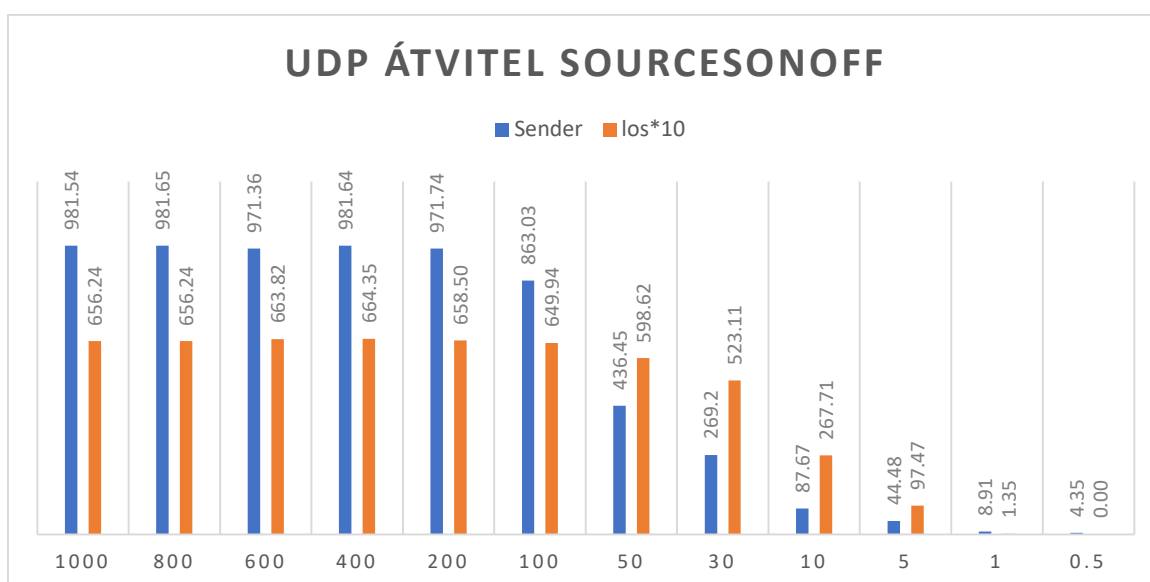
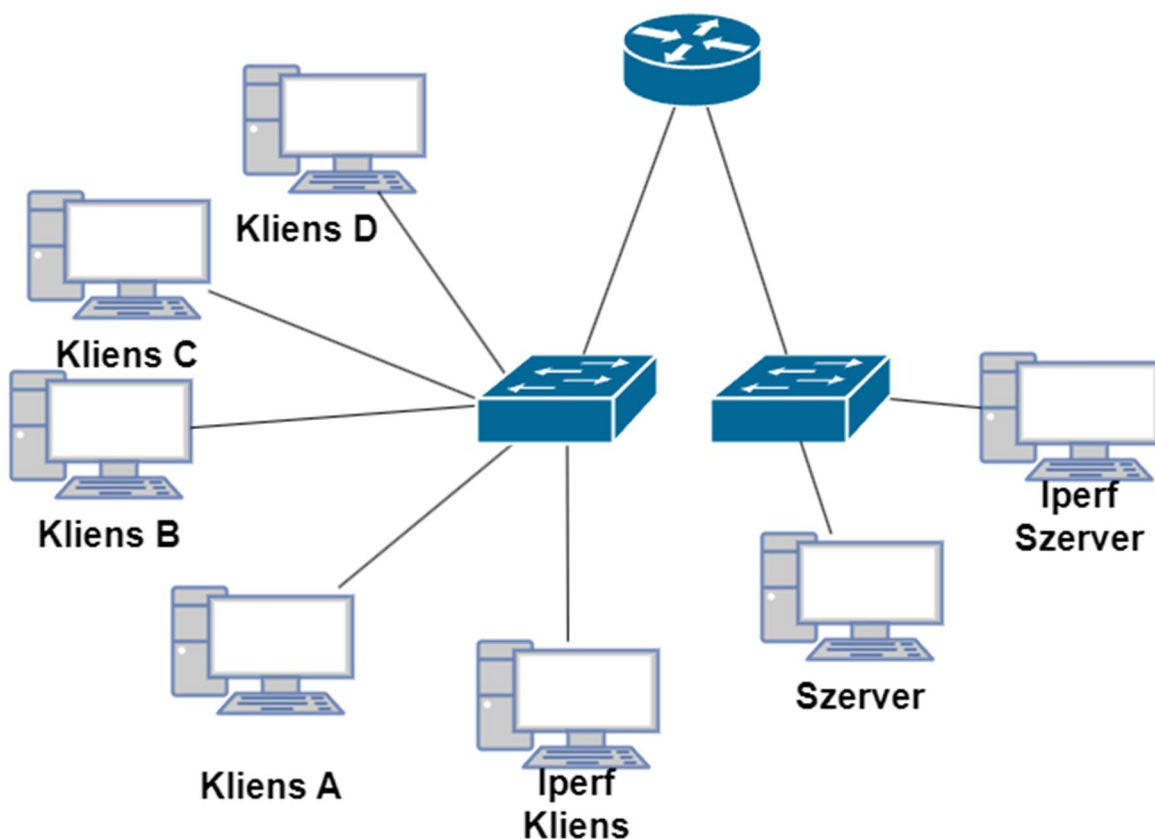


Diagramm 16
SourcesOnOff mérési eredmények UDP kapcsolat esetén

Ebben az esetben az összehasonlítás nem releváns, viszont egy érdekes kérdés lehet, hogy a hibát mi okozhatja. Ebben a dolgozatban a hiba detektálására és kijavítására nem kerül sor, viszont a többi mérésben ugyanúgy részt fog venni, mint a többi router.

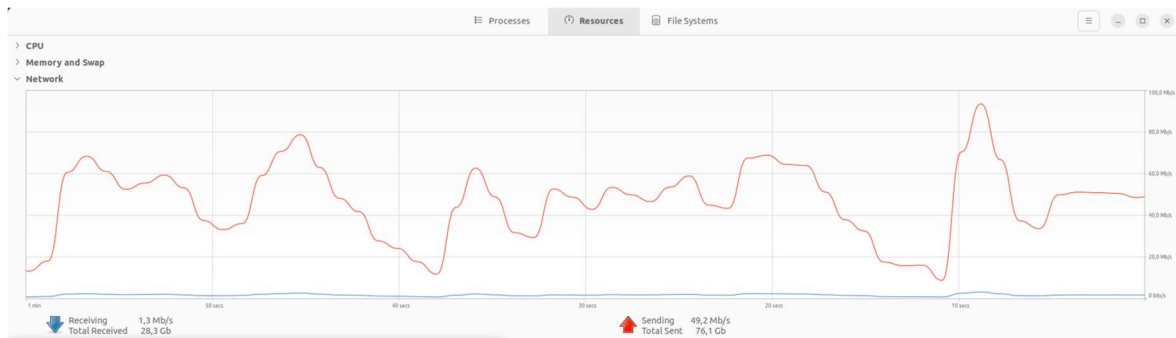
4.4. Terhelés közbeni mérési eredmények

A tényleges hálózati terhelés szimulálására egy kisebb gépekből álló server kliens kapcsolattal rendelkező kis helyi hálózatot raktam össze. Egy szervert futtattam az egyik gépen és 4 másik géppel „támadtam” a server gépet. Mivel az általam használt routernek 4 LAN bemenete van, ezért egy switch-et kellett a rendszerbe integrálni. Ugyanígy egy másik switch-et is a rendszerbe kellett integrálni, mivel csak egy WAN interfész található a routeren és nekem 2 darab szerverem van. A switch-ek képesek 1Gbps-os és 100Mbps adatátviteli sebességre is. A router maximális sebességére igazítva használtam a switch-eket. A megvalósításra a sourcesonoff programot használtam, mivel nem szerettem volna, hogy a „támadás” alatt konstans adatfolyam generálódjon. Ebben a terhelt hálózatban két másik gépet használva próbáltam egy kis adatot átjuttatni a hálózaton, amit az Iperf program segítségével tettem meg, mert az Iperf kiírja az értékeket. A teszt hálózatot a következő ábra 19 szemlélteti.

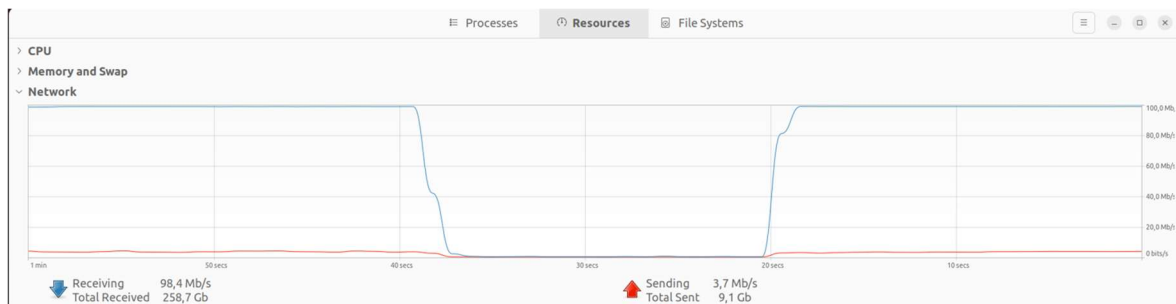


ábra 19
Terhelt hálózat felépítése

Először a Cisco routert teszteltem ezzel a fajta teszteléssel. Amint azt az ábra 20 is mutatja ugyan olyan szaggatott adatot generálok és küldök be a hálózatba. Ilyen fajta adatot 4 gépen generáltam ki majd egyetlen kliensre küldtem el, amit az ábra 21 mutat.



ábra 20
Cisco router kliens oldali mérése



ábra 21
Cisco router szerver oldali mérése

Amint azt a ábra 21 is látható, a szerver oldalon a sebesség maximális, ami azt jelenti, hogy a 4 darab gép teljesen leterheli az átviteli utat a routeren keresztül.

[ID]	Interval	Transfer	Bitrate	Retr	
[5]	0.00-10.00 sec	478 KBytes	392 Kbits/sec	63	sender
[5]	0.00-10.20 sec	379 KBytes	304 Kbits/sec		receiver

ábra 22
Iperf mérési eredménye CISCO 2800 router használatával

A fenti mérések alapján Diagramm 5 a Cisco router maximális átviteli sebessége 95 Mbps körül alakul. Mivel a rendszer most terhelve van, ezért ebben a mérésben látható miként alakul az átviteli sebesség. A leterhelt rendszeren a csökkenés nagyon látszik, pedig a terhelt hálózat mindössze 4 darab gépből tevődik össze. Ez a jelenség annak tudható be, hogy a Retr 63, minek jelentése, hogy ennyiszer lett újra küldve az adat. Ezt a folyamatot az is befolyásolja, hogy a router nem képes megfelelően kezelni az általam terhelt hálózatot.

[ID]	Interval		Transfer	Bitrate	Retr	
[5]	0.00-10.00	sec	288 KBytes	236 Kbits/sec	62	sender
[5]	0.00-10.05	sec	223 KBytes	182 Kbits/sec		receiver

ábra 23

Iperf mérési eredménye TP-LINK TL-WR941ND router használatával

Az alacsony árfekvésű routert megvizsgálva azt az észrevételt lehet lekövetkeztetni, hogy ez a routeren ugyan annyi adat küldődik újra, 62, de eközben az átviteli sebessége lassabb, mint a vállalati routernek. Ennek a routernek az adat irányítási képessége rosszabb, mint a vállalati routeré, ami egy elvárt eredmény.

[ID]	Interval		Transfer	Bitrate	Retr	
[5]	0.00-10.00	sec	693 KBytes	568 Kbits/sec	68	sender
[5]	0.00-10.04	sec	587 KBytes	479 Kbits/sec		receiver

ábra 24

Iperf mérési eredménye ASUS RT-N18U router használatával

A nagyobb sávszélességgel rendelkező routerek átviteli sebessége nem sokkal nagyobb, mint a kisebb sávszélességű routeré, ez jellemző az Asus routerre is. Itt is látható, hogy az átviteli sebesség néhány Kbps. Ennél a sebességénél jobbat vártam el, mikor a mérést elvégeztem. Ezt annak tudható be, hogy a hálózat leterheltsége a maximális érték körül mozog.

[ID]	Interval		Transfer	Bitrate	Retr	
[5]	0.00-10.00	sec	1.53 MBytes	1.29 Mbits/sec	108	sender
[5]	0.00-10.04	sec	1.45 MBytes	1.21 Mbits/sec		receiver

ábra 25

Iperf mérési eredménye TP-LINK TL-ER6120router használatával

A vállalati TP-LINK router ezt a hálózatot sokkal jobban kezeli annak ellenére is, hogy a router nem működik megfelelően. Itt az átviteli sebesség 1Mbps felett van, és az is látható, hogy az újraküldött adatok száma 108.

A mérésekről eredményeképpen az a következtetés vonható le, hogy terhelt hálózatban sem a kategóriás, sem a vállalati routerek nem mutatnak nagy eltérést, és az ilyen hálózatokban az adat átjuttatása igen nehéz feladat. A vállalati routerek egy kicsit könnyebben kezelik ezt a folyamatot, de az eddigi eredmények nem tükrözik az elvárt eredményeket.

4.5. Router szűrő funkció implementálása

A fenti mérési eredmények olyan routereken lettek elvégezve, amelyekben a beépített szűrő funkciók teljesen ki voltak kapcsolva. A dolgozat ezen pontján, azt vizsgálom meg, hogy mennyire befolyásolja a mérési eredményeket, ha a routerbe szűrő funkciót iktatok be.

TP-LINK
TL-ER6120

URL Filtering Web Filtering Access Rules Service

Access Rules

Policy: Block
Service: All Services
Interface: WAN
Source: IP/MASK
192.168.3.14 / 32
Destination: IP/MASK
192.168.4.14 / 32
Effective Time: 00:00 - 24:00
☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat
Description: (Optional)
☐ Priority: Insert as No. Entry

List of Rules

No.	Source	Destination	Policy	Service	Interface	Effective Time	Description	Action
<input type="checkbox"/> 55	192.168.3.3/32	192.168.4.3/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 56	192.168.3.4/32	192.168.4.4/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 57	192.168.3.6/32	192.168.4.5/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 58	192.168.3.7/32	192.168.4.7/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 59	192.168.3.8/32	192.168.4.8/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 60	192.168.3.9/32	192.168.4.9/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 61	192.168.3.10/32	192.168.4.10/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 62	192.168.3.11/32	192.168.4.11/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 63	192.168.3.12/32	192.168.4.12/32	Block	All Services	WAN	Always	---	
<input type="checkbox"/> 64	192.168.3.13/32	192.168.4.13/32	Block	All Services	WAN	Always	---	

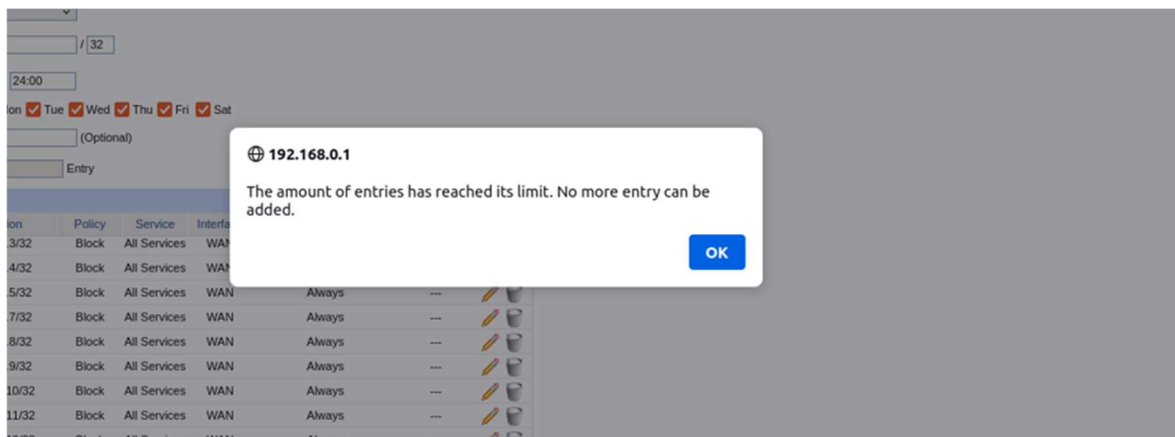
Select All Delete Search

Note:
1. If DMZ is disabled, no operation to the DMZ related rules is allowed except for deleting.
2. It is allowed to select Group for Source only when the effective interface is LAN or DMZ in private mode.

ábra 26

TP-LINK router szűrő funkció beállítása

A fenti ábrán látható, hogy a routerbe beépítve lehet IP cím alapján szűrni a forgalmat, megadott interfészen, különböző protokollok alapján. Az IP címek nem valódiak, ellenben ez nem befolyásolja a végeredményt, ugyanis minden csomag sorban végig megy az összes szabályon amíg valamelyik nem illeszkedik rá.



ábra 27
TP-LINK router szűrő maximális értéke

A blokkolni kívánt IP címeknek van egy felső korlátjuk, ami 64 IP cím beírását engedélyezi, ami arra enged következtetni, hogy ez a fajta szűrő nem fogja befolyásolni az átviteli sebességet.


```

diak@313x5: ~
[ 5] 0.00-10.05 sec 112 MBytes 93.8 Mbits/sec receiver
iperf Done.
diak@313x5:~$ iperf3 -c 192.168.33.1 -p 30000 -b1000M
Connecting to host 192.168.33.1, port 30000
[ 5] local 192.168.33.2 port 48214 connected to 192.168.33.1 port 30000
[ ID] Interval      Transfer    Bitrate      Retr  Cwnd
[ 5] 0.00-1.00 sec  28.5 MBytes 239 Mbits/sec  41    652 KBytes
[ 5] 1.00-2.00 sec  26.0 MBytes 218 Mbits/sec   0    735 KBytes
[ 5] 2.00-3.00 sec  25.9 MBytes 217 Mbits/sec   0    796 KBytes
[ 5] 3.00-4.00 sec  26.0 MBytes 218 Mbits/sec   0    841 KBytes
[ 5] 4.00-5.00 sec  26.1 MBytes 219 Mbits/sec   5    634 KBytes
[ 5] 5.00-6.00 sec  25.4 MBytes 213 Mbits/sec   0    675 KBytes
[ 5] 6.00-7.00 sec  25.2 MBytes 212 Mbits/sec   0    700 KBytes
[ 5] 7.00-8.00 sec  25.6 MBytes 215 Mbits/sec   0    713 KBytes
[ 5] 8.00-9.00 sec  25.9 MBytes 217 Mbits/sec   0    730 KBytes
[ 5] 9.00-10.00 sec 25.8 MBytes 216 Mbits/sec   0    757 KBytes
-----
[ ID] Interval      Transfer    Bitrate      Retr
[ 5] 0.00-10.00 sec  260 MBytes 218 Mbits/sec  46
[ 5] 0.00-10.06 sec  258 MBytes 215 Mbits/sec
sender
receiver
iperf Done.
diak@313x5:~$

```

ábra 28
Szűrő beiktatásával mért eredmény

Az ábra 28 mutatja, hogy a feltételezés igaz, mivel az átviteli sebességen nem rontott egy ilyen fajta szűrő beiktatása. A gyártó ezért is ad meg egy maximális korlátot.

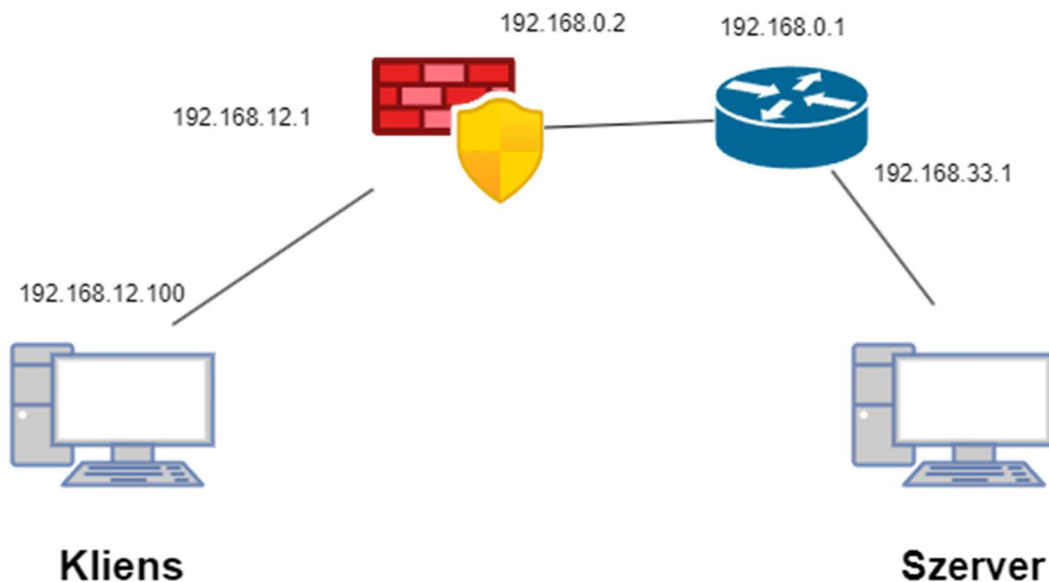
Network Services Filter					
Enable Network Services Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Filter table type	Black List ▾				
Well-Known Applications	User Defined ▾				
Date to Enable LAN to WAN Filter	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri				
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59				
Date to Enable LAN to WAN Filter	<input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun				
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59				
Filtered ICMP packet types					
Network Services Filter Table (Max Limit : 32)					
Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP ▾	
No data in table.					
Apply					

ábra 29
Asus router szűrő beállítása

Amint azt a fenti ábra 29 is mutatja az Asus routernél is elmondható, hogy a gyártó előre meghatároz egy megadott maximális értéket, amivel az átviteli sebességet nem befolyásolja.

4.6. Tűzfal beiktatása a rendszerbe

A fenti mérések eredménye csak egy routerrel összekötött hálózatban van megvalósítva. A következőkben ebbe a hálózatba egy tűzfal is beiktatásra kerül, amivel egy a gyakorlatban is implementált teljes hálózatot hoztam létre. [18]



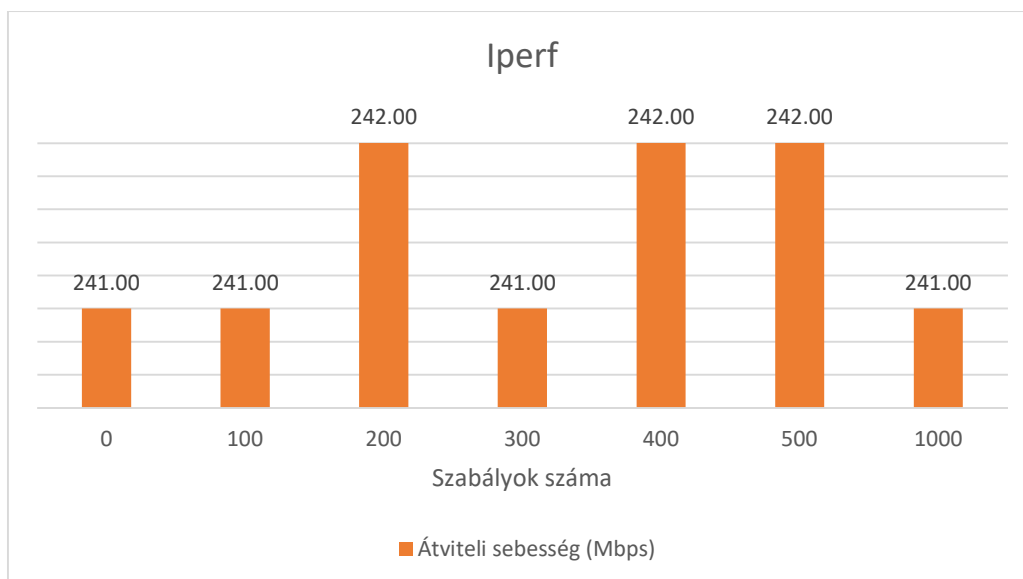
ábra 30
Tűzfalal ellátott hálózat

Ebben a hálózatban a tűzfalban szükségessé vált a NAT protokoll használata, pontosan, mint a routerekben. Az 192.168.0.0-ás hálózatot kell átfordítani az 192.168.12.0-ás hálózatra. Így elérve, hogy az adat a tűzfalon keresztül haladjon át.

A tűzfalban kezdetben 100 majd 200 majd 300, majd 500 és végül 1000 szabály került beírásra és a vizsgálat pedig, hogy mennyire befolyásolják a szabályok száma az átviteli sebességet.

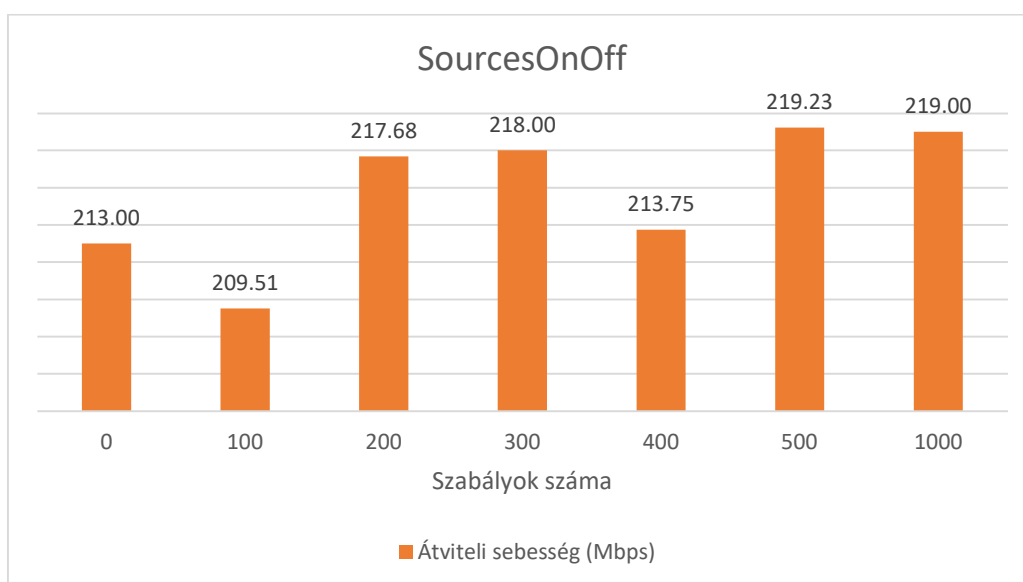
Az általam használt tűzfal paraméterei: 1 magos 3.7Ghz-s Intel Xeon X5450 processzor, 1GB ram és 2.35GB háttértár. A PfSense 2.7.2-es verziójú szoftver tűzfal van alkalmazva, ami az OSI modell 3. rétegében szűr.

Mivel a tűzfalban alkalmazott listát mindig sorba veszi a tűzfal ezért feltételezni lehet, hogy csökkenti az átviteli sebességet.



*Diagramm 17
Iperf mérési eredmények tűzfal beiktatásával*

A Diagramm 17-en megfigyelhető, hogy a tűzfalba beiktatott szabályok nem befolyásolják az átviteli sebességet. Nulla szabály és ezer szabály esetén nincsen eltérés az átviteli sebesség között. Mivel az Iperf egy konstans adatfolyamot generál, ezért nem változik a port száma és az adatfolyam, lehet ezért nem csökken az átviteli sebesség, tehát egy SourcesOnOff mérést is végeztem.



*Diagramm 18
SourcesOnOff mérési eredmények tűzfal beiktatásával*

A Diagramm 18-on látható, hogy a SourcesOnOff mérési eredményei is hasonló eredményt mutatnak az Iperf-hez, annak ellenére, hogy ez a program több portot nyit meg, így kizárva azt a lehetőséget, hogy egy konstans adatfolyamot generáljon. Ebből

következik, hogy a tűzfal szabálytáblája érdemben nem befolyásolja az adat átviteli sebességet.



*ábra 31
1 magos pfSense CPU kihasználtsága*



*ábra 32
2 magos pfSense CPU kihasználtsága*

A fenti két ábrán látható az 1 processzor magos és 2 processzor magos hardver felépítésű tűzfal közötti különbséget. Elmondható, hogy minél több processzor mag áll rendelkezésre, annál kevesebb erőforrást igényel ugyanannak az adatforgalomnak a feldolgozása. Levonható a következtetés: ahhoz, hogy egy PfSense tűzfal biztosítani tudja a megfelelő átviteli sebességet hardver erőforrásra van szüksége, azon belül is processzor erőforrásra. Viszont a tesztekkel sem sikerült egy 1 magos 3.7Ghz-s Intel Xeon X5450 processzorral rendelkező tűzfalat használva átviteli sebesség romlást okozni a tesztelt rendszeren.

5. ÖSSZEGZÉS

Összességében megállapítható, hogy a router választása során az ár nem mindig korrelál a teljesítménnyel és minőséggel. Az általam végzett tesztek során látható volt, hogy a vállalati TP-LINK router nem tudott megfelelni az elvárásoknak, és a Cisco router sem hozott kiemelkedő teljesítményt. Ez a részbeni csalódás, azonban részben érthető, figyelembe véve a technológiai fejlődés sebességét, mivel a Cisco és TP-LINK routerek megjelenése között kicsivel kevesebb, mint 10 év telt el.

Az ASUS router sok esetben jobb teljesítményt nyújtott, ami arra utalhat, hogy a gyártó jobban kihasználta a rendelkezésre álló technológiát, és hatékonyabban optimalizálta a routert a legújabb elvárásoknak. Emellett az újabb belépő/középkategóriás routerek gyakran olyan szolgáltatásokat és funkcionalitást kínálnak, amelyek versenyképesek a vállalati routerekkel. Ez azt jelenti, hogy a felhasználóknak nem feltétlenül kell magasabb árkategóriájú routerre költeniük ahhoz, hogy kielégítsék hálózati igényeiket.

Az általam tesztelt routerek között tapasztalt kis teljesítménybeli különbségek azt mutatják, hogy az ár és a minőség közötti kapcsolat nem mindig lineáris. Fontos lehet az adott felhasználási helyzet és igények alapos mérlegelése, mielőtt a router megvásárlására kerül sor. A megfelelő router kiválasztása sok esetben nem csak a gyártó vagy az ár alapján történik, hanem a konkrét igények, funkciók és teljesítmény alapján is.

A tűzfal beiktatása érdemben nem változtatja az átviteli sebességet, még akkor sem, hogyha sok szabályt tartalmaz. A tűzfal a szabály listát olyan hatékonyan tudja végig futtatni, hogy az az átviteli sebességbe egyáltalán nem szól bele. Ez egy fontos megállapítás, mivel a tűzfalak napjainkban az egyik kulcsa a hálózatok védelmének, a támadások, illetve kártékony szoftver, a rendszerbe való bejuttatásának

6. ÁBRAJEGYZÉK

ábra 1 OSI modell 7 rétege.....	13
ábra 2 TCP/IP modell 4 rétege	16
ábra 3 IPv4 képzése.....	19
ábra 4 IPv6 képzése.....	19
ábra 5 TCP kapcsolat felépítése	20
ábra 6 UDP kapcsolat felépítése.....	22
ábra 7 Router ikonja	23
ábra 8 Switch ikonja.....	26
ábra 9 DHCP folyamat	28
ábra 10 A Cisco Packet Tracer által támogatott protokollok	30
ábra 11 Rendszer összetétele	32
ábra 12 Teljes rendszer felépítése.....	33
ábra 13 Rendszer felépítése.....	35
ábra 14 Iperf3 mérési eredménye TCP kapcsolat során	37
ábra 15 Iperf3 mérési eredménye UDP kapcsolat során.....	37
ábra 16 Iperf által megvalósított mérés	38
ábra 17 Sourcesonoff kódja.....	39
ábra 18 SourcesOnOff által megvalósított mérés.....	40
ábra 19 Terhelt hálózat felépítése	50
ábra 20 Cisco router kliens oldali mérése	51
ábra 21 Cisco router szerver oldali mérése	51
ábra 22 Iperf mérési eredménye CISCO 2800 router használatával	51
ábra 23 Iperf mérési eredménye TP-LINK TL-WR941ND router használatával	52
ábra 24 Iperf mérési eredménye ASUS RT-N18U router használatával.....	52
ábra 25 Iperf mérési eredménye TP-LINK TL-ER6120router használatával	52
ábra 26 TP-LINK router szűrő funkció beállítása	53
ábra 27 TP-LINK router szűrő maximális értéke.....	54
ábra 28 Szűrő beiktatásával mért eredmény.....	54
ábra 29 Asus router szűrő beállítása.....	55
ábra 30 Tűzfallal ellátott hálózat.....	56
ábra 31 1 magos pfSense CPU kihasználtsága.....	58
ábra 32 2 magos pfSense CPU kihasználtsága.....	58

7. HIVATKOZÁSOK

- [1] I. Dr. Bartolits, „A távközlés regénye,” *Élet és irodalom*, pp. 19-28, 2000.
- [2] A. S. Tannenbaum és D. J. Wetherall, Számítógép-hálózatok, Budapest: Panem Könyvek, 2013.
- [3] „What is a protocol,” 2024. [Online]. Available: <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-protocol/>.
- [4] Ropolyi László, Az internet természete, Typotex Kft, 2006.
- [5] „What is the OSI Model?,” 2024. [Online]. Available: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/open-systems-interconnection-model-osi/>.
- [6] C. Joe, Tanuljuk meg a TCP/IP használatát 24 óra alatt!, negyedik szerk., Budapest: Kiskapu Kft., 2009.
- [7] „What are IP & TCP?,” 2024. [Online]. Available: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/tcp-ip/>.
- [8] „User Datagram Protocol (UDP),” 26 Február 2024. [Online]. Available: <https://www.geeksforgeeks.org/user-datagram-protocol-udp/>.
- [9] „TCP 3-Way Handshake Process,” 26 Október 2021. [Online]. Available: https://www.geeksforgeeks.org/tcp-3-way-handshake-process/?ref=next_article.
- [10] „What is a router?,” [Online]. Available: <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-router/>.
- [11] „What is a network switch?,” [Online]. Available: <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-network-switch/>.
- [12] Ookla, „Introducing a Better Measure of Latency,” 12 Május 2022. [Online]. Available: <https://www.ookla.com/articles/introducing-loaded-latency>.
- [13] D. Smith és S. Allen, „How To Test Your Internet Speed,” 20 Szeptember 2023. [Online]. Available: <https://www.forbes.com/home-improvement/home/how-to-test-your-internet-speed/>.
- [14] „Cisco Packet Tracer,” 2013. [Online]. Available: <http://www.cisco.com/web/learning/netacad/coursecatalog/PacketTracer.html>. [Hozzáférés dátuma: 4 12 2023].
- [15] P. Zoltán, „A számítógép-hálózatok tűzfalainak támadása,” *Military Engineer/Hadmérnök* 7.2, %1. kötet VII, pp. 335-341, 2012.
- [16] „iPerf - The ultimate speed test tool for TCP, UDP and SCTP,” [Online]. Available: <https://iperf.fr/iperf-doc.php>. [Hozzáférés dátuma: 23 Október 2023].

- [17] A. Varet és N. Larrieu, „Realistic Network Traffic Profile Generation: Theory and Practice,” *Computer and Information Science*, 18 Február 2014.
- [18] D. Zientara, *Mastering pfSense*, Birmingham: Packt Publishing Ltd., 2016.
- [19] J. Casada, *Tanuljuk meg a TCP/IP használatát 24 óra alatt*, Budapest: Kiskapu kiadó, 2010.