## TTMER25 -Adatátvitel hozzáférési hálózaton (ADSL2, ADSL2+)

1. ***Milyen feladatokat kell megoldani a mérési gyakorlaton?***

- internet szolgáltatás megvalósítása az internet és felhasználói között

- hálózati elemek megismerése, konfigurálása

- mérések végzése a hálózat ADSL és Ethernet rétegeiben

- hibakeresés és javítás

<http://alpha.tmit.bme.hu/meresek/ttmer25a.htm>

1. ***Ismertesse a mérésen használt hálózat fő elemeit, és azok fő feladatait!***

- ADSL2/2+ DSLAM ( ZyXEL AAM1212-51 )

- ADSL2/2+ MODEM + WLAN router ( ZyXEL P660HW-T1 )

- ADSL vonal szimulátor ( DSL JUPITER )

- Számítógépek: (router, csomag monitorozási, menedzselési, előfizetői terminál feladatokra )

PC - DSLGW - ISP router

PC - billentyűzetváltó 7-es gomb, Protokoll teszter (Wireshark), DSLAM konfigurálás

PC - billentyűzetváltó 3-as gomb, Internet user (WLAN terminal), jegyzőkönyv készítés

Notebook - MODEM konfigurálás

A szolgáltatás az internet szolgáltató (ISP) berendezésein (DSLGW, DSLAM, előfizetői kábelhálózat, modem) keresztül valósul meg.

A felhasználók hálózata egy NAT-olt helyi hálózat. A forgalom szétosztását a felhasználók között a DSLAM-ban levő VLAN switch végzi. A switch gyors működéséhez a felhasználókat VLAN-okba (Virtuális LAN) szervezi a szolgáltató Az IP cím - VLAN ID összerendelést és a NAT-olást a DSLGW végzi.

Az előfizetők és a szolgáltató közötti kapcsolatfelvételt, bontást, a jogosultság ellenőrzését a PPPoE szerver végzi.

Az internet forgalmat a szolgáltatótól a felhasználóig az ADSL vonalszakaszon továbbítjuk. Egy vonalszakasz egy előfizetői kábel érpárból és mindkét végén egy jelátalakítóból (modem) áll. A mérési összeállításban az előfizetői kábel érpárat - a keletkező zavarokkal együtt - szimuláljuk. A vonalszakasz szolgáltató oldali (LTU) modemjei a DSLAM-ban helyezkednek el. A felhasználó oldali (NTU) modem dobozában további hálózati elemek (router, többféle (100BASE-T, WLAN) interfész) is elhelyezkednek.

<http://alpha.tmit.bme.hu/meresek/ttmer25b.htm>

<http://alpha.tmit.bme.hu/meresek/ttmer25a.htm>

1. ***Magyarázza meg miben tér el az ADSL over ISDN és az ADSL over POTS?***
* ISDN/POTS - Az ADSL frekvenciasávja alatt ISDN vagy PSTN telefonszolgáltatás működhet. A két szolgáltatás szétválasztása a frekvenciatartományban villamos szűrőkkel (splitter) történik.
* Alsó frekvencia határ:
	+ ISDN-nél: 120 vagy 254 kHz
	+ POTS-nél: 25.875 vagy 138 kHz
1. ***Ismertesse az ADSL vonali réteg fő paramétereit!***

- **Bit rate, Stream Rate** az elérendő (tervezett) bitsebesség (specifikáció (max. min. érték))

- **Attainable bit rate** az elérhető - a DMT csatornákban mért jel/zaj viszony alapján meghatározott - bitsebesség

- **SNR (Signal to Noise Ratio) Margin, Stream Noise Margin** a mért jel/zaj viszony dB-ben a követelményhez viszonyítva.

Az ADSL rendszereket 10e-7 hibaarányra méretezik, e hibaarányhoz tartozó zajszint az SNR Margin (a relatív jel/zaj viszony) viszonyítási alapja (0 dB). (Emlékeztetőül, PCM rendszereknél ez a hibaarány érték 10e-6 volt.)

A jel/zaj viszonyra a menedzselő rendszerben követelményt (Desired Margin, Target SNR) is megadhatunk. A tipikus érték 6 dB. Ez azt jelenti, hogy a megkövetelt jel/zaj viszony 6 dB-el nagyobb, mint a 10e-7-es hibaarányhoz tartozó érték. Ez azt is jelenti, hogy a zajteljesítmény akár négyszeresére is növekedhet az összeköttetésben annak zavarása nélkül. A zaj túlnyomórészt áthallási zaj, ennek időbeli ingadozását okozhatja az, hogy egyes időintervallumokban változó számú előfizető használja az ADSL-t egy kábelben.

- **Line attenuation, Stream Attenuation** Az adott és vett jelteljesítményekből meghatározható előfizetői réz érpár csillapítás.

**- Output power, Stream Output Power** Az ADSL adó kimenőteljesítménye

**- Service mode** Az ADSL keret típusa

**- Trellis Encoding** Trellis vonali kódoló használata

**- Interleave delay** A késleltetés az interleave átviteli úton.

**- Bits/channel** DMT csatornánkénti bitkiosztás. Megadja, hány bitet lehet átvinni DMT-csatornánként.

<http://alpha.tmit.bme.hu/meresek/adslref.htm#linelayer>

1. ***A protokollstack melyik elemére hatnak a következő paraméterek: mode (g.dmt, adsl2, auto)?***

Az ADSL keret típusát határozza meg.

<http://alpha.tmit.bme.hu/meresek/adsld2.htm>

1. ***A protokollstack melyik elemére hatnak a következő paraméterek: VPI, VCI?
Az RFC 1483 eljárásait a protokollstack melyik két rétegének határán alkalmazzák?***

A továbbítás fizikai rétege a DSLAM és a NTU között ADSL, amin 53 bájtos ATM cellákat továbbítunk (AAL5). Az ATM keretfejléc mezői a VPI (Virtual Path Identifier, virtuális út azonosító) és a VCI (Virtual Circuit Identifier, virtuális csatorna azonosító).Az RFC1483 szabvány egy multiplexelési megoldást fogalmaz meg, azaz hogy internet/ethernet forgalom hogyan enkapszulálható ATM AAL5-be. Lényegében két multiplexelési megoldás adott:

* VC-multiplexálás: csomag típusonként külön virtuális csatorna (VPI, VCI) használata
* LLC-multiplexálás: a különféle csomagok keretezés után **közös** virtuális áramkörön továbbítódnak, LLC alréteg header beillesztése mellett
1. ***Milyen sebességtartományban és mekkora hatótávolsággal működnek a WLAN AP-k? Mi az összefüggés a kettő között?***

**Hatótávolság** tipikusan csak néhányszor 10 méter.

**Sebesség** nagyobb távolságon csak kisebb sebesség érhető el, de a maximális sebesség is némileg kisebb, mint a jelenlegi vezetékes hálózatoké. Ugyanakkor sok esetben vezetéknélküli link sebessége még mindig jelentősen meghaladja annak az összeköttetésnek a sebességét, amelyik az AP-t az internettel összeköti (gondoljunk egy ADSL összeköttetésre).

<http://alpha.tmit.bme.hu/meresek/wlan.htm>

1. ***Melyek a WLAN hálózatok előnyei és hátrányai a vezetékes hálózatokhoz képest? Soroljon fel 3-3 előnyt illetve hátrányt!***

**Előnyök:**

* **Kényelem** - például a nyilvános WLAN-hálózatok használhatósága.
* **Mobilitás** - az összeköttetés megszakadása nélkül, tehát on-line állapotban is.
* **Telepítés** - kisebb mértékben szükséges a vezetékezés, kevesebb a hálózatban a fix elem, elosztott rendszerek előtérbekerülése. Bizonyos esetekben az infrastruktúra hiánya miatt csak így lehetséges az internethez való kapcsolódás.
* **Bővíthetőség** - az elosztott rendszerek rugalmassága miatt is egyszerűbb, időben is gyorsabb.
* **Költségek -** kezdeti beruházás szükséges, de ez hamar megtérül.

**Hátrányok:**

* **Biztonság** - az antennák nem irányítottak, vagyis a rádiójelek bárki által foghatóak. A titkosítási módszerek meggátolhatják a lehallgatást, de a zavarást nem tudjuk megakadályozni.
* **Hatótávolság** - tipikusan csak néhányszor 10 méter.
* **Megbízhatóság** - a rádióhullámok terjedését több tényező befolyásolhatja, csökkentve a jelerősséget, a jel-zaj viszonyt. A fellépő interferenciajelenségek jelentősen ronthatják a demodulálás hatékonyságát.
* **Sebesség** - az előbbi szempontokkal összefüggésben nagyobb távolságon csak kisebb sebesség érhető el, de a maximális sebesség is némileg kisebb, mint a jelenlegi vezetékes hálózatoké. Ugyanakkor sok esetben vezetéknélküli link sebessége még mindig jelentősen meghaladja annak az összeköttetésnek a sebességét, amelyik az AP-t az internettel összeköti (gondoljunk egy ADSL összeköttetésre).
* **Rádiós emisszió** - tulajdonképpen elektroszmogot generálunk, amely egyrészt más WLAN-ok működését nehezíti (interferencia), másrészt más elektronikus eszközök hibás működéséhez vezethet, harmadrészt az emberi egészséget is károsíthatja.

<http://alpha.tmit.bme.hu/meresek/wlan.htm#wlanprocon>

1. ***Milyen frekvenciatartományt használunk az átvitelre a különböző WLAN-szabványok esetén?***

IEEE szabvány Működési frekvencia (GHz)

Eredeti 802.11 2,4

802.11a 5

802.11b 2,4

802.11g 2,4

<http://alpha.tmit.bme.hu/meresek/lanfiz.htm>

1. ***Milyen típusú vezetéknélküli architektúrákat különböztetünk meg? Röviden jellemezze őket!***

- építőelemei: vezetéknélküli állomások és hozzáférési pontok

- hálózati architektúrák:

- ad-hoc mód: a csomópontok közvetlenül egymással kommunikálnak (ha az állomások nem fixek: MANET)

- infrastruktúrális mód: minden kommunikáció a hozzáférési ponton keresztül zajlik, a bázisállomás a vezetékes internethálózatra csatlakozik

- monitor mode: az állomás passzívan lehallgatja egy adott csatorna összes kommunikációját -> megfelel a hálózati forgalom megfigyelésére és analizálására.

<http://alpha.tmit.bme.hu/meresek/wlan.htm#wlannet>

1. ***Milyen módszereket ismer a közös rádiós közeghez való hozzáférésre?***

A közös rádió közeghez való hozzáférésre kétféle megoldás lehet, egy központosított és egy elosztott, amelyek néha egyszerre is működhetnek:

* 1. Az elsődleges hozzáférési módszer a **DCF (Distributed Coordination Function)** nevet viseli és a CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance - A CSMA típusú eljárások egyike. Olyan esetekben használjuk, amikor a CSMA/CD-t nem lehet. Ilyen például a vezeték nélküli hálózatok esete.) protokollok családjából származik. A CSMA/CA protokoll az ütközések valószínűségének csökkentése érdekében véletlenszerű backoff módszert használ. A DCF esetén a véletlenszerű backoff idő diszkrét időtartamok egyenletes eloszlása, ahol az egyenletes tartomány maximális terjedelmét Contention Window-nak (CW), versengési ablaknak nevezik. Nyugtakeret hiánya sikertelen keretküldést jelent és ilyenkor a CW értéke duplájára nő. A versengő állomások számának növekedésével az exponenciális backoff mechanizmus lecsökkenti az ütközések számát. A DFC protokoll két kontroll keretet használ: a RTS (Request To Send) keretet, amely segítségével egy potenciális küldő engedélyt kér küldéshez a vevőtől, illetve a CTS (Clear To Send) keretet, amellyel a vevő válaszol a küldő RTS kérésére. Az RTS keret ugyanakkor jelzi a többi küldő számára, hogy NAV (Net Allocation Vector) ideig ne kezdeményezzen semmilyen fajta küldést. (IEEE 802.11 RTS/CTS exchange) Ez az RTS/CTS jelzésrendszer overhead-et eredményez, így kisméretű keretek átvitele esetén nem használja a MAC protokoll, mivel kisméretű keretek ütközési valószínűsége kicsi.
	2. Az AP-nek **PCF** (Point Coordination Function) funkciója is lehet, amely segítségével kontrollálni tudja a közeghez való hozzáférés prioritását, ezáltal az időérzékeny szolgálatokat is biztosítani tudja. A PCF PIFS (PCF Inter-Frame Spacing) időintervallumban egy beacon keretet küld, amellyel a cellában található minden állomást értesít, hogy ne kezdeményezzen küldést CFP (Contention-Free Period) ideig. Ezután az AP polling módszerrel versengés nélküli hozzáférést tud biztosítani az adott állomások számára. Annak megfelelően, hogy mekkora a rendszer terhelése, a CFP intervallum mérete változhat minden egyes CFP ismétlődő intervallumon belül. Az egymás melletti cellákban lévő PCF állomásoknak különböző csatornákat kell használniuk, ellenkező esetbe n ütközések fordulhatnak elő.

<http://alpha.tmit.bme.hu/meresek/wlan.htm#wlannet>

1. ***Mi az SS illetve a BSS? Miből származtatjuk az azonosítóikat (SSID illetve BSSID)?***

**SS - Service Set** - azon eszközök összessége, amelyek egy adott, specifikus vezetéknélküli lokális hálózathoz kapcsolódnak.

**SSID - Service Set Identifier** - a vezetéknélküli hálózatot azonosító név. Ha nem tiltjuk le, az AP üzenetszórásban hirdeti az SSID-t. Ennek alapján automatikusan (előzetes konfigurálás után) - vagy manuálisan - csatlakozhat egy állomás a hálózathoz. Az SSID 32 oktet hosszúságú bitsorozat. A gyártók a WLAN routereket többnyire a gyártóra utaló SSID-vel hozzák forgalomba, amit természetesen a felhasználó megváltoztathat.

**BSS - Basic Service Set** - az egymással kommunikálni tudó állomások összessége. Infrastruktúra módban egy AP és az általa kiszolgált állomások (STAs) összessége (nem keverendő össze az AP által lefedett területtel). Tulajdonképpen a WLAN hálózatok alapvető építőeleme. Kétféle BSS létezik: Independent BSS (IBSS) és infrastruktúra BSS.

**BSSID - Basic service Set Identifier** - a BSS-t a BSSID-vel azonosítjuk, ami minden infrastuktúra BSS esetén a vezetéknélküli hozzáférési pont MAC címe. Az IBSS esetén nincs AP, az IBSS-t kezdeményező állomás véletlenszerűen sorsol egy MAC-címet, amit aztán BSSID-ként használ.

<http://alpha.tmit.bme.hu/meresek/wlan.htm#wlanwords>

1. ***Milyen lehetőségeket ismer a WLAN hálózatok illetéktelen hozzáférésekkel szembeni védelmére?***

Fontos tudnunk, hogy védelem nélkül a rádiós adásokba bárki belehallgathat, aki az antenna adáskörzetében vezetéknélküli vevővel rendelkezik. A védekezési lehetőségeket sorba állíthatjuk. Egyre erősebbek ennek alapján a következő módszerek:

- Egyedi ESSID (ez alapértelmezett)

- Egyedi, rejtett ESSID

- MAC-cím szűrési táblák használata

- WEP titkosítás

- IEEE 802.1x EAP RADIUS autentikációval

- WPA (Wi-Fi Protected Access)

<http://alpha.tmit.bme.hu/meresek/wlan.htm#security>

1. ***Mit jelentenek a RADIUS, WEP, WPA betűszavak? Melyek a WEP gyengeségei?***

**RADIUS** – Remote Authentication Dial In User Service

hálózati protokoll, amely központosított AAA menedzsment szolgáltatást nyújt a hálózathoz csatlakozó és azt használó számítógépek felé.

A RADIUS három funkciót valósít meg:

1. Hitelesíti a felhasználót vagy az eszközt, mielőtt hozzáférést engedne számára a hálózathoz.
2. Engedélyezi ezeknek a felhasználóknak vagy eszközöknek, hogy bizonyos hálózati szolgáltatásokat igénybe vegyenek.
3. Számlázást végez a szolgáltatásokkal kapcsolatban.

**WEP** – Wired Equivalent Privacy

Az RC4 titkosító algoritmusra épül, mely 40 vagy 104 bites kulcsot használ kombinálva 24 bites inicializáló vektorral. RC4: titkos kulcsból és egy véletlen számból álló véletlen bájtsorozatot állítanak elő, majd xor művelet az üzenet bájtjaival. Egy M üzenet és ICV kontroll összeg titkosítása:
C = [ M || ICV(M) ] XOR [ RC4(K || IV) ]

Hitelesítés:

A hitelesítést kihívás-válasz alapú protokoll végzi, mely 4 üzenetből áll:

1. A kliens jelzi, hogy szeretné hitelesíteni magát (authenticate request)
2. Az AP generál egy véletlen számot, s azt kihívásként elküldi a kliensnek (authenticate challenge)
3. A kliens rejtjelezi a kihívást (véletlen szám) egy olyan kulccsal, amelyet mindketten ismernek és az eredményt visszaküldi az AP-nek.
4. Ha az AP sikeresen dekódolta az üzenetet, ez azt jelenti hogy a kliens valóban ismeri a megfelelő kulcsot, ezért válaszul egy authenticate success (hiba esetén failure) üzenetet küld a kliensnek.

Miután a hitelesítés megtörtént az AP és a kliens kódolt üzenetekkel kommunikálnak egymással. Az üzenetek kódolásához ugyanazt a kulcsot használják mint a hitelesítéshez, az algoritmus pedig az RC4 kulcsfolyam kódoló.

A WEP hiányosságai

- Ugyanazt a kulcsot használja hitelesítésre és kódolásra.

- A hitelesítés csak a hálózathoz való csatlakozás pillanatában történik és többet nem

- Csak a kliensnek kell hitelesítetnie magát, az AP-nek nem.

- Statikus kulcsokat alkalmaz, ezért egy nagy rendszerben a kulcsok cseréje időigényes feladat.

- WEP 128 bites biztonságot nyújt, olvashatjuk mindenhol. De ez nem igaz, mivel a 128 (64) bitbol 24 mindig nyíltan kerül átvitelre

- Az IV a WEP-nél használt implementációban 24 bit hosszúságú, tehát az összes lehetséges IV-k száma 224 = 16 777 216, ami csomagkapcsolt hálózati kommunikációnál nem nevezhető elég nagy számnak az ismétlődések gyakoriságát tekintve.

- Minden kliens ugyan azt a kulcsot használja az AP-vel való kommunikáció során, így mindenki üzenetét vissza tudja fejteni.

- Léteznek úgynevezett gyenge RC4 kulcsok, melyekbol az RC4 algoritmus nem teljesen véletlen bájtsorozatot állít elő. Ha valaki meg tudja figyelni egy gyenge kulcsból előállított bájtsorozat első néhány bájtját, akkor abból következtetni tud a kulcsra.

**WPA** - Wi-Fi Protected Access

- kötelezővé tette a felhasználó hitelesítését, törekedett az erősebb titkosításra, a kulcs menedzsment megvalósítására és a visszajátszás elleni védekezésre

- WPA: RC4-en alapuló TKIP -> a WEP-nél jelenlevő gyengeségek megvannak

- WPA2: CCMP -> erősebb titkosítás

<http://alpha.tmit.bme.hu/meresek/wlan.htm#security>

1. ***Mire jó a MAC ID filtering és hogyan támadható?***



1. ***Mit jelent, ha az erre képes ADSL modem routerként illetve bridge-ként működik?***

Ha ***bridge***-ként működik, akkor lényegében transzparens, egyetlen kliens kezelésére képes, akinek az egyetlen szolgáltatótól kapott IP címet továbbadja.

Ha ***router***ként működik, akkor több klienst is elláthat, ezeknek belső magánhálózati (NAT-olt) IP címeket osztva, kifelé egy gépnek látszanak.

1. ***Mire szolgál a VLAN? Hol használjuk ezt a technológiát a mérési összeállításban? Hány paramétert tartalmaz egy VLAN-tag, mik ezek?***

VLAN – Virtual Local Area Network

*A forgalom szétosztását a felhasználók között a DSLAM-ban levő VLAN switch végzi. A switch gyors működéséhez a felhasználókat VLAN-okba (Virtuális LAN) szervezi a szolgáltató. A VLAN taggelt forgalom a szolgáltatói oldalon lévő DSLGW és a DSLAM között továbbítódik.*

 A QTag prefix két paramétert tartalmaz VLAN-ok kialakításához:

* VLAN ID (1...4096) - VLAN azonosítója. Az azonos VLAN ID-vel rendelkező eszközök, portok egy VLAN-ba tartoznak.
* User Priority (0...7) - mellyel a VLAN kerethez egy prioritás paramétert rendelhetünk.
(Ez a paraméter kapcsolatba hozható a QoS paraméterrel)

<http://alpha.tmit.bme.hu/meresek/lanmac.htm>

1. ***Mire szolgál a PPP? Milyen szolgálatokkal rendelkezik ez a protokoll?***

**A PPP (Point-to-Point Protocol)** (IETF RFC 1661)

Két hálózati csomópont közti közvetlen kapcsolat felépítésére használható protokoll. Számos fizikai hálózaton: soros vonal, vezetékes és mobil telefonvonal és trönk, optikai link használható. Leggyakoribb alkalmazása: Internet szolgáltató és felhasználó összekapcsolása ADSL hálózaton.

**Szolgálatok:**

* authentication - jogosultság
* encryption - titkosítás
* compression - adat kompresszió

<http://alpha.tmit.bme.hu/meresek/lanmac.htm#ppprot>

1. ***Ismertesse a PPP részeit!***
* LCP - a PPP Link Control Protocolja (PT=0xC021) adatkapcsolat létesítéséhez, konfigurálásához és teszteléséhez.
* CHAP - Challenge Handshake Authentication Protocol (PT=0xC223)
* IPCP - PPP Internet Protocol Control Protocol, az LCP felett, e felett van az IP (RFC 1332 old:1172) (PT=0x8021)
* CCP - PPP Compression Control Protocol (RFC 1962)

<http://alpha.tmit.bme.hu/meresek/lanmac.htm#ppprot>

1. ***Ismertesse a PPP állapotait!***
* Dead - Nyugalmi állapot
* Establish - kapcsolat felépítés
* Authentication - jogosultság vizsgálat
* Network - adatátvitel
* Terminate - bontás

<http://alpha.tmit.bme.hu/meresek/lanmac.htm#ppprot>

1. ***Hogyan illesztjük a PPP protokoll üzenetcsomagjait ATM AAL5 és Ethernet keretekbe?***

**VC, LLC multiplexelés, PPPoA**

A fizikai rétegen túl az adatkapcsolati (ATM) réteg is nyújt adatfolyam **multiplexelés**i lehetőséget a felhasználó számára ATM VC-k (virtuális áramkörök) formájában. Egy ADSL összeköttetésben több ATM virtuális áramkör alakítható ki.

Az adatfolyamok multiplexelésére két eljárást dolgozták ki:

* **VC-multiplexing**: Csomag típusonként (pl. IP, IPX, DECnet, Appletalk) külön virtuális csatorna (VPI,VCI) használata.
* **LLC-multiplexing**: A különféle csomagokat keretezzük (encapsulation) majd egy közös virtuális áramkörön továbbítjuk. A keret fejléce a DLC LLC alrétegének [header](http://alpha.tmit.bme.hu/meresek/lanmac.htm#llcframe)-e. Innen az eljárás elnevezése.
a fejlécre azért is szükség van, mert az AAL5 keret nem tartalmaz **payload típus azonosító**t, így nem tudjuk, hogy a vételoldalon hogyan kezeljük a vett PDU-t.

A multiplexelés utáni AAL5 keretek felépítése:

Itt megkülönböztetett figyelemben részesítjük az ilyen rendszerekben a kapcsolatfelépítésre használt PPP protokoll multiplexelését az AAL5 keretbe. (PPPoA, RFC 2364)

VC-multiplexing: a payload változatlan formában kerül az AAL5 keretbe. Példák:

 Bridged Ethernet Routed Protocols PPPoA

 (RFC 1483) (RFC 1483)

 +----AAL5---+ +----AAL5---+ +----AAL5---+

 | | | | | |

 | Ethernet | | Payload | | PPP |

 | frame | | | | Payload |

 | | | | | |

 +-----------+ +-----------+ +-----------+

 | AAL5 | | AAL5 | | AAL5 |

 | trailer | | trailer | | trailer |

 +-----------+ +-----------+ +-----------+

LLC-multiplexing: a payload elé kerül az LLC header az AAL5 keretbe. Példák:

 Bridged Ethernet Routed Protocols PPPoA

 (RFC 1483) (RFC 1483)

 +----AAL5---+ +----AAL5---+ +----AAL5---+

 | LLC header| | LLC header| | LLC header|

 +-----------+ +-----------+ +-----------+

 | | | | | |

 | Ethernet | | IPv4 | | PPP |

 | frame | | frame | | payload |

 | | | | | |

 +-----------+ +-----------+ +-----------+

 | AAL5 | | AAL5 | | AAL5 |

 | trailer | | trailer | | trailer |

 +-----------+ +-----------+ +-----------+

1. ***Mire szolgál a NAT, és hol használható a mérési összeállításban?***

NAT: Network Address Translation

- hálózati címeket cserélő protokoll

- IP-címtér kimerülésének lassítása és biztonsági megfontolások

- aktív hálózati építőelem, amelyet tipikusan a border routerben vagy a tűzfalban helyezünk el

- megvizsgál minden rajta átmenő IP csomagot, ezeket megváltoztatva vagy változtatás nélkül továbbítja vagy eldobja

- a tűzfalaktól eltérően a NAT a csomag megváltoztatására is képes

- a változtatás az IP fejlécét (illetve esetleg a szállítási protokoll fejlécét) érinti

- a kifelé menő csomagban a forráscímet (és esetleg portszámot) változtatja meg, míg a befelé érkező csomagban a célcímmel (és esetleg portszámmal) teszi ugyanezt

- nemnyilvános IP-tartományokat a belső oldalon használjuk, míg kívül egy a belső kisebb tartományt használva tudjuk az Internetet elérni.

- a virtuális magánhálózatok számára természetes védelem, hogy a belső oldalon elhelyezett eszközök és szolgáltatások nem címezhetők meg és ezáltal nem érhetők el kívülről

*Maga a labor ADSL hálózata is egy NAT-olt környezet, hiszen kifelé egyetlen publikus IP-címmel rendelkezik. A bevezető alapján:*

* *NAT-ol a felhasználói router (pl. saját otthoni hálózat)*
* *a szolgáltató is NAT-olt IP-t ad a felhasználóknak, kifelé így több előfizető is egyetlen IP-címen látszódhat*

<http://alpha.tmit.bme.hu/meresek/lanip.htm#nat>

1. ***Mi a hasonlóság az ARP és a NAT között?***

ARP: Address Resolution Protocol

Az ARP az adatkapcsolati réteg egy protokollja. Elsődleges funkciója, hogy a hierarchikus kiosztású, hálózatfüggő IP-címet flat címzési struktúrájú, hordozható MAC-címre oldja fel, hiszen az Ethernet-frame-eket eszerint címezzük meg. Egy ismeretlen MAC-cím megszerzésére szolgál.

 *„Semmi közük egymáshoz. De annyi hasonlóság van, hogy az ARP-nél a router felveszi a közvetítő szerepét és mintegy elfedi a MAC címét az eredeti kérőnek”. Válasz by Marci. BTW ez a kérdés Pali bá szerint is baromság. ☺*

<http://alpha.tmit.bme.hu/meresek/lanmac.htm#arprot>

1. ***Mire szolgál a DHCP, és hol használható a mérési összeállításban?***

DHCP - Dynamic Host Configuration Protocol

- hálózati alkalmazás, mely segítségével az eszközök az IP hálózat használatához szükséges beállításokat automatikusan elvégezhetik

- jelentősen meggyorsítja az újabb hálózati végpontok hozzáadását

- A DHCP-kliensként konfigurált hálózati eszköz bekapcsolás után egy broadcast üzenettel felderíti a DHCP szervert.

- A szerver egyrészt rendelkezik egy kiosztható IP-címtérrel, másrészt további információkkal, amelyeket meg kell osztania a jelentkező kliensekkel (default gateway, domain name, DNS szerver elérhetősége stb.)

- Ha a DHCP-szerver érvényes kérést kap, akkor a kliensnek kioszt egy IP-címet és mellékeli az egyéb szükséges hálózati paramétereket

- IP cím kiosztása lehet:

 *dinamikus* (csak egy adott időre tartozik a klienshez),

 *automatikus* (nyilvántartja az összerendeléseket, lehetőleg a korábban használt címet rendeli hozzá),

 *statikus* (előre beállított)

<http://alpha.tmit.bme.hu/meresek/lanuser.htm#dhcp>

* *A ZyXEL modem konfigurálásánál a helyi hálózati beállításoknál alkalmazhatunk DHCP-t a címkiosztáshoz. (Ekkor megadandó: DHCP ( Server / None / Relay ), Client IP Pool Starting address, Size of Client IP Pool, Primary DNS server, Secondary DNS server, Remote DHCP server*
* *A szolgáltatói router NEM DHCP-t használ, hanem statikusan oszt címeket.*
1. ***Ismertesse vázlatosan a DNS működését!***

DNS – Domain Name System

- hierarchikus névrendszer

- hálózati eszközök szimbolikus nevei – numerikus azonosítók 🡪 a fordítást a DNS rendszer végzi.

- nevek és bináris számok közötti összerendeléseken túl egy *Resource Recordban (RR)* további információkat is nyilvántartanak: bejegyzés típusa, érvényesség ideje.

- domain nevek tere: fa struktúra – minden csomóponthoz vagy levélhez tartozhat bejegyzés, akár több is

- a fát zónákra osztjuk, egy ilyen zóna összekapcsolt csomópontok együtteséből áll, amelyet egy illetékes name server szolgál ki

- domain név: két vagy több részből áll (label), ezeket ponttal választjuk el

 - jobb szélső címke: top level domain www.example.**com**

- ettől balra minden címke egy subdomain-t jelöl

- a hierarchia csúcsát a root nameserverek szolgálják ki

- ezek alatt állnak az egyes subdomainek authoritative DNS szerverei

- a kliens oldal kezdeményezi a lekérdezések sorozatát, amely végül a teljes feloldáshoz vezet

- lekérdezés lehet rekurzív vagy nem rekurzív

<http://alpha.tmit.bme.hu/meresek/lanuser.htm#dns>