Mérési segédlet
a Kommunikációs hálózatok 2 Helyi hálózatok c. méréséhez

v1.4

BME TMIT 2021

Tartalomjegyzék

1. Bevezető

E mérés célja, hogy a hallgató praktikus ismereteket szerezzen a helyi hálózati technológiákról. E segédlet összefoglalja a szükséges elméleti hátteret, mely egyben kiegészítő anyag az előadásokhoz is. A mérés előtt kell elolvasni.

2. Ethernet keretek

Az Ethernet egy helyi hálózati technológiai család összefoglaló neve. Azért hívjuk „helyi" hálózatnak, mert mérete jellemzően nem nagyobb, mint egy lakás, kisvállalat, vagy nagyobb vállalatnak egy részlege. Az egyetemen sokszor még az egy tanszékhez tartozó gépeket is több Ethernet hálózatra bontva kötik össze. TCP/IP hálózatokban logikailag az IP réteg alatt helyezkedik el.

Az Ethernetet az IEEE 802.3 szabványcsoport definiálja. Az adatkapcsolati rétegben csomagkapcsolt formában zajlik az átvitel. Ennek alapegysége az Ethernet keret. A keretet egy bevezető (preambulum, angolul preamble) és keret kezdeti határoló (start of frame delimiter, SFD) előzi meg, amelyek a szinkronizáció céljára szolgálnak. A keret különböző fejlécmezőkkel kezdődik, melyeket az 1. ábra mutat be (1 oktet = 1 bájt = 8 bit). A fejléc után a hasznos adattartalom (payload) következik, amely rendszerint további rétegek (L3, pl. IP) protokoll adategységeit ágyazza be. Ezt követően egy 32 bites ellenőrző összeg (cyclic redundancy check, CRC)

következik, amely a keret integritásának ellenőrzését szolgálja. Legvégül az ún. keretköz (interframe/interpacket gap, IFG/IPG) következik.

Réteg	Preambulum	Kezdeti határoló (SFD)	MAC cél cím	MAC forrás cím	802.1q címke (opcionális)	EtherType vagy hossz	Hasznos adat	CRC	IFG/IPG
	7 oktet	1 oktet	6 oktet	6 oktet	(4 oktet)	2 oktet	46-1500 oktet	4 oktet	12 oktet
L2: Ethernet keret			← 64–1522 oktet →						
L1: Ethernet csomag és IPG	← 72–1530 oktet →								← 12 oktet →

1. ábra. 802.3 Ethernet keretszerkezet (forrás: wikipedia)

MAC címek

MAC (Medium Access Control, közeghozzáférés-vezérlés) címeknek nevezik az Ethernetben használatos azonosítóit az egyes végpontoknak (azaz tipikusan azok hálózati kártyáinak). A MAC címek 6 oktet (48 bit) hosszúságúak, először a cél, utána a forrás címe következik.

Bár ez a 6 oktet együtt képez egy oszthatatlan MAC címet, mégis logikailag több részre tagolható. Az első három oktet ún. szervezetileg egyedi azonosító (Organisationally Unique Identifier, OUI), a másik három oktet pedig hálózati csatoló (network interface controller, NIC) specifikus egyedi sorszám. A cím bizonyos bitpozíciói speciális jelentéssel bírnak:

- Az OUI első oktetjének 0. helyiértékű bitje:
  - 0: Unicast cím
  - 1: multicast cím
- Az OUI első oktetjének 1. helyiértékű bitje:
  - 0: globálisan egyedi (OUI által rögzített)
  - 1: lokálisan nyilvántartott

A csupa 1-es (ff:ff:ff:ff:ff:ff) cím ún. üzenetszórási (broadcast) cím, amelyet az üzenetszórási tartományban levő minden csomópont megkap. Az unicast címre szóló csomagok akkor veszi át a csatoló, ha az ő fizikai címére szól. Az egyéb célcímre küldött keretek elkapásához ún. promiszk (promiscuous) módban kell lennie a csatolónak. Ez utóbbi azt jelenti, hogy a csatoló azokat a kereteket is feldolgozza, amelyek nem neki szólnak.

Mivel a legtöbb hardvergyártó regisztrált OUI-val rendelkezik (akár többel is), számos adatbázis[1] létezik, amelyből megtudható egy MAC címről, hogy maga az eszköz mely gyártótól származik.

802.1q címke

A 802.1q címke, más néven VLAN címke (angolul tag) a virtuális helyi hálózatok kialakításához nélkülözhetetlen. A VLAN-okról a következő fejezetben szólunk részletesen.

EtherType

Ez a két oktetes mező a keretbe ágyazott protokoll adategység típusát határozza meg. A mérések során ún. Ethernet II más néven DIX (DEC+Intel+Xerox) keretekkel fogunk találkozni. Jellemző EtherType értékek:

[1] https://www.wireshark.org/tools/oui-lookup.html

- 0x0800: IPv4 adatcsomag
- 0x0806: ARP keret
- 0x86dd: IPv6 adatcsomag

A PC-n az erre szolgáló forgalomelkapó alkalmazásokkal (pl. Wireshark, tcpdump stb.) elmenthetők ezek a keretek, de csak a MAC célcímtől a hasznos adat végéig tartó mezőket fogjuk látni, a preamble-t, SFD-t és CRC-t már nem!

3. VLAN-ok

Egy Ethernet hálózaton belül a broadcast üzeneteket minden végpont megkapja. Ilyen broadcast üzenetek a címfeloldó protokoll (ARP) üzenetei is. Klasszikusan az egymáshoz fizikailag közel lévő számítógépeket ugyanabba az Ethernet kapcsolóba (switchbe) dugjuk. Ha egy vállalatnál az egyik osztály (pl. pénzügy) gépei egymáshoz közel vannak és egy másik osztályhoz (pl. HR) tartozó gépek egy másik emeleten találhatóak, akkor ezeknek könnyű egy-egy külön Ethernet hálózatot készíteni. Ez több szempontból is előnyös:

- menedzselhetőség: minden osztály rendszergazdája a saját hálózatáért felelős[2]
- skálázhatóság: a broadcast üzenetek osztályon belül maradnak, nem árasztják el az egész vállalatot
- biztonság: az esetleges LAN-on belüli visszaélések lehetősége is korlátozott

Ha azonban egy másik példában egy emeleten keverednek a két (vagy több) osztály számítógépei, akkor is célszerű lenne az elkülönítés. Két Ethernet kapcsoló felesleges beruházás lehet, ha egynek a befogadóképessége is elegendő, eggyel viszont az elkülönítés nem valósul meg.

E probléma feloldására született a virtuális helyi hálózatok (Virtual LAN, VLAN) koncepciója. Ilyet használva csak egy Ethernet kapcsoló kell, és beállíthatjuk például, hogy annak melyik portja melyik VLAN-hoz tartozik. A VLAN-okat az Ethernet kapcsoló egymástól elkülöníti, köztük nem lehetséges Ethernet üzenetszórás, vagy bármi más Ethernet szintű (2. rétegbeli) kommunikáció.

Ezen túlmenően arra is lehetőség lesz, hogy összekössük mondjuk két emelet Ethernet kapcsolóit úgy, hogy mindkettőhöz vegyesen csatlakoznak a két osztály gépei, és ezt az egészet logikailag két VLAN-ra bontsuk. Ehhez az is kell, hogy a két kapcsoló közötti kommunikációban az Ethernet kereteket megjelöljük, hogy meyik VLAN-hoz tartoznak. Erre való az ún. VLAN címke (a fejlécben a 802.1q címke).

A címkék használatának módját az IEEE 802.1q szabvány részletezi (ezt néhol .1q-ként rövidítik). A címke felhelyezése (*tagging*) azt jelenti, hogy egy interfészen belépő/kilépő csomagra az adott azonosítójú címke kerül fel, vagyis az Ethernet fejlécbe beszúrásra kerül az opcionális 4 oktet. Az első kettő a protokoll azonosító (tag protocol identifier, TPID) 0x8100 értékkel, a második kettő pedig címkeinformáció (tag control information, TCI): 3 bitnyi prioritásazonosító (priority code point, PCP), 1 bites DEI (drop eligible indicator) és 12 bitnyi VLAN azonosító (VID). Egy fizikai port lehet címke nélküli (untagged) és címkézett (tagged) tagja az adott VLAN-nak. Untagged módban az interfész bár része a VLAN üzenetszórási tartományának, nem kerül címke a rajta keresztül forgalmazott keretekre. Ehhez fontos megjegyezni, hogy egy port csak egyetlen VLAN-nak lehet untagged üzemmódú tagja, a többi VLAN tagsága már címkézett módú kell, hogy legyen.

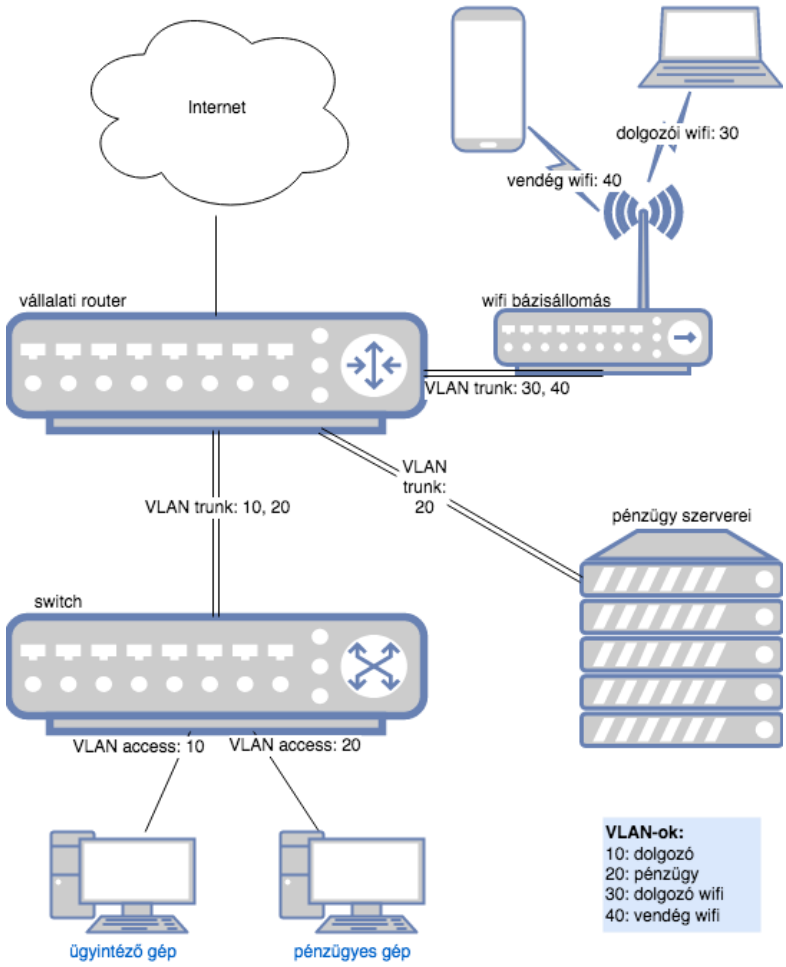
[2] Kicsit sántít a példa, nyilván nincs minden osztálynak külön rendszergazdája. Azonban pl. a BME VIK-en a tanszékeknek vannak saját rendszergazdáik, talán ez jobb példa lett volna.

A *trunk* kapcsolatokon jellemzően ilyen címkézett keretek haladnak, kivéve azokat, amelyeken ilyen címke nincs: ezek az ún. natív VLAN-hoz tartoznak. Mielőtt a csomag eléri azt az untagged módban működő portot, a címkét el kell távolítani. Ez a művelet az *untagging*.

Tehát minden VLAN önálló üzenetszórási tartományként (broadcast domain) viselkedik. Minden ilyen VLAN-nak azonosítót (címkét, tag-et) adunk a 0...4095 tartományból, amelynek praktikusan telephelyi szinten egyediek. Az infrastruktúra L2 és L3 eszközein ezt a logikai topológiát implementáljuk:

- a (tipikusan) gerinc kapcsolatokon, amelyeken több VLAN forgalmát is át kell vezetni, mindig címkézett kereteket forgalmazunk (abban az esetben is, ha jelen állapotban csak egyetlen VLAN forgalmát kell továbbítania, mert így a későbbiekben egyszerűen rendelhetünk további VLAN-okat a gerinckapcsolathoz)
- azokon a hozzáférési portokon, amelyeken végponti eszközök kapcsolóadnak egy VLAN-hoz, hozzáférési címke nélkül továbbítjuk az Ethernet kereteket

A hozzáférési portokról érkező gerinc portra továbbítandó Ethernet kereteket taggeljük (felcímkézzük), a kilépőket untaggeljük (leszedjük a címkét). A gerinckapcsolatokon (uplink portokon) ezen felül praktikusan VLAN szűrést is végzünk: eldobjuk azokat a kereteket, amelyek nem tartoznak a gerinckapcsolathoz rendelt VLAN-ok egyikéhez sem, a többieket a szokásos módon továbbítjuk.



2. ábra. Tipikus kisvállalati hálózat

Ahogy a 2. ábraán látható, az egyes VLAN-ok tetszőlegesen alakíthatók ki a 802.1q-t támogató hálózati eszközön keresztül. Így pl. a 20-as pénzügyes VLAN hozzáférhető a switch adott hozzáférési portján keresztül a pénzügyes munkaállomásról, de e switch másik, 10-es hozzáférési portján található ügyintézői gép nem kommunikálhat az adott alhálózaton.

Fontos megjegyezni, hogy a VLAN-ok önálló üzenetszórási tartományok, melyek között csak IP útválasztással lehetséges a kommunikáció, ezt nevezzük inter-VLAN routing-nak. Amennyiben egy Ethernet kapcsoló L3-as üzemmódot is támogat, úgy ez a funkció aktiválható rajta. Így bár MAC-cím szerint nem tudnak egymással kommunikálni az eltérő VLAN-ban található csomópontok, az inter-VLAN routing segítségével a hálózati rétegben, IP-címzéssel már lehetséges kettejük között az üzenetváltás az adott eszközön keresztül.

4. Vezetékes Ethernet

Az e fejezetben leírtak nem részei a mérésnek, azonban a téma megismerését teljesebbé teszi, ezért célszerű lehet elolvasni.

A vezetett hullámú (vezetékes) összeköttetések előnye, hogy jóval kevésbé érzékenyek a környezetükre. Az összeköttetés lehet rézvezető-alapú (jellemzően csavart érpárokkal) vagy optikai. Szabvány szerinti megnevezésük az alábbiak szerint alakul:

- fizikai rétegben elérhető névleges átviteli bitsebesség (M)bit/s-ban (10, 100, 1000, 10G, stb.)
- jelzés szerint: BASE, BROAD, PASS
- kötőjel után átviteli közeg jelzése (T: csavart érpár (twisted pair), S: rövid hullámhosszú (850 nm) optikai (multimódusú), L: hosszú hullámú (1300 nm) optikai (általában mono módusú), F: változó hullámhosszú optikai, stb.
- vonali kódolás: X: 4b/5b (Fast Ethernet) vagy 8b/10b, R: 64b/66b nagy blokkos
- opcionálisan: alkalmazott LAN fizikai sávok kapcsolatonként: 1, 2, 4 vagy 10; WAN kapcsolatoknál a maximális kábelhossz km-ben.

Ennek megfelelően néhány, a legtöbbször előforduló szabvány:

- Fast Ethernet:
    - 100BASE-TX: Cat5 két csavart érpáras összeköttetés, 100 Mbit/s, full duplex
        - 100BASE-FX, -SX: optikai multimódusú, maximum 300 m (SX) maximum 2 km-ig (FX), full duplex
    - 100BASE-LX10: optikai monomódusú, maximum 10 km
- Gigabit Ethernet:
    - 1000BASE-T: PAM-5 kódolást alkalmazó csavart érpáras szabvány, legalább Cat5e kábelezés ajánlott
    - 1000BASE-SX: rövid hullámhosszú, multimódusú optikai átvitel, maximum 550 m-ig
    - 1000BASE-LX: hosszú hullámú monomódusú optikai átvitel, maximum 10 km-ig

A csavart érpáras kábelt CatX (Category X) jelzéssel szokták ellátni, utalva a szerkezetére és az alkalmazott rézvezető átviteli képességeire. A leggyakoribbak:

- Category 5, Class E (Cat5e): 100 MHz, 1 Gbit/s-ig
- Category 6, Class A (Cat6a): 500 MHz, 10 Gbit/s-ig

A szabványok a maximális 100 m hosszig írják elő a teljesítendő paramétereket. A kábelek lehetnek árnyékolatlanok (unshielded twisted pair, UTP), de az érpárak és/vagy maga az érpár köteg fóliás árnyékolást is

kaphat, az érpárak közötti áthallás ill. a környezetből érkező magas frekvenciás zaj elleni védelem gyanánt (foiled twisted pair, FTP). További, alacsony frekvenciás védelem végett kerülhet rézszálas szövet is az érpárkötegre (screened/shielded twisted pair, STP).

5. Wi-Fi

Az e fejezetben leírtak nem részei a mérésnek, azonban a téma megismerését teljesebbé teszi, ezért célszerű lehet elolvasni.

A köznyelvben „Wi-Fi”-nek hívott vezeték nélküli hozzáférési technológiát az IEEE 802.11 szabványcsalád (a Wi-Fi non-profit szervezet támogatásával) fedi le, amely egy LAN hozzáférési technológia, amely az OSI modell 1. és 2. rétegét fedi le. Jellemzően a 2,4, 5 és 60 GHz körüli frekvenciatartományokat használják. Fél-duplex módú a kommunikáció (egyszerre csak az egyik fél ad), CSMA/CA érzékeléssel[3] a csomagküldés előtt. A legelterjedtebb változatai:

- 802.11b/g: a 2,4 GHz ISM (nemzetközileg fenntartott ipari, tudományos és orvosi, industrial, scientific and medical) sávban, elméleti 11 („b” szabvány), ill. 54 Mbit/s („g” szabvány) maximális sebességgel (a gyakorlatban 22 Mbit/s körüli). A „g”-t támogató eszközök visszafelé a „b” szabvánnyal is kompatibilisek voltak, és egyszerre akár azonos csatornákon is tudtak kommunikálni, de a „b”-s eszköz becsatlakozását követően a „g”-sek is csak alacsonyabb sebességen tudtak működni.
- 802.11n: megjelent az 5 GHz-es sáv használata (bár még csak opcionálisan), ill. a több antenna szimultán használata, vagyis a MIMO (multiple input, multiple output), az elméleti sávszélességet 600 Mbit/s-ig növelve.
- 802.11ac: az 5 GHz-es tartományban szélesebb (80 vagy 160 MHz) csatornák, 256QAM kódolás és mu-MIMO (multi user MIMO) megjelenése, akár 1300 Mbit/s elméleti sávszélesség. A modern eszközök zöme támogatja

A fenti szabványok a vezetékes környezetben megszokott kerettípusok mellett menedzsment és vezérlő kereteket is alkalmaznak. Ilyen pl. a beacon menedzsment keret, amely az adott vezeték nélküli hálózat hirdetésére szolgál, hogy a kliensek rá tudjanak találni. (Ez le is tiltható, ilyenkor explicit módon kell megkísérelni a csatlakozást.)

Előnyök és hátrányok

A Wi-Fi technológiák bár nagyon elterjedtek, bizonyos korlátokkal kell számolnunk, ha a hagyományos, vezetékes LAN technológiákkal párhuzamosan szeretnénk használni:

- Az osztott közeg miatt sokkal inkább hasonlít a hub-szerű üzenetszórásos működésre.
- A gyakorlatban elérhető sávszélesség sok tényezőtől függ: szakaszcsillapítás, interferencia, egyszerre forgalmazni kívánó eszközök száma, stb.
- Nem biztosít késleltetésre vonatkozó garanciákat, így a szolgáltatásminőség (quality of service, QoS) adott szintje nehezen vagy egyáltalán nem biztosítható vele.
- Szigorú környezetben a közeg publikus hozzáférése még akkor is rizikót jelenthet, ha az alkalmazott titkosító, hozzáférés szabályzó protokollok, algoritmusok korszerűnek számítanak.

[3] Vivőjel-érzékeléses többszörös hozzáférés, ütközéselkerüléssel (CSMA/CA – Carrier sense multiple access with collision avoidance)

Eszközök és üzemmódok

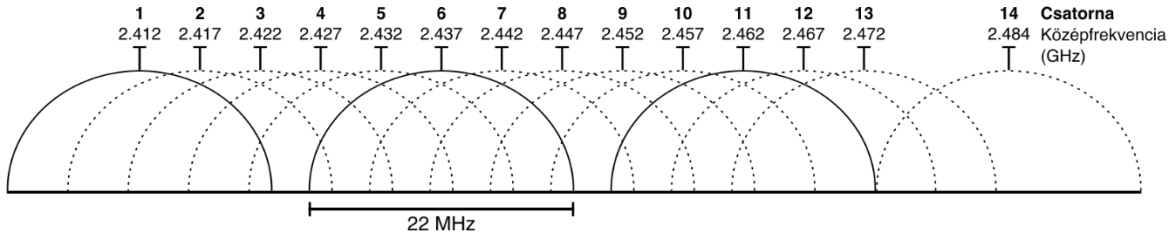
Egy Wi-Fi hálózat neve az SSID (Service-Set Identifier), vagyis hálózati név. A Wi-Fi bázisállomás (access point, AP) egy vezeték nélküli hálózati eszköz, amely a hozzá kapcsolódó vezeték nélküli kliensek és a felhordó (uplink) kapcsolata közötti átvitelt bonyolítja le. Ezt az üzemmódot infrastruktúra módnak is hívjuk. Egy AP akár több SSID-t is kiszolgálhat.

Lehetőség van két eszközt központi csomópont nélkül is összekapcsolni, ezt ún. ad-hoc módnak hívjuk.

A vezeték nélküli hálózatok lefedettségét kiterjeszteni hivatott működési mód az ún. WDS (wireless distribution system, WDS) tulajdonképpen egy jelismétlőt (repeater) valósít meg, de nem a fizikai réteg kiterjesztésével, hanem a WDS módú eszköz kliensként egy AP adott SSID-jéhez kapcsolódik és ezzel egyidőben a saját rádióján ugyanazon SSID-jű hálózatot szolgáltatja AP-ként. Olyan esetekben alkalmazzák, amikor két AP között nem teremthető vezetékes összeköttetés.

Csatornák és adóteljesítmény

A különböző sávokban egymással átfedő frekvenciatartományok alkotják a csatornákat, a 3. ábra a 2,4 GHz-es sáv kiosztását szemlélteti.



3. ábra. Csatornakiosztás a 2,4 GHz-es ISM sávban (forrás: wikipedia)

WiFi hálózat kiépítésénél célszerű figyelembe venni ezeket, ill. az esetlegesen a környezetben dolgozó további WiFi eszközöket, hogy a lehető legjobb jel/zaj viszonyú cellákat alakíthassuk ki. Az egymás mellé kerülő cellákat például érdemes az átlapolásmentes csatornákkal kialakítani. Az alkalmazható csatornák országonként, ill. földrészenként eltérhetnek, érdemes tájékozódni bázisállomás telepítésekor, de a legtöbb eszközben beállítható, mely országban tartózkodunk, így a kiválasztást a firmware megoldja.

Bázisállomások esetében fontos a megválasztott adóteljesítmény is. Itt is igaz a „kevesebb néha több” elve: az indokolatlanul magas adóteljesítmény interferenciát okozhat, ami rontja az átviteli teljesítményt, továbbá a hatóságilag engedélyezett teljesítmény túllépését is eredményezheti.

Hazánkban az illetékes hatóság (NMHH) szabályozza az alkalmazható maximális hatásos izotróp sugárzási teljesítményt (effective isotropic radiated power, EIRP), amely a 2,4 GHz-es sávban 100 mW, az 5 GHz-es tartományban 200 mW. Az effektív érték kiszámításához a rádiós adóteljesítményen túl az antennakábel csillapítását és az adóantenna nyereségét is figyelembe kell venni. Az adóteljesítményt gyakran dBm-ben jelzik, ez logaritmikus skálán fejezi ki a mW-ban megadott teljesítményt (ld. 4. ábra). Az antenna nyereséget dBi-ben adják meg, amelynél a skála az elméleti referenciának tekintett izotropikus (tökéletesen gömbszerűen sugárzó) antennához viszonyított nyereséget fejezi ki. Az átvitel mindkét végpontján található valamilyen antenna, ezek nyeresége együtt csökkenti az átviteli közeg csillapításából származó veszteséget.

Watt	dBm
0 W	nem definiált
0^+ W	-∞ dBm
0.00001 W	-20 dBm
0.0001 W	-10 dBm
0.001 W	0 dBm
0.01 W	10 dBm
0.1 W	20 dBm
1 W	30 dBm
10 W	40 dBm
100 W	50 dBm
1000 W	60 dBm
10000 W	70 dBm

4. ábra. Watt-dBm konverziós tábla (forrás: https://www.everythingrf.com/rf-calculators/watt-to-dbm)

Biztonság

A rádiós közeg használata miatt a WiFi hálózatok biztonsága fontos terület. A korai WEP (RC4/CRC32) és WPA (TKIP/MIC) biztonsági technológiák könnyen feltörhetőnek bizonyultak és jelenleg a WPA2 (IEEE 802.11i, WiFi Protected Access 2) ajánlott, amely AES-CCMP blokk titkosítást és CBC-MAC integritás ellenőrzést alkalmaz.

Az egyszerű lakossági alkalmazhatóság végett lehetőség van az osztott kulcsú (Pre-Shared Key, PSK) használatára, amely azt jelenti, hogy az adott SSID-hez csatlakozó összes kliens egy közös kulccsal csatlakozik. Ez természetesen komoly adatbiztonsági korlát, ezért célszerű ún. vállalati (enterprise) azonosítási megoldás alkalmazása, ezeket EAP (Extensible Authentication Protocol) gyűjtőnéven találjuk. Ezen megoldások célja, hogy szállítási rétegbeli titkosítást alkalmazva lehetőséget nyújtson a kliensek azonosítására (például tanúsítvánnyal, jelszóval), illetve a kliensek is ellenőrizhetik, hogy megbízható hálózathoz kapcsolódnak-e a szervertanúsítvány ellenőrzésével. Az infrastruktúra mögé központi autentikációs megoldást (pl. RADIUS) kell telepíteni, amely összetettsége miatt nem képezi e mérés anyagát.

6. Tűzfal

A tűzfal tipikus feladata bizonyos rétegen áthaladó hálózati forgalom nyomon követése és egy meghatározott szabályrendszer mentén a forgalom korlátozása vagy átengedése. A hálózati eszközökben a leggyakoribb a csomagszintű (jellemzően a 4. rétegig) feldolgozást végző tűzfal. Kiegészítő funkciók is előfordulnak, ilyen pl. a címfordítás (network address translation, NAT) és portfordítás (port address translation, PAT). Léteznek alkalmazás szintű tűzfalak is, de ezek alkalmazása a kommunikációs útvonalakon nem triviális a manapság egyre gyakoribb titkosítás miatt, komoly heurisztikára van szükség a működésükhöz.

A tipikus csomagszintű tűzfalnak 3 alapvető szabályrendszere, szakszóval lánca van: forward, input, output. Az első a rajta áthaladó, a második a konkrét eszközt megcélzó, a harmadik az eszközből kiinduló forgalomra alkalmazandó. Minden lánchoz rendelhetünk egy irányelvet: megengedő vagy tiltó, attól függően, hogy mi történjen azokkal a csomagokkal, amelyekre a lánc egyetlen szabálya sem teljesül.

A szabályainkat azután az adott láncokhoz kapcsolódóan sokféle módon definiálhatjuk, pl. cél-/forráscím, protokoll, portszám, interfész, kapcsolat állapot, és sok egyéb, hálózati protokollokhoz kapcsolódó módokon. A szabályban meg kell adnunk egy műveletet is, amely az illeszkedéskor bekövetkezik, pl. elfogadás (accept), eldobás (drop), stb.

A tűzfal működésekor a csomagtovábbításkor a feldolgozandó csomagok az érvényben levő szabályláncok szerint lesznek megítélve: ha egy szabály illeszkedik, a kapcsolt művelet végrehajtódik. Ha nem és tovább folytatható (nem mondta a szabály, hogy stop) az illesztés folytatódik a következő szabállyal. A szabályok után pedig az alapelv lép érvénybe.

Például beállíthatjuk, hogy egy tartományba engedjen be a tűzfal minden olyat csomagot, ami egy adott másik IP címtartományból érkezik (forráscím), vagy adott portra igyekszik (pl. http: 80-as port), azonban minden más csomagot dobjon el.

7. Mikrotik RouterOS

A Mikrotik saját fejlesztésű, Linux alapú, de zárt forrású firmware-e, elsősorban a saját RouterBoard alapú platformján (switchek, routerek, bázisállomások) történő alkalmazásra. Előnye az egységesség (minden hardverre ugyanolyan firmware), ill. a hosszú támogatás (a régi hardverekre is felrakható a korszerű firmware). Az eszköz megvásárlásakor kapjuk a firmware-t is, de bizonyos funkciók licencdíjasok, pl. az x86 PC-re telepítés is.

A RouterOS konfigurálása legkényelmesebben a WinBox ingyenes grafikus alkalmazással történhet (a „gyakorlati útmutató” vezet be a használatába), de webböngészőből (WebFig) és gyakorlott üzemeltetők parancssorból (ssh-n vagy a GUI-kon keresztül) is végezhetik.

Vállalati jellegű, több AP-ból álló hálózat kialakításához a központi menedzsmentet segítő *CAPsMAN* (Controlled Access Point system Manager) funkció segíti: az AP-k CAP-pá (controlled access point) minősíthetők, onnantól csak AP feladatokat (hozzáférés vezérlés, felhasználói azonosítás) látnak el és ezek a beállítások (pl. RADIUS szerver, WPA/WPA2 kulcsok) központilag konfigurálhatók, de akár központilag is frissíthetők.

hAP ac^2

A méréshez használt router 1+4 vezetékes Gigabit Ethernet portjából az #1-es (Internet/POE In) a WAN kapcsolathoz van rendelve (de akár LAN porttá is konfigurálható). A vezetékes portokat ether1-től ether5-ig azonosítja a RouterOS.

A routerünk rendelkezik két rádiós interfésszel is: az egyik a 802.11b/g/n szabvány kiszolgálásához, *wlan1* néven. A 802.11ac szabványt pedig a *wlan2* nevű interfész működteti. Az interfészek mindegyike egyenként is letiltható.

8. Wireshark

A Wireshark egy nyílt forráskódú protokoll vizsgálatot segítő szoftver. Hálózati forgalmat lehet vele elkapni és lementeni (pcap/pcapng formátumba), amit később is megnyithatunk, elemezhetünk, visszajátszhatunk (pl. tcpreplay-jel). A szoftver a csomagok bináris tartalmának megjelenítésén túl képes a számára ismert protokollok dekódolására, fejlécek megjelenítésére. Ezen túl bizonyos protokollok (pl. TCP) esetén képes a csomagfolyamok lekövetésére, azaz az összetartozó csomagok együttes megjelenítésére is.

A mérés során e fejezet további részére nem lesz szükség. (Máskor persze jól jöhetnek az itt leírtak.)

Capture mód

Csomagelkapásnak, angolul capture-nek nevezzük, amikor a wireshark-kal adott hálózati csatolón érkező csomagokat elkapjuk és elmentjük (haladók akár át is irányíthatják, ún. nevesített csővezetékek/named pipes segítségével). Az elkapás praktikusan válogatás nélküli (promiscuous) módban zajlik, ami nemcsak az elkapást végző csomópontnak szóló csomagok lementését teszi lehetővé, hanem mindent, amit az interfész "lát". Ez például vezeték nélküli hálózati kapcsolat esetén vagy porttükrözés esetén lehet hasznos.

Az elkapást alapesetben végezhetjük GUI-val, de akár konzolról, a *dumpcap* nevű parancssoros alkalmazás segítségével is.

Capture filter

Csomagelkapás során hasznos lehet, főleg aggregált kapcsolat esetén, ha nem mentünk le minden csomagot, csak azokat, melyekre a vizsgálat során biztosan kíváncsiak vagyunk. Ilyenkor ún. capture filterrel, vagyis elkapás- szintű szűrési kifejezéssel tudjuk megadni, mit kapjon/mentsen el a Wireshark.

A legsűrűbben használt kifejezések:

- szűrés IP-címre: "host x.x.x.x" vagy "host domainnév"
- szűrés alhálózatra: "net hálózat/maszkbitek" vagy "net hálózat mask maszk"
- szűkítés forrásra: "src" előtag
- szűkítés célra: "dst" előtag
- szűrés protokollra: "proto x", ahol x "udp", "tcp", "icmp", "arp" stb., az első háromnál elhagyható a "proto"
- szűrés portra: "port x", ahol x lehet IANA szolgáltatás név is "pl. port domain" vagy "port 53"
- szűrés porttartományra, pl.: "tcp[0:2]>1500 and tcp[0:2]<1550", vagyis az első két bájtja a TCP fejlécnek (forrás)
- újabb libpcapek (0.9.1 felett): "tcp portrange x-y"
- speciális:
    - "broadcast", "multicast"

A kifejezés elemeit *and* vagy *or* logikai operátorokkal kapcsolhatjuk össze, zárójelezhetjük, illetve a *not* operátor is használható.

Display filter

Szűrni a már elkapott csomagsorozatban is lehet. Ez a szűrés csak a megjelenítést befolyásolja, az elmentett fájl tartalmát nem. Ha illeszkedik rá a kifejezés, akkor megjelenik, egyébként nem. A kifejezés szintaxisa némileg eltér a capture filtertől:

- logikai kifejezések: protokoll mezők illesztése operátorokkal, pl. ip.src, tcp.window_size
- operátorok: ==, eq, !=, contains, matches, !, pl. ip.src==192.168.0.0/16, tcp.port eq 25
- kifejezések sorozata logikai kapcsolókkal elválasztva: &&, ||, and, or, pl. http.request.uri matches "gl=se$"
- ld. Wireshark display filter reference: https://wiki.wireshark.org/DisplayFilters

Protokollelemzés

A csomaglistában a kiválasztott csomag részletes protokoll információi megtekinthetőek, rétegről rétegre lenyitva az egyes rétegeinek fejléceit.

Előfordulhat, hogy a szoftver nem ismeri fel automatikusan, milyen protokollok vannak beágyazva, például olyan RTP, ami ugyan UDP-be van ágyazva, de nincs szokásos portszáma, egyedi fejléce. Ilyenkor a csomagot kijelölve explicit mondható meg, milyen protokollal állunk szemben: Decode as...

A tipikus webböngészés több párhuzamos TCP kapcsolat nyitását jelenti időről időre. A Wireshark az egyes TCP folyamokat ki tudja gyűjteni, mindegyikhez rendel egy folyam azonosítót (tcp.stream).

- Statistics → Conversations: protokoll+forrás/cél IP cím/port alapján felderíti a folyamokat és megjeleníti. Itt látható, hogy mettől meddig zajlottak a folyamok, mennyi adat mozgott rajtuk
- Statistics → I/O Graph: átviteli grafikont tudunk rajzoltatni egy vagy több kiválasztott csomagsorozatra, amit display filterrel tudunk meghatározni
- Telephony → RTP Streams: hasonló, mint a Conversations, de az RTP folyamnak bizonyos tulajdonságait is méri, pl. csomagvesztés, jitter

9. Ellenőrző kérdések

E mérés korábban egyetemi laborban történt, most már hivatalosan is távollétben végezhető járványhelyzettől függetlenül. A jelenléti mérések esetén ilyen beugró kérdéseket tettünk fel. Otthoni mérés esetén természetesen nincsen beugró sem, ezt a részt mégsem töröltük: átolvasva maguk ellenőrizhetik, mennyire értették meg az e dokumentumban foglaltakat.

1. Mit jelent az Ethernet MAC cím?
2. Hány oktet hosszú az Ethernet MAC cím?
3. Honnan ismerjük meg a broadcast Ethernet kereteket?
4. Honnan tudjuk egy (nem címkenélküli) Ethernet keretről, hogy melyik VLAN-ba tartozik?
5. Mit határoz meg az Ethertype mező?
6. Egy fizikai port hány VLAN-nak lehet címke nélküli tagja?
7. Mennyi a VLAN azonosító maximális értéke?
8. Milyen átviteli jellemzői vannak a 1000BASE-T szabványnak?
9. Mekkora az elérhető maximális sávszélesség Cat6a kábel alkalmazása esetén?
10. Milyen frekvenciatartományokat használ a 802.11ac szabvány?
11. Mekkora hazánkban a legnagyobb engedélyezett sugárzási teljesítmény a 802.11n szabvány esetében?
12. Milyen titkosítást célszerű alkalmazni egy otthoni WiFi védelmére? Miért?
13. Milyen tényezőktől függ egy 802.11 rádiós összeköttetésen elérhető gyakorlati bitsebesség?

14. Adjon meg három olyan feltételt, melyre a Wireshark capture filterével rá tud szűrni!
15. Mi a különbség a capture és a display filter között?