

Gyakorlati tudnivalók

a Kommunikációs hálózatok 2 Helyi hálózatok c. méréséhez

v1.1

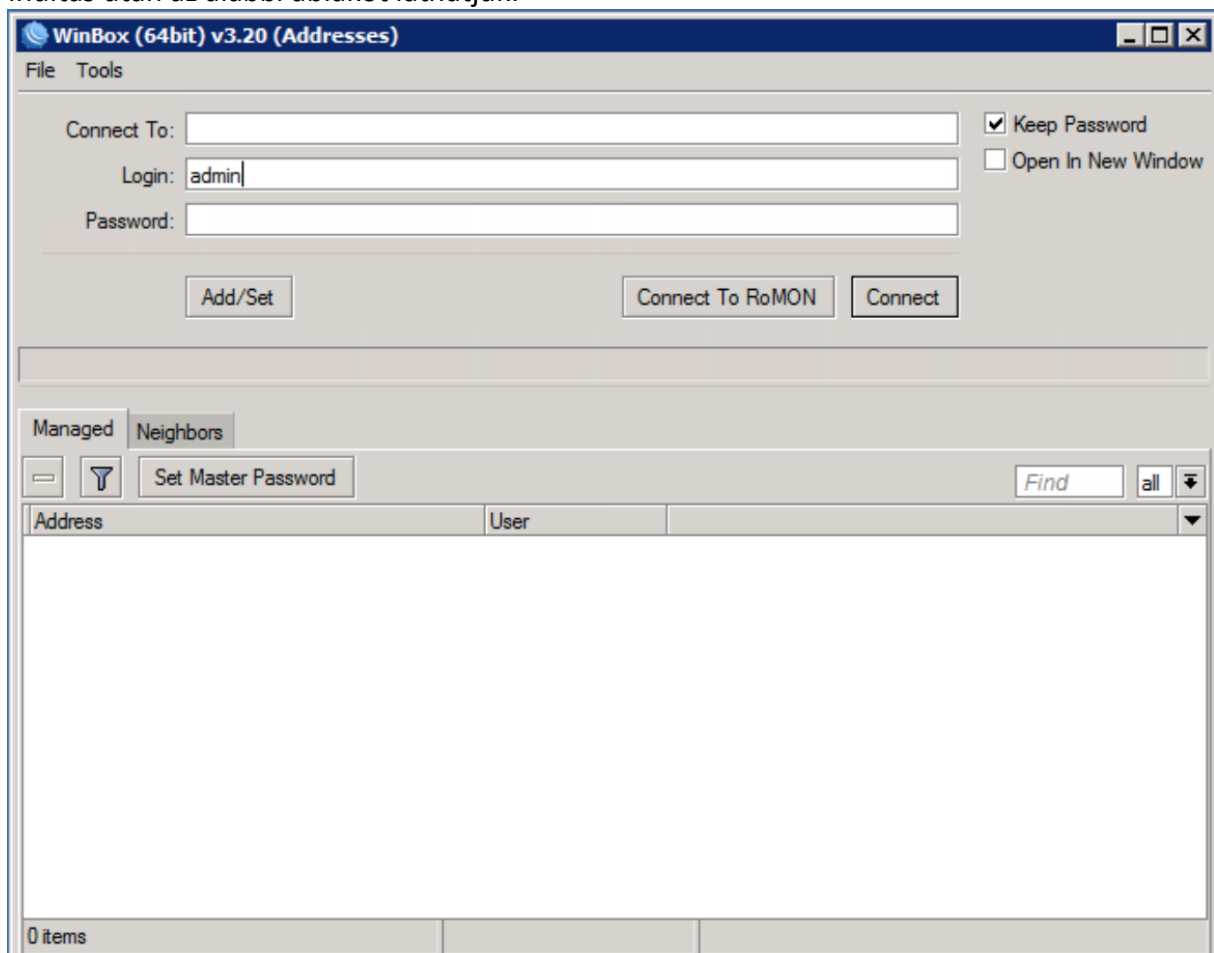
Az itt leírtakat nem kell a mérés előtt áttanulmányozni, legfeljebb csak annyira, hogy tudjuk, kb. mit tartalmaz e dokumentum. A mérés során azonban célszerű elővenni, amikor a WinBox használatára kerül a sor, illetve a Wireshark használatában lehet a segítségükre. A mérési útmutatóban jelöltük ezeket a pontokat.

A WinBox használata

A program indításához a következő ikont keressük:



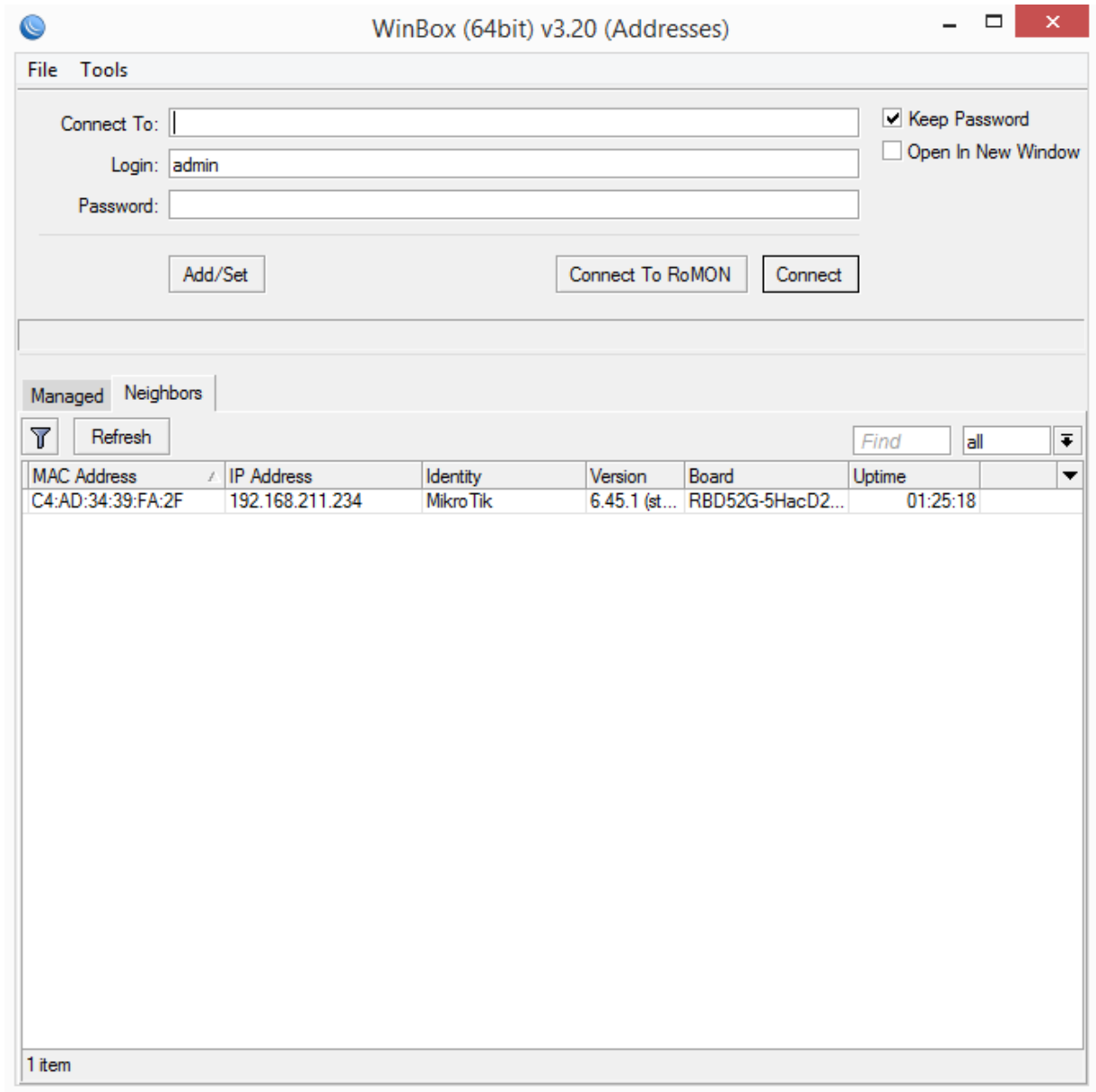
Indítás után az alábbi ablakot láthatjuk:



A *Managed* fülön a *Connect To*-hoz a kezelni kívánt eszköz IP-címét vagy MAC-címét írjuk, valamint az adminisztrátori login nevet (alapértelmezés szerint admin) és a hozzá tartozó

jelszót (alapértelmezetten üres). Megjegyzi az utolsó sikeres csatlakozott eszköz címét, ill. továbbiakat is felvehetünk itt.

A *Neighbors* fülön a felderített RouterOS-t futtató eszközök listáját találhatjuk:



The screenshot shows the WinBox (64bit) v3.20 (Addresses) window. The 'Neighbors' tab is active, displaying a table of discovered devices. The table has columns for MAC Address, IP Address, Identity, Version, Board, and Uptime. One device is listed: MAC Address C4:AD:34:39:FA:2F, IP Address 192.168.211.234, Identity MikroTik, Version 6.45.1 (st...), Board RBD52G-5HacD2..., and Uptime 01:25:18. The status bar at the bottom indicates '1 item'.

MAC Address	IP Address	Identity	Version	Board	Uptime
C4:AD:34:39:FA:2F	192.168.211.234	MikroTik	6.45.1 (st...	RBD52G-5HacD2...	01:25:18

A beazonosítást segítheti az *identity* mező (ha már adtunk egyedi nevet) ill. a MAC- és IP-cím. Figyeljünk, hogy mindig ahhoz az eszközhöz csatlakozzunk, amelyet valóban konfigurálni szeretnénk.

Csatlakozás (a *Connect* gombra klikkelve¹) után hasonló fogad minket:

¹ A RoMON (router management overlay network) egy központosított menedzsment réteg, a mérések során nem ezzel dolgozunk, így a *Connect to RoMON* gomb helyett a *Connect*-et használjuk!



Az elvégzett konfigurációs beállítások ugyan azonnali érvényűek, de hasznos lehet az ún. Safe Mode aktiválása. Ha bekapcsoljuk, a WinBox-ból való kilépéskor megerősítést fog kérni a véglegesítésre. Ha ez nem történik meg, akkor visszavonja a session-ben elvégzett összes beállítást. Ezáltal megelőzhetjük, hogy kizárjuk magunkat, ill. hogy emiatt reset-elni kelljen az eszközt.

A menüsor alatti sáv dashboard kiegészíthető pár érdekes mérőeszközzel, amelyek a Dashboard menün keresztül érhetők el: dátum, idő, CPU terhelés, memóriefoglaltság és uptime.

A főablak bal oldalsávja a főmenü, legfontosabb pontjai:

- Quick Set: gyorsbeállító "varázsló", a leggyakoribb funkciók gyors beállításához (pl. tipikus otthoni wifi router beállításához)
- CAPsMAN: központosított Wi-Fi hálózat kiépítéséhez szükséges funkciók
- Interfaces: interfész-ek, VLAN-ok
- Wireless: rádiók, vezeték nélküli profilok
- Bridge: hálózati híd kialakítása
- PPP: pont-pont kapcsolatok kialakítása (pl. betárcsázós, PPPoE)
- Switch: beépített hálózati kapcsoló konfigurálása
- Mesh: vezeték nélküli eszközök hálózata (decentralizált)
- IP, IPv6: IP beállítások
- Routing: útvonal választás
- System: az eszköz adminisztrációja (pl. pontos idő, licenzek, beállítások mentése, stb.)
- Dot1X: végponti autentikációs beállítások
- Log: rendszerüzenetek

- Tools: hasznos segédeszközök (ping, forgalom generátor, stb.)
- New Terminal: parancssori ablak (pl. scripteléshez)

...

Azon főmenüpontok, amelyek mellett jobbra nyíl található, második szinttel is rendelkeznek, a levélelemek egy-egy ablakot nyitnak meg. A WinBox többablakos felület, ami rendkívül kényelmessé teszi az amúgy borzasztó sok funkció áttekintését. Az ablakok rendelkezhetnek fülekkel, ill. egy eszközsorral, ami tipikusan így néz ki:



- +/- gomb: hozzáadás/törlés (kontextustól függően), némely funkciónál a + lenyíló menüt is takar (ha lefele mutató nyíl található jel mellett)
- pipa/kereszt: kijelölt elem(ek) engedélyezése/letiltása (figyelem, a használata azonnali érvényű!)
- sárga cetli (komment): megjegyzés fűzése az elemhez (a listában általában az elem felett fog megjelenni, hacsak az "Inline Comments"-et nem engedélyezzük a Settings menüben)
- szűrő: ha a kontextusban értelmezhető, a listában bizonyos elemekre lehet vele keresni

Az ablakok egyébként a jobb felső sarkukban levő kereszttel bezárhatók, ill. a mellette levővel minimalizálhatók, a fejlécüket megfogva mozgathatók. Ha a nem felelne meg a méretük (ahogy az oszlopok), át is méretezhetők, ill. a kilógó részek görgethetők.

Interfaces menü

- *Interface* fül: az egyes interfészek listája (beleértve a rádiókat, virtuálisat, VLAN-t, bridge-et stb.), itt le is tudjuk őket tiltani (ld. pipa/kereszt toolbar gomb), de a legfontosabb statisztikák is megjeleníthetők
- *Interface List* fül: az interfészeket lehet csoportosítani, hogy akár együtt is hivatkozhatók legyenek (pl. tűzfalban stb.), alapból a LAN és WAN csoportok vannak itt
- *Ethernet* fül: a vezetékes ethernet csatlók
- *VLAN* fül: definiált VLAN-ok, új hozzáadása esetén meg kell adnunk legalább a VLAN azonosítót és a szülő interfész nevét

...

Wireless menü – erre a méréshez nem lesz szükség

- *WiFi Interfaces* fül: fizikai, virtuális (további Wi-Fi hálózatok létrehozásához), WDS (lefedettség kiterjesztéséhez), bizonyos mezők megjelenítéséhez az *Advanced Mode* bekapcsolása szükséges a jobboldali gombsoron
 - *SSID* mező: itt tudjuk megadni, mi legyen a létrejövő hálózat neve
 - *Security Profile*: az azonos fülön létrehozható profil hozzárendelése (pl. az autentikáció paramétereinek megadásához)

- *WPS Mode*: Wi-Fi Protected Setup (gombnyomásra érvényesíthető automatikus biztonsági beállítások), amelyet nem fogunk használni, hiszen mi gondoskodunk a paraméterezésről
 - *Frequency Mode: regulatory-domain*: a helyi szabályzásnak megfelelő frekvencia használat; *manual-txpower*: mint az előbbi, csak teljesítménykorlát nélkül; *superchannel*: teszteléshez, minden, a rádió által támogatott frekvencia engedélyezésével
 - *Country*: az ország kiválasztása, amiből az eszköz tudja, milyen frekvenciákat és maximális teljesítményt használhat
 - *Antenna Gain*: nyereség dBi-ben, a maximális kimenő teljesítmény kiszámításához (egész érték; minimum 3, router antennái kb. 2.5 dBi nyereségűek)
 - *VLAN Mode*: az alapértelmezés a *no tag*, vagyis nem tageljük a WiFi forgalmat ezen a hálózaton, ha viszont tagelni szeretnénk, akkor állítsuk *use tag*-re és alább adjuk meg a VLAN azonosítót
 - *VLAN ID*: VLAN azonosító (alapértelmezés szerint 1)
 - *Hide SSID*: pipáljuk be, ha nem kívánjuk hirdetni a hálózatot
- Egyéb részletes beállítások lehetségesek a további füleken.
- *Registration* fül: itt láthatók az asszociált (felcsatlakozott) felhasználók, megjelenítve a fizikai címüket és egyéb átviteli jellemzőiket, a kapcsolatot itt meg is lehet szakítani
 - *Connect List*: ha az eszközzel más vezeték nélküli hálózathoz szeretnénk csatlakozni, itt lehet megadni a kapcsolatot
 - *Security Profiles*: egy-egy Wi-Fi hálózat kapcsolódási jellemzőit állíthatjuk be itt: biztonsági protokollok, kulcsok, autentikációs metódus, stb. Először itt kell definiálni őket, majd fel lehet használni a *WiFi Interfaces*-ben (AP üzemmódhoz) vagy a *Connect List*-nél a kliens módhoz.

A kimenő teljesítményt közvetlenül nem tudjuk szabályozni pusztán a *WiFi Interfaces* → *Tx Power* fülön, mert a firmware igyekszik az adóteljesítményt, ill. a maximális kimenő teljesítményt (EIRP) a helyi szabályozáshoz igazítani. Hogy hatásosan le tudjuk csökkenteni a tényleges kisugárzott teljesítményt, a *WiFi Interfaces* → *Wireless* → *Antenna Gain* mezőt emeljük fel 30 dBi-re.

Bridge menü

- *Bridge* fül: hídkapcsolatok listája
- *Ports*: az interfész-híd összerendelések
- *VLANs*: itt az *Interfaces* menüben létrehozott VLAN-okat rendelhetjük bridge-ekhez, valamint taggelési, untaggelési szabályokat adhatunk meg, a már létrehozottaknál láthatjuk az aktuális taggelés, untaggelési mechanizmust is

...

IP menü

- *ARP*: ARP táblázat: milyen MAC-IP összerendeléseket ismer az eszköz, indokolt esetben mi is vehetünk fel új bejegyzéseket

- *Addresses*: IP-címek listája: az interfészeknek – beleértve a VLAN-okat is – IP-címeket oszthatunk, amelyeket átjáróként (vagy menedzsmentc címként) használhatunk
- *DHCP Client*: ha valamely interfészen IP-címet akarunk igényelni, itt adhatjuk meg. Az alapkonfigurációnak rendszerint része, hogy a WAN kapcsolatú szolgáló interfészre DHCP-n kér címet.
- *DHCP Server*: ha valamely VLAN-on (alapkonfiguráció szerint a *bridge-en*) IP-címet szeretnénk osztani, itt tudunk DHCP szervert definiálni:
 - *DHCP* fül: szerver/interfész lista
 - *Networks* fül: a DHCP szervernek ismernie kell az adott hálózat címét, maszkját és átjáróját (tipikusan az *Addresses*-ben megadott cím), itt tuduk meadni
 - *Leases*: itt listázhatjuk, milyen MAC-címre milyen IP-ket osztogattunk, ill. azok meddig érvényesek. Vethetünk fel statikus bejegyzéseket és érvényteleníthetünk is.
 - *Options/Option Sets*: ha speciális DHCP paramétereket, pl. boot szerver cím, stb. szeretnénk hirdetni, akkor itt vehetjük fel. A DNS szerver nevét, átjárót nem kell külön felvenni itt.
- *DNS*: az eszköz DNS gyorsítótárának beállításai
- *Firewall*: tűzfal beállítása
 - *Filter Rules*: szűrőszabályok kezelése; a # a sorrendet mutatja, a ::: a megjegyzéseket; a feltételmezőkön túl az illeszkedő csomagok mennyiségét (*Bytes* oszlop) és számát (*Packets* oszlop) is láthatjuk, ez segíthet a hibakeresésben
 - *NAT*: cím/port fordítási szabályok
 - *Connections*: kapcsolat nyilvántartó táblázat
- ...
- *Pool*: IP-cím tartományok megadása, ezekből tud a DHCP szerver címeket kiosztani. A pool-nak nevet adhatunk, megmondhatjuk, mettől meddig osztható ki (pl. 192.168.88.2-192.168.88.10), ill. hogy mely legyen a következő pool, ha ez már kifogyott
- *Routes*: útvonal táblázat, átjárók, statikusakat is vehetünk fel, ha szükséges (interfész, VLAN definiálásakor ide automatikusan bekerül az útvonal)

...

System menü

- *Clock*: rendszeridő és dátum, akár NTP szinkronnal is
- *Identity*: az eszköz hosztneve, itt tudjuk módosítani is
- *Packages*: kiegészítő csomagok letöltése
- *Password*: adminisztrátori jelszó módosítása
- *Reset Configuration*: a gyári beállítások visszatöltése
- *Reboot*: újraindítás, elég ritkán kell

...

A Wireshark használata

(Ez a fejezet jóval bővebb, mint amire a méréshez valójában szükség van.)

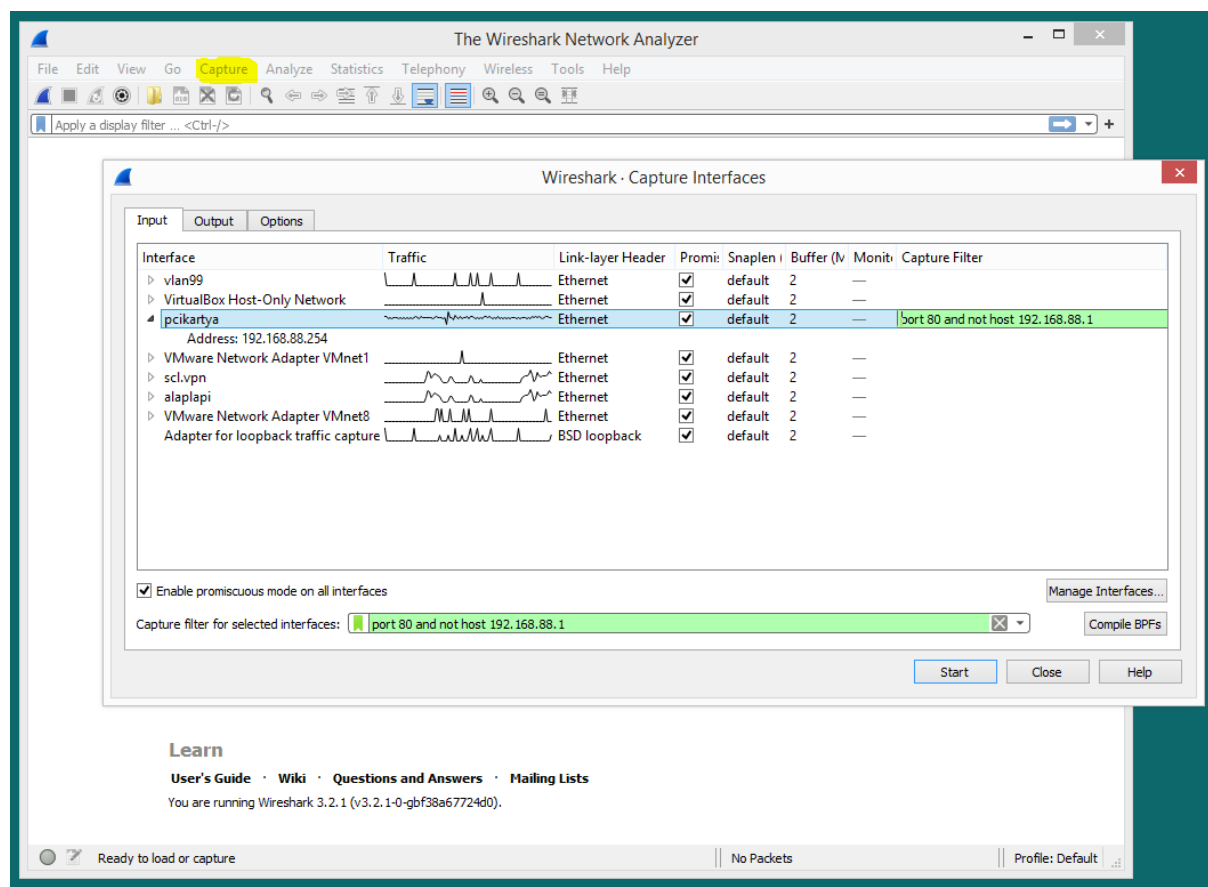


Az indításhoz a Wireshark-ot keressük meg, az ikonja ehhez hasonlatos:

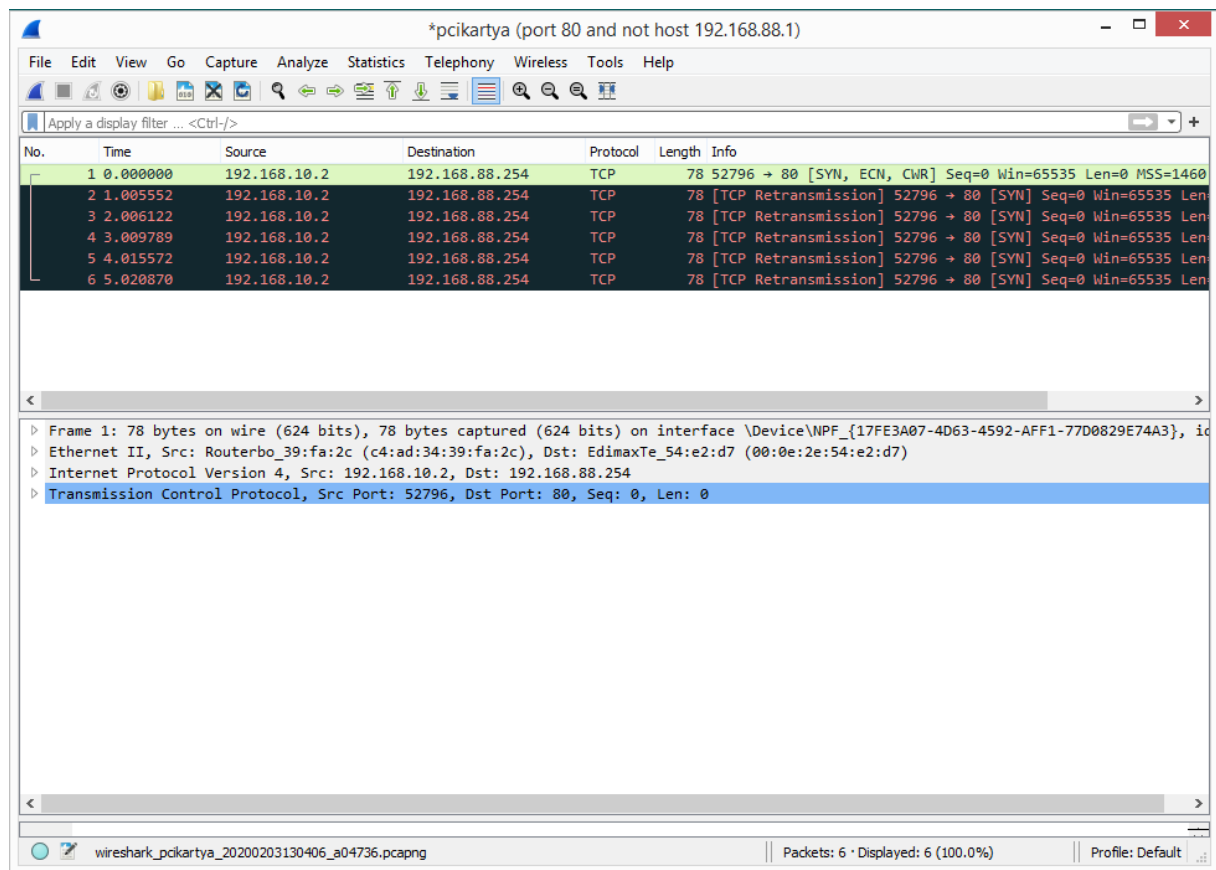
A nyitóképernyőn azon interfészek listája található, amelyekről adott jogosultsági szinttel tudunk csomagot elkapni. Továbbá a legutóbb megnyitott pcap fájlok listája.

Csomagelkapás indítása adott interfészen, egyszerű capture filterrel:

Capture → Options, megkeressük a szóban forgó interfészt (segíthet az IP-címe és neve is) és a Capture Filter oszlopban opcionálisan megadhatunk egy szabályt, majd Start.



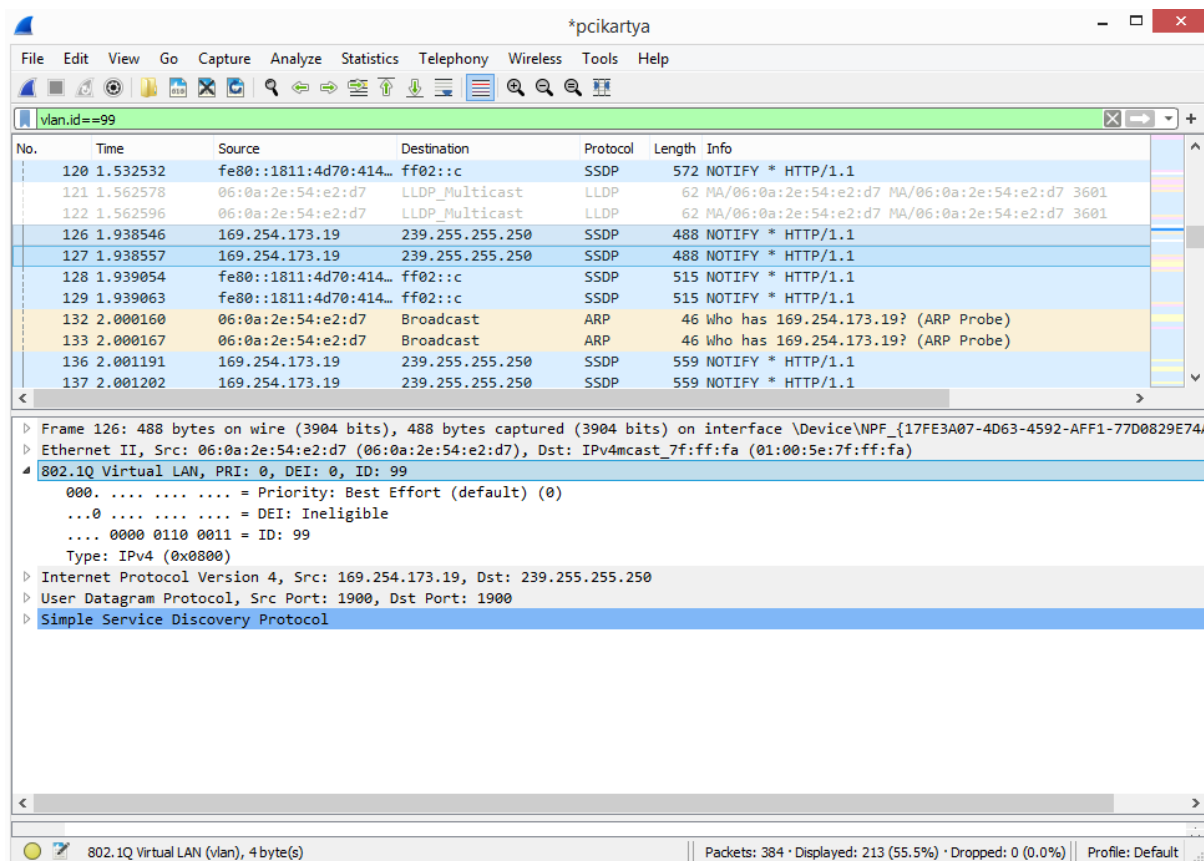
Az elkapást indítva az alábbi kiosztású képernyőhöz jutunk (a fenti csomagelkapási szabály eredményeképp). Azt látjuk, hogy a 192.168.10.2-es címről TCP kapcsolat felépítése indul (csomag #1, TCP-SYN). Normális esetben erre egy TCP-ACK csomagot kellene válaszul lássunk. Ilyet ebben a példában nem látunk, mindössze bizonyos időközönként újra érkező SYN csomagokat. Vagyis ez a TCP kapcsolat nem tudott felépülni.



A menü és eszköztár alatt egy, a böngészők címsorához hasonló szövegbeviteli sávot találunk. Ez a megjelenítési szűrő kifejezés megadására szolgál. Ha üres, akkor minden elkapott csomagot látni fogunk.

Ez alatt a csomagsorozatot fogjuk látni. Alapértelmezés szerint az elkapás szerint rendezve. A csomaglista folyamatosan bővül, egészen amíg le nem állítjuk az elkapást a stop gombbal. A listában kiválasztott csomag részletesen megtekinthető a csomaglista alatti, lenyíló menüket tartalmazó blokkban. Itt minden felismert protokoll fejléce meg fog jelenni egy lenyíló menü formájában, ahol a protokollhoz kapcsolódó fejléczmezők tekinthetők meg. A beágyazás természetesen befele haladva tekinthető meg.

Az alábbi ábrán a megjelenítési szűrő használatát láthatjuk: a címsorba írt kifejezéssel csak az adott tulajdonsággal rendelkező (most a 99-es VLAN azonosítójú) csomagok jelennek meg.



Távoli csomagelkapás

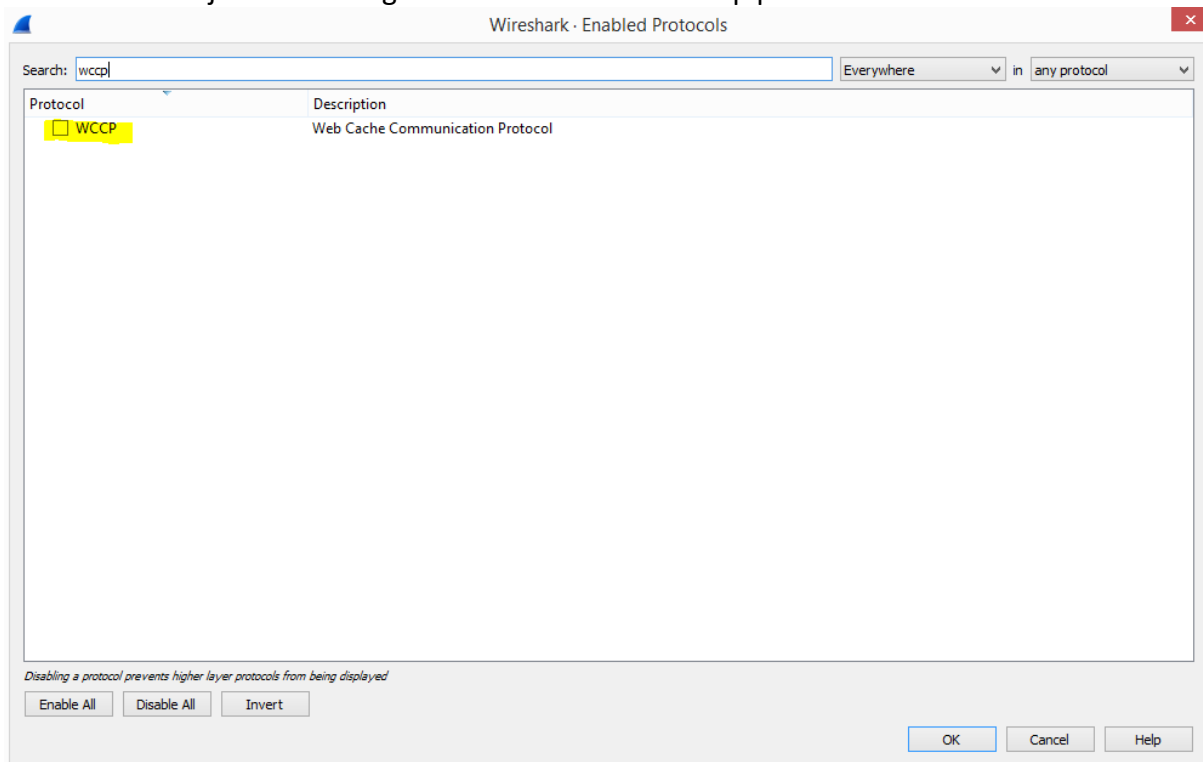
Hasznos funkció lehet, ha a routeren megjelenő forgalmat valamilyen módon ki tudjuk csatolni és egy távoli csomópont felé irányítani vagy akár lementeni. Ezt a funkciót a RouterOS Tools → *Packet Sniffer* pontjában konfigurálhatjuk.

A sniffert a *Start / Stop* gombokkal kapcsolgathatjuk. A beállítások megváltoztatása csak kikapcsolt állapotban lehetséges. Ha a routerre szeretnénk menteni a forgalmat, érdemes egy megfelelő USB drive-ot dugni az USB portra, majd a File Name-nél megadni az elérési utat és a fájlnévet. (Az USB drive-ról csatolt fájlrendszer elérési útját a Files menüpontban kereshetjük meg.)

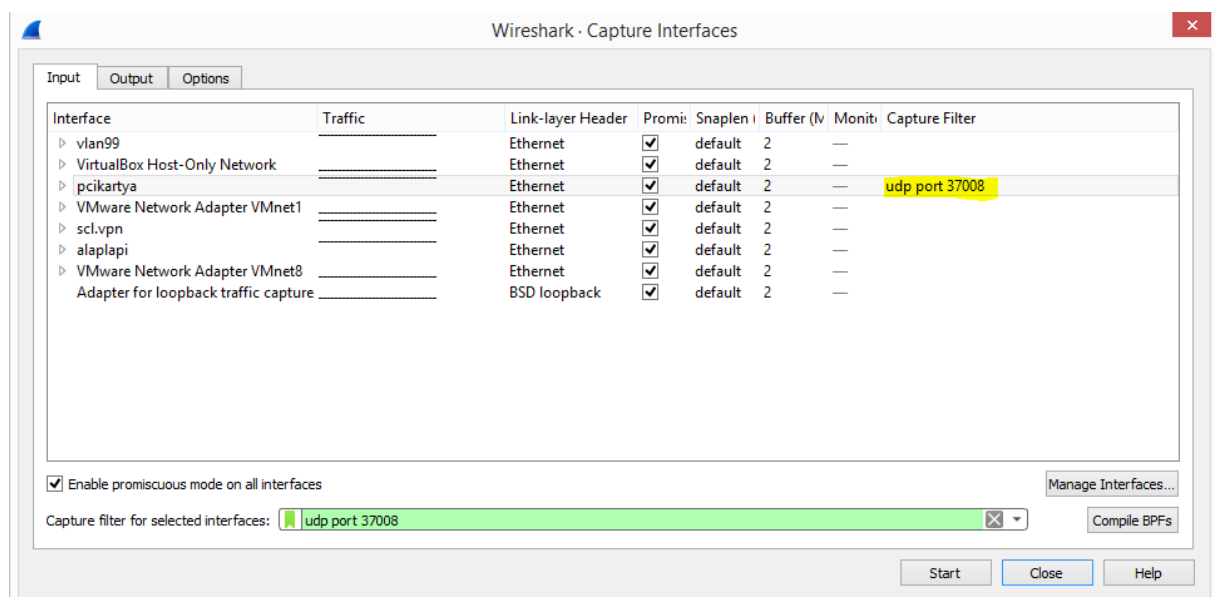
A távoli elkapáshoz szükséges beállítások a *Streaming* fülön találhatók. Az elkapott forgalom továbbítását a *Streaming Enabled* bepipálásával engedélyezhetjük. A *Server*-nél meg kell adnunk a csomópont IP-címét. Amennyiben szűrni szeretnénk a forgalmat (pl. bizonyos típusú csomagok elkapása, stb.), akkor a *Filter Stream*-et kell bepipálnunk és a *Filter* fülön különféle szűrési lehetőségeket tudunk beállítani. Érdekes lehet adott interfészen áthaladó forgalom elkapása, vagy adott IP protokoll vagy portszám szerinti elkapás.

A beállítások elvégzése (*Apply*) után a *Start*-tal indítható a streamelés. A forgalmat a 37008-as portra tartó UDP csomagokba fogja beágyazni a sniffer.

Hogy a Wireshark-kal el tudjuk kapni és meg tudjuk tekinteni ezeket a csomagokat, először is ki kell kapcsolnunk a WCCP protokoll felismerését, amelyet a Wireshark *Analyze* → *Enabled Protocols* menüjében kell megkeresnünk és törölnünk a pipát:



Ezután az elkapást úgy indítjuk, hogy csak a fenti portszámra érkező csomagokat kapjuk el:



Az így elkapott UDP csomagokban Ethernet keretek lesznek beágyazva, további protokollokat tartalmazva, ahogy azokat a routeren futó sniffer elkapta. Az alábbi képen egy VLAN tag-et is tartalmazó csomagot is láthatunk:

*pcikartya (udp port 37008)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

vlan.id==99

No.	Time	Source	Destination	Protocol	Length	Info
5	5.491338	192.168.99.253	192.168.99.1	TCP	111	[TCP ACKed unseen segment] 49270 → 8291 [ACK] Seq=185 Ack=524 Win=261 Len=0
11	15.241376	192.168.99.253	192.168.99.1	TCP	189	[TCP ACKed unseen segment] 49270 → 8291 [PSH, ACK] Seq=85 Ack=102 Win=257 Len=100
14	15.303754	192.168.99.253	192.168.99.1	TCP	111	[TCP ACKed unseen segment] 49270 → 8291 [ACK] Seq=185 Ack=524 Win=261 Len=0
15	15.653938	192.168.99.253	192.168.99.1	TCP	205	49270 → 8291 [PSH, ACK] Seq=85 Ack=102 Win=257 Len=100
17	15.700689	192.168.99.253	192.168.99.1	TCP	111	49270 → 8291 [ACK] Seq=185 Ack=524 Win=261 Len=0
20	19.607088	0a:12:2e:54:e2:d7	Routerbo_39:fa:2c	ARP	111	Who has 192.168.99.1? Tell 192.168.99.253

Frame 15: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface \Device\NPF_{17FE3A07-4D63-4592-AFF1-77D0829E74A3}

Ethernet II, Src: Routerbo_39:fa:2c (c4:ad:34:39:fa:2c), Dst: 0a:12:2e:54:e2:d7 (0a:12:2e:54:e2:d7)

Internet Protocol Version 4, Src: 192.168.99.1, Dst: 192.168.99.253

User Datagram Protocol, Src Port: 56861, Dst Port: 37008

TZSP: Ethernet

Ethernet II, Src: 0a:12:2e:54:e2:d7 (0a:12:2e:54:e2:d7), Dst: Routerbo_39:fa:2c (c4:ad:34:39:fa:2c)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 99

Internet Protocol Version 4, Src: 192.168.99.253, Dst: 192.168.99.1

Transmission Control Protocol, Src Port: 49270, Dst Port: 8291, Seq: 85, Ack: 102, Len: 100

Data (100 bytes)

wireshark_pcikartya_20200212094810_a03068.pcapng

Packets: 31 · Displayed: 6 (19.4%) · Dropped: 0 (0.0%) · Profile: Default