SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Mérési utasítás ARP és ICMP protokollok vizsgálata

Ezen a mérésen a hallgatók az ARP és az ICMP protokollok működését tanulmányozzák az előző méréseken megismert Wireshark segítségével.
A mérés folyamán a hallgatók jegyzőkönyvet készítenek: a tárgy honlapjáról letöltött előkészített mérési jegyzőkönyvet kell kitölteni. A jegyzőkönyvbe mindig kerüljenek be a kiadott parancsok és a kapott válaszok! A feladatok elvégzését képernyőképekkel is dokumentálhatja. A jegyzőkönyvben töltse ki a táblázatokat, és itt adjon választ a kérdésekre! (A mérési utasításba ne írjon bele!)

FIGYELEM! A mérés elvégzése fegyelmezett és tempós munkát igényel! Amennyiben valahol elakad, kérjen segítségét a mérésvezetőtől!

Előkészítő feladat

Töltse le a tárgy oldaláról (http://www.tilb.sze.hu/cgi-bin/tilb.cgi?0=m&1=targyak&2=NGB_TA007_1) a 6. méréshez tartozó jegyzőkönyvet és nevezze át úgy, hogy a fájl nevében a saját Neptun kódja szerepeljen! Ha például a Neptun kódja *NK7SZG*, akkor a fájl neve **szgh_jegyzokonyv_6_NK7SZG.odt** legyen! Nyissa meg a jegyzőkönyvet az Libreoffice programmal!

ARP

Az ARP protokoll feladata egy adott IP című gép MAC címének kiderítése. Ilyen leképzésre mindig olyan esetben van szükség, amikor a hálózati szint az alatta levő adatkapcsolati szint szolgáltatását veszi igénybe: a 3. réteg csomagját egy keretbe beágyazva el kell küldenie egy szomszédos állomásnak. Fontos, hogy ilyenkor a forrás és cél azonos fizikai hálózaton vannak, ezért az ARP *broadcast* segítségével képes a feladatot megoldani. A switchek a broadcast üzeneteket (adott VLANon belül) továbbítják az összes portjukra, így az ARP kérés biztosan eljut ahhoz az állomáshoz is, amelyik a kérdéses IP cím gazdája. A választ már *unicast*tal küldi, hiszen a kérés forrása ismert. Annak érdekében, hogy az ARP működését meg tudjuk figyelni, törölnünk kell a számítógép által korábban eltárolt IP cím – MAC cím párokat. Mivel az *ARP cache* teljes ürítését a Linux **arp** parancsa nem támogatja (más Unix implementációk, pl. BSD rendszerek ezt lehetővé teszik), ezért vizsgálataink előtt mindig a keresett IP cím alapján adunk ki egy törlést a következő formában:

```
arp –d <IP cím>
```

Például a laborban a fekete gépeknél a default gateway szerepét betöltő 192.168.100.1 IP című gép MAC címének törlése: **`arp –d 192.168.100.1`**

Ha a helyi gépünk és a kérdéses gép között van forgalom, akkor a törlés után hamarosan ismét bekerül annak MAC címe az ARP cache-be. Ezért a törlést közvetlenül a mérés előtt kell elvégezni, amit a legegyszerűbben úgy tehetünk meg, hogy: vagy a két parancsot (törlés és a mérés indítása) egyetlen parancssorba írjuk pontosvesszővel elválasztva, vagy készítünk egy batch fájlt.

A mérés alatt a /root könyvtárban található **myping** programot kell használni!

Ha a PATH nem tartalmazza az a könyvtárat, ahova a batch fájl elhelyeztünk, akkor futtatásához meg kell adnunk az elérési útvonalát is. (Például, ha abban a könyvtárban vagyunk, ahova helyeztünk, akkor a futtatása:
./myping <IP cím>)

Tehát a **/root** könyvtárba belépve adjuk majd ki a parancsot. **`./myping <IP CÍM>`**

1. feladat

Indítsa el a forgalom rögzítését a Wireshark programmal azon az interfészen, amelyikkel a 192.168.100.0 hálózatra kapcsolódik (ez a fekete gépeken általában az eth0), pingelje meg a 192.168.100.1 IP című gépet az elkészített batch fájl segítségével, majd néhány üzenet visszaérkezése után állítsa le a pingelést és a forgalom rögzítését is! Elemezze a rögzített forgalmat: keresse meg az ARP kérést és a választ, majd vizsgálja meg ennek a két üzenetnek a tartalmát!
Töltse ki az alábbi táblázatot az *Ethernet* szintű információk alapján! A MAC címeknél a teljes 6 bájtos címet írja, ne a gyártó nevét! A keret fajtáját a *broadcast*, *multicast* és *unicast* lehetőségek közül válassza ki a cél MAC cím alapján! Az *Ethertype* mező értékét hexadecimálisan adja meg!

```
cd /root
./myping 192.168.100.1
```

	forrás MAC címe	cél MAC címe	keret fajtája	EtherType értéke
ARP kérés				
ARP válasz				

Ha helyesen töltötte ki a táblázatot, akkor az Ethertype mező értéke mindkét sorban ugyanaz. Miből, hogyan derül ki, hogy melyik a kérés és melyik a válasz? (Nézze meg az ARP protokoll mezőit!) Vizsgálja meg az ARP protokoll többi mezőjét is!

ICMP

Az ICMP protokoll feladata az IP protocol stack *szolgálati közlemény*einek továbbítása. Az ICMP üzenetek közül most csak az *echo* és az *echo reply* típusúakkal foglalkozunk, a következő mérésen más típust is megismerünk.

2. feladat

Indítsa el a forgalom rögzítését a Wireshark programmal azon az interfészen, amelyikkel a 192.168.100.0 hálózatra kapcsolódik (eth0), küldjön egy darab ICMP *echo* üzenetet a 192.168.100.1

IP című gépnek (**ping –c 1 192.168.100.1**), majd a **193.224.128.1** IP című gépnek, végül állítsa le a forgalom rögzítését!

Töltse ki az alábbi táblázatot!

	MAC forrás	MAC cél	Ethertype	IP forrás	IP cél	IP fölötti protokoll	ICMP típus
1. echo							
1. válasz							
2. echo							
2. válasz							

A megfigyeltek alapján adjon választ a következő kérdésekre!
- Milyen protokoll fölött utaznak az ICMP üzenetek?
- Miből derül ki, hogy ICMP üzenetről van szó (és nem TCP vagy UDP)?
- Miből derül ki, hogy melyik ICMP üzenetről van szó?
- Mi az oka annak, hogy a két megpingelt gép esetén (bár az IP címek eltérőek), a MAC címek azonosak? (Segítség: a MAC és az IP címeket eltérő rétegben használjuk!)

A mérés értékelése

Amennyiben szeretné, röviden értékelheti is a mérést! (Mennyire volt érhető, követhető a mérési utasítás, milyen mértékben találja hasznosnak a mérést a tárgy anyagának mélyebb megismerése szempontjából? Ötletek, javaslatok a mérés fejlesztésére…)

A jegyzőkönyv beadása

Ha teheti, még egyszer olvassa át és tisztázza le a jegyzőkönyvet!

Ha szeretné, a jegyzőkönyvet elviheti, de egy másolatot mindenképpen hagyjon belőle azon a gépen, ahol dolgozott! A **/root könyvtárban!!!!**