SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Mérési utasítás A DHCP protokoll és a traceroute vizsgálata

Ezen a mérésen a hallgatók a DHCP protokoll és a **`traceroute`** UNIX parancs működését tanulmányozzák a már 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 7. 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_7_NK7SZG.odt** legyen! Nyissa meg a jegyzőkönyvet az OpenOffice.org programmal! Amennyiben a program nincs fent, akkor telepítse a korábban megismert módon! (**`apt-get install openoffice.org`**)

DHCP

Az DHCP protokoll célja, hogy a számítógépek a hálózati kapcsolathoz különféle információkat kérhessenek le. Ebben a mérésben a lehetőségek közül csak néhányat vizsgálunk meg. Mivel a gép már rendelkezik IP címmel, ezért először vissza fogjuk adni azt.

1. feladat

Indítsa el a forgalom rögzítését a Wireshark programmal azon az interfészen, amelyikkel a 192.168.100.0 hálózatra kapcsolódik, adja vissza az IP címét (**`dhclient -r`**), majd kérjen újat (**`dhclient -v eth0`**), várja ki türelmesen, amíg a parancs végrehajtása befejeződik, végül állítsa le a forgalom rögzítését!

Összesen 5 DHCP üzenetet kell látnia, ezek közül az első (DHCP release) az IP cím visszaadásához, a további 4 (DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK) az új cím kéréséhez tartozik. Először az első üzenettel foglalkozunk. Válaszoljon az alábbi kérdésekre:

- Az Ethernet keret melyik mezőjének milyen értékéből tudja megmondani, hogy milyen hálózati protokollt használ a DHCP?
- Az IP datagram melyik mezőjének milyen értékéből tudja megmondani, hogy az IP fölött milyen szállítási szintű protokollt használ a DHCP?

- Az UDP datagram mely mezőinek milyen értékéből tudja megmondani, hogy milyen protokoll üzenete utazik benne?
- A DHCP üzenet (vigyázat, a Wireshark *Bootstrap Protocol*nak hívja!) melyik mezőjének milyen értékéből tudja megmondani, hogy most éppen IP címet adunk vissza?

Vizsgálja meg a további 4 üzenetet is! Töltse ki az alábbi táblázatot!

	forrás MAC cím	cél MAC cím	forrás IP cím	cél IP cím
DHCP Discover				
DHCP Offer				
DHCP Request				
DHCP ACK				

Gondolkozzon el rajta, hogy miért ezek az értékek kerültek a táblázatba! Fogalmazza meg megfigyeléseit az alábbi kérdések segítségével!

- A DHCP Discover küldésekor van-e a gépnek érvényes IP címe, illetve tudja-e hogy kihez forduljon?
- A DHCP Offer küldésekor az ajánlatot tevő szerver ismeri-e a kérést küldő gép MAC címét?
- A DHCP Request küldésekor a kapott ajánlat alapján (és más ajánlat hiányában) a felajánlott címet megigénylő gép használhatja-e már az ajánlatban szereplő címet?

Amennyire ideje engedi, vizsgálja meg és próbálja értelmezni a 4 üzenet többi mezőjének értékét is!

A `traceroute` parancs működésének vizsgálata

A **`traceroute`** feladata annak kiderítése, hogy egy adott cél felé milyen útvonalválasztókon keresztül jut el egy datagram, valamint ezek válaszidejének a meghatározása. Ennek érdekében UDP adatcsomagot küld a célként megadott gép felé 1-től 1-esével növekvő TTL értékkel: minden értékkel 3 adatcsomagot küld.

2. feladat

Indítsa el a forgalom rögzítését a Wireshark programmal azon az interfészen, amelyikkel a 192.168.100.0 hálózatra kapcsolódik, adja ki a **`traceroute www.bme.hu`** parancsot, figyelje meg a program kimenetét; adjon ki egy **`ping www.bme.hu`** parancsot is, végül állítsa le a forgalom rögzítését!

Jegyzőkönyvezze a kiadott parancsokat és azok kimenetét!

Válaszoljon az alábbi kérdésekre!

- Mennyi az IP protokoll esetén a TTL maximális kezdőértéke? (Segítség: a TTL mező 8 bites.)

  A Linux ebből 64-et használ!

- A **`traceroute`** parancs kimenete alapján a helyi géptől az **`www.bme.hu`** gépnek megfelelő **`decor.eik.bme.hu`** gépig hány útvonalválasztón halad keresztül a datagram?

- Mennyi a **`ping`** által kiírt TTL érték a visszaérkező csomagnál?

- Milyen összefüggést talál a fenti 3 szám között?

Vizsgálja meg a Wireshark által rögzített forgalmat! Keresse meg a helyi géptől a **`www.bme.hu`** gép felé küldött első UDP datagramot! Ennek alapján töltse ki az alábbi táblázatot!

forrás IP cím	cél IP cím	IP TTL	UDP forrás port	UDP cél port	UDP adatmező tartalma

Keresse meg a csomag által kiváltott ICMP hibaüzenetet! A datagram mely része alapján tudja biztosan, hogy ezt a hibaüzenetet a fenti datagram váltotta ki? (Segítség: használja a fenti táblázat értékeit!)

Keresse meg az utolsó olyan UDP csomagot, amelyre válaszként "Time-to-live exceeded" ICMP hibaüzenet érkezett! Mennyi az IP fejrész TTL mezőjének értéke?

Mennyi az IP fejrész TTL mezőjének értéke a következő UDP datagramnál?

Erre milyen hibaüzenetet küldött vissza a www.bme.hu gép? (ICMP type és code mezők értelmezése)

Mi az oka ennek az üzenetnek?

Hogyan használja fel a **`traceroute`** parancs a működése során az ICMP üzeneteket? (Mit jelentenek ezek számára, melyiknél mit kell tennie?)

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? Ötleteket adhat, javaslatokat tehet a mérés fejlesztésére.)

A jegyzőkönyv beadása

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

SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Ha szeretné, a jegyzőkönyvet elviheti, de egy másolatot mindenképpen hagyjon belőle a gépen, ahol dolgozott!