

Hálózatok építése és üzemeltetése

Vizsga konzultáció

Vizsga

- ▶ Google kvíz
 - Teszt feladatok, ZH-hoz hasonlóan
 - Egyedi gyakorlati feladatok, amihez a HaEpUz VM saját példányát kell futtatni (BME Cloud, Smallville), kiugrókhoz hasonlóan
- ▶ Felkészülés
 - Előadások anyagai
 - slide-ok, videók
 - Gyakorlatok anyagai
 - slide-ok, videók
 - gyakorló feladatok és kiugrók
 - HaEpUz VM + **csináljátok végig a feladatokat!**

Vizsga

▶ Témakörök:

- ▶ Linux alapok
- ▶ szoftver szerszámok (ping, traceroute, netstat, tcpdump, wireshark, ifconfig, route, arp, ip, iptables, nslookup, dig, dhclient)
- ▶ bash, python
- ▶ hálózati funkciók (nat, firewall, dhcp, dns)
- ▶ routing protokollok
- ▶ SDN, OpenFlow
- ▶ Internet
- ▶ **Mininet használata!**

Egy-két problémás ZH feladat

- ▶ Egy hoszt eth0 interfészén a default gateway-t szeretnénk beállítani. Melyik parancs(ok) végzi(k) el helyesen a konfigurációt?

- A. `sudo route add default gw 192.168.0.1`
- B. `sudo ip route add default via 192.168.0.1`
- C. `sudo route add default gw 192.168.0.1 netmask 255.255.255.0`
- D. `sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.0.1 eth0`

- ▶ Az alábbiak közül melyik Python utasítás értékelődik ki logikai igaz, azaz True értékként?
 - A. 0
 - B. None
 - C. []
 - D. [0, False, None, (), {}]

- ▶ Mi(ke)t eredményez a következő parancs? Melyik állítás(ok) helyes(ek)?

```
▶ $ iptables -t nat -A POSTROUTING -s 10.20.30.0.0/8 -o eth6 \  
-j MASQUERADE
```

- A. port forwarding beállítása, kívülről hozzáférhetővé válik a 10.20.30.0/8-as tartomány
- B. egy új címfordítási szabály hozzáadása a nat tábla POSTROUTING láncához, melynek segítségével a 10.20.30.0/8-as belső hálózatról kijutunk a külső hálózatra, ha ahhoz az eth6 interfészen keresztül csatlakozunk
- C. egy új címfordítási szabály hozzáadása a nat táblához, ami a 10.20.30.0/8-as címeket cseréli le, ha a csomag az eth6 interfészen érkezett
- D. egy új címfordítási szabály hozzáadása a nat táblához, ami a 10.20.30.0/8-as címeket cseréli le, ha a csomag az eth6 interfészen kerül majd kiküldésre

Bónusz feladat IMSc pontokért

1/108x5

- ▶ Egyszerű hálózatunkban a client gép a 10.0.0.0/24-es hálózaton keresztül kapcsolódik a gateway géphez és azon keresztül a külvilághoz. Feltételezhetjük, hogy a client gép jól van konfigurálva. A client gépen a ping parancs futtatása után megvizsgáltuk a gateway gépet és az alábbi parancsokra a megadott válaszokat kaptuk. Milyen konfigurációs parancsok kiadása szükséges a gateway gépen, hogy a korábbi ping parancs működjön a client gépen?

Bónusz feladat IMSc pontokért

1/108x5

```
CLIENT:
=====
haepuz@haepuz-client:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.0.0.1 0.0.0.0 UG 0 0 0 enp0s9
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s9
192.168.56.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s8
haepuz@haepuz-client:~$
haepuz@haepuz-client:~$ ping -c1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

haepuz@haepuz-client:~$
```

```
GATEWAY:
=====
haepuz@haepuz-gw:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 enp0s10
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s9
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s10
192.168.56.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s8
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$ sudo iptables -t nat -nvL
Chain PREROUTING (policy ACCEPT 1 packets, 84 bytes)
pkts bytes target prot opt in out source destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 MASQUERADE all -- * enp0s9 10.0.0.0/24 0.0.0.0/0
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 69 packets, 10902 bytes)
pkts bytes target prot opt in out source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 49 packets, 5904 bytes)
pkts bytes target prot opt in out source destination
haepuz@haepuz-gw:~$
```

ZH utáni témák



SDN

- ▶ Melyik NEM képzelhető el SDN alkalmazásként?
 - A. tűzfal
 - B. új TCP verzió saját torlódásvezérlési mechanizmussal
 - C. terhelés elosztó
 - D. legrövidebb útválasztás

SDN

▶ A lenti OpenFlow folyambejegyzés...

```
▶ cookie=0x0, duration=30s, table=0, n_packets=40, n_bytes=60000,  
idle_timeout=15, hard_timeout=35, idle_age=5, priority=65535, tcp,  
in_port=1, vlan_tci=0x0000, dl_src=00:00:00:00:00:01,  
dl_dst=00:00:00:00:00:02, nw_src=10.0.0.1, nw_dst=10.0.0.2, nw_tos=0,  
tp_src=1111, tp_dst=2222 actions=output:2
```

- A. 8s múlva még aktív lesz, ha csak egyetlen illeszkedő csomag érkezik pont 4s múlva
- B. 15s múlva még aktív lesz, ha csak egyetlen illeszkedő csomag érkezik pont 8s múlva
- C. átlagosan több mint 5 kbps forgalmat továbbított
- D. által továbbított csomagok átlagos hossza kisebb mint 1000 byte.

SDN

- ▶ Egy reaktív logikájú kontrolleralkalmazás ...
 - A. nem működik megfelelően, ha a kapcsolók és a kontroller közti kapcsolat átmenetileg megszakad
 - B. a proaktív párjánál nagyobb csomagkésleltetést eredményez(het)
 - C. nem tudja a csomagok IP címét figyelembe venni
 - D. készíthető POX-ban.

Internet

- ▶ Az alábbi állítások közül mi igaz az Internetre?
 - A. Az Internet topológiáját az IANA nevű szervezet felügyeli.
 - B. Az Internet topológiája mérnöki tervezés és optimalizáció eredménye.
 - C. Az Internet spontán önszerveződéssel jött létre a különböző hálózatok lokális döntései nyomán.
 - D. Az Internet topológiáját a BGP protokoll segítségével lehet központilag megadni.

Internet

- ▶ Melyik állítás(ok) igaz(ak) az Internet alapegységeire, az Autonóm rendszerekre (AS, Autonomous systems)?
 - A. Az AS egy adminisztratív egységbe tartozó mérnökiileg tervezett hálózat.
 - B. A BME saját hálózata egy AS.
 - C. A TMIT saját hálózata egy AS.
 - D. Az AS-eknek sorszámuk van, melyet a IANA nevű szervezet regisztrál.

Internet

- ▶ Melyek a hasonlóságok az Internet, a Facebook és a Debian csomagfüggőségek hálózatában?

- A. Mindegyik spontán önszerveződéssel jött létre.
- B. Mindegyik skálafüggetlen fokszámeloszlású.
- C. Mindegyiknek az alapegységei (csomópontjai) elektronikus áramkörök.
- D. Mindegyik kifejezetten sűrű hálózat.

Gyakorlati feladatok

- ▶ Megadott script futtatása a saját HaEpUz VM-ben → saját Mininet környezet létrehozása, indítása
- ▶ Konkrét feladatok, kérdések
 - végrehajtás, munka a VM-ben
 - válaszok megadása a Google kvízben
 - opciók vagy
 - szövegdoboz a szintaktikailag helyes, kipróbált parancsok bemásolásával

Gyakorlati feladatok

- ▶ Példák a kvízekből

Kvíz: gyak3

▶ GW, CLIENT, INTERNET setup...

- Ubuntu környezetben pl. a "sudo ntpdate ntp.ubuntu.com" parancs segítségével oldható meg az óra szinkronizálása egy központi szerverhez az NTP protokoll használatával. Szinkronizáld a CLIENT VM óráját! Ehhez milyen parancs(ok) kiadására volt szükség a GW VM-en?

Kvíz: gyak3

▶ GW, CLIENT, INTERNET setup...

- Ubuntu környezetben pl. a "sudo ntpdate ntp.ubuntu.com" parancs segítségével oldható meg az óra szinkronizálása egy központi szerverhez az NTP protokoll használatával. Szinkronizáld a CLIENT VM óráját! Ehhez milyen parancs(ok) kiadására volt szükség a GW VM-en?
- `sudo iptables -A FORWARD -p udp --sport 123 -j ACCEPT`
- `sudo iptables -A FORWARD -p udp --dport 123 -j ACCEPT`

Kvíz: gyak4

▶ Saját mininetes hálózat indítása, környezet előkészítése

- `wget -nv -O- https://sb.tmit.bme.hu/haepuz/ts | sudo sh /dev/stdin $NEPTUN`
- ha nem akarjuk mindig a jelszót másolgatni: hozzunk létre a `.ssh` könyvtárban egy kulcspárt és a publikus kulcsot adjuk hozzá az `authorized_keys` fájlhoz. Pl.:
 - `cd ~/.ssh`
 - `ssh-keygen [3x enter]`
 - `cat id_rsa.pub >> authorized_keys`

Kvíz: gyak4

- ▶ Mininet hálózat: hosztok, szerverek, routerek (és persze switch-ek, linkek)
 - Ha a "Host A" gépről pingeljük a "Server" gépet, a "Host A" melyik interfészén történik a kommunikáció? Add meg a kérdéses interfész nevét!
 - Add meg az előző kérdés megválaszolásához (a forgalom megfigyeléséhez) használt parancsot!
 - A "Host B" gépről nem tudjuk pingelni a "Server" gépet, pedig innen is hasonlóan kéne működni, mint a "Host A" gépről. Milyen parancs volt az, amivel sikerült felderíteni a hibát? (A hiba felderítéséhez persze több parancs használata szükséges, hacsak nem elsőre találjuk el. Itt most arra vagyunk kíváncsiak, amivel meglett a hiba.)
 - Add meg az előző hiba javításához használt parancsot/parancsokat!

Kvíz: gyak4 (bónusz)

► Mininet hálózat:

- A "Host A" és "Host C" eszközök között milyen interfészekon halad a forgalom? Add meg a parancsot, amivel ezt feltérképezted és add meg a parancs kimenetét!
- A "Host C" egy /24-es alhálózatra csatlakozik. Rajta kívül még több más eszköz is csatlakozik ugyanerre az alhálózatra. A "Host A" gépről próbáld pingelni a "Host C"-nél eggyel nagyobb IP címmel rendelkező eszközt! Melyik IP címről érkezik válasz? Hány interfészen halad át a csomag?
- Jelentkezz be arra az eszközre, amelyikhez az utolsó azonosított interfész tartozik! (A bejelentkezéshez használható IP cím a hálózat indításakor szintén listázásra került.) Mi okozza a hibát? Add meg a felderítéshez használt egyetlen parancsot, annak kimenetéről a hibát okozó sort, valamint egy egy mondatos magyarázatot arról, hogy ez mit jelent!
- Adjál olyan megoldást a problémára, ami a kérdéses alhálózat minden elemére javítja a hibát! Másold be a használt parancsot/parancsokat!

Gyakorlati feladatok

- ▶ További példák

Példa 1

- ▶ Saját mininetes hálózat és kontroller indítása, környezet előkészítése
 - `wget -nv -O- https://sb.tmit.bme.hu/haepuz/table_error | sh /dev/stdin $NEPTUN`
 - egy felugró ablakban elindul egy mininetes hálózatemuláció és egy másik ablakban pedig egy pox kontroller
 - Próbáld ki, hogy a h1 hosztról nem lehet pingelni a h10-es hosztot. Azért nem, mert az egyik switch egyik folyamtábla-bejegyzésében szándékosan el van írva az output port értéke. A feladat megkeresni, hogy az elrontott folyamtábla-bejegyzéshez milyen cookie érték tartozik. A megoldás mezőbe ezt a cookie értéket kell hexadecimális formában beírni (pl. 0xa4).

Példa 2

- ▶ Saját mininetes hálózat és kontroller indítása, környezet előkészítése (mininet, pox terminálok)
 - `wget -nv -O- https://sb.tmit.bme.hu/haepuz/star | sh /dev/stdin $NEPTUN`
 - A pox kontroller és a mininetes hálózat elindítása után a h1 hosztról sikeresen lehet pingelni a h2 hosztot. Azonban a ping kérésekre nem a h2 hoszt válaszol, mert a kontroller eltéríti a ping forgalmat egy másik hoszthoz, valamint a forgalomról egy másolatot is kiküldet a kapcsolóval egy nem létező porton. Mi annak a hosztnak a neve, ami a h2 felé küldött ping kérésekre válaszol (pl: h73)?
 - Mi annak a nem létező portnak a száma (pl: 211), ahova a kontroller a másolatot küldeti a kapcsolóval?
 - Hány darab folyambejegyzés található a kapcsoló folyamatáblájában?

Gyakorlati feladatok

- ▶ Még milyen jellegű feladatok várhatók?

Hálózati funkciók

▶ Saját környezet indítása után...

- a Troubleshooting gyakorlat bármelyik feladata (vagy ahhoz hasonló feladat...)
- például:
 - ki kell találni, hogy mi a hiba a saját hálózatban
 - javítani kell a hibát
 - a már működő hálózatban le kell futtatni egy parancsot és a kapott választ kell megadni a kvízben

Hálózati funkciók

▶ Saját környezet indítása után...

- milyen topológiájú hálózat indult el a Mininetben? (pl. opciók: 3 elemű lánc, 2 szintű fa, csillag, ...)
- h1 hosztról h5 hoszt milyen átlagos körülfordulási idővel érhető el? (pl. opciók: adott idő intervallumok)
- gateway - client konfiguráció, pl.
 - h1: client
 - r1: gateway
 - h5: remote server a külvilágban
 - mit kell konfigurálni?

- .

Hálózati funkciók

▶ Saját környezet indítása után...

- milyen topológiájú hálózat indult el a Mininetben? (pl. opciók: 3 elemű lánc, 2 szintű fa, csillag, ...)
- h1 hosztról h5 hoszt milyen átlagos körülfordulási idővel érhető el? (pl. opciók: adott idő intervallumok)
- gateway - client konfiguráció, pl.
 - h1: client
 - r1: gateway
 - h5: remote server a külvilágban
 - mit kell konfigurálni?
 - (ip_forward), nat (snat, dnat), firewall (esetleg dhcp, egyszerűsített dns)

OpenFlow

▶ Saját környezet indítása után...

- hány darab folyambejegyzés található a kapcsoló folyamatáblájában?
- ha az első bejegyzésre folyamatosan érkezik illeszkedő forgalom, akkor az indítás után hány másodperccel törlődik a bejegyzés?
- ha a második bejegyzésre sosem érkezik illeszkedő forgalom, akkor az indítás után hány másodperccel törlődik a bejegyzés?

OpenFlow

- ▶ Saját környezet indítása után...
 - OpenFlow hálózat, nem az elvárt működés, mi az oka?
 - hibakeresés
 - flow táblák, bejegyzések, számlálók vizsgálata
 - hibás bejegyzések azonosítása
 - hibás bejegyzések javítása
 - működés validálása