

Hálózatok építése és üzemeltetése

Vizsgakonzultáció

Vizsga

- ▶ Google kvíz
 - Teszt feladatok, ZH-hoz hasonlóan
 - Egyedi gyakorlati feladatok, amihez a HaEpUz VM saját példányát kell futtatni (BME Cloud, Fured), kiugrókhoz hasonlóan
- ▶ Felkészülés
 - Előadások anyagai
 - slide-ok
 - Gyakorlatok anyagai
 - slide-ok
 - 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

► Mi(k)re használható a következő parancs?

► `$ traceroute www.bme.hu`

- A. célhoszt elérhetőségének tesztelésére
- B. küldő és fogadó gépek közti egyirányú késleltetés mérésére
- C. küldő és fogadó gépek közti "hop szám" mérésére
- D. küldő és fogadó gépek közti útvonal felderítésére

- ▶ 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`

- ▶ `ls -l` parancs eredményeként a következőt kapjuk.
Melyik parancs(ok) NEM eredményezi(k) azt, hogy a user csoport végrehajtási jogot kapjon a pelda fájlra?
 - ▶ `-rwxr----- 1 bela user 7 Oct 24 19:19 pelda`

- A. `chmod a+rxw pelda`
- B. `chmod ug=rx pelda`
- C. `chmod oug+rw pelda`
- D. `chmod u+xwr pelda`

- ▶ Az alábbiak közül melyik Python utasítás(ok) értékelődik(értékelődnek) 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

1x1,8x2,1x4

- ▶ Egyszerű hálózatunkban a client gép a 10.0.0.0/24-es hálózton 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

1x1,8x2,1x4

```
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 az opcionális HF-ekből

HF: gyak3

► GW, CLIENT, INTERNET setup...

- A feladatokat a BME Cloud-ban (Füred) futtatott VM-eken kell megoldani, abban a környezetben, amit a 3. gyakorlaton használtunk. Három saját VM-et kell indítani (gateway, client: "HaEpUz 2022 v19" template-ből indítva; internet: "HaEpUz 2022 v17" template-ből indítva). Dolgozni az xfce4 grafikus desktop környezettel "ellátott" GW gépen érdemes, amihez rdp kliens segítségével tudsz kapcsolódni, a gyakorlaton látott módon. Innen külön terminálokból indított ssh kapcsolatokkal tudsz átlépni a másik két gépre. (A belépési adatok a Cloud dashboardról másolhatók ki.)
- Készítsük elő a 3. gyakorlaton látott alap munkakörnyezetet!

HF: gyak3

- ▶ GW, CLIENT, INTERNET setup...
 - A CLIENT VM-edről hány hop-on és milyen útvonalon keresztül érhető el a 152.66.247.212 IP című gép? Vesszővel elválasztva add meg a hop-számot és a célhoszt előtti utolsó router IP címét! Ha szükséges, installáld a szükséges programo(ka)t a CLIENT VM-en!

HF: gyak3

- ▶ GW, CLIENT, INTERNET setup...
 - A CLIENT VM-edről hány hop-on és milyen útvonalon keresztül érhető el a 152.66.247.212 IP című gép? Vesszővel elválasztva add meg a hop-számot és a célhoszt előtti utolsó router IP címét! Ha szükséges, installáld a szükséges programo(ka)t a CLIENT VM-en!
 - `traceroute 152.66.247.212`
 - `13,152.66.245.249`

gyak3 gyakorló feladatok

► traceroute

- Vizsgáljuk meg, hogy a GW VM milyen útvonalon (routereken keresztül) éri el a `www.stanford.edu` gépet és analizáljuk azt is, hogy ennek hogy történik a felderítése a traceroute program segítségével! Ehhez a következő lépéseket hajtsuk végre:
 - Találjuk ki a `www.stanford.edu` névhez tartozó IPv4 címet!
 - A Wireshark program segítségével vizsgáljuk a beazonosított IPv4 címre kimenő és onnan bejövő forgalmakat (a releváns interfészen)!
 - A traceroute program default beállításával indítsuk a vizsgálatot a `www.stanford.edu` gépre!

gyak3 gyakorló feladatok

► traceroute

- Milyen típusú forgalommal történik a tesztelés és milyen lépésekben? Milyen protokoll, IP cím, port szám, TTL érték, stb. van beállítva, hány csomaggal történik a vizsgálat?
- Honnan milyen válaszok érkeznek?
- Ezek alapján hogyan azonosítható az útvonal?

gyak3 gyakorló feladatok

► traceroute

- Milyen típusú forgalommal történik a tesztelés és milyen lépésekben? Milyen protokoll, IP cím, port szám, TTL érték, stb. van beállítva, hány csomaggal történik a vizsgálat?
 - default 3 UDP csomag/port a célcímre, destination port: 33434, 33435, 33436 TTL=1, ...
- Honnan milyen válaszok érkeznek?
 - Routers válaszolnak, ICMP üzenet: TTL exceeded
- Ezek alapján hogyan azonosítható az útvonal?
 - Akinél “elfogy” a TTL válaszol, aki tovább engedi nem küld választ (tipikusan nem használt portok)

gyak3 gyakorló feladatok

► traceroute

- Hány hop-ból áll az útvonal? Milyen IPv4 című routerekből áll az útvonal?
- Alakítsuk át úgy a vizsgálatot, hogy ICMP Echo Request csomagokkal történjen a tesztelés és ne kelljen kivárni a felesleges mérések eredményét! Vizsgáljuk a forgalmat wireshark segítségével.

gyak3 gyakorló feladatok

► traceroute

- Hány hop-ból áll az útvonal? Milyen IPv4 című routerekből áll az útvonal?
 - Mérésfüggő útvonal és hop szám
- Alakítsuk át úgy a vizsgálatot, hogy ICMP Echo Request csomagokkal történjen a tesztelés és ne kelljen kivárni a felesleges mérések eredményét! Vizsgáljuk a forgalmat wireshark segítségével.
 - `sudo traceroute -m 8 -I www.stanford.edu`

HF: 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`

Gyakorlati feladatok

► További példák

Példa 1

- ▶ Saját mininetes hálózat és kontroller indítása, környezet előkészítése
 - `wget -nv -O- http://ib213.tmit.bme.hu:8888/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- http://ib213.tmit.bme.hu:8888/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