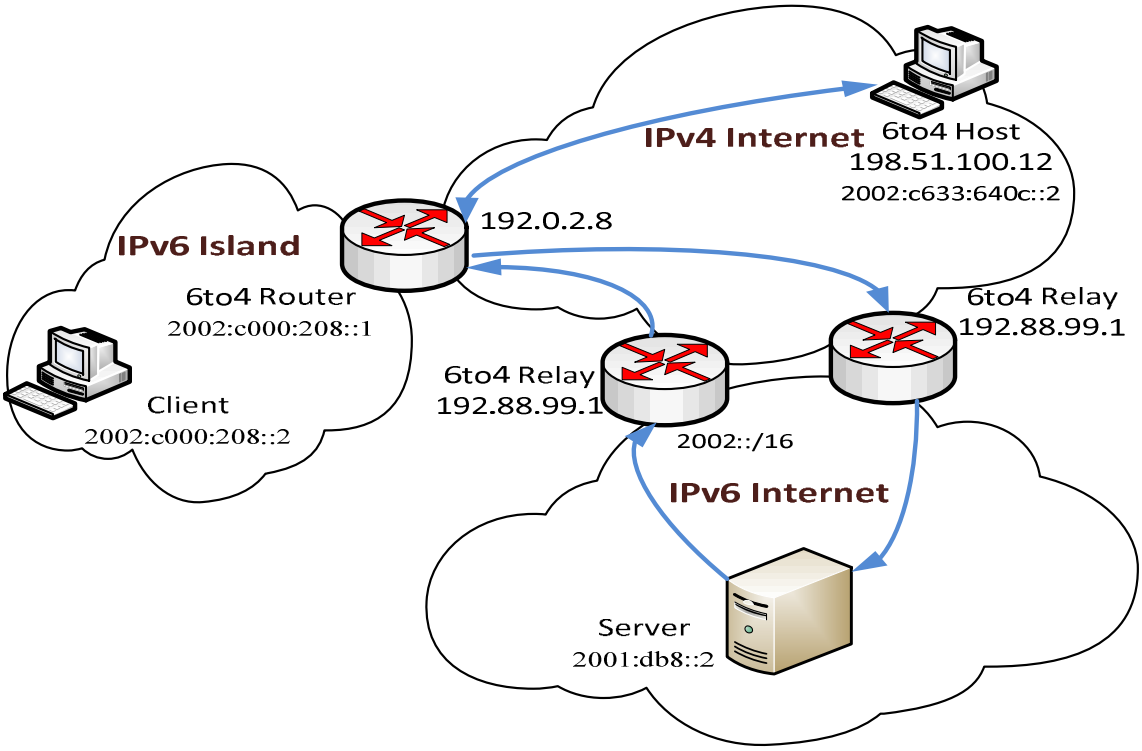
Mérési utasítás 6to4

A 6to4

A 6to4 segítségével az IPv6 képes eszközök egy csak IPv4-et támogató környezetben képesek IPv6 segítségével kommunikálni. Ehhez az RFC 3056-ban rögzített automatikus tunnelt alkalmazzák, mely a 41-es protokollazonosítót használja.

Két 6to4-es hoszt kommunikációja során a kommunikáció a két számítógép között közvetlenül IPv4-es protokoll fölött valósul meg. Ezzel szemben, ha az egyik hoszt nem 6to4-es IPv6-os címmel rendelkezik, a sikeres kommunikációhoz szükség van egy 6to4 relay igénybevételére is, melyekből több is található az interneten. Ezek a relayek anycast címzéssel érhetőek el a 192.88.99.1-es IPv4-es címen és a 6to4 tunnelben érkező csomagok kicsomagolását, és a válasz IPv6 csomagok 6to4 tunnelbe becsomagolását végzik.



Annak megállapítására, hogy egy hoszt 6to4 címet használ-e, az IPv6 cím prefixe használható. A 6to4 hosztok a 2002::/16 prefixet használják a következő formátumban:

2002::/16 prefix + publikus IPv4 cím 32 bitje + 16 bit subnet ID.

Feladatok

1. 6to4 beállítása

Mentse le a `/etc/network/interfaces` állományt a `/root` könyvtárba a

```
cp /etc/network/interfaces /root
```

paranccsal.

Állítsa be számítógépének IPv4-es címét a fixen a következő értékre: 193.224.131.133+gép sorszáma (Pl: fekete2: 193.224.131.135, fekete5: 193.224.131.138), majd állítsa be a netmask /28-as értékre, és az alapátjárót a 193.224.131.129-es címre. Ehhez a `/etc/network/interfaces` állomány módosítása szükséges, melyet elvégezhet bármelyik megismert szövegszerkesztővel. (Pl: vi editor, joe, mcedit) A módosítással egyidejűleg végezze el a 6to4 beállításokat is az állományban. Ehhez ki kell számolnia az ön IPv4-es címével használható 6to4 címet is a 6to4 leírásánál ismertetett módon. A subnet ID minden gép esetében legyen 0, a host ID, pedig 1. (Pl: fekete2: 2002:c1e0:8387::1, fekete5: 2002:c1e0:838a::1) Ha a számolás nehézséget okoz, használhatja a Debian `ipv6calc` parancsát a következő példa alapján:

```
ipv6calc --action conv6to4 193.224.131.138
```

Ha az ipv6calc nincs telepítve, úgy az `apt-get install ipv6calc` kiadásával telepítheti azt. A számítás után elvégezheti a szükséges módosításokat a megadott példa alapján (fekete6-os gép):

```
auto lo eth0 tun6to4          #Elinduló interfészek
iface eth0 inet static        #Statikus IP cím beállítás eth0 interfészen
 address 193.224.131.139      #A gép IPv4 címe
 netmask 255.255.255.240      #Netmaszk
 gateway 193.224.131.129      #Alapátjáró
iface tun6to4 inet6 v4tunnel #6to4 tunnel interfész
 address 2002:c1e0:838b::1    #6to4 IPv6 cím
 netmask 16                   #6to4 prefixhossz
 gateway ::192.88.99.1        #6to4 relay címe
 endpoint any                 #Minden 6to4 hoszttal kommunikáljon
 local 193.224.131.139        #A 6to4 tunnel helyi címe (megegyezik az IPv4
címmel)
```

Mivel a laborban van IPv6, annak használatát most le kell tiltanunk. Ehhez létre kell hozni egy `/etc/sysctl.d/ipv6.conf` állományt a következő tartalommal:

```
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.eth0.autoconf = 0
```

Ha ezzel is elkészült, indítsa újra a számítógépet.

Belépés után írassa ki az interfészeket az ifconfig paranccsal. Ha mindent jól csinált, akkor hasonló kimenetet kell kapnia:

```
eth0      Link encap:Ethernet  HWaddr 44:8a:5b:60:46:43
          inet addr:80.64.65.75  Bcast:80.64.65.127  Mask:255.255.255.192
          inet6 addr: fe80::468a:5bff:fe60:4643/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2389 errors:0 dropped:22 overruns:0 frame:0
          TX packets:1236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

```
          RX bytes:193742 (189.2 KiB)  TX bytes:118024 (115.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:276 (276.0 B)  TX bytes:276 (276.0 B)

tun6to4   Link encap:IPv6-in-IPv4
          inet6 addr: ::80.64.65.75/96 Scope:Compat
          inet6 addr: 2002:5040:414b::1/16 Scope:Global
          UP RUNNING NOARP  MTU:1480  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1572 (1.5 KiB)  TX bytes:5048 (4.9 KiB)
```

Jól látszik, hogy az eth0 interfész csak link local IPv6 címmel rendelkezik, valamint a tun6to4 interfésznek van egy 6to4-es prefixű IPv6-os címe.

2. 6to4 relay vizsgálata

Nézze meg, hogy milyen távolságra van a legközelebbi 6to4 relay. Ehhez a `traceroute 192.88.99.1` parancsot használhatja. Hány hop van az átjáróig?

3. `ping6 -c4` parancs segítségével ellenőrizze a kapcsolatot a www.bme.hu hoszt felé! Milyen átlagos válaszidőt kapott?

   `ping -c4` paranccsal is ellenőrizze a kapcsolatot! Milyen átlagos válaszidőt kapott?

   Mi lehet az oka az eltérésnek?

4. Indítson csomagelkapást a WireShark segítségével, majd nyisson egy tetszőleges web böngészőt, majd nyissa meg a http://www.kame.net honlapot. A weboldal szerint ön IPv6 protokoll segítségével csatlakozott? (Mozog a teknőc?)

   Állítsa le a csomagelkapást!

5. Keresse meg a WireShark segítségével, hogy milyen protokollazonosítót használ a 6to4! Hol találta meg?

6. Állítsa vissza az eredeti `/etc/network/interfaces` állományt, és törölje le a `/etc/sysctl.d/ipv6.conf` állományt:

```
cp /root/interfaces /etc/network/interfaces
rm /etc/sysctl.d/ipv6.conf
```

   Indítsa újra a számítógépet!

SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Mérési utasítás SSH, SCP

Mérés célja:

A távoli hozzáférést biztosító parancsok vizsgálata, működésük elsajátítása.

SSH, SCP

Az SSH távoli hozzáférést nyújt azon kiszolgálókhoz melyeken működik SSH kiszolgáló. A szokásos CLI-n (Command Line Interface) felül Linux és más UNIX-like rendszerekben lehetőség nyílik SSH tunnelezésre mellyel egy biztonságos adatcsatornát hozhatunk létre.

Az SSH-ra épül az SCP, mellyel biztonságosan másolhatunk át állományokat egyik gépről a másikra.

1. **feladat**

Hozzon létre számítógépén egy üres állományt, melynek neve az ön számítógépének neve. Ehhez a `touch` parancs használható. Pl:

```
touch fekete1
```

Lépjen be a szemben lévő fekete gépre root felhasználóként.

```
ssh root@fekete<szembengépszám>   vagy   ssh -l root fekete<szembengépszám>
```

Ha ez lesz az „első” belépés a számítógépre, akkor rákérdez a számítógép, hogy elfogadjuk-e a szemben lévő gép RSA ujjlenyomatát. Vagyis ekkor történik a kulcs csere. A kérdésre **„yes”** a válasz.
Ez után az SSH véglegesen hozzáadta a szemben lévő gép adatait a */etc/.ssh/known_hosts* fájlhoz.
A root jelszót megadva lépjünk be a gépre!

(Amennyiben nem lép be, úgy a szemben lévő gép bontotta a kapcsolatot, amíg a feladatot olvasta; kérem lépjen be újra! Ekkor már nem fog semmit kérdezni, hisz az előbb már engedélyeztük a kapcsolódást.)

Ezek után root jogokkal felvértezve adhatunk ki parancsot a másik gépen.

2. **feladat**

Nyisson meg egy másik terminált számítógépén, majd ebben másolja át a szemben lévő gépre az 1-es pontban létrehozott állományt.

```
scp /root/fekete<sajátgépszám> root@fekete<szembengépszám>:/root/
```

Térjen vissza abba a terminál ablakba, melyben az SSH-t futtatta. ls parancs segítségével nézze meg, hogy sikeres volt-e a másolás. Majd távolítsa el az állományt!

```
ls -lh
```

```
rm fekete<sajátgépszám>
```

3. feladat.

A mérés végeztével töröljük ki a host információkat a saját gépen /root/.ssh/known_hosts fájlból, hogy a következő mérésen is az „első” belépést tudjuk szimulálni.

echo > /root/.ssh/known_hosts