A feladat

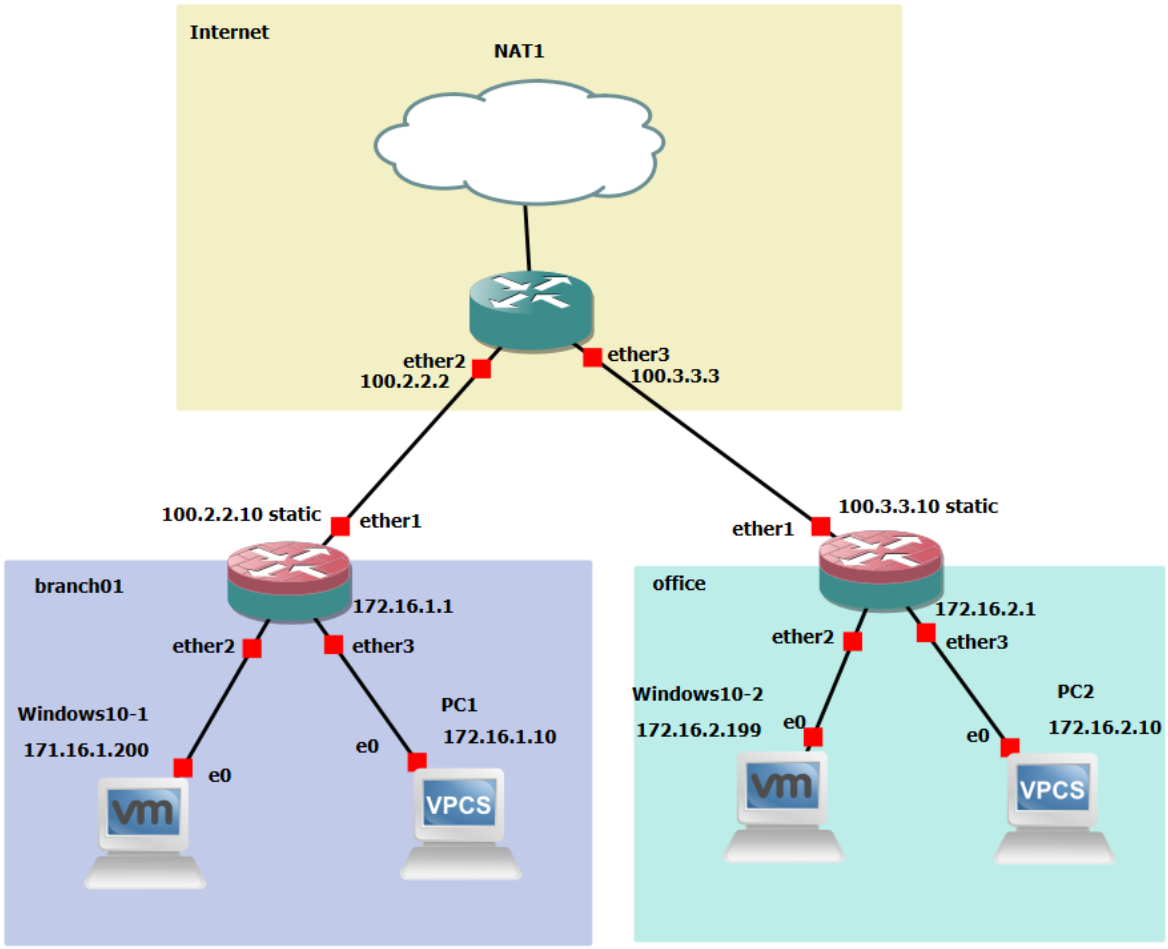
Ebben a példában egy olyan hálózatot veszünk alapul, ahol két külön site (telephely) van. Mindkettő külön internet kapcsolattal rendelkezik. Mindkét site egy MikroTik router-en keresztül kapcsolódik az internetre. Az a célunk, hogy a router-ek mögötti két LAN-t összekapcsoljuk egymással, a következő módon:

- A broadcast üzenetek ne menjenek át egyik LAN-ból a másikba.
- Az egyik LAN-ból elérhető legyen a másik, és fordítva.
- A két LAN egy olyan alagúton keresztül legyen összekötve, ami a lehető legnagyobb biztonságot nyújtja, lehetőleg hatékonyan (nagy sebességgel).

Ez a felállás gyakran előfordul például olyan cégeknél, amik több telephellyel rendelkeznek. Az egyik site lehet például a központi iroda, a másik egy raktár vagy egy gyár/üzem stb. Ez a modell később könnyen kiegészíthető három vagy még több site összekapcsolására.

Példa hálózat

A példa hálózatban a két site neve `branch01` és `office`. Ezek egy vállalat két telephelyét jelképezik. Az office a központi iroda.



Internet kapcsolat

Az internetet egy olyan routerrel szimuláltam, ami különböző alhálózatokat ad az összes portjára. Az ether2 portjára 100.2.2.2/24, az ether3 portjára 100.3.3.3/24 az ether4 portjára 100.4.4.4/24 stb. Ezekre a portokra DHCP szervereket is beállítottam. (Az igazi internet felé az ether1-internet nevű porttal csatlakozik egy VMWare NAT adapterhez, ez az ábrán egy felhőként jelenik meg.) Ez a router úgy van beállítva, hogy az alhálózatok között korlátozás nélkül minden csomagot továbbít. Felfoghatjuk ezt a router-t úgy, mint az internet szolgáltató (ISP) távoli elérési pontja.

Tehát bármely hozzá csatlakozó eszköz másik címet kap, ráadásul másik alhálózatban. Ez nagyon hasonló ahhoz, mint amikor az egyes site-ok különböző ISP-n keresztül különböző címtartományban levő "nyilvános" címeket kapnak. Ezek "nyilvánosak" olyan értelemben, hogy az internetet reprezentáló router korlátozás nélkül továbbítja a csomagokat minden ilyen nyilvános cím között. Ez a felépítés azért is jó, mert így bármelyik "internet" felé menő illetve onnan érkező csomagot egyszerűen meg lehet vizsgálni (pl. wireshark-kal), ez könnyűvé teszi a tesztelést.

Az "internet router"-nek ez a kezdeti konfigurációja:

```
/interface ethernet
set [ find default-name=ether1 ] name=ether1-internet
/interface list
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=pool-2 ranges=100.2.2.100-100.2.2.200
add name=pool-3 ranges=100.3.3.100-100.3.3.200
add name=pool-4 ranges=100.4.4.100-100.4.4.200
add name=pool-5 ranges=100.5.5.100-100.5.5.200
/ip dhcp-server
add address-pool=pool-2 disabled=no interface=ether2 name=dhcp-eth2
add address-pool=pool-3 disabled=no interface=ether3 name=dhcp-eth3
add address-pool=pool-4 disabled=no interface=ether4 name=dhcp-eth4
add address-pool=pool-5 disabled=no interface=ether5 name=dhcp-eth5
/interface list member
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
/ip address
add address=100.2.2.2/24 interface=ether2 network=100.2.2.0
add address=100.3.3.3/24 interface=ether3 network=100.3.3.0
add address=100.4.4.4/24 interface=ether4 network=100.4.4.0
add address=100.5.5.5/24 interface=ether5 network=100.5.5.0
/ip dhcp-client
add disabled=no interface=ether1-internet
/ip dhcp-server network
add address=100.2.2.0/24 dns-server=100.2.2.2 gateway=100.2.2.2
add address=100.3.3.0/24 dns-server=100.3.3.3 gateway=100.3.3.3
add address=100.4.4.0/24 dns-server=100.4.4.4 gateway=100.4.4.4
add address=100.5.5.0/24 dns-server=100.5.5.5 gateway=100.5.5.5
/ip dns
set allow-remote-requests=yes servers=1.1.1.1,1.0.0.1
/ip firewall nat
add action=accept chain=srcnat disabled=yes out-interface-list=LAN
add action=masquerade chain=srcnat out-interface=ether1-internet
/system identity
```

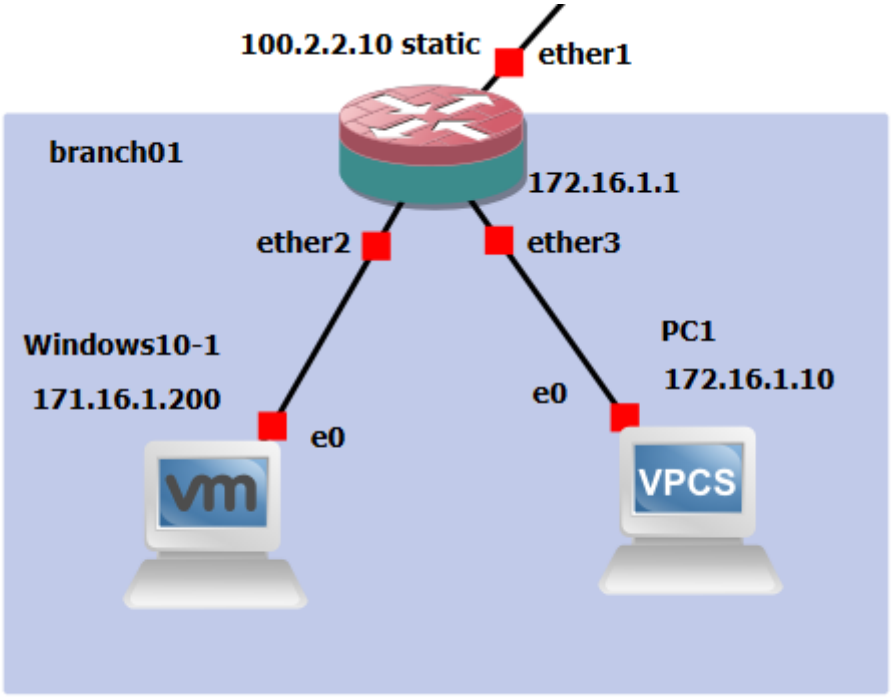
```
set name=internet-routeros
```

Site-ok kezdeti állapota

A két darab site neve `branch01` és `office`. Az első példában azt feltételezzük, hogy a site-ok tetején levő router-ek fix, statikus címeket kapnak. Egy későbbi példában be fogom mutatni azt is, hogy hogyan lehet ezt megoldani dinamikusan változó címek esetén.

Teszt branch01

A "nyilvános" címe az "internet" felé 100.2.2.10. A belső LAN hálózat címe 172.16.1.0/24, ezen belül a router címe 172.16.1.1.



A `branch01` kezdeti konfigurációja a következő:

```
/interface bridge
add name=bridge-branch01
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=pool-branch ranges=172.16.1.100-172.16.1.200
/ip dhcp-server
add address-pool=pool-branch disabled=no interface=bridge-branch01 name=dhcp-branch01
/interface bridge port
```

```
add bridge=bridge-branch01 interface=ether2
add bridge=bridge-branch01 interface=ether3
/ip address
add address=172.16.1.1/24 interface=bridge-branch01 network=172.16.1.0
add address=100.2.2.10/24 interface=ether1 network=100.2.2.0
/ip dhcp-server network
add address=172.16.1.0/24 dns-server=172.16.1.1 gateway=172.16.1.1
/ip dns
set allow-remote-requests=yes servers=1.1.1.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/ip route
add distance=1 gateway=100.2.2.2
/system identity
set name=routeros-branch01
```

> Fontos látni, hogy ez a teszt router a masquerade-on kívül semmiféle tűzfal szabályt nem tartalmaz. Ez a tesztelés alatt megfelelő. **Éles környezetben be kell állítani tűzfal szabályokat.** Egy példa beállítást a cikkben később közzéteszek.

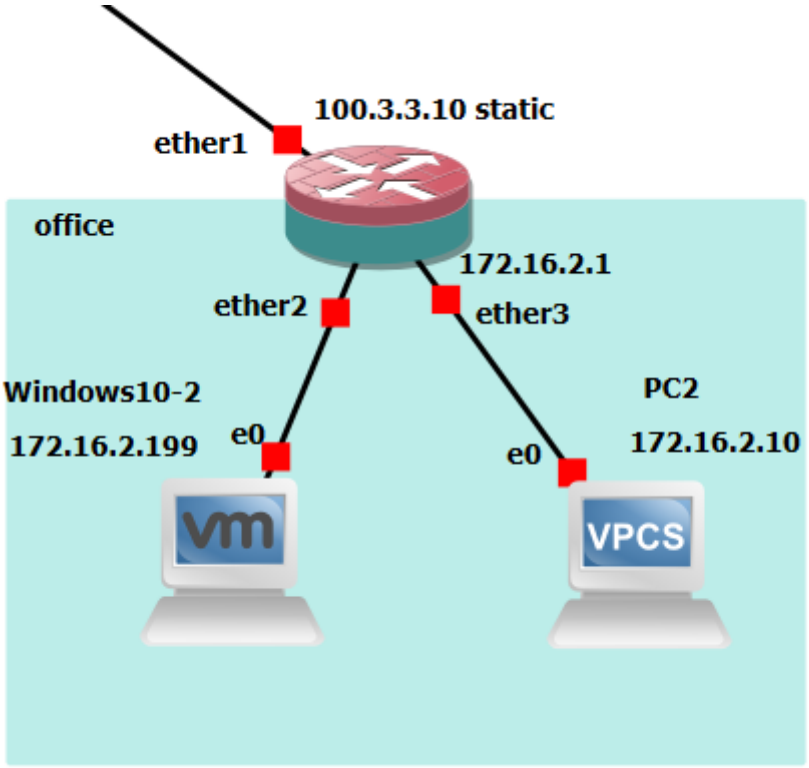
A `branch01` hálózaton belülre tettem egy Windows 10 és egy virtuális teszt PC gépet. Ezek címei:

- 172.16.1.200 a windows gépnek, dinamikus címmel
- 172.16.1.10 a virtual PC-nek, statikus címmel

Az alagutat elsősorban a virtual pc-vel teszteltem. Ennek oka, hogy egyszerre sok Windows 10 VM indítása annyira leterhelte a host gépet, hogy ez sok esetben csomagvesztéshez vezetett, és elérhetetlennek látszódtak olyan kapcsolatok, amik normál esetben működtek volna. A Windows 10 gépeket általában csak a router-ek konfigurálásának idejére kapcsoltam be.

Teszt office

Ez nagyon hasonló a `branch01`-hez, csak az alhálózatok címei térnek el:



A "nyilvános" címe az "internet" felé 100.3.3.10. A belső LAN hálózat címe 172.16.2.0/24, ezen belül a router címe 172.16.2.1.

Itt a teljes (kezdeti) konfigurációja, alig több mint 20 sor:

```
/interface bridge
add name=bridge-office
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=pool-office ranges=172.16.2.100-172.16.2.200
/ip dhcp-server
add address-pool=pool-office disabled=no interface=bridge-office name=dhcp-office
/interface bridge port
add bridge=bridge-office interface=ether2
add bridge=bridge-office interface=ether3
/ip address
add address=172.16.2.1/24 interface=bridge-office network=172.16.2.0
add address=100.3.3.10/24 interface=ether1 network=100.3.3.0
/ip dhcp-server network
add address=172.16.2.0/24 dns-server=172.16.2.1 gateway=172.16.2.1
/ip dns
set allow-remote-requests=yes servers=1.1.1.1
```

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/ip route
add distance=1 gateway=100.3.3.3
/system identity
set name=routeros-office
```

Az `office` hálózaton belülre is tettem egy Windows 10 és egy teszt PC gépet. Ezek címei:

- 172.16.2.199 a windows gépnek, dinamikus címmel
- 172.16.2.10 a virtual PC-nek, statikus címmel

Revision #10
Created 2 January 2021 17:47:48 by Gandalf
Updated 9 January 2021 13:13:08 by Gandalf