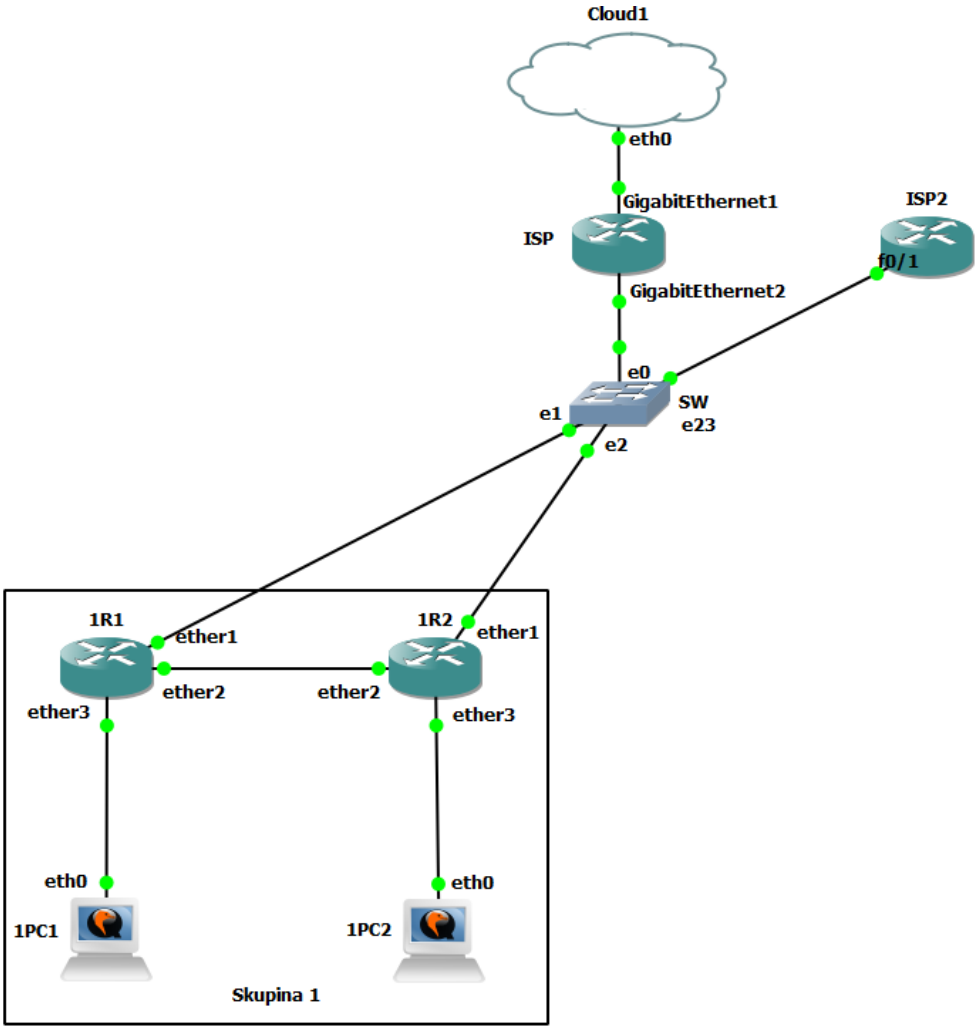
PS2 / Cvičenie 10 / **Mikrotik**

Topológia

Pracuje sa v dvojiciach v **1 spoločnej** topológii, dvojica konfiguruje zariadenia vo vyznačenom štvorci.

- Pri práci v GNS3:
  - Učiteľ naklonuje topológiu (**1x**): PS2-lab10-Mikrotik--TEMPLATE (v GNS3), a použije podľa možnosti názov pre klon: *PS2-lab10-Mikrotik-**MK-2023***, kde MK sú iniciály cvičiaceho (napr. MK pre Martin Kontšek) na danom termíne cvičenia, a za 2023 tam treba dosadiť aktuálny rok, kedy sa realizuje dané cvičenie.
  - Upozornenie: TEMPLATE topológia sa nesmie spúšťať, len klonovať/duplikovať !
- Pri práci na reálnych zariadeniach:
  - Topológia je rovnaká, na reálnych zariadeniach treba spraviť „system reset“ pomocou príkazu:
    `/system/reset-configuration no-defaults=yes skip-backup=yes`



Príklad odporúčanej IP adresácie (vzor pre skupinu 1)

Device	Interface	IP Address	Subnet Mask	Default Gateway
1R1	ether1	získaná cez PPPoE (rozsah 192.168.1.0/24)		
	ether2	10.1.12.1	255.255.255.0	N/A
	ether3	10.1.1.1	255.255.255.0	N/A
	lo0	10.1.111.1	255.255.255.0	N/A
1R2	ether1	získaná cez PPPoE (rozsah 192.168.1.0/24)		
	ether2	10.1.12.2	255.255.255.0	N/A
	ether3	10.1.2.1	255.255.255.0	N/A
	lo0	10.1.222.2	255.255.255.0	N/A
1PC1	eth0	od DHCP servera		
1PC2	eth0	od DHCP servera		

Postup:

1. **Základná konfigurácia:**
   a. Nakreslite si topológiu na papier (aspoň jeden za dvojicu) a rozdeľte si pridelený IPv4 rozsah 10.#.0.0/24. Všetko si zaznačte do obrázku s topológiou.
   b. Pripojte sa na router pomocou konzoly z GNS3. (login admin, bez hesla)
      i. Upozornenie: Niekedy sa stáva, že konzola začne príkazy vypisovať štýlom jeden znak na jeden riadok. Vtedy pomôže viac krát po sebe vypnúť a zapnúť smerovač.
   c. Zistite HW a SW informácie o smerovači, na ktorom ste pripojení:
      ```
      system resource print
      ```
      i. Aká verzia RouterOS tam je, koľko máte RAM, akú architektúru CPU?
   d. Odporúčanie: všetky konfiguračné zmeny si overujte pomocou print príkazov, napr:
      ```
      ip address print
      ```
   e. Vymažeme konfiguráciu DHCP klienta na rozhraní ether1
      ```
      ip dhcp-client remove 0
      ```
   f. Na rozhraní smerovača R1 smerom k hlavnému prepínaču MAIN ip nenastavujte, neskôr ju získate cez PPPoE. Nakonfigurujte ale ostatné IP adresy.
   g. Nastavte hostnames #R1, #R2, za # dajte číslo skupiny.
   h. Zmeňte heslo pre používateľa admin (napríklad na: class)
   i. Zakážte nepotrebné manažment služby v časti IP services (telnet, ftp, api, api-ssl)
   j. Vypíšte si celú doterajšiu konfiguráciu (príkaz `/export`) a skontrolujte, či obsahuje zadané konfiguračné príkazy
   k. Overte, či cez protokol CDP (alebo LLDP/MNDP) vidíte susedné smerovače. Mali by ste ich vidieť za rozhraniami podľa topológie a taktiež ich IP adresu nakonfigurovanú na rozhraní k vám (`ip neighbor print detail`).
2. **DHCPv4**
   a. Nastavte DHCP server na vašom smerovači
      i. R1, R2 – vytvorte pool pre počítače na priamo pripojeniej sieti
      ii. R1, R2 – vytvorte definíciu siete pre dhcp server a zadefinujte gateway a ľubovoľný verejný DNS server
      iii. R1, R2 – vytvorte definíciu samotného DHCP servera na rozhraní vedúcemu ku klientovi (ether3) a priraďte mu pool

b. Nakonfigurujte počítač na získanie adresy z DHCP a na PC overte získanie IP z poolu. Získavanie adresy cez DHCP by malo byť defaultne nastavené, pri problémoch:
v /etc/network/interfaces, nad ostatnú konfiguráciu pre eth0:
```
auto eth0
```
a pridať:
```
iface eth0 inet dhcp
```
c. R1,R2 – overte pridelenie IP cez DHCP (zobrazte Lease)
d. Overte IP konektivitu medzi routrami a medzi PC a GW.
e. Overte, či cez protokol CDP vidíte počítač (`ip neighbor print detail`).

3. PPPoE

a. V tejto úlohe je potrebná konfigurácia na ISP smerovači, preto najrýchlejšia skupina vloží na ISP 1 a 2 config, korý je na konci tohto dokumentu, a dá vedieť ostatným, že je to pripravené. Je vysoko odporúčané, aby si každý pozrel daný config, čo obsahuje.
b. Na R1 a R2 pridajte nakonfigurujte PPPoE klienta (pridajte rozhranie typu pppoe-client) na rozhraní ***ether1***, povoľte ***chap*** a ***pap*** autentifikáciu, povoľte získanie ***default route*** a ***dns*** a výsledné rozhranie nazvite „***wan***“. Ako meno použite **hostname** smerovača a heslo „***Mi1krotik1login***“.
c. Zistite, či sa pppoe spojenie zostavilo.
d. Zo smerovačov otestujte konektivitu na 1.1.1.1 (loopback na ISP2) – mala by byť úspešná
e. Zo smerovačov otestujte konektivitu na 8.8.8.8 – mala by byť neúspešná
f. Preskúmajte smerovaciu tabuľku na R1 a R2. Vidíte tam default route?
g. Odstráňte konfiguráciu PPPoE klienta z R1 aj R2.

4. WinBox, SSH, WebFig

a. Na rozhranie ether1 na smerovačoch R1 a R2 nakonfigurujte statickú IP v tvare: 192.168.1.#R/24 – kde # je číslo skupiny a R číslo smerovača.
b. Pridajte statickú default route na next hop 192.168.1.1
c. Nakonfigurujte adresu DNS servera na 9.9.9.9.
d. Otestujte konektivitu na internet zo smerovačov R1 a R2
    i. IP aj DNS
e. Pripojte sa na smerovače R1 a R2 pomocou nástroja Winbox:
    i. Stiahnite Winbox so stránky mikrotik.com (sekcia Software) https://mt.lv/winbox64
    ii. Ako adresu zadajte „VEREJNA_IP_F0/0_ISP:111#R”, kde:
        - VEREJNA_IP_F0/0_ISP – zistí najrýchlejšia skupina na ISP, a oznámi ostatným skupinám (IP na rozhraní f0/0 ISP smerovača z rozsahu 158.193.152.0)
        - # - číslo skupiny
        - R – číslo smerovača
    iii. Meno a heslo použite konto admin, ktoré ste nastavovali v úlohe 1.h.
    iv. Po pripojení si pozrite stavy rozhraní a nakonfigurované IP adresy, alebo iné, doteraz nakonfigurované položky.
    v. Vyskúšajte si otvoriť z hlavného menu Terminál, v ktorom môžete zadávať príkazy ako do konzoly
    vi. Preskúmajte, či nie sú dostupné aktualizácie RouterOS a aké verzie RouterOS sú dostupné v jednotlivých vetvách (vetva = Channel).
f. Pripojte sa na smerovače R1 a R2 pomocou SSH (napr. pomocou Putty)
    i. IP: VEREJNA_IP_F0/0_ISP
    ii. port: 222#R
    iii. Meno a heslo použite konto admin, ktoré ste nastavovali v úlohe 1.h.

iv. Ďalšie úlohy môžete vypracovávať aj pomocou SSH pripojenia

g. Pripojte sa na smerovače R1 a R2 pomocou nástroja WebFig.
   i. vo webovom prehliadači zadajte url: http://VEREJNA_IP_F0/0_ISP:333#R
   ii. Meno a heslo použite konto admin, ktoré ste nastavovali v úlohe 1.h.
   iii. Preskúmajte nástroj WebFig.

5. NAT

a. Na **R1** a **R2** nastavte **NAT** pre odchádzajúce pakety **do Internetu – PAT s preťažením rozhrania (ether1)** pre privátnu sieť, na ktorej sa nachádza počítač
b. Otestujte konektivitu na internet z počítača.

6. OSPFv2

a. Nakonfigurujte OSPFv2 medzi smerovačmi R1 a R2, nastavte router-id na 1.1.1.1(R1) a 2.2.2.2(R2), pričom do procesu pridajte sieť medzi smerovačmi ako aj siete vedúce k PC. Pozor!: na rozdiel informácii v prednáške, ktoré sú pre RouterOS v6, vo verzii 7.1, ktorú máte na cvičení, je potrebné OSPFv2 konfigurovať nasledovne:
   i. inštanciu ospf je treba vytvoriť. Default inštancia tam nie je.
   ```
   routing ospf instance add name=default router-id=1.1.1.1 disabled=no
   ```
   ii. vytvoriť OSPF oblasť 0:
   ```
   routing ospf area add instance=default name=backbone area-id=0.0.0.0
   ```
   iii. pridať siete do OSPF procesu
   ```
   routing ospf interface-template add network=10.1.1.0/24 area=backbone
   routing ospf interface-template add network=10.1.12.0/24 area=backbone
   ```
b. Overte konektivitu medzi PC1 a PC2.
c. Skontrolujte, či sú požadované smerovacie záznamy naučené cez OSPF v smerovacej tabuľke
d. Preskúmajte OSFP tabuľku.
e. Viac informácii o smerovacích protokoloch v RouterOS v7 nájdete tu: https://help.mikrotik.com/docs/display/ROS/ROSv7+Basic+Routing+Examples

7. Firewall – dobrovoľná úloha (nie je v prednáške)

Návody:
https://help.mikrotik.com/docs/display/ROS/Building+Your+First+Firewall
https://help.mikrotik.com/docs/display/ROS/Basic+Concepts
https://help.mikrotik.com/docs/display/ROS/Filter

Každý na svojom smerovači premyslite konfiguráciu Firewallu tak, aby:

a. Smerom von zo siete, kde je PC boli povolené z aplikačných služieb iba:
   i. HTTPs kamkoľvek
   ii. ICMP kamkoľvek
   iii. SSH iba na internet a na lokálny smerovač (PC1 na R1)
   iv. Nezabudni zvážiť, čo všetko ti v sieti okrem toho ešte beží, a je nutné, aby to ACL neblokoval, ale povoľoval:
      - Hints:
         - Klienti dostávajú IPv4 adresy dynamicky
         - Chcete využívať pri browsovaní aj doménové mená
         - Prípadne iné...?
b. Smerom dnu do vnútornej siete: len už vytvorené spojenia (established)
c. Ochrániť smerovač samotný: povoliť dnu len SSH, WinBox, WebFig a už vytvorené spojenia z vnútra

Konfigurácia ISP

```
conf t
hostname ISP

int gi1
 ip add dhcp
 ip nat outside
 no shut

int gi2
 ip add 192.168.1.1 255.255.255.0
 ip nat inside
 no shut

access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitEthernet 1 overload

ip nat inside source static tcp 192.168.1.11 8291 interface gi 1 11111
ip nat inside source static tcp 192.168.1.11 22 interface gi 1 22211
ip nat inside source static tcp 192.168.1.11 80 interface gi 1 33311
ip nat inside source static tcp 192.168.1.12 8291 interface gi 1 11112
ip nat inside source static tcp 192.168.1.12 22 interface gi 1 22212
ip nat inside source static tcp 192.168.1.12 80 interface gi 1 33312
ip nat inside source static tcp 192.168.1.21 8291 interface gi 1 11121
ip nat inside source static tcp 192.168.1.21 22 interface gi 1 22221
ip nat inside source static tcp 192.168.1.21 80 interface gi 1 33321
ip nat inside source static tcp 192.168.1.22 8291 interface gi 1 11122
ip nat inside source static tcp 192.168.1.22 22 interface gi 1 22222
ip nat inside source static tcp 192.168.1.22 80 interface gi 1 33322
ip nat inside source static tcp 192.168.1.31 8291 interface gi 1 11131
ip nat inside source static tcp 192.168.1.31 22 interface gi 1 22231
ip nat inside source static tcp 192.168.1.31 80 interface gi 1 33331
ip nat inside source static tcp 192.168.1.32 8291 interface gi 1 11132
ip nat inside source static tcp 192.168.1.32 22 interface gi 1 22232
ip nat inside source static tcp 192.168.1.32 80 interface gi 1 33332
ip nat inside source static tcp 192.168.1.41 8291 interface gi 1 11141
ip nat inside source static tcp 192.168.1.41 22 interface gi 1 22241
ip nat inside source static tcp 192.168.1.41 80 interface gi 1 33341
ip nat inside source static tcp 192.168.1.42 8291 interface gi 1 11142
ip nat inside source static tcp 192.168.1.42 22 interface gi 1 22242
ip nat inside source static tcp 192.168.1.42 80 interface gi 1 33342
ip nat inside source static tcp 192.168.1.51 8291 interface gi 1 11151
ip nat inside source static tcp 192.168.1.51 22 interface gi 1 22251
ip nat inside source static tcp 192.168.1.51 80 interface gi 1 33351
ip nat inside source static tcp 192.168.1.52 8291 interface gi 1 11152
ip nat inside source static tcp 192.168.1.52 22 interface gi 1 22252
ip nat inside source static tcp 192.168.1.52 80 interface gi 1 33352
ip nat inside source static tcp 192.168.1.61 8291 interface gi 1 11161
ip nat inside source static tcp 192.168.1.61 22 interface gi 1 22261
ip nat inside source static tcp 192.168.1.61 80 interface gi 1 33361
ip nat inside source static tcp 192.168.1.62 8291 interface gi 1 11162
ip nat inside source static tcp 192.168.1.62 22 interface gi 1 22262
ip nat inside source static tcp 192.168.1.62 80 interface gi 1 33362
ip nat inside source static tcp 192.168.1.71 8291 interface gi 1 11171
ip nat inside source static tcp 192.168.1.71 22 interface gi 1 22271
```

```
ip nat inside source static tcp 192.168.1.71 80 interface gi 1 33371
ip nat inside source static tcp 192.168.1.72 8291 interface gi 1 11172
ip nat inside source static tcp 192.168.1.72 22 interface gi 1 22272
ip nat inside source static tcp 192.168.1.72 80 interface gi 1 33372
ip nat inside source static tcp 192.168.1.81 8291 interface gi 1 11181
ip nat inside source static tcp 192.168.1.81 22 interface gi 1 22281
ip nat inside source static tcp 192.168.1.81 80 interface gi 1 33381
ip nat inside source static tcp 192.168.1.82 8291 interface gi 1 11182
ip nat inside source static tcp 192.168.1.82 22 interface gi 1 22282
ip nat inside source static tcp 192.168.1.82 80 interface gi 1 33382
ip nat inside source static tcp 192.168.1.91 8291 interface gi 1 11191
ip nat inside source static tcp 192.168.1.91 22 interface gi 1 22291
ip nat inside source static tcp 192.168.1.91 80 interface gi 1 33391
ip nat inside source static tcp 192.168.1.92 8291 interface gi 1 11192
ip nat inside source static tcp 192.168.1.92 22 interface gi 1 22292
ip nat inside source static tcp 192.168.1.92 80 interface gi 1 33392

lldp run
```

Konfigurácia ISP2

```
conf t

int lo0
 ip add 192.168.1.1 255.255.255.255

int lo1
 ip add 1.1.1.1 255.255.255.255

ip local pool BAZEN 192.168.1.10 192.168.1.50

int Virtual-Template 1
 ip unnumbered Loopback 0
 peer default ip address pool BAZEN
 mtu 1492
 ppp mtu adaptive
 ip tcp adjust-mss 1452
 ppp ipcp dns 9.9.9.9
 ppp authentication pap chap
 exit

bba-group pppoe global
 virtual-template 1
 exit

int fa0/1
 pppoe enable group global
 no shut

username 1R1 privilege 15 password Mi1krotik1login
username 1R2 privilege 15 password Mi1krotik1login
username 2R1 privilege 15 password Mi1krotik1login
username 2R2 privilege 15 password Mi1krotik1login
username 3R1 privilege 15 password Mi1krotik1login
username 3R2 privilege 15 password Mi1krotik1login
username 4R1 privilege 15 password Mi1krotik1login
username 4R2 privilege 15 password Mi1krotik1login
username 5R1 privilege 15 password Mi1krotik1login
username 5R2 privilege 15 password Mi1krotik1login
username 6R1 privilege 15 password Mi1krotik1login
```

```
username 6R2 privilege 15 password Mi1krotik1login
username 7R1 privilege 15 password Mi1krotik1login
username 7R2 privilege 15 password Mi1krotik1login
username 8R1 privilege 15 password Mi1krotik1login
username 8R2 privilege 15 password Mi1krotik1login
username 9R1 privilege 15 password Mi1krotik1login
username 9R2 privilege 15 password Mi1krotik1login
username 10R1 privilege 15 password Mi1krotik1login
username 10R2 privilege 15 password Mi1krotik1login
```