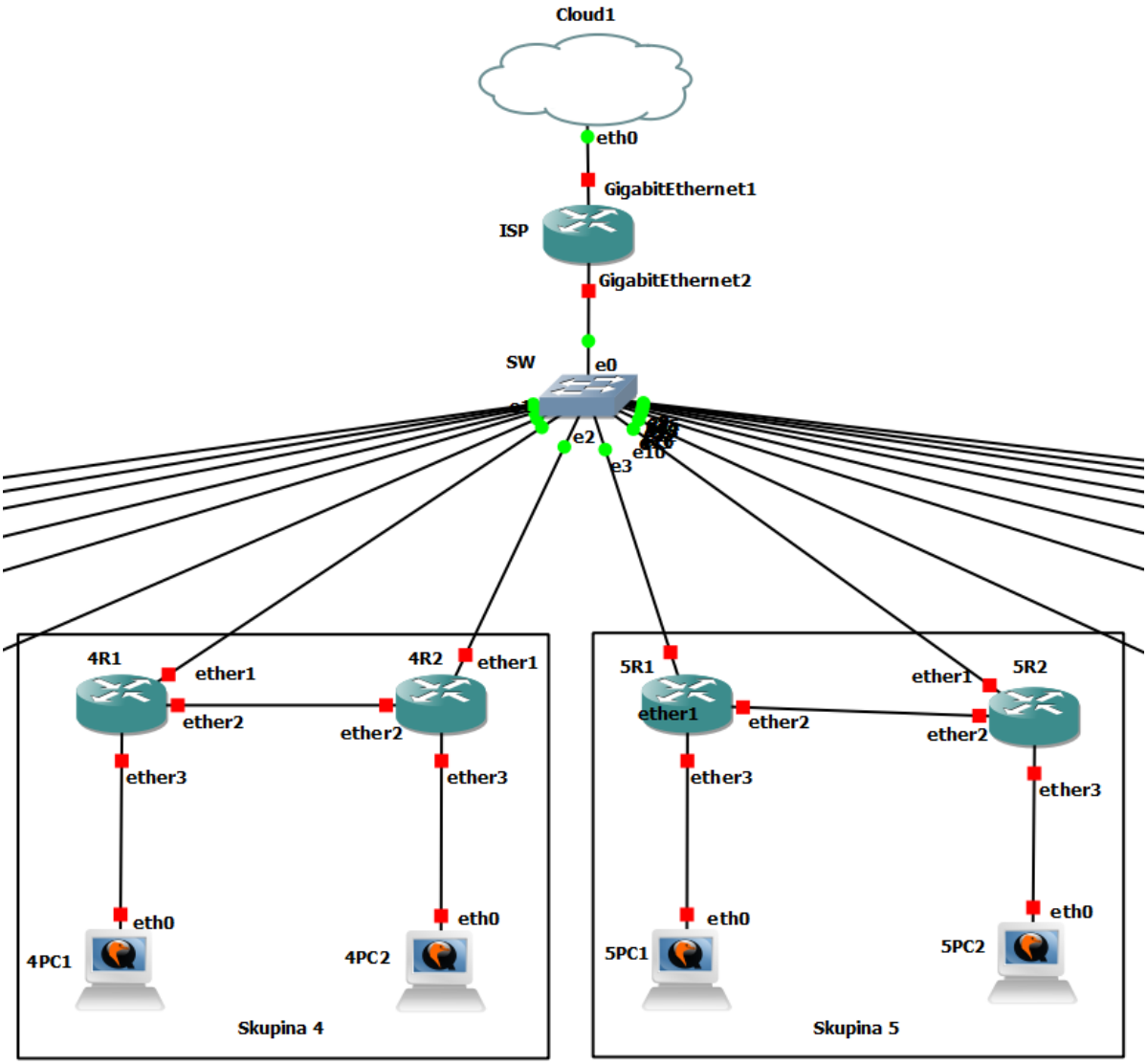
PS2 / Cvičenie 11 / **Sieťová automatizácia**

Topológia

Pracuje sa v **dvojiciach** (pri nepárnom počte študentov pracuje jeden študent sám).
R1 a R2 sú v každej skupine **Mikrotik** smerovače, ISP je **Cisco** smerovač.

Učiteľ naklonuje **1x** topológiu: kontsek-2021-PS2-CV11-Automatizacia-vzor
(v GNS3, všetci pracujú v jednej topoĺogii)

Učiteľ si môže všetky vytvorené žiadosti do Postmanu naimportovať zo súborov
„PS2_cv11_LAB_Automatizacia_2021_04_28_MK-cisco.postman_collection“ a
„PS2_cv11_LAB_Automatizacia_2021_04_28_MK-mikrotik.postman_collection“ (návod v úlohe 1.h).
Pozor ale na IP a port v jednotlivých žiadostiach.



Príklad odporúčanej IP adresácie (vzor pre skupinu 1)

Device	Interface	IP Address	Subnet Mask	Default Gateway
1R1	ether1	192.168.1.11	255.255.255.0	192.168.1.1
	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	192.168.1.12	255.255.255.0	192.168.1.1
	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		

Obsah

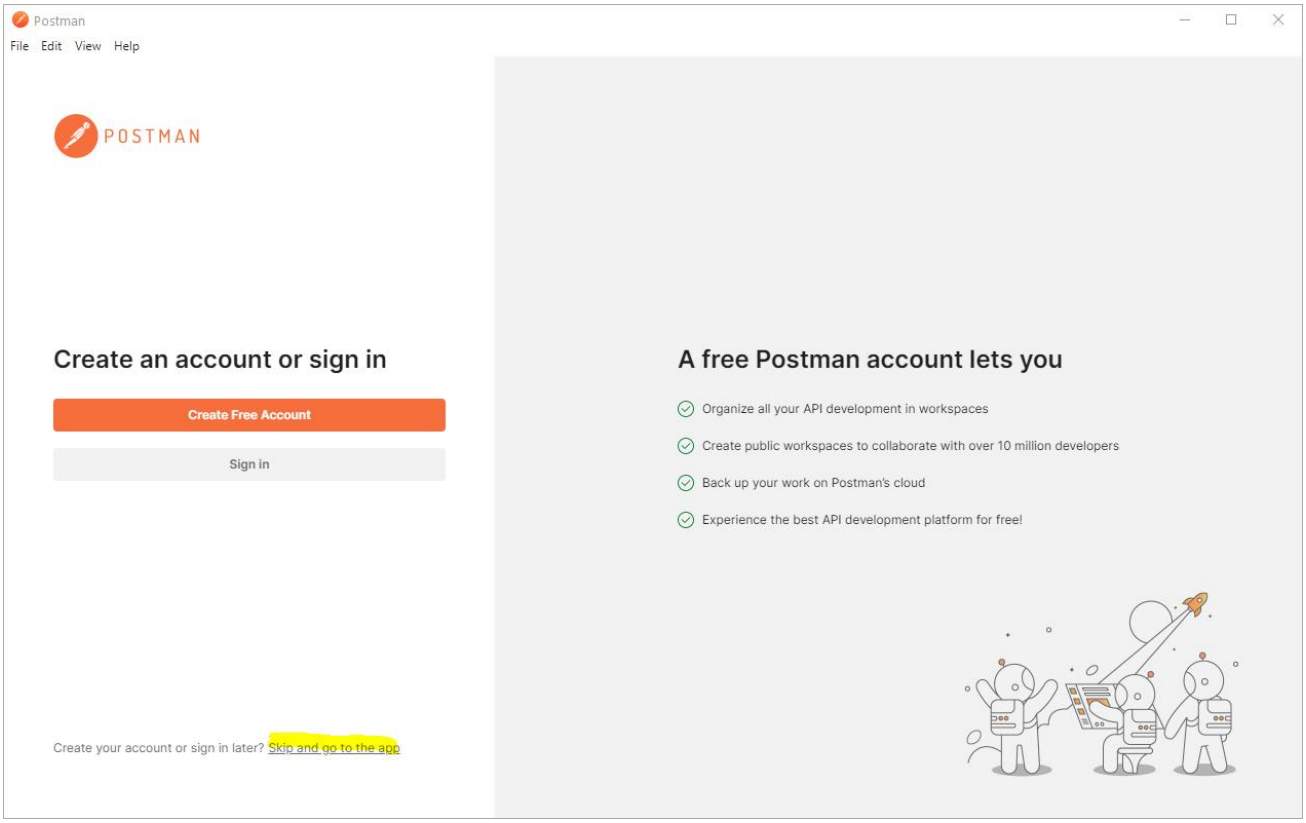
Postup:

0. Konfigurácia ISP a pridanie mien do topológie

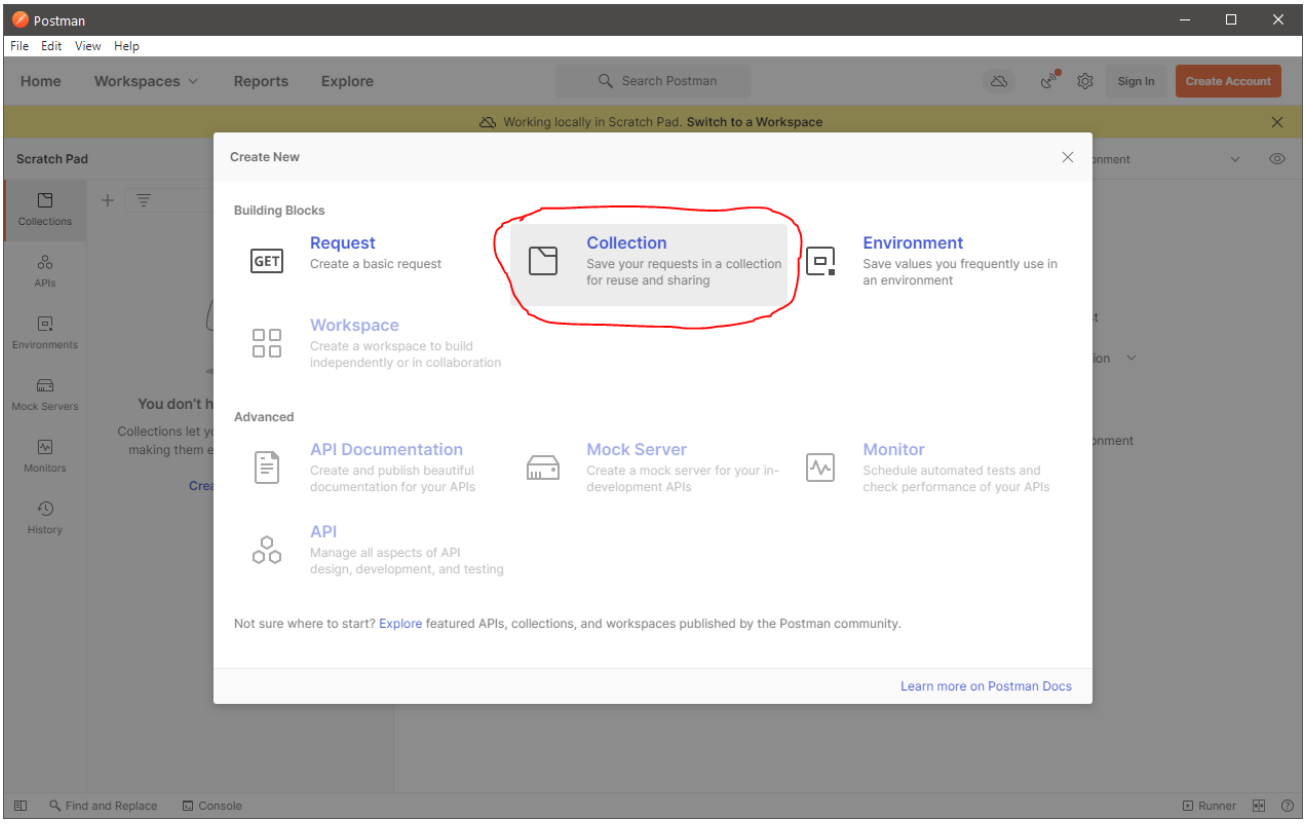
a. Najrýchlejšia skupina nahrá na ISP konfiguráciu, ktorá je na konci tohto zadania a dá vedieť ostatným, že je hotové.
b. Každý si pridá pod svoju časť topológie mená ľudí, ktorí robia spolu v skupine

1. Inštalácia nástroja Postman

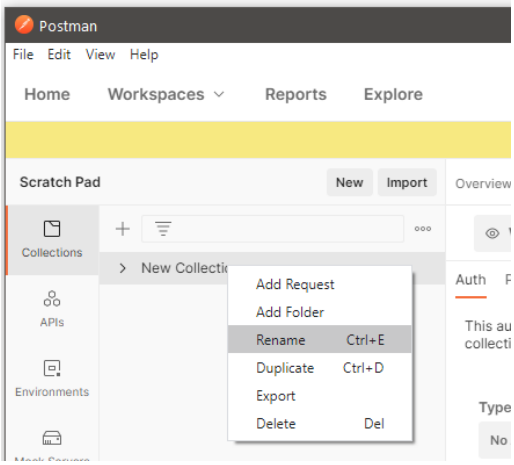
a. Stiahnite si nástroj Postman z adresy https://www.postman.com/downloads/
   i. Ak sa vám zobrazila prázdna stránka, vyskúšajte stránku otvoriť v inom prehliadači.
   ii. Alebo použite tento link pre 64-bit verziu Postmanu na Windows: https://dl.pstmn.io/download/latest/win64
b. Nainštalujte nástroj Postman otvorením inštalačného súboru a následne ho spustite.
c. Po spustení nie je potrebné vytvárať bezplatný účet (jeho doplnkové funkcie nebudeme používať). Stačí kliknúť na voľbu „Skip and go to the app“.



d. V hlavnom okne si vytvorte 2 kolekcie s názvami Cisco a Mikrotik. Kolekciu vytvoríte pomocou tlačidla New -> Collection.



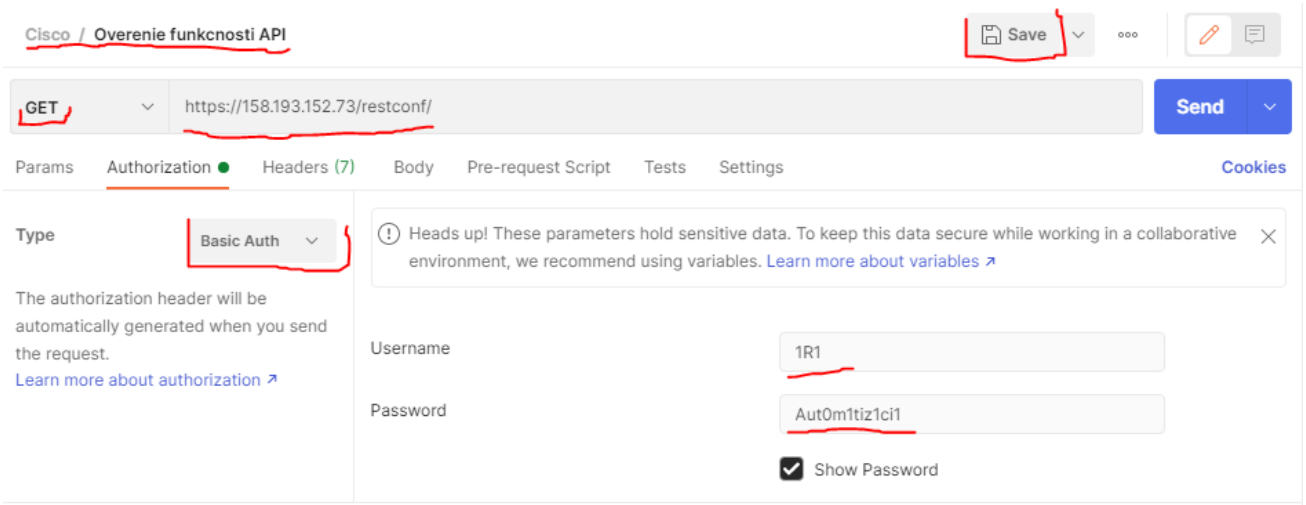
e. Vytvorenú kolekciu premenujete pravým kliknutím na názov kolekcie a výberom voľby Rename.



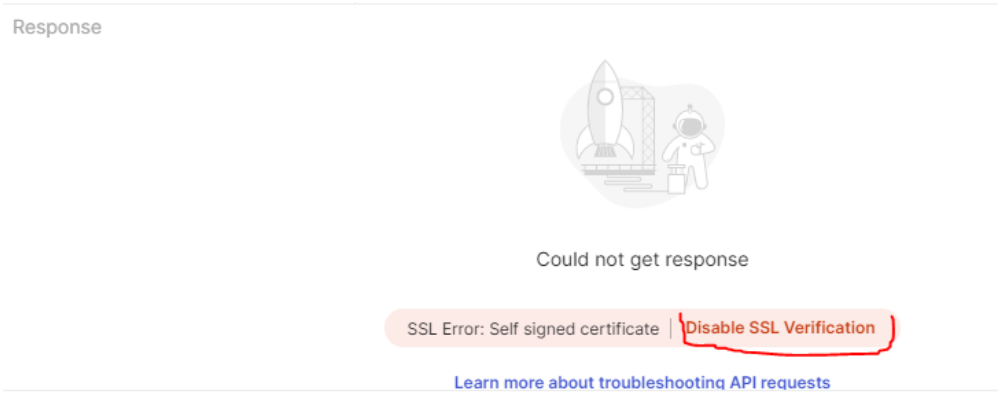
f. Do kolekcie je následne možné pridávať Requesty (volania REST API) voľbou New -> Request.
g. Kolekciu je možné exportovať do textového súboru pravým kliknutím na kolekciu a výberom voľby Export.
h. Výsledný súbor je následne možné naimportovať pomocou voľby Import.

2. Konfigurácia Cisco smerovača ISP cez RESTCONF

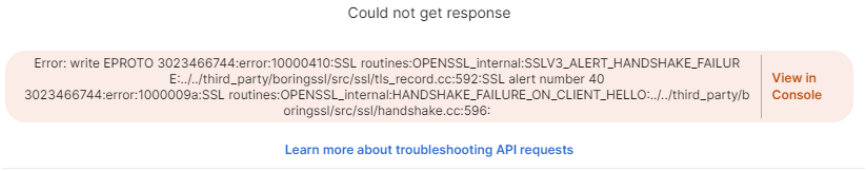
a. Vytvorte nový request v kolekcii Cisco (aj všetky ďalšie requesty v tejto úlohe budeme vytvárať v kolekcii Cisco), ktorý pomenujte „Overenie funkcnosti API“.
   i. Typ žiadosti: GET
   ii. URL: https://*VEREJNA_IP_g1_ISP*/restconf/
      - Verejnú IP si zistite na ISP (`sh ip int br`)
   iii. Na karte Authorization vyberte typ Basic Auth a zadajte prihlasovacie údaje:
      - meno: hostname vášho smerovača (1R1...)
      - heslo: Aut0m1tiz1ci1
   iv. Žiadosť uložte tlačidlom Save.



b. Žiadosť vykonajte tlačidlom Send. Upozorňujeme na možné chyby a ich riešenie:
   i. ak sa vám objaví chyba SSL error, vyberte voľbu Disable SSL Verification (používame self-signed certifikáty)



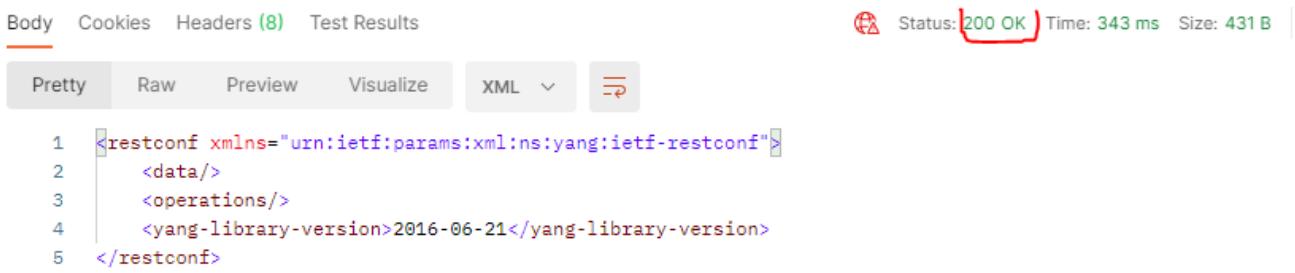
ii. V jednom prípade pri SSL chybe:



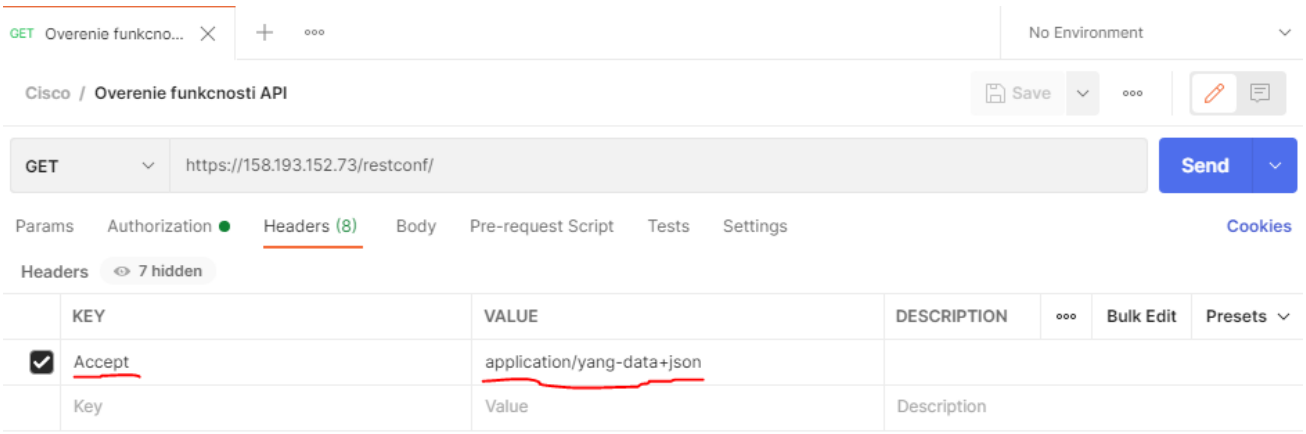
bolo potrebné doplniť tento príkaz do konfigurácie ISP:
`ip http authentication local`

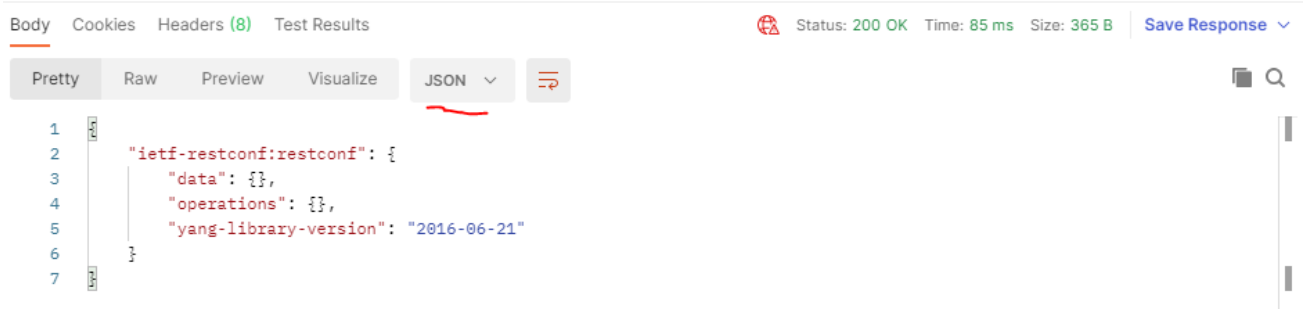
iii. Ak nepomáha nič z vyššie popísaných riešení, uložte konfiguráciu na ISP a reštartujte ho.

c. úspešná odpoveď by mala byť indikovaná http odpoveďou 200 OK a v časti response by ste mali vidieť telo vo formáte XML.



d. Inštruujte smerovač, aby vám odpoveď vrátil vo formáte JSON.
   i. žiadosť upravte tak, že do časti Headers pridajte kľúč „Accept“ s hodnotou „application/yang-data+json“.
   ii. Po odoslaní žiadosti by mala byť odpoveď vo formáte JSON.





e. Vytvorte novú žiadosť, ktorá vypíše informácie o sieťových rozhraniach na smerovači:
   i. Názov: Vypis rozhrania
   ii. Typ žiadosti: GET
   iii. URL: https://VEREJNA_IP_g1_ISP/restconf/data/ietf-interfaces:interfaces
   iv. nezabudnite pridať autorizáciu rovnako, ako v predchádzajúcej žiadosti
      - TIP: Autorizáciu môžete nastaviť aj na celú kolekciu (v nastaveniach kolekcie) a potom v žiadosti zadať typ autorizácie Inherit auth from parent
   v. nastavte, aby odpoveď bola vo formáte JSON
   vi. žiadosť odošlite a prezrite si, ako vyzerá reprezentácia informácii o sieťových rozhraniach vo formáte JSON.

f. Vytvorte novú žiadosť, ktorá vypíše informácie o rozhraní Loopback0:
   i. Názov: Vypis lo0
   ii. Typ žiadosti: GET
   iii. URL: https://VEREJNA_IP_g1_ISP/restconf/data/ietf-interfaces:interfaces/interface=Loopback0
   iv. nezabudnite pridať autorizáciu rovnako, ako v predchádzajúcej žiadosti
   v. nastavte, aby odpoveď bola vo formáte JSON
   vi. odpoveď preskúmajte, a JSON text si skopírujte na použitie v ďalšej úlohe.

g. Vytvorte novú žiadosť, ktorá vytvorí nové rozhranie Loopback#R:
      - # - číslo skupiny
      - R – číslo smerovača
   ii. Názov: Vytvor lo#R
   iii. Typ žiadosti: PUT

iv. URL: https://VEREJNA_IP_g1_ISP/ restconf/data/ietf-interfaces:interfaces/interface=Loopback#R
v. nezabudnite pridať autorizáciu rovnako, ako v predchádzajúcej žiadosti
vi. nastavte, aby odpoveď bola vo formáte JSON
vii. Inštruujte smerovač, že mu posielate údaje vo formáte JSON
- pridajte do Headers kľúč „Content-Type“ s hodnotou „application/yang-data+json“

viii. pridajte telo žiadosti (karta Body), typ „raw“, tak že vložíte skopírovanú JSON odpoveď z minulej žiadosti a upravíte ju nasledovne:
- názov rozhrania: Loopback#R
- popis rozhrania: vymyslite si nejaký reťazec
- ip adresa: 192.0.2.#R

ix. žiadosť odošlite, odpoveď by mala byť typu 201 Created.
x. overte, že sa rozhranie s požadovanými parametrami správne vytvorilo tak, že zavoláte vopred vytvorenú žiadosť „Vypis rozhrania“.

h. Vytvorte novú žiadosť, ktorá vymaže rozhranie Loopback#R:
- # - číslo skupiny
- R – číslo smerovača

ii. Názov: Vymaz lo#R
iii. Typ žiadosti: DELETE
iv. URL: https://VEREJNA_IP_g1_ISP/ restconf/data/ietf-interfaces:interfaces/interface=Loopback#R
v. nezabudnite pridať autorizáciu rovnako, ako v predchádzajúcej žiadosti
vi. nastavte, aby odpoveď bola vo formáte JSON
vii. žiadosť odošlite, odpoveď by mala byť typu 204 No Content.
viii. overte, že sa rozhranie správne vymazalo tak, že zavoláte vopred vytvorenú žiadosť „Vypis rozhrania“.

3. Základná konfigurácia Mikrotik smerovača

a. Prihláste sa na svoj smerovač pomocou konzoly GNS3.
i. meno: admin
ii. prázdne heslo

b. Odporúčanie: všetky konfiguračné zmeny si overujte pomocou print príkazov, napr:
```
ip address print
```

c. Vymažeme konfiguráciu DHCP klienta na rozhraní ether1
```
ip dhcp-client remove 0
```

d. 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.
```
ip address add address=192.168.1.11/24 interface=ether1
```

e. Pridajte statickú default route na next hop 192.168.1.1
```
ip route add dst-address=0.0.0.0/0 gateway=192.168.1.1
```

f. Nakonfigurujte adresu DNS servera na 9.9.9.9.
```
ip dns set servers=9.9.9.9
```

g. Otestujte konektivitu na internet zo smerovačov R1 a R2
i. IP aj DNS

h. Nastavte hostnames #R1, #R2, za # dajte číslo skupiny.
```
system identity set name=1R1
```

i. Zmeňte heslo pre používateľa admin (napríklad na: class)

```
user set admin password=class
```

j. Zakážte nepotrebné manažment služby v časti IP services (telnet, ftp, api, api-ssl)

```
ip service disable telnet,ftp,api,api-ssl
```

k. Vypíšte si celú doterajšiu konfiguráciu (príkaz `/export`) a skontrolujte, či obsahuje zadané konfiguračné príkazy

l. 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`).

4. Zapnutie REST API na Mikrotiku

Pre zapnutie REST API je potrebné povoliť https prístup na Mikrotik, čo vyžaduje získanie SSL certifikátov. My si ich vygenerujeme priamo na smerovači.

a. Vytvorte si certifikát certifikačnej autority:
```
/certificate add name=LocalCA common-name=LocalCA key-usage=key-cert-sign,crl-sign
```
b. Certifikát podpíšte.
```
/certificate sign LocalCA
```
c. Vytvorte certifikát pre smerovač.
```
/certificate add name=REST common-name=192.168.1.#R
```
d. Certifikát podpíšte certifikačnou autoritou.
```
/certificate sign REST ca=LocalCA
```
e. povoľte HTTPS a nastavte mu vygenerovaný certifikát.
```
/ip service set www-ssl certificate=REST disabled=no
```
f. Overte, či je HTTPS zapnuté cez webový prehliadač.
   i. URL: https://VEREJNA_IP_g1_ISP:333#R
   ii. Mali by ste vidieť WebFig rozhranie. Skúste sa do neho prihlásiť.

5. Konfigurácia sieťových rozhraní a info o smerovači cez Mikrotik REST API

Plnú dokumentáciu k Mikrotik REST API nájdete tu:
https://help.mikrotik.com/docs/display/ROS/REST+API

a. V kolekcii Mikrotik, vytvorte zložku (pravý klik na kolekciu – Add Folder) s číslom a názvom úlohy (5. Konfiguracia sietovych rozhrani). Aj všetky ďalšie žiadosti vytvárajte v kolekcii Mikrotik a organizuje do zložiek podľa číselných úloh.

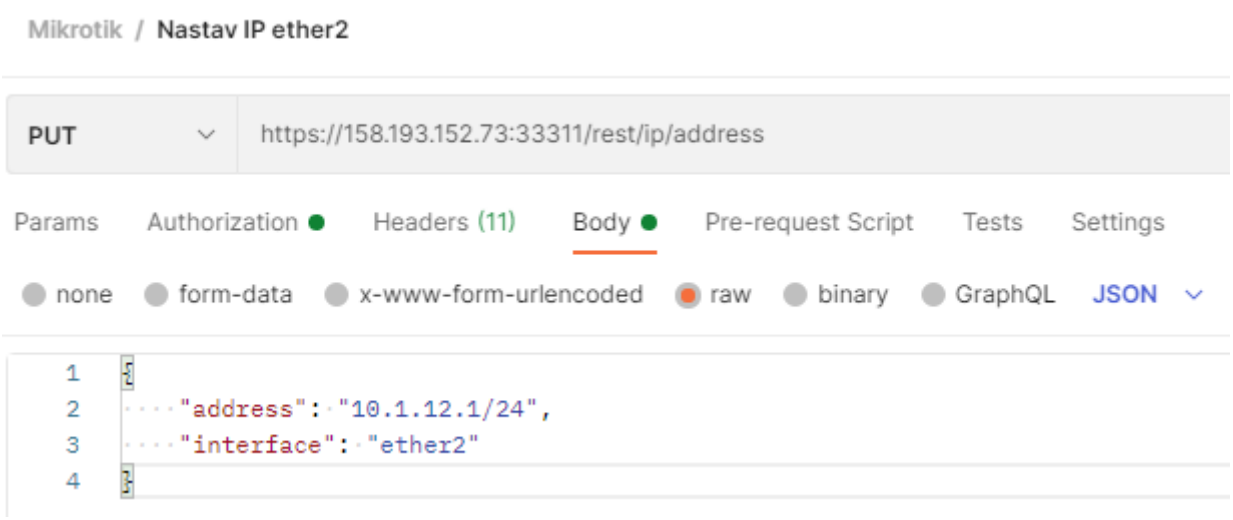
b. Vytvorte novú žiadosť, ktorá vypíše informácie o sieťových rozhraniach na smerovači:
   i. Názov: Vypis rozhrania
   ii. Typ žiadosti: GET
   iii. URL: https://VEREJNA_IP_g1_ISP:333#R/rest/ip/address
   iv. nezabudnite pridať autorizáciu rovnako, ako v prípade cisco smerovača
      - meno a heslo použite na prístup do mikrotiku
      - TIP: Autorizáciu môžete nastaviť aj na celú kolekciu (v nastaveniach kolekcie) a potom v žiadosti zadať typ autorizácie Inherit auth from parent
   v. žiadosť odošlite a prezrite si, ako vyzerá reprezentácia informácii o sieťových rozhraniach vo formáte JSON. Žiadosť si skopírujte do ďalšieho kroku.

c. Vytvorte novú žiadosť, ktorá nastaví IP adresu 10.#.12.R/24 na rozhranie ether2:
   i. Názov: Nastav IP ether2
   ii. Typ žiadosti: PUT
   iii. URL: https://VEREJNA_IP_g1_ISP:333#R/rest/ip/address
   iv. nezabudnite pridať autorizáciu
   v. pri Mikrotik žiadostiach vždy pridávajte parametre do Headers:

- kľúč „Content-Type“ hodnota „application/json“
- kľúč „Accept“ hodnota „application/json“
-

vi. telo žiadosti (karta Body, typ raw) vytvorte na základe predchádzajúcej žiadosti. Parameter *id neuvádzajte (vygeneruje ho smerovač – nezodpovedá indexu v CLI). Stačí uviesť iba parametre, ktoré sú požadované v CLI.

vii. Príklad tela pre 1R1:



viii. žiadosť odošlite a odpoveď by mala byť typu 201 Created

ix. v tele odpovede by ste mali vidieť plnú JSON reprezentáciu konfigurácie

x. konfiguráciu overte zavolaním žiadosti „Vypis rozhrania“

d. Vytvorte novú žiadosť s menom „Nastav IP ether3“, ktorá nastaví IP adresu 10.#.R.1/24 na rozhranie ether3

e. Vytvorte novú žiadosť s menom „System info“, ktorá vypíše informácie o systéme (ekvivalent príkazu system resource print)

f. Vytvorte novú žiadosť s menom „Vytvor lo0“, ktorá vytvorí rozhranie bridge s názvom lo0.

g. Vytvorte novú žiadosť s menom „Nastav IP lo0“, ktorá nastaví IP adresu 10.#.0.1/24 na rozhranie lo0

- poznamenajte si ID nastavenej IP adresy (budete ho potrebovať na ďalšiu žiadosť)

h. Vytvorte novú žiadosť s menom „Oprav IP lo0“, ktorá upraví IP adresu na rozhraní lo0 na 10.#.RRR.R/24.

i. Názov: Oprav IP lo0

ii. Typ žiadosti: PATCH

iii. URL: https://VEREJNA_IP_g1_ISP:333#R/rest/ip/address/*ID

- nahraďte ID s číslom ID z predchádzajúceho requestu

iv. do tela vám stačí špecifikovať parameter address

i. Vytvorte novú žiadosť s menom „Vymaz IP lo0“, ktorá vymaze IP adresu na rozhraní.

i. Názov: Vymaz IP lo0

ii. Typ žiadosti: DELETE

iii. URL: https://VEREJNA_IP_g1_ISP:333#R/rest/ip/address/*ID

- nahraďte ID s číslom ID z predchádzajúceho requestu

iv. telo by malo byť prázdne

v. Odpoveď by mala byť typu 204 No Content

j. Overte konfiguráciu žiadosťou „Vypis rozhrania“

6. Konfigurácia DHCPv4 cez Mikrotik REST API

Všetky žiadosti z tejto úlohy ukladajte do zložky s názvom „6. DHCPv4“.

a. Nastavte DHCP server na vašom smerovači, aby prideľoval IP adresy pre priamo pripojený PC

i. R1, R2 – vytvorte pool pre počítače na priamo pripojeniej sieti

- názov žiadosti: Vytvor pool

ii. R1, R2 – vytvorte definíciu siete pre dhcp server a zadefinujte gateway a ľubovoľný verejný DNS server

- názov žiadosti: Vytvor siet

iii. R1, R2 – vytvorte definíciu samotného DHCP servera na rozhraní vedúcemu ku klientovi (ether3) a priraďte mu pool

- názov žiadosti: Vytvor dhcp-server

b. Nakonfigurujte počítač na získanie adresy z DHCP a na PC overte získanie IP z poolu

c. R1,R2 – overte pridelenie IP cez DHCP (zobrazte Lease)

- názov žiadosti: Vypis lease

d. Overte IP konektivitu medzi routrami a medzi PC a GW.

e. Overte, či cez protokol CDP vidíte počítač (`ip neighbor print detail`).

- názov žiadosti: Vypis susedov

7. Konfigurácia NAT cez Mikrotik REST API

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

- názov žiadosti: Vytvor pNAT

b. Otestujte konektivitu na internet z počítača.

8. Konfigurácia OSPFv2 cez Mikrotik REST API

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.

- názov žiadosti: Vytvor instanciu

```
routing ospf instance add name=default router-id=1.1.1.1 disabled=no
```

ii. vytvoriť OSPF oblasť 0:

- názov žiadosti: Vytvor oblast

```
routing ospf area add instance=default name=backbone area-id=0.0.0.0
```

iii. pridať siete do OSPF procesu

- názov žiadosti: Pridaj siet ku PC
- názov žiadosti: Pridaj siet ku susedovi

```
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

- názov žiadosti: Vypis smerovaciu tabulku

d. Preskúmajte OSFP tabuľku.

- názov žiadosti: Vypis OSPF tabulku

e. Viac informácii o smerovacích protokoloch v RouterOS v7 nájdete tu: https://help.mikrotik.com/docs/display/ROS/ROSv7+Basic+Routing+Examples

9. **Konfigurácia Firewall-u cez Mikrotik REST API – 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 a vytvorte žiadosti 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 lo0
 ip add 192.0.2.1 255.255.255.255
 desc Novy loopback

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 192.168.1.11 443 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 192.168.1.12 443 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 192.168.1.21 443 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 192.168.1.22 443 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 192.168.1.31 443 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 192.168.1.32 443 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 192.168.1.41 443 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 192.168.1.42 443 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 192.168.1.51 443 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 192.168.1.52 443 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 192.168.1.61 443 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 192.168.1.62 443 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 192.168.1.71 443 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 192.168.1.72 443 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 192.168.1.81 443 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 192.168.1.82 443 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 192.168.1.91 443 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 192.168.1.92 443 interface gi 1 33392

lldp run

username 1R1 privilege 15 password 0 Aut0m1tiz1ci1
username 1R2 privilege 15 password 0 Aut0m1tiz1ci1
username 2R1 privilege 15 password 0 Aut0m1tiz1ci1
username 2R2 privilege 15 password 0 Aut0m1tiz1ci1
username 3R1 privilege 15 password 0 Aut0m1tiz1ci1
username 3R2 privilege 15 password 0 Aut0m1tiz1ci1
username 4R1 privilege 15 password 0 Aut0m1tiz1ci1
username 4R2 privilege 15 password 0 Aut0m1tiz1ci1
username 5R1 privilege 15 password 0 Aut0m1tiz1ci1
username 5R2 privilege 15 password 0 Aut0m1tiz1ci1
username 6R1 privilege 15 password 0 Aut0m1tiz1ci1
username 6R2 privilege 15 password 0 Aut0m1tiz1ci1
username 7R1 privilege 15 password 0 Aut0m1tiz1ci1
username 7R2 privilege 15 password 0 Aut0m1tiz1ci1
username 8R1 privilege 15 password 0 Aut0m1tiz1ci1
username 8R2 privilege 15 password 0 Aut0m1tiz1ci1
username 9R1 privilege 15 password 0 Aut0m1tiz1ci1
username 9R2 privilege 15 password 0 Aut0m1tiz1ci1
username 10R1 privilege 15 password 0 Aut0m1tiz1ci1
username 10R2 privilege 15 password 0 Aut0m1tiz1ci1

netconf-yang
restconf
```