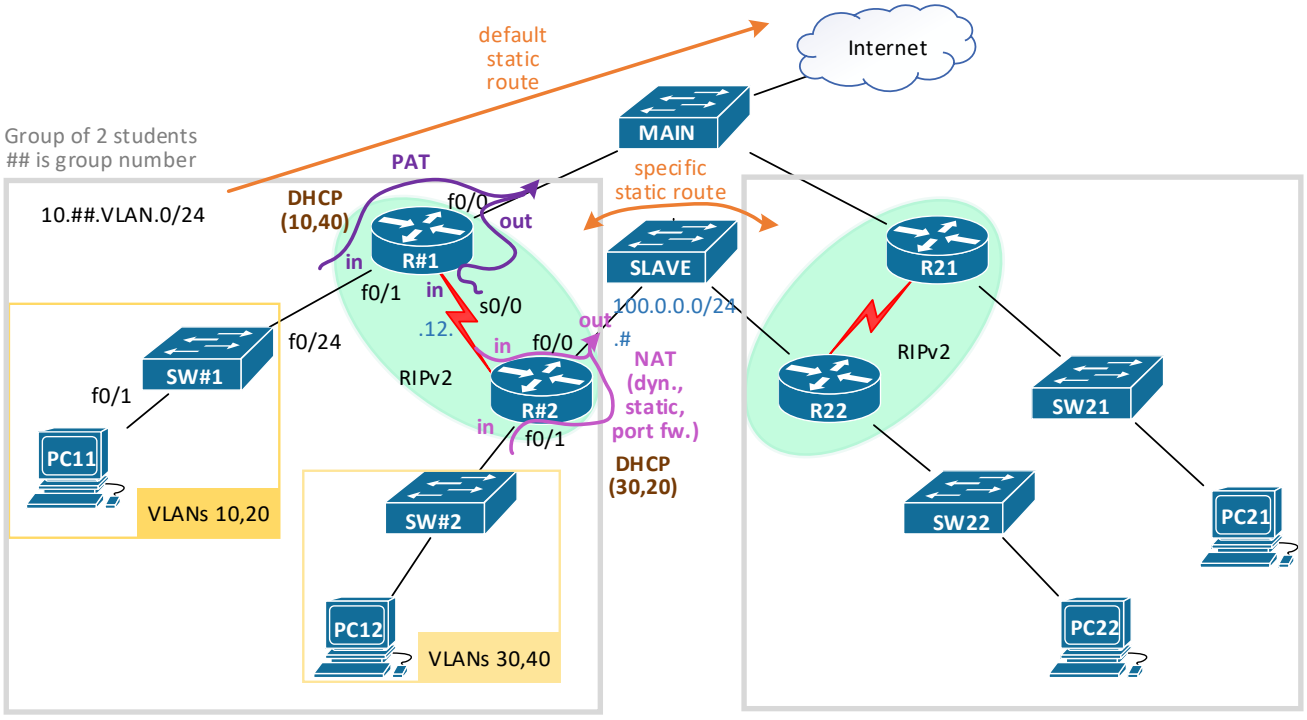
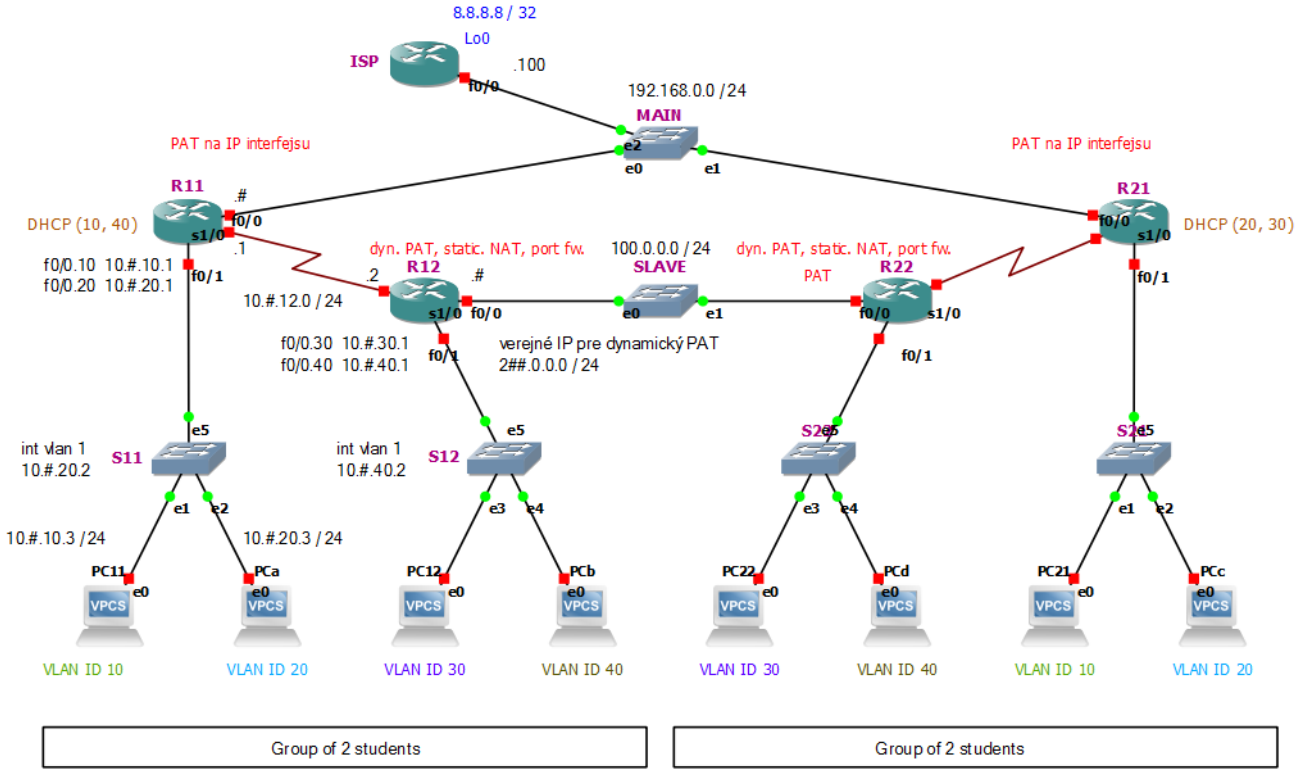
PS1 / Cvičenie 10 / **NAT,DHCPv4**

Topológia

Variant A – pre reálne laboratórium a prácu na reálnom hardvéry:



Variant B – pre virtuálne laboratórium a prácu v GNS3 emulátore:

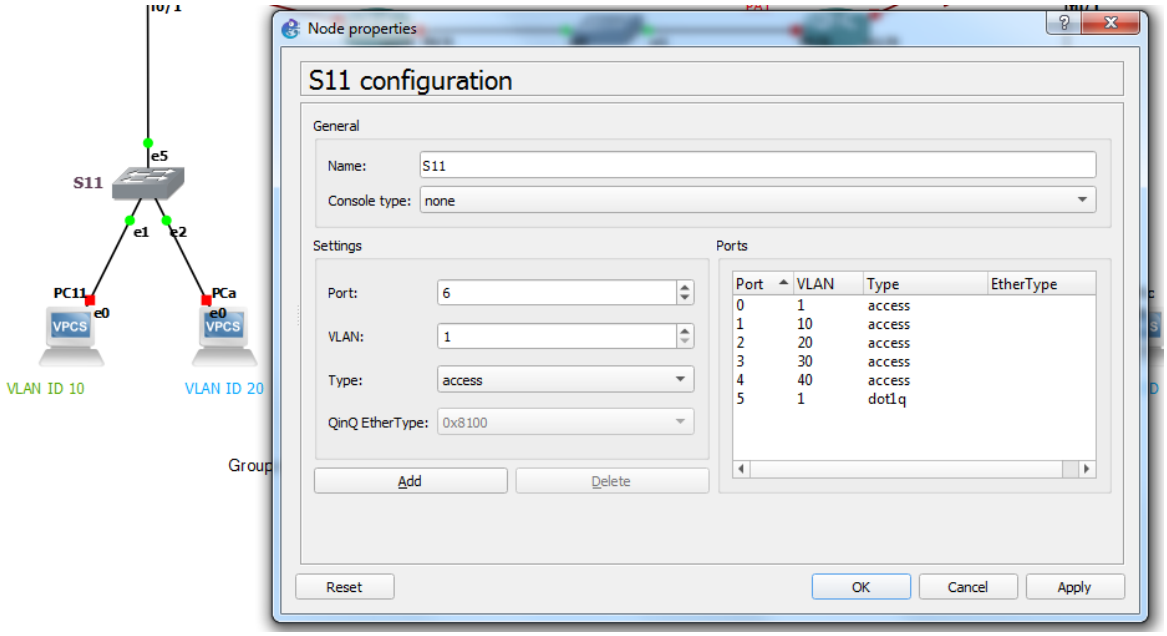


Postup

Šedým písmom budú značené extra inštrukcie, platné iba pri práci v emulátore GNS3, začínať budú vždy reťazcom „GNS:“.

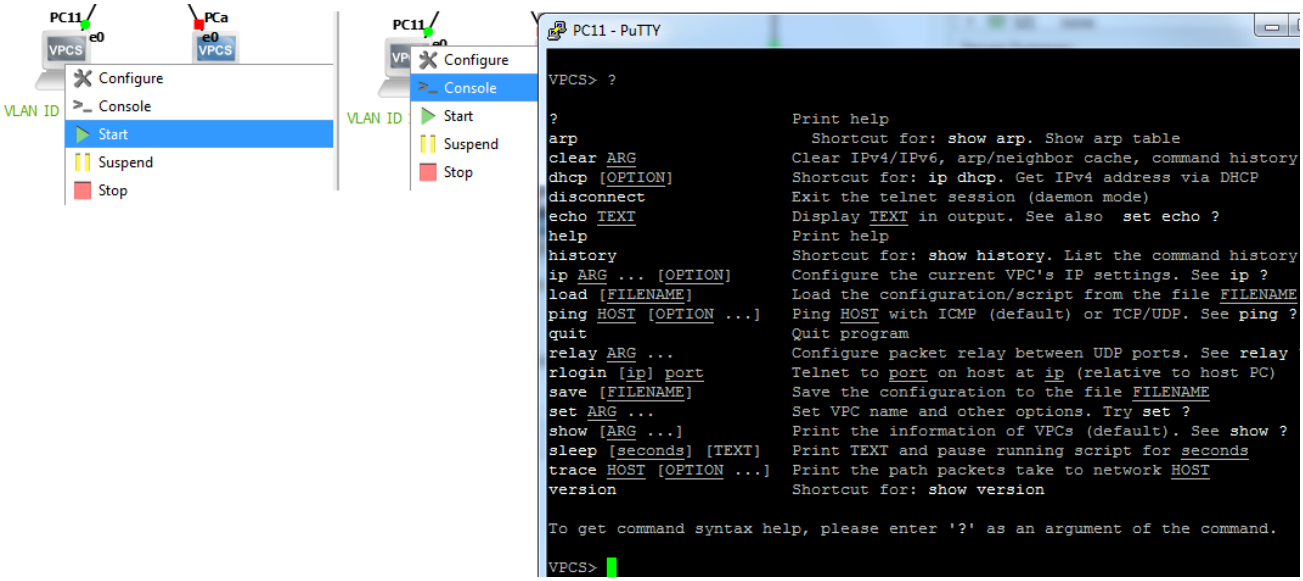
1. **Základná konfigurácia:**
   a. GNS: otvorte si topológiu na GNS serveri .125,
   projekt 1-PS1_cv10_NAT_DHCPv4_RIPv2_TEMPLATE-OS-02.
   Internetový oblak je nahradený ISP rútrom, na ktorom je loopback. Internet je tam nahradený smerovačom ISP s interfejsom loopback. Sieť horného prepínača MAIN má IP adresu 192.168.0.0./24.
   Nakreslite si topológiu na papier (aspoň jeden za dvojicu) a rozdeľte si pridelený IPv4 rozsah 10.##.VLAN.0/24 pre 4 VLANs (10, 20 na R1, 30, 40 na R2) a pre WAN linku medzi R1 a R2 použite ako tretí oktet číslo „***12***“. Smerovačom (subrozhraniam pre VLANy) prideľte najnižšiu IP z rozsahu, prepínaču (SVI) druhú najnižšiu (S#1 zo siete VLAN 20, S#2 zo siete VLAN 40) . Všetko si zaznačte do obrázku s topológiou.
   b. GNS: R1 f0/0 dajte pevnú IP adresu 192.168.0.#.
   Na rozhraní smerovača R1 smerom k hlavnému prepínaču MAIN nastavte získanie adresy z DHCP servera od ISP – katedrový smerovač `(ip address dhcp)`
      i. Overte si získanú adresu, aj obsah smerovacej tabuľky - pribudne vám jedna statická cesta a default route – tú budete chcieť neskôr redistribuovať v RIPv2.
   c. Na rozhraní k susednej skupine pripojenej cez SLAVE prepínač použite rozsah 100.0.0.0/24 a pre rozhranie použite IPv4 adresu s posledným oktetom podľa čísla skupiny (100.0.0.#)
   d. Nastavte hostnames R##1, R##2, SW##1, SW##2, za ## dajte číslo skupiny (01, 02, ..., 10).
   e. Pre efektívnosť práce nastavte:
      i. Zabráňte na prepínačoch výpis hlášok do písaného textu na konzole (zmiešavanie vstupu a výstupu CMD) `(line console 0, logging synchronous)`
      ii. Vypnite prekladanie doménových mien na IP adresy `(no ip domain-lookup)`
2. **VLANs a interVLAN routing**
   a. Nastavte vhodne trunk porty a access porty na prepínači
      i. GNS: ako trunk je nastavený e5 (2-klik otvorí nastavovacie GUI – tam pozri)
      Trunk 1x (fa0/24), over: `sh int trunk`
      ii. GNS: jeden port do každej VLAN – pozri GUI
      Access porty – po 5 portov do každej VLAN (na SW1 sú iba VLANy 10 a 20, na SW2 iba VLANy 30 a 40), over: `sh vlan`

GNS: Prepínač klikni dvakrát, otvorí sa okno. Pozri priradenie portov do VLAN a nastavenie trunk portu.



b. Vyriešte interVLAN routing na smerovačoch
   i. Každý smerovač bude mať 2 subrozhrania (R1 pre VLAN 10 a 20, R2 pre VLAN 30 a 40)
   ii. GNS: PC#1 dajte adresu 10.##.10.3, PC#2 dajte adresu 10.##.30.3, S#1 10.##.20.2, S#2 10.##.40.2.
   PC#1:
   ? - príkazy
   ip 10.9.10.3 255.255.255.0 10.9.10.1 - na konci brána GW
   show ip
   ping 10.9.10.1 OK
   Počítaču dajte IPv4 adresu z prvej VLAN a prepínaču dajte IPv4 adresu z druhej VLAN (nezabudnite preň nastaviť aj default gateway – subrozhranie smerovača pre danú VLAN) a overte interVLAN routing, zatiaľ iba oddelene, medzi VLAN 10 a 20, a oddelene medzi VLAN 30, a 40.

GNS: Počítač – Start - treba dvakrát opakovať, aby sa počítač naštartoval.



3. RIPv2

a. Nastavte RIPv2, aby ste mali konektivitu k VLANs na susednom smerovači v dvojici, neaktivujte RIP pre rozhranie vedúce k ISP, ani na rozhraní k susednej dvojici (!) pripojenej cez SLAVE prepínač, iba vo vašej vnútornej časti topológie. Do internetu máte statickú default route (vďaka DHCP, ktorým získavate adresu na vonkajšom rozhraní smerovača R1, ip address dhcp) a v RIP zapnite šírenie default route na R1. Ku susednej skupine budete neskôr riešiť špecifickú statickú cestu. Vhodné by bolo ešte v RIP redistribuovať aj priamo pripojenú sieť na R2, aby ste mali konektivity aj k sieti 100.0.0.0/24 (`redistribute connected` na R2)

i. Otestujte konektivitu medzi počítačmi – s vašim kolegom v dvojici ako aj prístup (ping) na prepínač

b. **KONTROLA VYUČUJÚCIM**:

i. Ukážte úspešný ping z PC11 vo VLAN 10 na prepínač SW1 vo VLAN 20, a ping z PC12 vo VLAN 30 na prepínač SW2 vo VLAN 40.

ii. Ukážte úspešný ping z PC11 na PC vášho kolegu v dvojici, ako aj na vonkajšiu IPv4 adresu na R2 v sieti 100.0.0.0.

4. DHCPv4

a. Nastavte DHCP server na vašom smerovači

i. R1 – vytvorte pool pre lokálnu VLAN10 a druhý pool pre VLAN40 pre počítače zo susedovej VLAN (aby sme si vyskúšali aj relay agentov)

ii. R2: Nezabudnite na subrozhraní pre VLAN40 nastaviť relay agenta (DHCP pool pre VLAN40 je na susednom smerovači!, takže requesty by ste mali preposielať na IP adresu R1)

iii. R2 – vytvorte pool pre VLAN30 a VLAN20 pre počítače zo susedovej VLAN (aby sme si vyskúšali aj relay agentov)

iv. R1: Nezabudnite na subrozhraní pre VLAN20 nastaviť relay agenta (DHCP pool pre VLAN20 je na susednom smerovači, takže requesty by ste mali preposielať na IP adresu R2)

v. Overte na koncových PC pridelenie dynamickej IPv4 adresy.
GNS:
PC#1: cez DHCP ziskaj IP

? - ip dhcp
show ip - nemá IP
ip dhcp - napíše: DDORA IP 10.9.10.3/24 GW 10.9.10.1
show ip - už má IP
Aby ste overili prideľovanie pre každú VLAN, musíte si počítač pre tieto testy, raz zaradiť do jednej, raz do druhej VLAN, resp. do správneho portu na prepínači, ktorý je ako prístupový pre danú VLAN.

b. **KONTROLA VYUČUJÚCIM**:
   i. Ukážte pridelenú IPv4 adresu cez DHCP pre PC11 vo VLAN20 a pre PC12 vo VLAN40 (ten ťažší prípad).

5. NAT

a. Na **R1** nastavte **NAT** pre odchádzajúce pakety **do Internetu – PAT s preťažením rozhrania**
   i. Na R1 nastavte preklad všetkých privátnych adries vo vašej topológii (10.#.0.0/16) na IPv4 adresu vášho ethernetového rozhrania f0/0 vedúceho k hlavnému prepínaču a ISP (zväčša verejná IP). (Ak sú IP adresy nakonfigurované na subinterfejsoch, tak dajte príkaz „ip nat inside“ na subinterfejsy, a nie na fyzický interfejs.)
   ii. GNS: PCs vedia ping lo0 na ISP.
   Overte, že oba vaše PCs sa vedia dostať do internetu – otvor prehliadač a ukáž
   iii. **KONTROLA VYUČUJÚCIM:** Zobraz si vzdelavanie.uniza.sk na oboch vašich PC v topológii.

b. Na **R2** nastavte **PAT a statický NAT** pre pakety idúce **k susednej dvojici**
   i. **Dynamické PAT (NAT overloading)**
      - Na R2 nastavte preklad všetkých privátnych adries vo vašej topológii (10.#.0.0/16), okrem druhej a tretej IPv4 adresy z VLAN 30 (tie budeš riešiť v statickom NAT v bode ii aj iii, preto premysli ako má vyzerať ACL pre NAT). Adresy prekjlaj na zakúpený rozsah verejných IPv4 adries 2##.0.0.0/24 (## je číslo vašej skupiny 01, 02,...10), pričom začni od tretej použiteľnej IPv4 adresy z tohto rozsahu (prvé dve si vyhraď na adresy pre servery, ktoré budete riešiť v bode ii. Statickým NAT)
        - Overte záznamy v smerovacej tabuľke
      - **KONTROLA VYUČUJÚCIM**:
        - z vašich počítačov otestujte konektivitu cez ping na rozhranie smerovača R2 v susednej dvojici vedúce k vašemu spoločnému prepínaču, následne pozrite záznamy cez `show ip nat translations` – mali by tam byť viditeľné, ak nie, troubleshootuj!
   ii. **Statické NAT** pre 3. IPv4 adresu z VLAN 30 na verejnú IPv4 adresu 2##.0.0.1
      - Nakonfiguruj požadované statické NAT pre danú adresu.
      - Nastavte na R2 statickú cestu k susednej dvojici k ich verejnému rozsahu IPv4 adries (2##.0.0.0/24, kde## je číslo skupiny 01, 02,...10) a oznamujte ju v RIPv2. Redistribuujte aj priamo pripojené siete v RIPv2 `(redistribute connected)` – aby R1 videl aj sieť 100.#.0.0 (ak ste to ešte nespravili v bode 3 pri RIP).
        - Overte záznamy v smerovacej tabuľke
        - Skontrolujte susednú dvojicu, či už má nastavenú statickú cestu k vám a či ju redistribuuje v RIPv2
      -
      - GNS: Len zo susedovho smerovača ping 207.0.0.1 (PC ktorý má skutočnú adresu 10.7.30.3). Pozri záznam v tabuľke prekladov „sh ip int trans“.
      Popros kolegu v susednej dvojici, aby sa pokúsil pripojiť na TFTP server,

ktorý si spustíš na počítači, ktorý bude mať túto 3. privátnu IPv4 adresu, pre ktorú robíš na R2 statický NAT preklad

- Kolega sa musí pripájať na tvoju verejnú IPv4 adresu. Rovnako by mal fungovať aj ping v poriadku.
- Over záznamy `v show ip nat translations`!
  - Ak susedná dvojica zaostáva, a nemá ešte krok 5bi, použi ich smerovač R2 a z neho spravte copy run tftp – na vašu verejnú IPv4 adresu 20.0.0.1

- **KONTROLA VYUČUJÚCIM**:
  - Ukáž skopírovaný config na vašom PC a záznam v `show ip nat translations`

iii. **Port forwarding** pre 2. privátnu IPv4 adresu z VLAN 30 (IPv4 adresa prepínača) na verejnú IPv4 adresu 2##.0.0.2, so špecifikovaním protokolu TCP pre služby **SSH**, t.j. použi vnútorný port 22 a vonkajší port 2222 (ak si netrúfaš na SSH, sprav telnet, potom porty 23 a 2323)

- Popros kolegu v susednej dvojici, aby sa pokúsil pripojiť zo svojho počítača cez SSH (alebo telnet) na verejnú IPv4 adresu 2##.0.0.2 (použi putty a zmeň port na 2222, resp. 2323), malo by ísť, a over záznamy v show ip nat translations. Ping by ísť nemal, keďže port forwardingom riešite iba prístup na službu SSH
  - Ak susedná dvojica zaostáva, pripoj sa cez SSH (resp. TELNET) z ich smerovača R2
- **KONTROLA VYUČUJÚCIM**:
  - Ukáž, že ide ssh pripojenie a ping nejde (viď predošlý bod).

Konfigurácia ISP nie je v tomto cvičení potrebná, pretože všetky študentské topológie sa pripájajú na MAIN prepínač, ktorý ide priamo do reálnej siete, bez smerovača ISP. Na R1 potom študentské topológie dostanú IP adresu z katedrového DHCP servera.

Konfigurácia ISP smerovača (pre učiteľa, alebo šikovného študenta)

Pokiaľ priraďovanie IP adries z katedrového DHCP servera z nejakého dôvodu zlyhá, je možné alternatívne použiť ISP smerovač (zapojiť ho na MAIN prepínač a do siete), ktorý poskytne DHCP pool pre študentské topológie, a potom je potrebné zrealizovať tieto kroky:

KROK 0: Ak neostala na smerovači pôvodná/základná konfigurácia (IPv6 tunel a pod.), treba ju nakopírovať z flash (v opačnom prípade tento krok preskočiť). Súbory vo flash pamäti možno prehľadať príkazom `dir` v privilegovanom móde, náš súbor bude mať v názve slovo „`basic`“ a nejaké reťazce okolo. Zistite presný názov (dir) a následne použite tento príkaz v privilegovanom móde (reťazec `basic-config-b303` upravte podľa reálneho názvu súboru, ak nenájdete presne tento):

```
configure replace flash:basic-config-b303.text
```

KROK 1: A k tejto základnej konfigurácii pridať toto (ctrl+c, ctrl+v najprv do notepadu, aby sa vymazalo formátovanie a následne odtiaľ ctrl+c, ctrl+v v globálnom config móde na smerovači):

```
!
hostname ISP
!
interface GigabitEthernet0/0/0
no shut
ip address 10.100.0.254 255.255.0.0
ip nat inside
!
interface GigabitEthernet0/0/1
no shut
ip nat outside
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
!
ip route 10.1.0.0 255.255.0.0 10.100.0.1
ip route 10.2.0.0 255.255.0.0 10.100.0.2
ip route 10.3.0.0 255.255.0.0 10.100.0.3
ip route 10.4.0.0 255.255.0.0 10.100.0.4
ip route 10.5.0.0 255.255.0.0 10.100.0.5
ip route 10.6.0.0 255.255.0.0 10.100.0.6
ip route 10.7.0.0 255.255.0.0 10.100.0.7
ip route 10.8.0.0 255.255.0.0 10.100.0.8
ip route 10.9.0.0 255.255.0.0 10.100.0.9
ip route 10.10.0.0 255.255.0.0 10.100.0.10
!
! DHCP pool
ip dhcp pool Pool_for_student_groups
network 10.100.0.0 255.255.0.0
default-router 10.100.0.254
dns-server 158.193.152.4
!
dns-server 158.193.152.11
!
ip dhcp excluded-address 10.100.0.254
!
!sh ip dhcp bindings
```