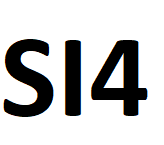
**MATURITNÍ LAB**

**Jakub Kuzník**

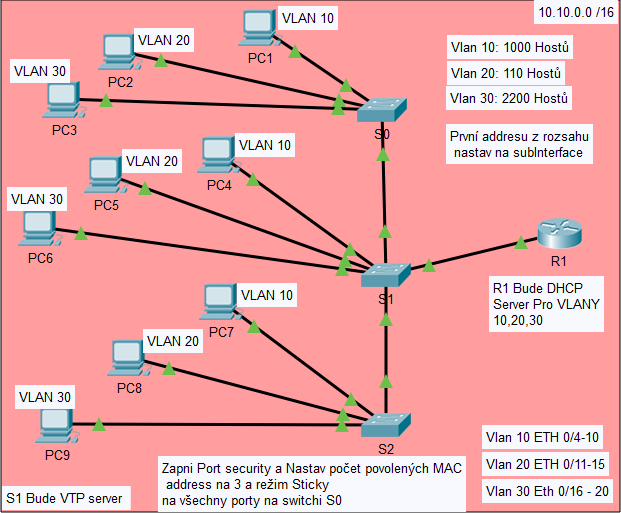


2019/2020





Dílčí úloha č. 1.



Zadání

1. Spočítejte a přidělte Ip addresy z daného rozsahu (10.10.0.0/16) a první adresu z jednotlivých rozsahů nastavte na Subinterface
2. Nastavte Hostname podle schématu
3. Nastavte VLANY, pomocí VTP serveru, který bude na switchi S1 vlany pojmenujte vlan10(ucitele) vlan20(vedeni) vlan30(studenti)

FE0/4-10 budou VLAN 10 FE0/11-15 VLAN 20 FE0/16–20 VLAN 30

1. Vytvořte DHCP server na R1 pro jednotlivé vlany zakažte použití prvních dvou addres v každém vlanu
2. Na všech FastEthernet portech na S0 Zajisti Port security – zapni port security, Nastav počet povolených mac addres na 3, Nastav režim sticky, Vypni všechny Gigabitové porty

**Vypracovaní:**

**1.**!!! trunk – po trunku může jít více vlanu proto se dává například mezí router a switch   
!!! 802.1Q je protokol, který řídí značkovaní(tagovaní) vlanu   
!!! nativni vlan – z bezpečnostního hlediska je dobré ho měnit defaultně je to vlan 1 a jde po něm netagovana( komunikace a protokoly jako jsou cdp VTP, STP

Prvně je třeba rozpočítat IP addresy pro jednotlivé Vlany. Sítě budeme pomoci VLSM rozdělovat od největších po nejmenší.

POZOR!! První a poslední adresu nemůžu použít, první adresa je adresa sítě a poslední broadcast

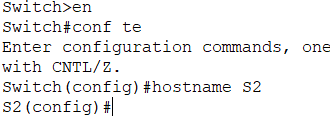
|  |  |  |  |
| --- | --- | --- | --- |
|  | Počet hostu (jak velká to bude síť) | Rozsah | Maska |
| VLAN 10 | **1000 hostů**  nejbližší vyšší číslo je 1024 | 10.10.16.0 – 10.10.19.255 | /22  255.255.252.0 |
| VLAN 20 | **110 hostů**  nejbližší vyšší číslo je 128 | 10.10.20.0 -10.10.20.127 | /25  255.255.255.128 |
| VLAN 30 | **2200 hostů**  nejbližší vyšší číslo je 4096 | 10.10.0.0-10.10.15.255 | /20  255.255.240.0 |

**Teď musíme nastavit Ip addresy na nezbytné místa což jsou subinterface. Ze subinterface se nám dostanou addresy na jednotlivé počítače pomocí dhcp serveru.**

Prvně si zapne interface   
Připojíme se na subinterface nastavíme ip adresu (první adresu z rozsahu) a vždycky když děláme z VLANY, tak musíme dat encapsulation dot1Q + číslo VLANU   
 číslo vlanu 

**2.**

Na všech zařízeních je nezbytné nastavit Hostname podle schématu



**3.**

VTP server funguje tak, že jeden switch bude vtp server ostatní vtp clienti. My tedy uděláme vtp server ze switche S1 na něm vytvoříme vlany 10,20,30 a ty se nám automaticky udělají pomocí vtp protokolu i na ostatních switchích.

Ještě, než začneme z vtp je potřeba udělat TRUNKY mezi switchi a routerem

  
  
  
  
-prvně musíme přidat switche do jedné VTP domény


Nastavíme role


Bez hesla by to nefungovalo


A teď na S1 vytvoříme vlany, které pojmenujeme a které by se nám automaticky měly dostat na ostatní switche


Dále je nezbytné jednotlivým portům přidělit vlany

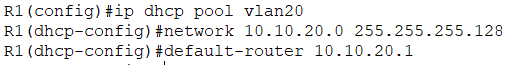
**TOTO PROVEDEME NA VŠECH SWITCHICH**

  
+  
  
 

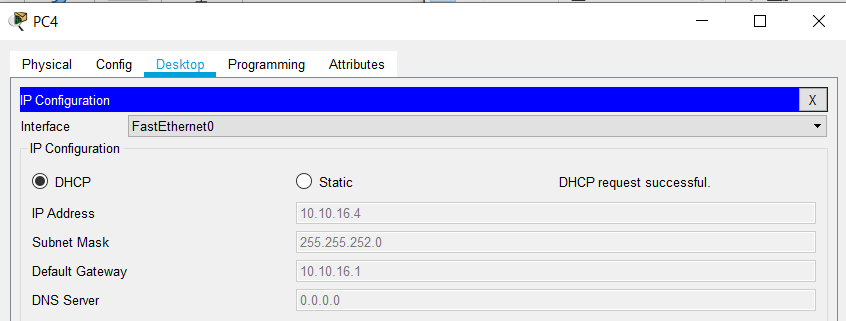
**4.**aby nám fungoval DHCP server musíme mít nakonfigurované subinterface což už máme   
- Prvně budeme muset excludnout(zakázat přidělovani) addresy následujícím způsobem zakážeme první dvě addresy z každého rozsahu

!! **default router = gateway**



Ted už vytvoříme dhcp pooly pro jednotlive vlany    
  


Ještě přepneme pc na DHCP a měli bychom dostat addresy

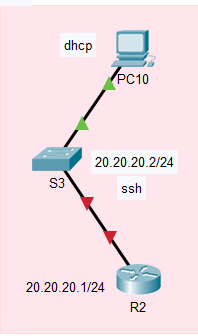


**5**.


**Zadání:**

Dílčí úloha č.2.

1. nastav ip addressy Vytvoř DHCP server na R2
2. Vytvoř ssh na S3 switchi dej ip addressu: 20.20.20.2/24   
   3. Nastav odhlašování na SSH po třech minutách   
   4. zakázano prerušování psaného textu  
   5. vypněte hledaní DNS
3. na R2 popiš interface, který vede do LAN sítě

**Vypracování**

**1.**

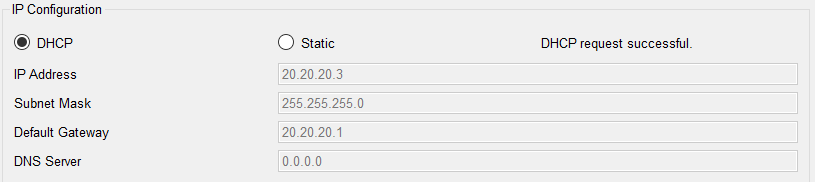
**- na R2fa0/0 nastav 20.20.20.1**

Prvně si musíme uvědomit, že nechceme, aby dhcp přidělovalo ip adresu co máme nastavenou na routeru a na switchi (tímto příkazem jsem odebral z dhcp rozsah address 20.20.20.0-20.20.20.2

.  
Pak si vytvoříme dhcp pool, a to je vše



Ještě přepnu pc na dhcp



**2.**Pro funkčnost ssh potřebuju přidělit switchi ip adresu, kterou přidělím na vlan 1



SSH musí splňovat pár podmínek první je heslo do enablu  
  
Vytvoříme doménu   
  
vytvoříme si usera  
  
vytvoříme rsa klíč  
  
s velikosti 1024

  
připojíme se na line vty což je console   
  
A přepojíme telnet(console) na ssh   
  
Pak už jenom login local  
  
na závěr se připojíme z pc10

3.  



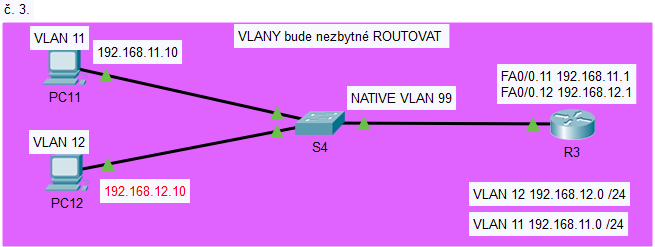

4.  


5.  


6.



**Zadání:**



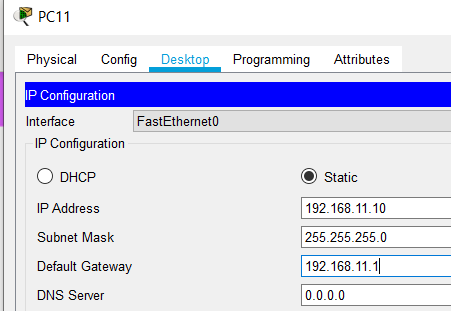
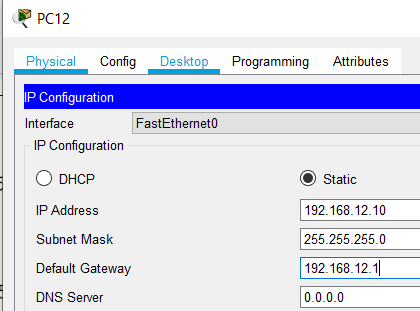
1. Nastavme ip addresy
2. Vytvoříme vlany a přidělíme je na jednotlivé porty
3. Změníme native vlan mezi S4 a R3 na VLAN99

**Vypracování:  
!! Na úvod by jsme si měli uvědomit že native vlan je vlan po, kterém jde všechna neoznačená komunikace defaultně je to vlan1 a mění se z bezpečnostních důvodů**

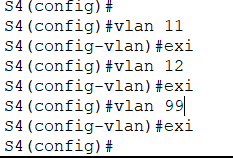
1.  
zapneme si interface, na kterém budou subinterface.



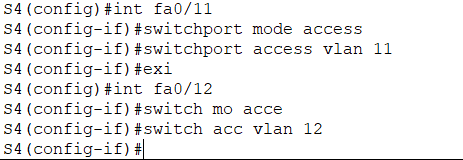
Na sub interface vždy musíme nejdřív nastavit zuapouzdření dot1Q + číslo VLANU   
   
To stejné platí pro druhý subinterface   
  
ještě nastavíme addresy pro jednotlivé pc

2.  
Vytvoříme si VLANY



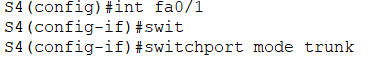
Přidělíme vlany na porty



3.

Je třeba si uvědomit že skrz native vlan chodí untaged komunikace a protokoly jako je stp a cdp bezpečnostní opatření je nemít přiděleny nativ vlan na žadném portu

Přepneme do modu trunk aby tam mohla procházet více než 1VLAN

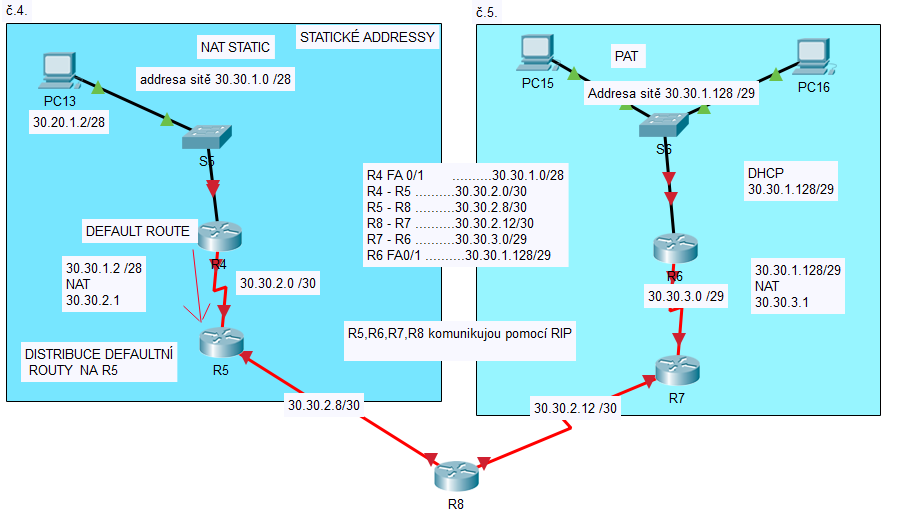
  
změníme native vlan



A nakonec povolíme všechny vlany



**Zadání:**



R4 FA0/1 30.30.1.0

R4 – R5 30.30.2.0/30

R5 – R8 30.30.2.8/30

R8 – R7 30.30.2.12/30

R7 – R6 30.30.3.0/29

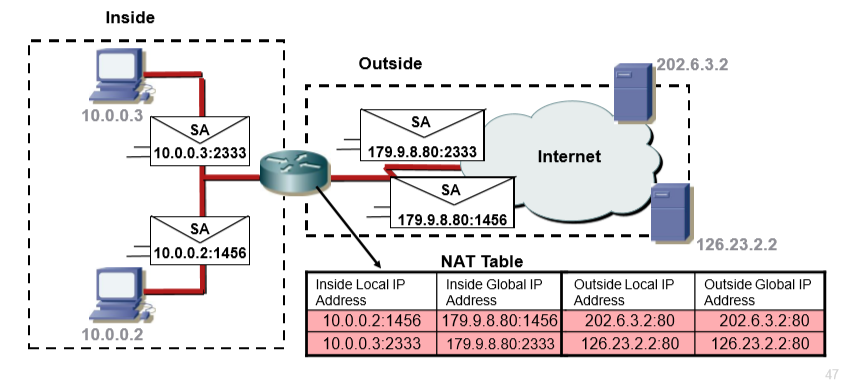
R6 FA0/1 30.30.1.128/29

Úkoly:

1. Přiděl zařízením ip addresy, jak si můžeme všimnout, tak to máme zapsané v tvaru adresa sítě a maska.
2. NA R6 vytvoř dhcp server pro síť 30.30.1.128/29
3. Na R4 uděláme STATICKY NAT 30.20.1.2 na wan adresu 30.20.2.1
4. Na R6 uděláme PAT sítě 30.30.1.128/29 na adresy 30.30.3.1
5. Na R4 uděláme defaultní routu
6. Mezi R5 R8 R7 R6 bude RIP

**Vypracovaní**.

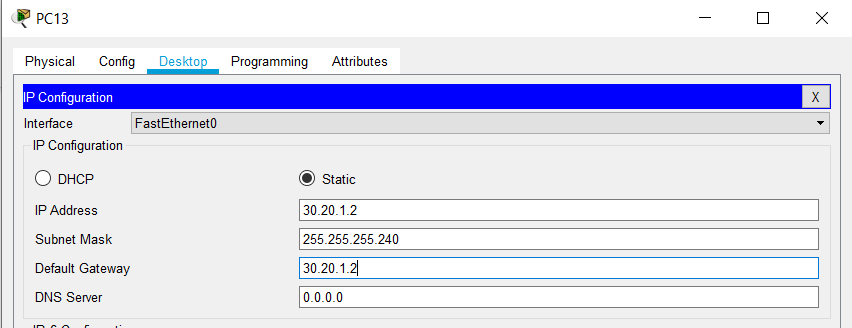
**NAT** – slouží k tomu, aby se na internetu šetřili addresy nejčastěji překládáme nějaké privatní addresy na jednu veřejnou.  
**STATIC NAT** – překládám 1:1 addresy   
**DYNAMIC NAT** – mám rozsah veřejných ip address na které můžu překládat   
**PAT** – pat nám překladá lokalní adresy na jednu veřejnou a za tu veřejnou ještě přidá číslo portu, které je jedinečné   
Obrázek vystihující PAT

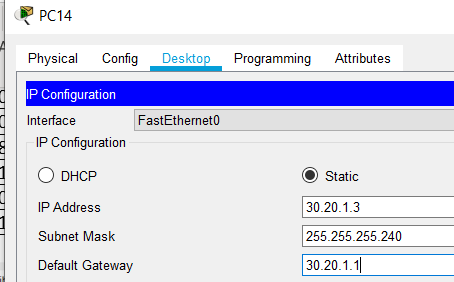


1.

Pokud máme adresu sítě zadanou v tomto tvaru je nutné si uvědomit z jakým rozsahem vlastně pracujeme. Dále je nutné pochopit masky   
To, jak si addressy rozvrhneme je v podstatě jedno.

|  |  |  |  |
| --- | --- | --- | --- |
| Zadaní | Rozsah | Použitelné addresy | Maska |
| 30.30.1.0/28 | 30.30.1.0–30.30.1.15 | 30.30.1.1 – 30.30.1.14 | 255.255.255.240 |
| 30.30.2.0/30 | 30.30.2.0-30.30.2.3 | 30.30.2.1 - 30.30.2.2 | 255.255.255.252 |
| 30.30.2.8/30 | 30.30.2.8-30.30.2.11 | 30.30.2.9 – 30.30.2.10 | 255.255.255.252 |
| 30.30.2.12/30 | 30.30.2.12-30.30.2.15 | 30.30.2.13 – 30.30.2.14 | 255.255.255.252 |
| 30.30.3.0/29 | 30.30.3.0-30.30.3.7 | 30.30.3.1 – 30.30.3.6 | 255.255.255.248 |
| 30.30.1.128/29 | 30.30.1.128-30.30.1.135 | 30.30.1.129 – 30.30.1.134 | 255.255.255.248 |





Ip add na R4



Adresa na venkovním interface   
 –  

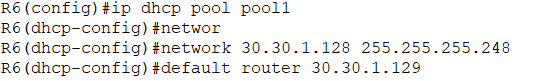

**ROUTER R5**  
  
  
   
  
**ROUTER R8**  
  
  
  
  
**ROUTER R7**  
  

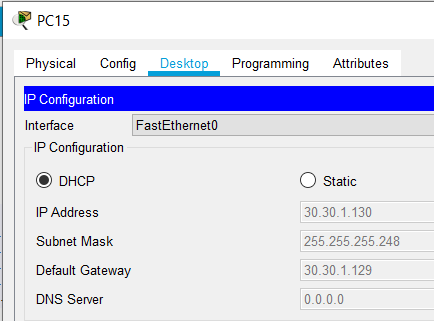

  


**R6**  
  

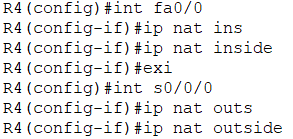

**2.**

Vytvoříme dhcp pool s názvem pool1

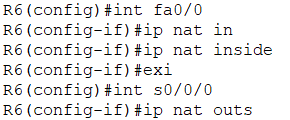
 **PC15 a PC16** by měly dostat addresu z DHCP



**3.** U natu si musíme vždy nastavit směry inside a outside

  
  
**4.**

**Prvně si opět uděláme směry**



PAT nám umožňuje překládat více addres do jedné veřejné

Vytvořím si access list 1 s addresami, které budu překládat

  
vytvořím pool veřejných addres

  
udělám pat



**5.**



**6.**

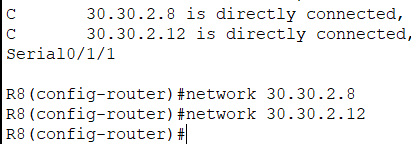
Opišeme vždykcy sitě z show ip int brief   

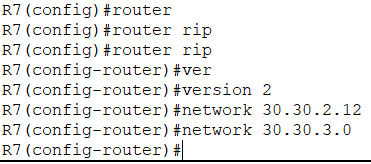



R8



Tady jde vidět jak to opisuju z show ip route

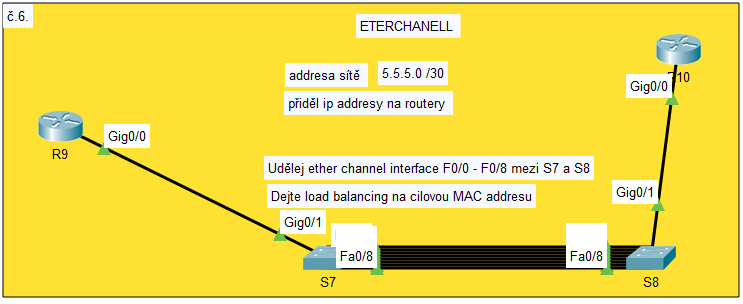
  
R7

  
R6





**Zadání**

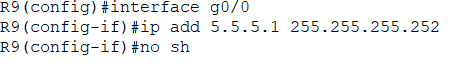


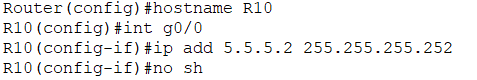
1. Nastav Ip addresy
2. Agreguj linky fa0/0 – fa0/8 mezi S7 a S8
3. Nastavte load balancing na cilovou MAC adresu
4. Na S7 nastavte heslo na consoli
5. Na S8 nastavte heslo na telnet cisco a vypněte přerušován í psaného textu

**Vypracování:**

**1.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sít** | **Rozsah** | **Použitelné addresy** | **Maska** |
| **5.5.5.0/30** | **5.5.5.0-5.5.5.3** | **5.5.5.1-.5.5.5.2** | **255.255.255.252** |





**2.**

Když agregujeme linky musíme vytvořit virtuální „interface“ neboli channel, do kterého všechny porty přiřadíme. To udělám následovně





**Nyní už můžu porty upravovat zde**



 **3.**



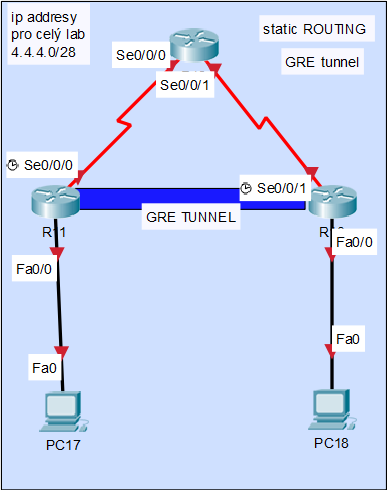
**4.**



**5.**



**Zadání**



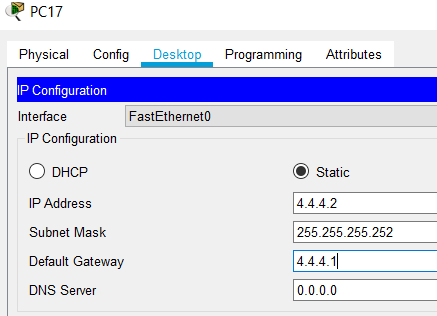
1. Rozděl addresní prostor 4.4.4.0/28 mezi všechny zařízení
2. Routuj pomocí static routingu
3. Udělej GRE tunnel mezi R11 a R13

1.

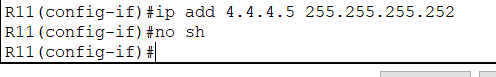
Takto jsem rozdělil rozsah na 4 sítě + jsem přidal gre tunnel

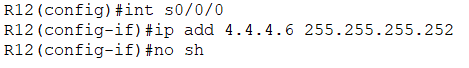
|  |  |  |  |
| --- | --- | --- | --- |
| Addresa sítě | Rozsah | Použitelné addresy | Maska |
| 4.4.4.0/30 | 4.4.4.0-4.4.4.3 | 4.4.4.1-4.4.4.2 | 255.255.255.252 |
| 4.4.4.4/30 | 4.4.4.4-.4.4.4.7 | 4.4.4.5-4.4.4.6 | 255.255.255.252 |
| 4.4.4.8/30 | 4.4.4.8-4.4.4.11 | 4.4.4.9-4.4.4.10 | 255.255.255.252 |
| 4.4.4.12/30 | 4.4.4.12-4.4.4.15 | 4.4.4.13-4.4.4.14 | 255.255.255.252 |
| 4.4.4.128/30 | 4.4.4.128-4.4.4.131 | 4.4.4.129-4.4.4.130 | 255.255.255.252 |

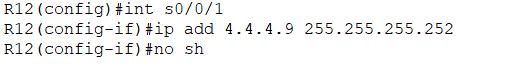
Ip addresace

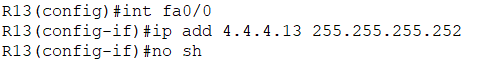
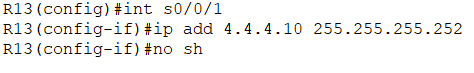
  


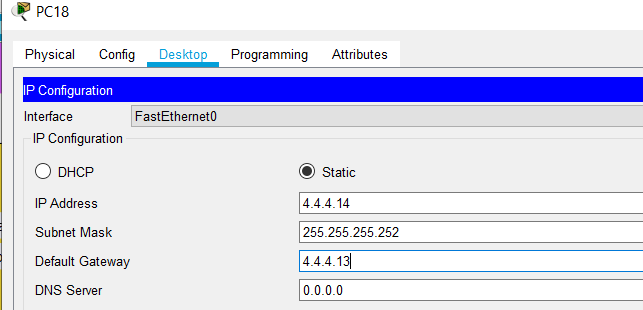












2.

Každá router musí mít cestu do každé sítě, která k němu není přímo připojena

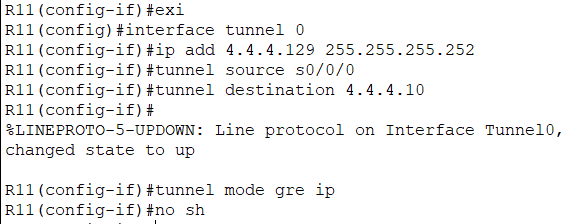
Ip route ADDRESA sítě do, které chci maska sítě do které chci NEXT HOP



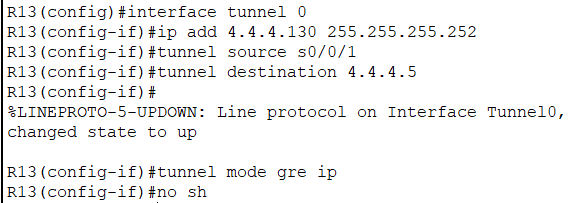




3.  
vytvoříme si interface tunnel 0 // na ten později přidáme adresu, atak   
**tunnel destination** / je addresa routeru na druhé straně (ne ta na tunelu ale na fyzickém interface)  
**tunnel source** //odchozí interface   
**tunnel mode gre ip** //mode gre ip

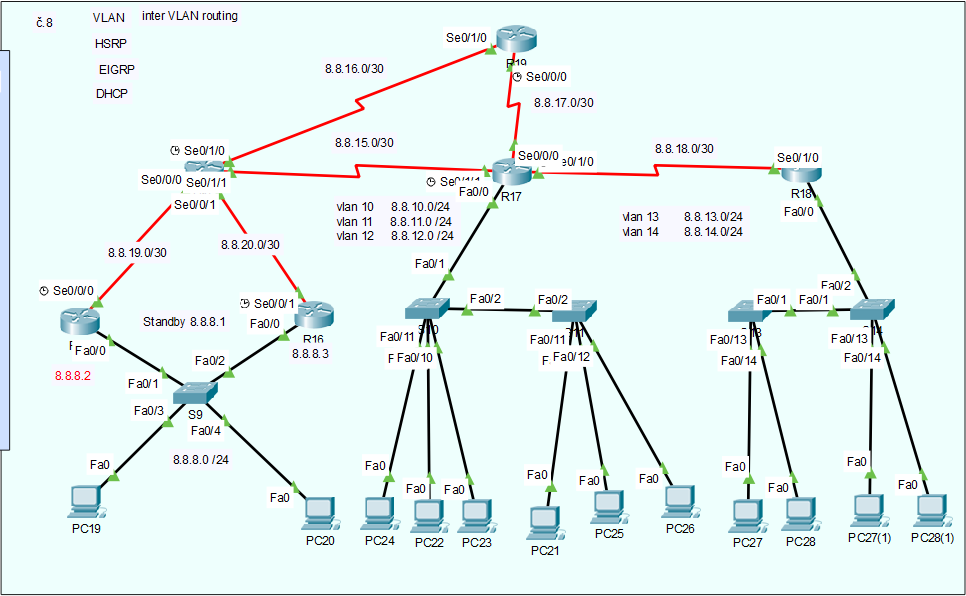
  
poté je nezbytné ještě udělat novou statickou routu protože jsme vytvořili novou síť

Síť, do které chci maska a next hop tunnelu



,

**Zadaní:**



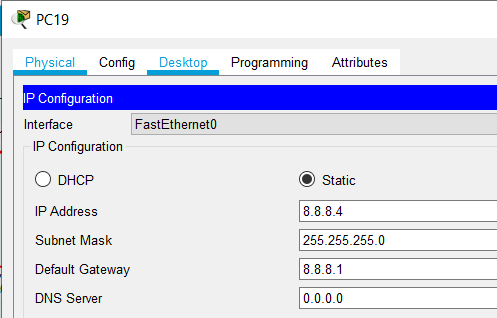
1. Nastavíme ip addresy na všechny zařízení
2. Vytvoř vlany na S10 S11 S13 S14 a přiděl portům vlany   
   S10 F0/11 VLAN11 F0/12 VLAN12 F0/13 VLAN 13  
   S11 F0/11 VLAN11 F0/12 VLAN12 F0/13 VLAN 13  
   S13 F0/13 VLAN13 F0/14 VLAN14   
   S14 F0/13 VLAN13 F0/14 VLAN14
3. Na R17 uděléj DHCP server pro vlan 10
4. Uděláme HSRP z PC19 a PC20 na R15 a R16 default gateway bude 8.8.8.1/24 router r16 bude preempt
5. Udělej EIGRP mezi všemi routery v jednom autonomním systému s číslem 2 a vypni sumarizaci   
   zajisti, aby lan sitě nepřijimaly eigrp pakety

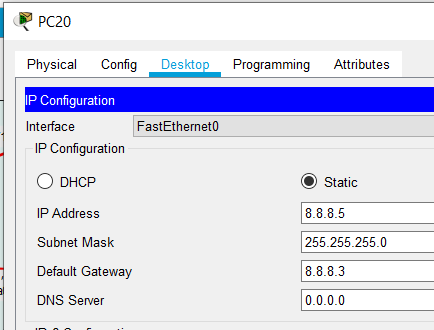
1.

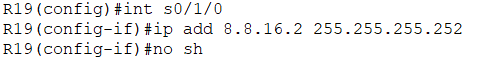
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN** | **Addresa sítě** | **Rozsah** | **Použitelné addresy** | **Maska** |
|  | 8.8.8.0/24 | 8.8.8.0-8.8.8.255 | 8.8.8.1-8.8.8.254 | 255.255.255.0 |
| 10 | 8.8.10.0/24 | 8.8.10.0-8.8.10.255 | 8.8.10.1-8.8.10.254 | 255.255.255.0 |
| 11 | 8.8.11.0/24 | 8.8.11.0-8.8.11.255 | 8.8.11.1-8.8.11.254 | 255.255.255.0 |
| 12 | 8.8.12.0/24 | 8.8.12.0-8.8.12.255 | 8.8.12.1-8.8.12.254 | 255.255.255.0 |
| 13 | 8.8.13.0/24 | 8.8.13.0-8.8.13.255 | 8.8.13.1-8.8.13.254 | 255.255.255.0 |
| 14 | 8.8.14.0/24 | 8.8.14.0-8.8.14.255 | 8.8.14.1-8.8.14.254 | 255.255.255.0 |
|  | 8.8.15.0 | 8.8.15.0-8.8.15.3 | 8.8.15.1-8.8.15.2 | 255.255.255.252 |
|  | 8.8.16.0 | 8.8.16.0-8.8.16.3 | 8.8.16.1-8.8.16.2 | 255.255.255.252 |
|  | 8.8.17.0 | 8.8.17.0-8.8.17.3 | 8.8.17.1-8.8.17.2 | 255.255.255.252 |
|  | 8.8.18.0 | 8.8.18.0-8.8.18.3 | 8.8.18.1-8.8.18.2 | 255.255.255.252 |
|  | 8.8.19.0 | 8.8.19.0-8.8.19.3 | 8.8.19.1-8.8.19.2 | 255.255.255.252 |
|  | 8.8.20.0 | 8.8.20.0-8.8.20.3 | 8.8.20.1-8.8.20.2 | 255.255.255.252 |

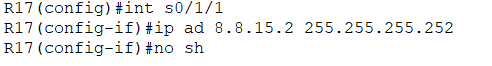
**JE TŘEBA SI UVĚDOMIT ŽE JEDNU ADDRESU BUDU MÍT PRO HSRP VIRTUÁL INTERFACE A TA BUDE DEFAULT GATEWAY PRO 8.8.8.0**

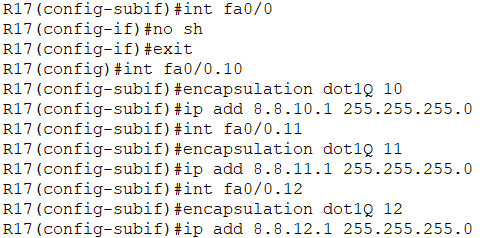
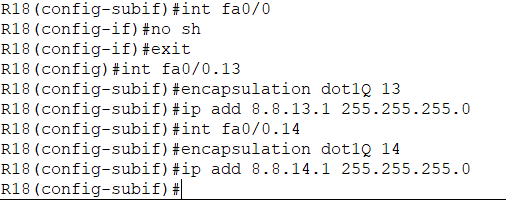




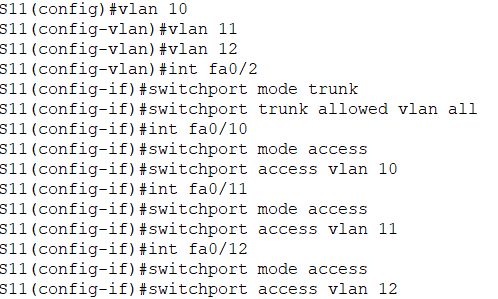
  
  
  

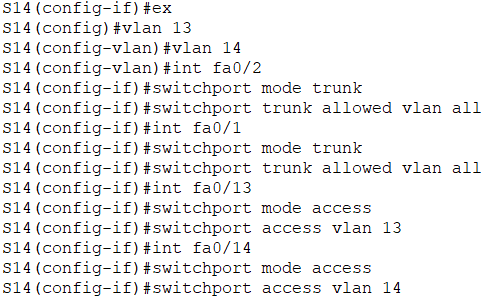

  

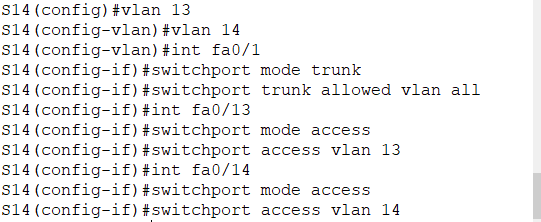
**2.**

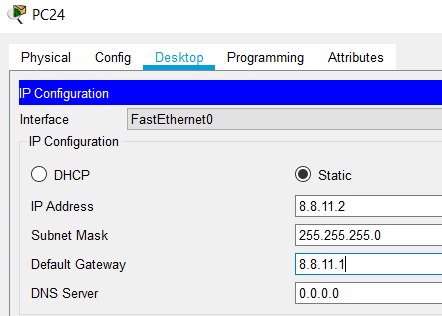
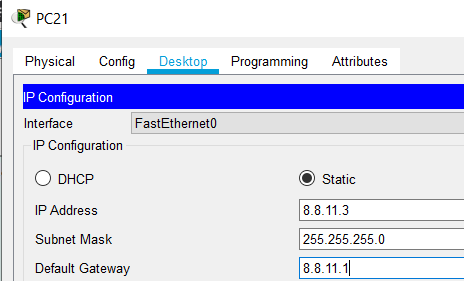
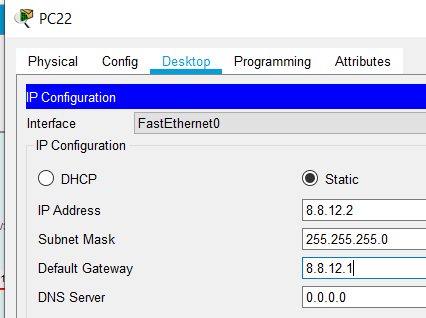


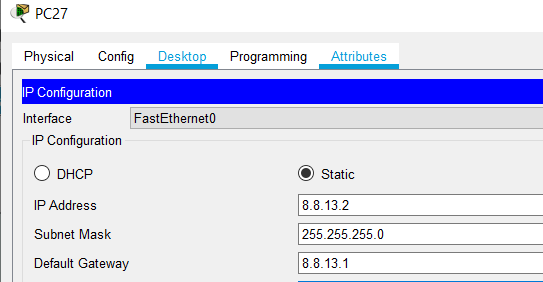
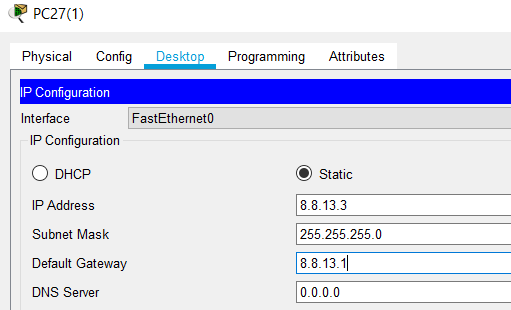
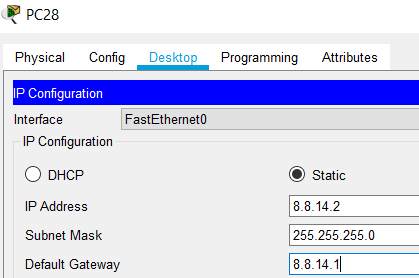


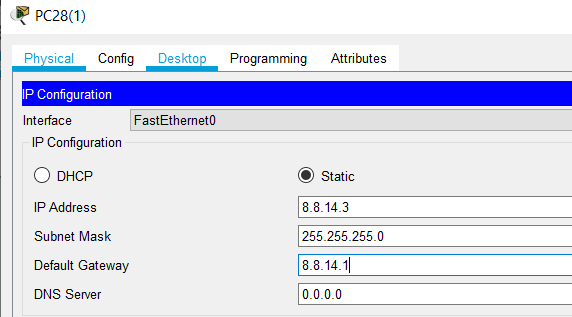


**Tohle je S13 ne S14 omlouvám se za chybu**





3.  
DHCP na R17

Excludnu si bránu   


Vytvořím pool nastavím rozsah a nastavím bránu na 8.8.10.1

  
4.

HSRP nám umožňuje mít 2 Gatewaye proto budeme potřebovat dva routery a jeden virtuální (standby) interface

Standby ip na jedné straně



R16 bude preempt

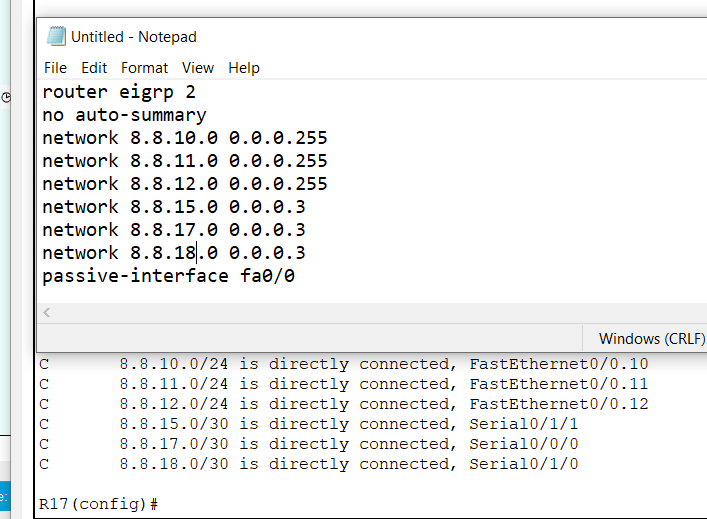


5.  
**EIGRP funguje stejně jako ostatní dynamické protokoly proste použijeme na routerech příkaz show ip route a vepíšeme všechny sítě do eigrp**

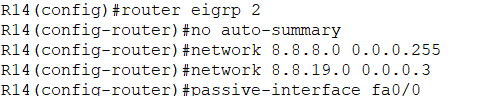
**WILD CARD MASK – od 255.255.255.255 odečteme masku**

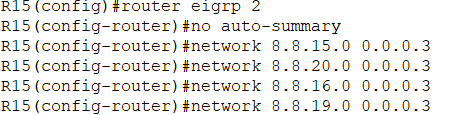
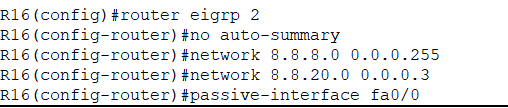
**Př maska 255.255.255.0 bude zapsaná jako 0.0.0.255  
maska 255.255.255.252 bude zapsaná jako 0.0.0.3**

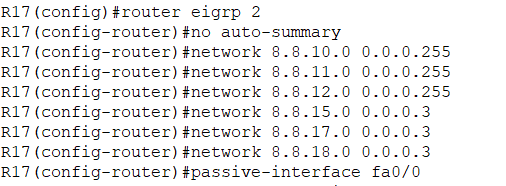
**Sítě se vepisují   
network + addresa sítě + WILD CARD MASK**

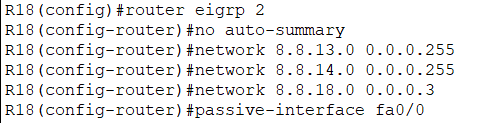
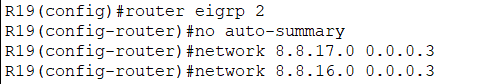
**Tento screen ukazuje, jak se to dělá** 

**Vypracování**

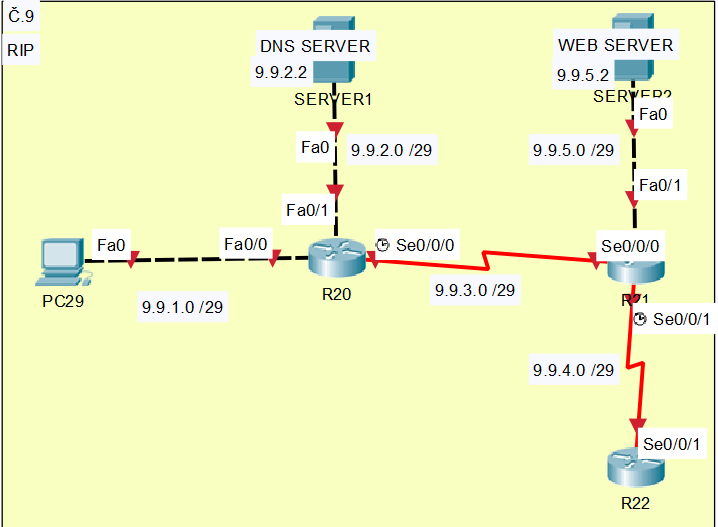








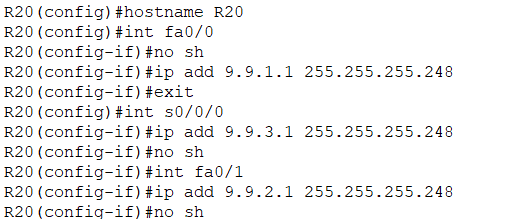
**Zadání:**

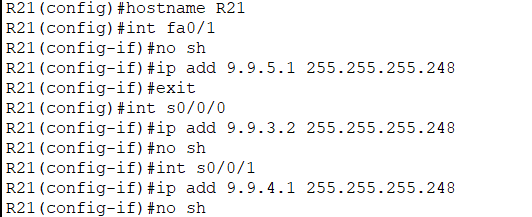


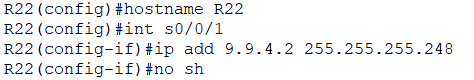
1. **Nastav ip addresy na všechny zařízení na pc29 navíc nastvte dns server (servery mají addres 9.9.2.2, 9.9.5.2)**
2. **Nastavte dns server a web server.   
   web server bude mit domenový nazev cisco.com  
   dns server bude mít dns zápis na web server**
3. **Nastavte routovací protokol RIP mezi jednotlivými ROUTERY**

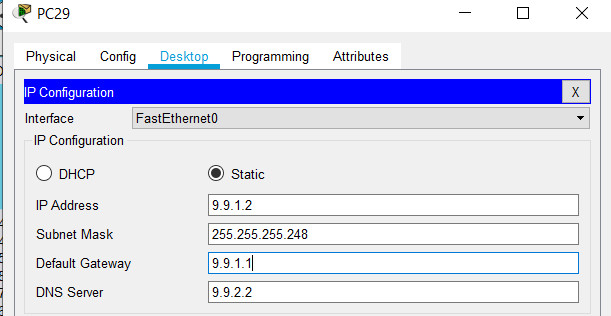
**Vypracování:**

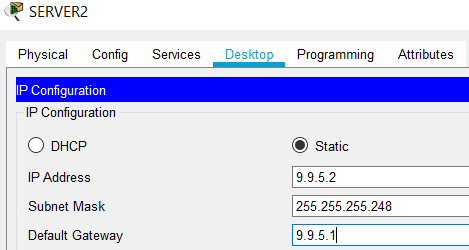
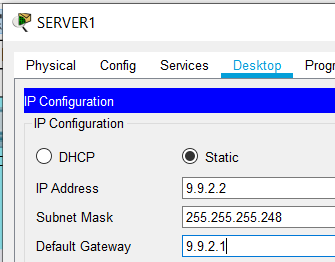
|  |  |  |  |
| --- | --- | --- | --- |
| **Adressa sítě** | **Rozsah** | **Použitelné addresy** | **Maska** |
| **9.9.1.0/29** | **9.9.1.0 – 9.9.1.7** | **9.9.9.1-9.9.9.6** | **255.255.255.248** |
| **9.9.2.0/29** | **9.9.1.0 – 9.9.1.7** | **9.9.9.1-9.9.9.6** | **255.255.255.248** |
| **9.9.3.0/29** | **9.9.1.0 – 9.9.1.7** | **9.9.9.1-9.9.9.6** | **255.255.255.248** |
| **9.9.4.0/29** | **9.9.1.0 – 9.9.1.7** | **9.9.9.1-9.9.9.6** | **255.255.255.248** |
| **9.9.5.0/29** | **9.9.1.0 – 9.9.1.7** | **9.9.9.1-9.9.9.6** | **255.255.255.248** |





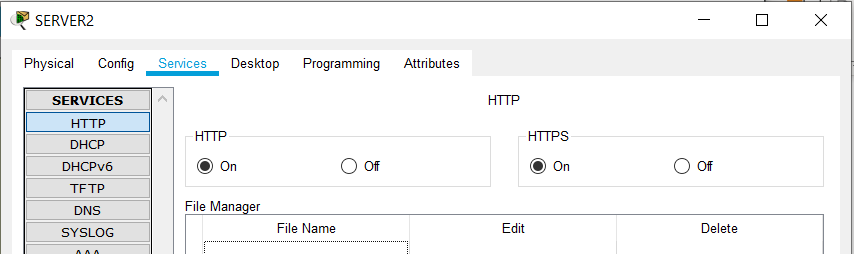


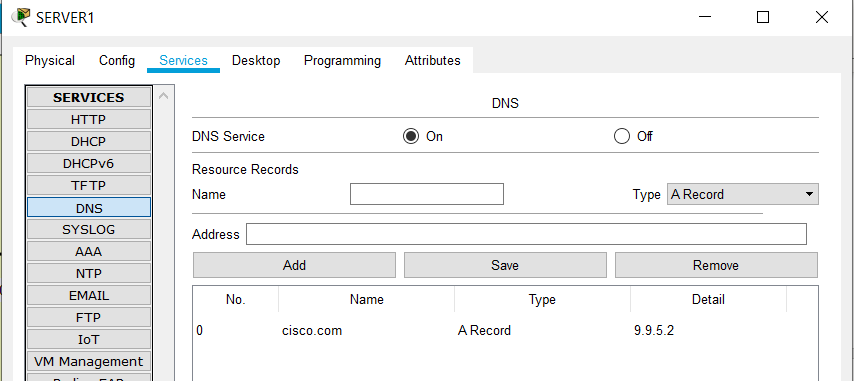




**2.**

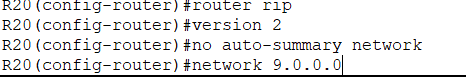
**Web Server:**

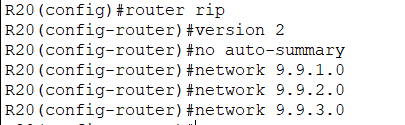


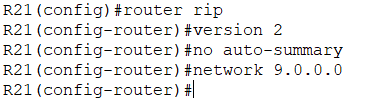


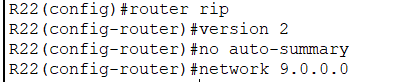
**3.**

**V routovacím protokolu RIP musím vepsat všechny sítě z (show ip route) routovací tabulky do ripu. Pokud však použiji no auto summary stačí jak použiju sesumarizovanou síť**

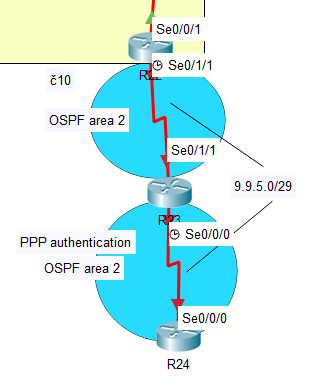


**Alternativní zápis je:**





**Zadání:**



1. **Nastav ip addressy rozděl addresní prostor 9.9.5.0/29 mezi R22xR23 a R23xR24**
2. **Nastav ospf mezi jednotlivými routery modrá barva znázorňuje areu2 Redistribuj RIP protokol do ospf a ospf do Rip**
3. **Mezi R23 a R24 nastav PPP s pap autentifikaci s libovolným heslem**

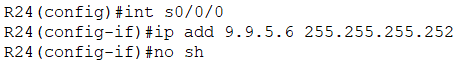
**Vypracování:**

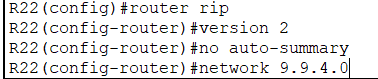
1.

Ze sítě 9.9.5.0/29 si udělám sítě 9.9.5.0/30 a 9.9.5.4/30

|  |  |  |  |
| --- | --- | --- | --- |
| Adresa sítě | Rozsah | Použitelné addresy | Maska |
| 9.9.5.0/30 | 9.9.5.0-9.9.5.3 | 9.9.5.1-9.9.5.2 | 255.255.255.252 |
| 9.9.5.4/30 | 9.9.5.4-9.9.5.7 | 9.9.5.5-9.9.5.7 | 255.255.255.252 |





2.  
Do ripu si na R22 přidávám jenom tu síť která je na RIP straně routeru   


Ted je třeba redistribuovat ospf do ripu a rip do ospf

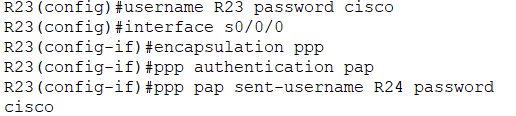


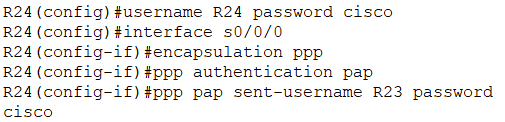




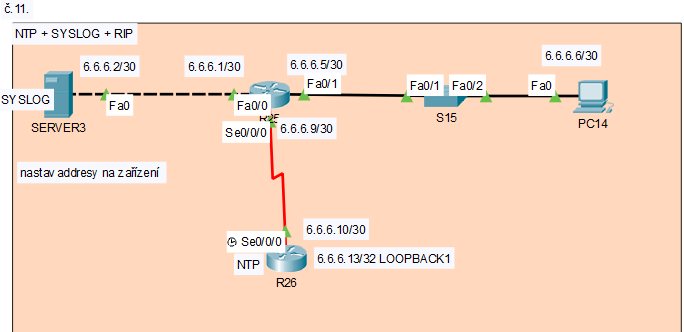


3.



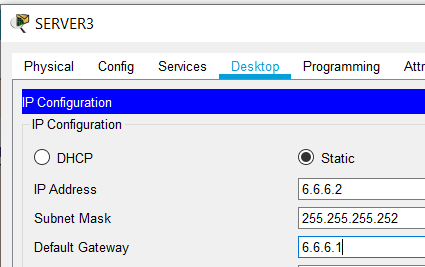


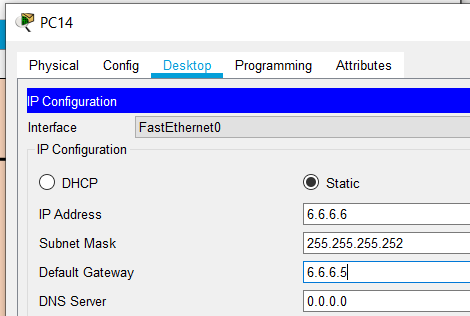
Zadaní číslo 11.

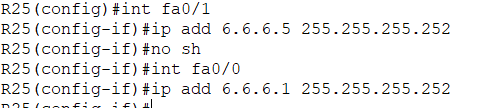


1. Nastav ip addresy zařízením
2. Routujte pomocí protokolu RIP
3. R26 bude NTP server pro R25 jako addresa serveru bude použita addresa 6.6.6.12/32 z loopbacku
4. Zajisti at se posilají logy s přesností na milisekundy na syslog server 6.6.6.2 z R26

**Vypracování**

**1.**



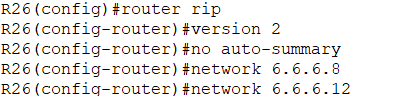
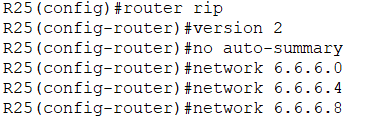








2



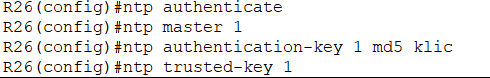
3.

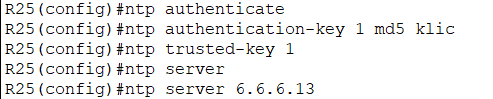
Normálně mají síťové zařízení svůj vlastní časový mechanismus. Zařízením však můžeme nastavit tzn. NTP server podle, kterého se zařízení synchronují a všechny mají stejný čas.

Na obou zařízeních musí být nastavený klíč a trusted key jeden je ntp master a ten co příjma ntp pakety si jenom nastaví ntp server



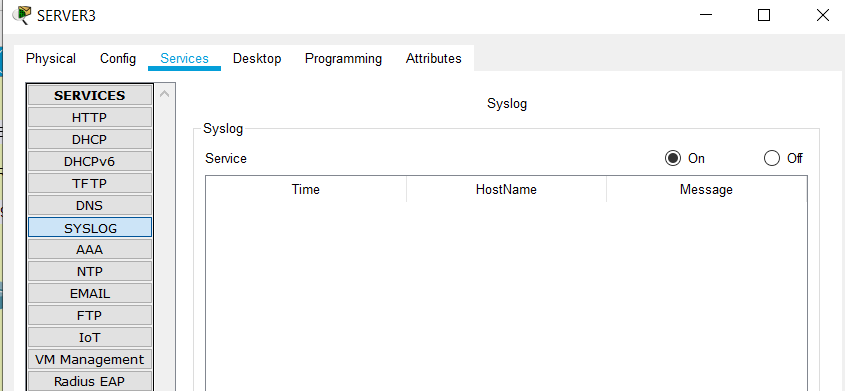
Povolili jsme ntp komunikaci, nastavili r26 jako master vytvořili klic s nazvem klijc a nastavili duveryhodne klice na 1



Nastavili jsme to stejne akorát není master ale má svůj server 

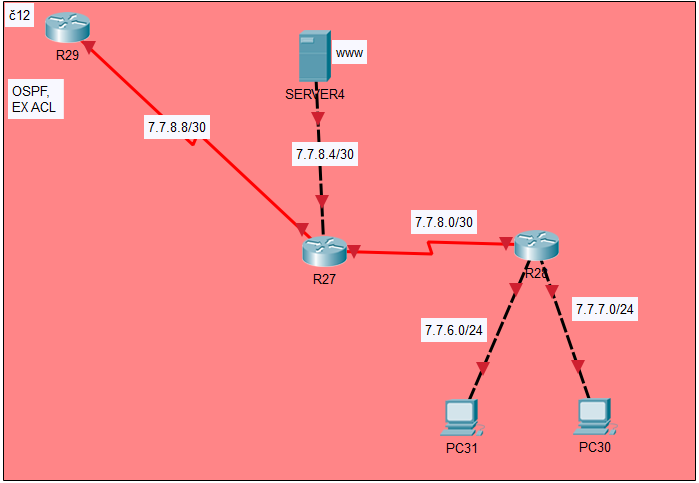
4.

Syslog službu mám zaplou



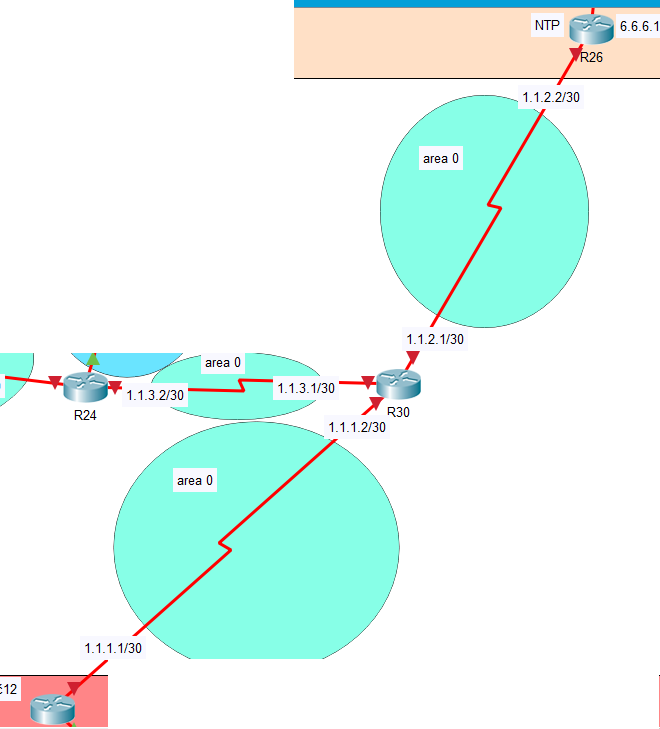


**Extendet access list**



1. Nastav ip addresy
2. Nastav ospf vše v arei 3
3. Ze sítě 7.7.7.0/24 Zakaž všechny porty na SERVER4 kromně http (zkouška: icmp nebude fungovat, ale webovka jo)

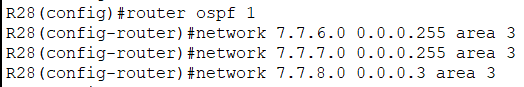
ZÁVĚREČNÉ ROUTOVÁNÍ

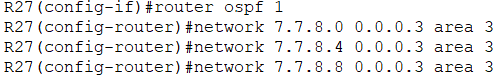


1.

|  |  |  |  |
| --- | --- | --- | --- |
| Název zařízení | Číslo interfaceu | Ip addresa | Maska |
| R28 | Fa0/1 | 7.7.6.1 | 255.255.255.0 |
|  | Fa0/0 | 7.7.7.1 | 255.255.255.0 |
|  | S0/0/0 | 7.7.8.1 | 255.255.255.252 |
| R27 | S0/0/0 | 7.7.8.2 | 255.255.255.252 |
|  | Fa0/0 | 7.7.8.5 | 255.255.255.252 |
|  | S0/0/1 | 7.7.8.9 | 255.255.255.252 |
| R29 | S0/0/1 | 7.7.8.10 | 255.255.255.252 |
| PC30 |  | 7.7.7.10 | 255.255.255.0 |
| PC31 |  | 7.7.6.10 | 255.255.255.0 |
| SERVER4 |  | 7.7.8.6 | 255.255.255.252 |

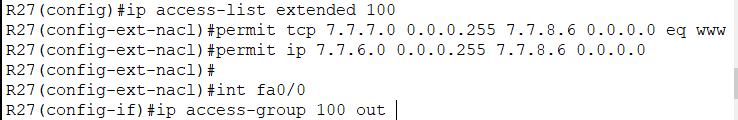
2.



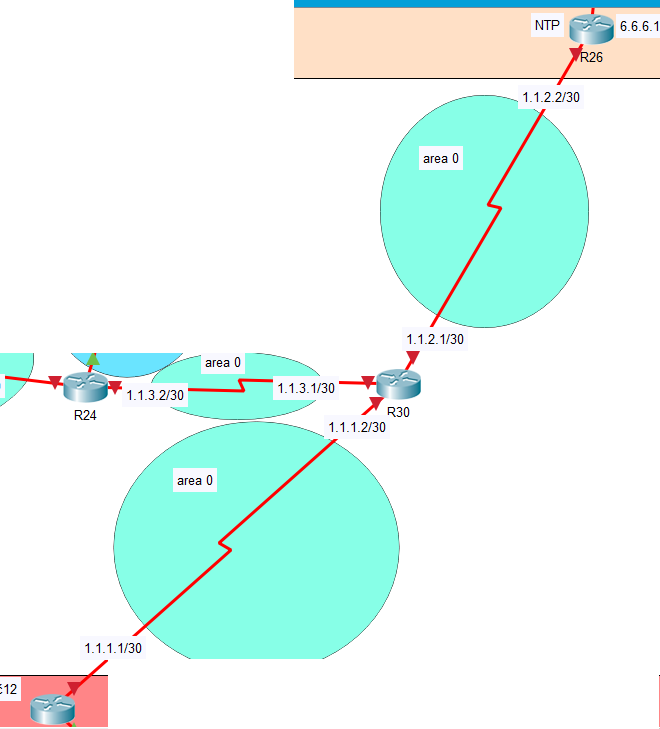




3.

U access listu je vždycky poslední příkaz ten který zakáže všechno ostatní a zároveň je třeba si uvědomit směr tady to je out of interface čili pakety budou zahoreny na R27 int fa0/0 než vůbec dojdou k serveru 

Dilčí část



Ip addresy jsou na schématu

1. Nastav ip
2. Nakonfiguruj ospf
3. Redistrubuj protokoly

R26

router ospf 1

network 1.1.2.0 0.0.0.3 area 0

redistribute rip metric 0 subnets tag 0

router rip

redistribute ospf 1

R29

router ospf 1

network 1.1.1.0 0.0.0.3 area 0

R30

router ospf 1

network 1.1.1.0 0.0.0.3 area 0

network 1.1.2.0 0.0.0.3 area 0

network 1.1.3.0 0.0.0.3 area 0

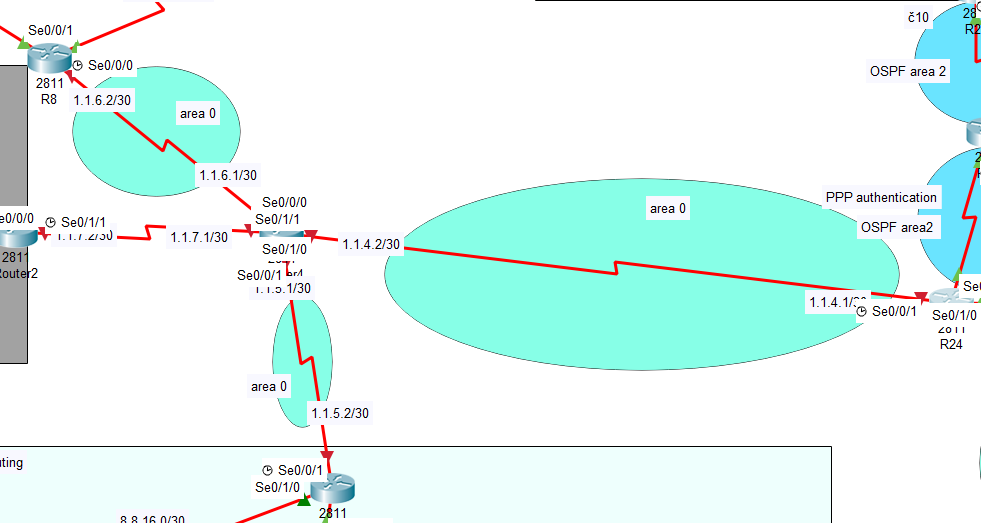
R24

router ospf 1

network 1.1.3.0 0.0.0.3 area 0

network 1.1.4.0 0.0.0.3 area 0

Další část



R31

router ospf 1

network 1.1.4.0 0.0.0.3 area 0

network 1.1.5.0 0.0.0.3 area 0

network 1.1.6.0 0.0.0.3 area 0

network 1.1.7.0 0.0.0.3 area 0

R19

router ospf 1

network 1.1.5.0 0.0.0.3 area 0

redistribute eigrp 2 metric 0 subnets tag 0

router eigrp 2

redistribute ospf 1

R8

router ospf 1

network 1.1.6.0 0.0.0.3 area 0

redistribute rip metric 0 subnets tag 0

router rip

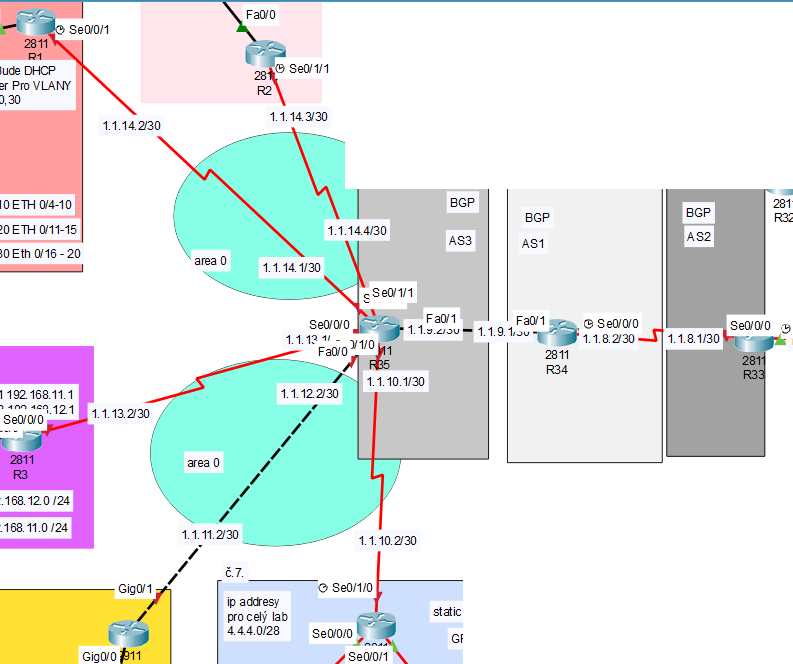
redistribute ospf 1

R33

router ospf 1

network 1.1.7.0 0.0.0.3 area 0

Poslední dílčí úloha



R2

router ospf 1

network 1.1.15.0 0.0.0.3 area 0

R1

router ospf 1

network 1.1.14.0 0.0.0.3 area 0

R3

router ospf 1

network 1.1.13.0 0.0.0.3 area 0

R10

router ospf 1

network 1.1.11.0 0.0.0.3 area 0

R12

router ospf 12

network 1.1.10.0 0.0.0.3 area 0

R35

router ospf 1

network 1.1.15.0 0.0.0.3 area 0

network 1.1.14.0 0.0.0.3 area 0

network 1.1.13.0 0.0.0.3 area 0

network 1.1.11.0 0.0.0.3 area 0

network 1.1.10.0 0.0.0.3 area 0

router bgp 3

neighbor 1.1.9.1 remote-as 1

redistribute ospf 1

R34

router bgp 1

neighbor 1.1.9.2 remote-as 3

neighbor 1.1.8.1 remote-as 2

redistribute ospf 1

R33

router bgp 1

neighbor 1.1.2.2 remote-as 1

redistribute ospf 1