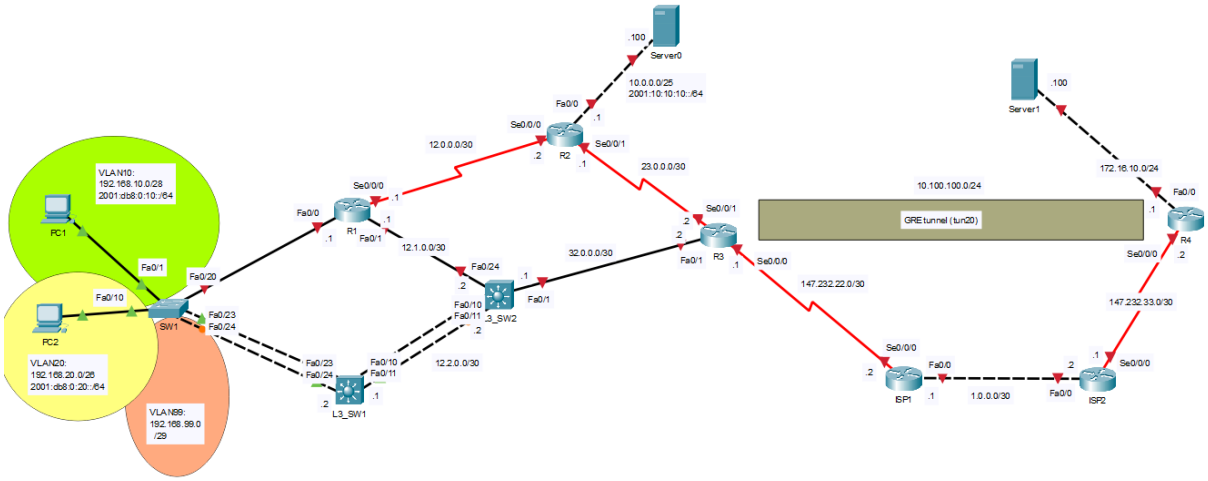
NAG2020 – Riešenie

Topológia:



Úlohy a riešenie:

1. Na prepínači SW1 vytvorte VLAN 10, 20 a 99. Rozhranie, ku ktorému je pripojené zariadenie PC1 priraďte do VLAN 10. Rozhranie, ku ktorému sa pripája zariadenie PC2 nech je vo VLAN 20. Zabezpečte, aby VLAN 20 bola VLAN, ktorej dáta budú prenášané trunk rozhraniami neznačené. Na prepínač SW1 nakonfigurujte tretiu použiteľnú adresu z VLAN 99. Zabezpečte možnosť komunikácie s prepínačom aj zo vzdialených sietí.

SW1:

```
vlan 10
vlan 20
vlan 99
interface fa0/1
  switchport mode access
  switchport access vlan 10
interface fa0/10
  switchport mode access
  switchport access vlan 20
interface vlan 99
  ip address 192.168.99.3 255.255.255.248
ip default-gateway 192.168.99.6
```

2. Uistite sa, že rozhranie Fa0/1 na prepínači SW1 má implementované nasledujúce bezpečnostné mechanizmy. Maximálny počet MAC adries nech je 2, v prípade, ak dôjde k porušeniu bezpečnostných pravidiel, nech dané rozhranie prestane preposielať dáta zo zariadenia, ktoré porušuje pravidlá.

Porušenie pravidiel nesmie spôsobiť vygenerovanie log. správy o porušení. Nastavte tiež mechanizmus učenia sa bezpečných MAC adries, ktorý naučené MAC adresy automaticky prevedie do bežiacej konfigurácie.

SW1:
```
interface fa0/1
  switchport port-security maximum 2
  switchport port-security violation protect
  switchport port-security mac-address sticky
  switchport port-security
```

3. Medzi zariadeniami SW1 a L3_SW1 vytvorte etherchannel, ktorý umožňuje vložiť do etherchannelu maximálne 8 fyzických rozhraní. Vytvorené rozhranie Port-Channel nech má číslo 4. Zabezpečte, aby obe zariadenia boli aktívne pri vyjednávaní EtherChannelu.

SW1:
```
interface range fa0/23-24
  channel-group 4 mode desirable
```

L3_SW1:
```
interface range fa0/23-24
  channel-group 4 mode desirable
```

4. Zabezpečte, aby zariadenie L3_SW1 bolo koreňovým prepínačom v rámci protokolu STP pre všetky tri VLAN. Konfiguračne mu priraďte najlepšiu možnú hodnotu priority. Na prepínači SW1 nastavte rozhrania kde sú pripojené koncové zariadenia tak, aby zariadenia vedeli komunikovať okamžite po pripojení sa na prepínač. Tiež implementujte bezpečnostný mechanizmus, ktorý neumožní na príslušné rozhrania pripojiť prepínač.

L3_SW1:
```
vlan 10
vlan 20
vlan 99
spanning-tree vlan 10 priority 0
spanning-tree vlan 20 priority 0
spanning-tree vlan 99 priority 0
```

SW1:
```
interface range fa0/1, fa0/10
  spanning-tree portfast
  spanning-tree bpduguard enable
```

5. Medzi zariadeniami L3_SW1 a L3_SW2 vytvorte **L3** EtherChannel, ktorý je možné použiť medzi zariadeniami od rôznych výrobcov. Zariadenie L3_SW1 má byť v stave, v ktorom samo nevyžaduje vytvorenie EtherChannelu, ale v prípade aktivity z druhej strany EtherChannel vytvorí. Zariadenie L3_SW2 nakonfigurujte tak, aby podnecovalo vytvorenie EtherChannelu. Číslo vytvoreného PortChannelu nech je 3. Adresáciu na jednotlivých rozhraniach nakonfigurujte podľa údajov v topológii.

L3_SW1:
```
interface range fa0/10-11
  no switchport
  channel-group 3 mode passive
interface port-channel 3
  ip address 12.2.0.1 255.255.255.252
```

L3_SW2:
```
interface range fa0/10-11
  no switchport
  channel-group 3 mode active
interface port-channel 3
  ip address 12.2.0.2 255.255.255.252
```

6. Podľa topológie nakonfigurujte sieťové nastavenia na všetky zariadenia.

Nasledujúce úlohy obsahujú aj pokyny ku konfigurácií sieťových nastavení, teda v tejto chvíli túto úlohu preskočím.

R1:
```
interface se0/0/0
  ip address 12.0.0.1 255.255.255.252
  no shutdown
interface fa0/1
  ip address 12.1.0.1 255.255.255.252
  no shutdown
```

R2:
```
interface se0/0/0
  ip address 12.0.0.2 255.255.255.252
  no shutdown
interface se0/0/1
  ip address 23.0.0.1 255.255.255.252
  no shutdown
interface fa0/0
  ip address 10.0.0.1 255.255.255.128
  no shutdown
```

R3:

```
interface fa0/1
  ip address 32.0.0.2 255.255.255.252
  no shutdown
interface se0/0/0
  ip address 147.232.22.1 255.255.255.252
  no shutdown
int se0/0/0
  ip address 147.232.22.1 255.255.255.252
  no shutdown
interface se0/0/1
  ip address 23.0.0.2 255.255.255.252
  no shutdown
```

ISP1:

```
int se0/0/0
  ip address 147.232.22.2 255.255.255.252
  no shutdown
  int fa0/0
  ip address 1.0.0.1 255.255.255.252
  no shutdown
```

ISP2:

```
int fa0/0
  ip address 1.0.0.2 255.255.255.252
  no shutdown
  int se0/0/0
  ip address 147.232.33.1 255.255.255.252
  no shutdown
```

R4:

```
int se0/0/0
  ip address 147.232.33.2 255.255.255.252
  no shutdown
  int fa0/0
  ip add 172.16.10.1 255.255.255.0
  no shutdown
```

L3_SW2:

```
int fa0/1
  no switchport
  ip add 32.0.0.1 255.255.255.252
interface fa0/24
  no switchport
  ip address 12.1.0.2 255.255.255.252
```

Server0:
IPv4 adresa: `10.0.0.100`
IPv4 maska: `255.255.255.128`
IPv4 brána: `10.0.0.1`

Server1:
IPv4 adresa: `172.16.10.100`
IPv4 maska: `255.255.255.0`
IPv4 brána: `172.16.10.1`

7. Zariadenia R1 a L3_SW1 predstavujú bránu do siete pre zariadenia PC1 a PC2. Implementujte pre všetky tri VLAN protokol redundancie brány, ktorý je cisco proprietárnym protokolom, ktorý nemá v základnom nastavení implementovaný mechanizmus rozkladania záťaže. Zariadenia R1 a L3_SW1 zároveň majú za úlohu zabezpečiť smerovanie dát medzi VLAN. V prípade vytvárania subrozhraní použite číslo subrozhraní totožné s číslom VLAN, pre ktoré dané subrozhrania vytvárate. Na zariadení L3_SW1 využite na smerovanie dát medzi VLAN SVI. Čo sa adresácie týka, tak zariadenie R1 nech využíva vždy prvú použiteľnú adresu a zariadenie L3_SW1 nech využíva druhú použiteľnú adresu z daných VLAN.

   Čo sa týka redundancie brány, tak číslo virtuálnej skupiny je totožné s číslom VLAN. Tiež zabezpečte, aby zariadenie R1 bolo aktívnym zariadením pre VLAN 10 a 99. Pre VLAN 20 nech je aktívnym zariadením zariadenie L3_SW1. Virtuálne IP adresy nech sú posledné použiteľné adresy z daných VLAN. Aktívne zariadenia nech majú nakonfigurovanú najlepšiu možnú prioritu.

R1:
```
interface fa0/0.10
  encapsulation dot1Q 10
  ip address 192.168.10.1 255.255.255.240
  standby 10 ip 192.168.10.14
  standby 10 priority 255
interface fa0/0.20
  encapsulation dot1Q 20 native
  ip address 192.168.20.1 255.255.255.192
  standby 20 ip 192.168.20.62
interface fa0/0.99
  encapsulation dot1Q 99
  ip address 192.168.99.1 255.255.255.248
  standby 99 ip 192.168.99.6
```

```
  standby 99 priority 255
interface fa0/0
  no shutdown
```

L3_SW1:

```
interface port-channel 4
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 20
interface vlan 10
  ip address 192.168.10.2 255.255.255.240
  standby 10 ip 192.168.10.14
interface vlan 20
  ip address 192.168.20.2 255.255.255.192
  standby 20 ip 192.168.20.62
  standby 20 priority 255
interface vlan 99
  ip address 192.168.99.2 255.255.255.248
  standby 99 ip 192.168.99.6
ip routing
```

SW1:

```
interface range fa0/20, fa0/23-24
  switchport mode trunk
  switchport trunk native vlan 20
```

8. Smerovač R2 naučte o existencii siete VLAN 10. Primárna cesta do tejto VLAN nech vedie cez zariadenie R1. Nastavte tiež záložnú cestu do tejto VLAN cez zariadenie R3. V oboch prípadoch využite na určenie smeru výstupné rozhranie. Záložnej ceste priraďte administratívnu vzdialenosť 10.

   Smerovač R3 naučte o existencií siete VLAN 10 tak, že ako primárnu cestu využite cestu cez zariadenie L3_SW2 (využite tvar statickej cesty, ktorý je pre danú prepojovaciu technológiu vhodný). Ako záložnú cestu (AD = 100) pre smerovač R3 využite cestu cez zariadenie R2, kde na určenie smeru využite výstupné rozhranie.

   V prípade zariadenia L3_SW2 vytvorte primárnu statickú cestu cez zariadenie R1, kde na určenie smeru využite next-hop IPv4 adresu. Záložná cesta (AD = 10) nech je cez zariadenie L3_SW1, kde na určenie smeru využite vhodný tvar statickej cesty.

Statickou cestou naučte smerovač R1 o existencii zariadenia Server0 (nie o existencii celej siete!!!). Na určenie smeru využite výstupné rozhranie.

R2:

```
ip route 192.168.10.0 255.255.255.240 se0/0/0
ip route 192.168.10.0 255.255.255.240 se0/0/1 10
```

R3:

```
ip route 192.168.10.0 255.255.255.240 32.0.0.1
ip route 192.168.10.0 255.255.255.240 serial 0/0/1 100
```

L3_SW2:

```
ip route 192.168.10.0 255.255.255.240 12.1.0.1
ip route 192.168.10.0 255.255.255.240 12.2.0.1 10
```

R1:

```
ip route 10.0.0.100 255.255.255.255 se0/0/0
```

9. Naučte o existencií siete VLAN 20 (dosiahnuteľná cez zariadenia R1 a L3_SW1) nasledovné zariadenia: R2, L3_SW2 a R3. Na vyriešenie tejto úlohy využite **LEN** protokol EIGRP v rámci AS 100. Protokol EIGRP má byť spustený aj na zariadeniach R1 a L3_SW1. Uistite sa, že pri konfigurácií protokolu EIGRP využijete wildcard 0.0.0.0. Nezabudnite na to, že do siete VLAN 20 sa má dať dostať aj využitím všetkých záložných ciest.

R1:

```
router eigrp 100
  no auto-summary
  network 192.168.20.1 0.0.0.0
  network 12.0.0.1 0.0.0.0
  network 12.1.0.1 0.0.0.0
```

L3_SW1:

```
router eigrp 100
  no auto-summary
  network 192.168.20.2 0.0.0.0
  network 12.2.0.1 0.0.0.0
```

L3_SW2:

```
ip routing
router eigrp 100
  no auto-summary
```

```
  network 12.2.0.2 0.0.0.0
  network 12.1.0.2 0.0.0.0
  network 32.0.0.1 0.0.0.0
```

R2:

```
router eigrp 100
  no auto-summary
  network 12.0.0.2 0.0.0.0
  network 23.0.0.1 0.0.0.0
```

R3:

```
router eigrp 100
  no auto-summary
  network 32.0.0.2 0.0.0.0
  network 23.0.0.2 0.0.0.0
```

10. Naučte o existencií siete VLAN 99 (dosiahnuteľná cez zariadenia R1 a L3_SW1) nasledovné zariadenia: R2, L3_SW2 a R3. Na vyriešenie tejto úlohy využite **LEN** protokol OSPF v rámci oblasti 0. Protokol OSPF má byť spustený aj na zariadeniach R1 a L3_SW1. Uistite sa, že pri konfigurácií protokolu OSPF využijete wildcard podľa príslušnej masky daných sietí. Nezabudnite na to, že do siete VLAN 99 sa má dať dostať aj využitím všetkých záložných ciest. Číslo OSPF procesu nech je 1 na všetkých zariadeniach.

R1:

```
router ospf 1
  network 192.168.99.0 0.0.0.7 area 0
  network 12.0.0.0 0.0.0.3 area 0
  network 12.1.0.0 0.0.0.3 area 0
```

L3_SW1:

```
router ospf 1
  network 192.168.99.0 0.0.0.7 area 0
  network 12.2.0.0 0.0.0.3 area 0
```

L3_SW2:

```
router ospf 1
  network 12.1.0.0 0.0.0.3 area 0
  network 12.2.0.0 0.0.0.3 area 0
  network 32.0.0.0 0.0.0.3 area 0
```

R2:

```
router ospf 1
  network 12.0.0.0 0.0.0.3 area 0
```

```
  network 23.0.0.0 0.0.0.3 area 0
```

R3:

```
router ospf 1
  network 23.0.0.0 0.0.0.3 area 0
  network 32.0.0.0 0.0.0.3 area 0
```

11. Zabezpečte, aby zariadenie R3 smerovalo komunikáciu do neznámych sietí na smerovač ISP1. Smer definujte výstupným rozhraním. Informáciu o tejto statickej ceste distribuujte do LAN sieti protokolom OSPF (proces 1), ale len v prípade, ak je daná statická cesta aj nakonfigurovaná.

R3:

```
ip route 0.0.0.0 0.0.0.0 se0/0/0
router ospf 1
  default-information originate
```

12. Medzi smerovačmi ISP1 (AS 100) a ISP2 (AS 200) spusťte protokol BGP a oznámte do neho siete, ktoré sa nachádzajú na rozhraniach se0/0/0.

ISP1:

```
router bgp 100
  neighbor 1.0.0.2 remote-as 200
  network 147.232.22.0 mask 255.255.255.252
```

ISP2:

```
router bgp 200
  neighbor 1.0.0.1 remote-as 100
  network 147.232.33.0 mask 255.255.255.252
```

13. Medzi zariadením R3 a R4 vytvorte GRE tunel s číslom 20, ktorý umožní komunikáciu so zariadením Server1 využitím súkromných adries len z VLAN 20. Z pohľadu smerovania využite protokol EIGRP (AS 100), kde pri definovaní rozhraní využite wildcard 0.0.0.0. Vytvorený tunel nech používa sieť 10.100.100.0/24 pričom na smerovači R3 nech je nakonfigurovaná prvá použiteľná adresa a na smerovači R4 posledná použiteľná adresa. Zabezpečte, aby smerovač R4 posielal všetku komunikáciu do neznámych sieti na smerovač ISP2. Na vyriešenie tejto úlohy využite statickú cestu, ktorá bude využívať na určenie smeru výstupné rozhranie.

R3:

```
interface tunnel 20
  ip address 10.100.100.1 255.255.255.0
  tunnel source se0/0/0
```

```
  tunnel destination 147.232.33.2
router eigrp 100
  network 10.100.100.1 0.0.0.0
```

R4:

```
ip route 0.0.0.0 0.0.0.0 se0/0/0
int tunnel 20
  ip address 10.100.100.254 255.255.255.0
  tunnel source se0/0/0
  tunnel destination 147.232.22.1
router eigrp 100
  no auto-summary
  network 10.100.100.254 0.0.0.0
  network 172.16.10.1 0.0.0.0
```

14. Zabezpečte komunikáciu medzi zariadením PC1 a zariadením Server0 využitím protokolu IPv6. Smerovania nech sa zúčastňujú len zariadenia R1 a R2. Ako smerovací protokol využite protokol OSPF (číslo procesu nech je 1, oblasť je 0). Na smerovače (LAN rozhranie) priraďte prvé použiteľné adresy. Adresovanie na seriovej linke nastavte tak, aby ste pri tom nepoužili príkaz, ktorý obsahuje kľúčové slovo "address".

R1:

```
ipv6 unicast-routing
interface fa0/0.10
  ipv6 address 2001:db8:0:10::1/64
  ipv6 ospf 1 area 0
interface se0/0/0
  ipv6 enable
  ipv6 ospf 1 area 0
```

R2:

```
ipv6 unicast-routing
interface fa0/0
  ipv6 address 2001:10:10:10::1/64
  ipv6 ospf 1 area 0
int se0/0/0
  ipv6 enable
  ipv6 ospf 1 area 0
```

15. Zabezpečte komunikáciu medzi zariadením PC2 a zariadením Server0 využitím protokolu IPv6. Smerovania nech sa zúčastňujú len zariadenia R1 a R2. Ako smerovací protokol využite protokol RIP (názov inštancie nech

je **NAG**). Na smerovače (LAN rozhranie) priraďte prvé použiteľné adresy. Adresovanie na seriovej linke nastavte tak, aby ste pri tom nepoužili príkaz, ktorý obsahuje kľúčové slovo "address".

R1:

```
interface fa0/0.20
  ipv6 address 2001:db8:0:20::1/64
  ipv6 rip NAG enable
interface se0/0/0
  ipv6 rip NAG enable
```

R2:

```
interface se0/0/0
  ipv6 rip NAG enable
  interface fa0/0
  ipv6 rip NAG enable
```

16. Zabezpečte, aby smerovač R2 (12.0.0.2) plnil úlohu DHCP servera pre zariadenia vo VLAN 10. Pool nech sa volá L10. Tiež vylúčte IPv4 adresy, ktoré nemajú byť prideľované z prideľovania DHCP servera. Nezabudnite k sieťovým nastaveniam, ktoré budú prideľované zahrnúť aj adresu servera, ktorý bude prekladať doménové názvy na IPv4 adresy (10.0.0.100). Mechanizmus DHCP relay konfigurujte na zariadení, ktoré má pre danú VLAN preposielať komunikáciu.

R2:

```
ip dhcp excluded-address 192.168.10.1 192.168.10.2
ip dhcp excluded-address 192.168.10.14
ip dhcp pool L10
  default-router 192.168.10.14
  dns-server 10.0.0.100
  network 192.168.10.0 255.255.255.240
```

R1:

```
interface fa0/0.10
  ip helper-address 12.0.0.2
```

L3_SW1:

```
interface vlan 10
  ip helper-address 12.0.0.2
```

17. Zabezpečte, aby zariadenie R3 umožňovalo prekladať všetky adresy z VLAN 10 na verejnú adresu, ktorá je podľa topológie priradená rozhraniu se0/0/0. Komunikovať majú vedieť všetky zariadenia súčasne. Prístupový zoznam,

ktorým identifikujete sieť VLAN10 nech má číslo 10. Pri konfigurácií prekladu nesmiete vytvoriť žiaden Pool.

R3:

```
access-list 10 permit 192.168.10.0 0.0.0.15
ip nat inside source list 10 interface se0/0/0 overload
interface fa0/1
  ip nat inside
int se0/0/1
  ip nat inside
int se0/0/0
  ip nat outside
```

18. Zabezpečte, aby všetky SYSLOG správy zo zariadenia R1 boli odosielané na zariadenie Server0.

R1:

```
logging 10.0.0.100
```

KONIEC ZADANIA