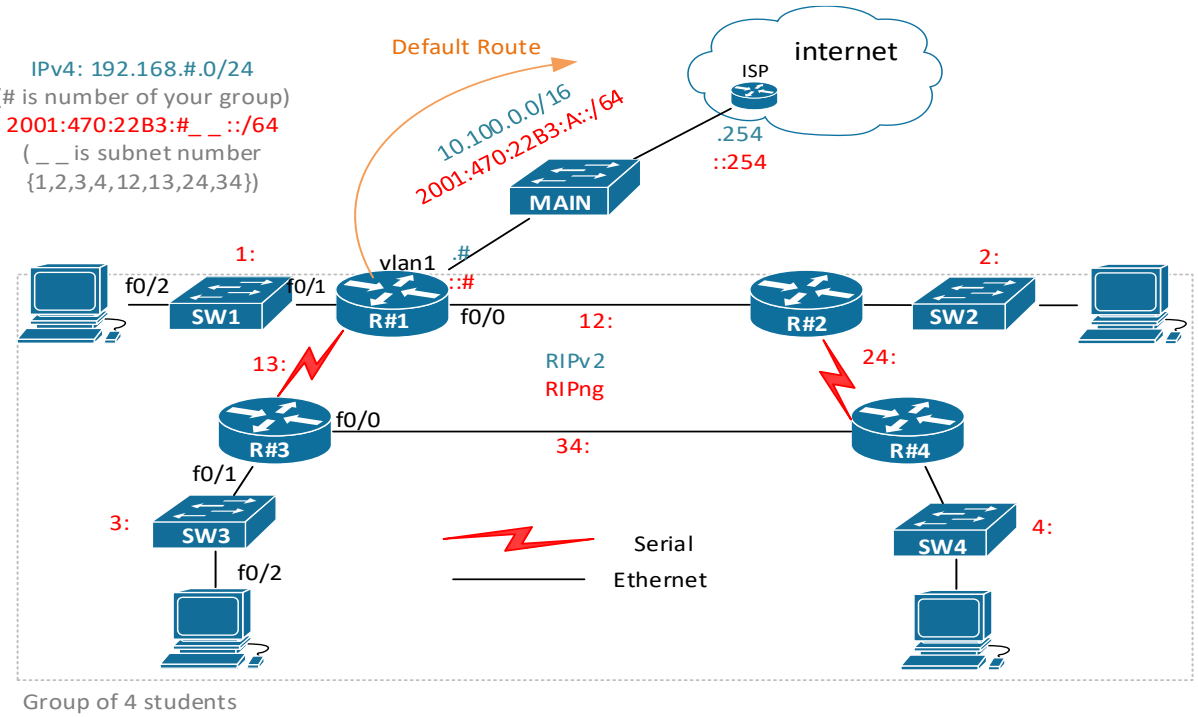
PS1 / cvičenie 04 / **Konfigurácia prepínača a port security**

Topológia



Group of 4 students

Inštrukcie k zapojeniu a adresovaniu

- Štvorica smerovačov do kruhu, na každom jeden prepínač (2960 alebo 3560) a pripojenie na PC
  - **Nepoužívajte prepínač 3750** (Kvôli tomu, že nemá podporu pre LLDP protokol. Beží tam IOS ver. 12)
- Pracuje sa vo štvoriciach (pri nepárnom počte študentov môžu byť aj trojice alebo pätice)
  - **R1** si vyberte taký, ktorý má 3 ethernetové rozhrania (aby sme sa vyhli čo najviac sériovým rozhraniam). Ako tretie rozhranie možno použiť jeden port z modulu **HWIC-4ESW**:
    - Ideálne nech vedie k hlavnému prepínaču
    - Konfigurovať IP adresu potom ale treba takto: `int vlan 1, ip add ADRESA MASKA` (rovnako ako keď konfigurujete IP adresu prepínaču pre vzdialený manažment)
    - Tieto moduly obsahuje 16 smerovačov v labe RB303
- IPv4 rozsah pre skupinu (podobne ako minule): **192.168.#.0/24**, # je číslo skupiny
  - Rozsah si subsieťujte, počítajte že LAN sú veľkosti 32
- IPv6 sa rieši až na koniec, ak vyjde čas. IPv6 rozsah pre skupinu (podobne ako minule): **2001:470:22B3:#_ _::/64**, kde # je číslo vašej skupiny a na miesto _ _ doplníme číslo subsiete:
  - pre LAN použite čísla subsietí: 1, 2, 3, 4 podľa toho na ktorý smerovač je pripojená daná LAN
  - pre WAN linky medzi smerovačmi použite číslo subsiete 12, 13, 34, 24, podľa toho z ktorého na ktorý smerovač daná linka vedie (12 je linka medzi R1 a R2)
  - nezabudnite zmeniť aj link-local adresy na smerovačoch tak, že link-local adresy všetkých rozhraní smerovača X budú FE80::X (pre R1 to bude FE80::1 na všetkých jeho 4 rozhraniach), inak IPv6 smerovacia tabuľka nebude prehľadná

- kroky, ktoré sú v postupe tohto zadania zvýraznené modrým, je potrebné si dokumentovať (prezentujete priebežne vyučujúcemu)

Zadanie

1. **Základná konfigurácia** prepínača (aj smerovača) – nastavte:
   a. Hostname R#1, R#2, … (pre skupinu 2 to bude R21, R22, R23, R24)
   b. Zmeňte veľkosť histórie príkazov na počet 50 (`terminal history size 50`), defaultne je 10.
   c. Správu dňa (MOTD)
   d. Heslá – na konzolu, telnet (pre prepínač), ssh (pre smerovač), do privilegovaného módu, zašifrujte všetky heslá
   e. Vypnite automatické vyhľadávanie doménových mien (DNS lookup) – toto by ste mali ideálne na začiatku každého cvičenia.
      i. keď budete chcieť neskôr použiť DNS, treba to znova povoliť
   f. Nastavte používanie DNS servera 8.8.8.8 `(ip name-server 8.8.8.8)`
      i. Aby sme vedeli ako, ale nevyužijeme, lebo.. bod e.
   g. Nastavte ochranu proti zmiešavaniu vstupu a výstupu CMD `(line console 0, logging synchronous)`
   h. Nastavte IP adresy všetkým zariadeniam v topológií – aj prepínačom (pre vzdialené prihlasovanie), prepínaču aj default-gateway
      i. Odteraz si môžete otvoriť dve inštancie PuTTY, v jednej sa pripojiť na prepínač cez konzolové pripojenie, v druhej na smerovač cez SSH.
   i. Zobrazte si sumárny prehľad o IP adresách rozhraní (na SW, aj R)
   j. Zálohujte bežiacu konfiguráciu do NVRAM pamäti (odporúčame robiť priebežne)
   k. Zobrazte si prepínaciu tabuľku na prepínači `(show mac-address table)`
      i. Zabezpečte aby obsahovala nejaké data
      ii. Čo sa z nej dá vyčítať?
   l. Zobrazte si ARP tabuľku na prepínači
      i. Zabezpečte aby obsahovala nejaké dáta
      ii. Čo sa z nej dá vyčítať?
      iii. Odchyťte ARP komunikáciu Wiresharkom, preskúmajte ARP hlavičku (pre request a response), a v akých PDU nižších vrstiev sa prenáša
   m. Zobrazte si smerovaciu tabuľku na smerovači
   n. Zobrazte si výpisy rôznych show príkazov na prepínači `(sh run, sh vlan, sh flash, sh version, sh int status, sh int, sh ip int br, sh history)`.
2. **LEDky**
   a. Všimnite si aké LEDky na prepínači vám svietia a prečo.
   Pre kontrolu, čo ktorá LED znamená, aj keď budete neskôr meniť význam LED pre porty, tak pripomenutie máte v prednáške, alebo aj na tomto zdroji:
   https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/hardware/installation/guide/2960_hg/higover.html
   v sekcii textu:
   LEDs
   You can use the switch LEDs to monitor switch activity and its performance.
   ...
   b. LEDky pri portoch vám aktuálne ukazujú status – aktivitu na porte. Zmeňte zobrazovanie daných LED, aby signalizovali DUPLEX (použite tlačidlo MODE). Čo signalizujú? (full/half?) Zmeňte teraz port na smerovači na half duplex (robí sa na rozhraní), a odsledujte čo sa stane

– sledujte hlášky z prepínača a sledujte aj LED pri portoch na prepínači. Zaznamenajte si zmeny a vráťte nastavenie znovu do full duplex.

c. Zmeňte teraz nastavenie LED pre porty tak, aby signalizovali SPEED. (použite MODE tlačidlo). Zistite aké rýchle máte porty na prepínači `(show int.. )`. Odsledujte čo ukazujú LEDky. Zmeňte teraz prepoj medzi smerovačom a prepínačom na pomalší (t.j. ak bol 100Mbps, nastavte 10 Mbps...). Overte svoju konfiguráciu `(show int..)` a odsledujte teraz LEDky na portoch.

d. Po experimentoch vráťte zobrazovanie LED, aj nastavenia portov do pôvodného stavu.

e. *Pozn.*: Na niektorých prepínačoch je aj možnosť signalizácie LEDiek pre UTIL (utilization). Vysvetlenie nájdete na konci dokumentu v *prílohe A*.

3. **CDP**
   a. Overte či je CDP aktivované globálne aj na rozhraniach `(show cdp, show cdp interface, sho cdp status, show cdp ?)`
   b. Zobrazte si info o susedných cisco zariadeniach cez CDP protokol `(show cdp neighbors)`
   c. Viete zistiť IP adresu susedného zariadenia cez CDP? Napr. z prepínača info o smerovači? `(show cdp neighbors details)`
   d. Odchyťte CDP na PC cez Wireshark, preskúmajte CDP správu, a v akom Ethernetovom rámci sa prenáša (Ethernet II? LLC? SNAP?)
      i. Pozrite aj na akú cieľovú MAC adresu sa dané CDP správy posielajú (rozbaľte si hlavičku Ethernet rámca)
      Hint: Verejne známe multicastové MAC adresy si môžete pozrieť napríklad tu: https://embeddist.wordpress.com/2015/10/07/well-known-ethernet-multicast-address/
4. **LLDP**
   a. Overte či je LLDP aktivované `(show lldp, R(config)#(no) lldp run)`
      i. Na prepínačoch 3550 alebo 3750 s verziou IOSu 12 nie je LLDP podporované. Preto si v tomto bode zaznačte, na akom modeli zariadenia, s akým IOSom ste pracovali `(show version)`, a pokračujte na takom (smerovač alebo prepínač), na ktorom je podporované
   b. Zobrazte si info o susedných zariadeniach cez LLDP protokol `(sh lldp neighbors)`
   c. Viete zistiť IP adresu susedného zariadenia cez LLDP? Napr. z prepínača info o smerovači? `(sh lldp neighbors detail)`
   d. Odchyťte LLDP na PC cez Wireshark, preskúmajte LLDP správu, a v akom Ethernetovom rámci sa prenáša (Ethernet II, LLC, alebo SNAP?)
      i. Pozrite aj na akú cieľovú MAC adresu sa dané LLDP správy posielajú (rozbaľte si hlavičku Ethernet rámca)
      Hint: Verejne známe multicastové MAC adresy si môžete pozrieť napríklad tu: https://embeddist.wordpress.com/2015/10/07/well-known-ethernet-multicast-address/
5. **Port-security**
   a. Aktivujte pre port na ktorom máte pripojený počítač port-security s predvolenými nastaveniami.
   `(int f0/x, switchport mode access, switchport port-security)`
      i. Čo sa blokuje? Čo sa udeje keď nastane porušenie? Koľko je povolených MAC na porte? Overte si aktuálne nastavenie port security `(sh port-security int f0/x)`
      ii. Aký je toto typ zabezpečenia portov? (static, dynamic, sticky?)

iii. Otestujte či to funguje - pripojením svojho PC a potom si požičajte susedove (iná MAC) – v tomto prípade by sa nemala udiať žiadna zmena. Prečo?
iv. Následne si požičajte hub (v labe máme aktuálne na toto cvičenie pripravené dva, v ľavom a pravom racku, položené na smerovačoch) a vložte ho medzi váš prepínač a dva počítače
- Pingnite zo svojho aj susedovho PC smerovač.
- V akom stave je port po narušení bezpečnosti na porte? `(sh int f0/x status)`
- Ako dostanem port opäť do pôvodného stavu (active)? `(int f0/X, shut, no shut` – pozor nestačí iba `no shut)`

v. Akým príkazom vieme doplniť do predošlého, aby dynamicky povolilo iba 2 MAC adresy pre daný port? (ale nerobíme to, lebo nemáme dostatok PC na testovanie, na skúške sa môže objaviť)
vi. Vypnite port, na ktorom ste robili tento experiment, pred tým ako pôjdete na ďalší

b. Na inom porte nastavte statické port-security iba na 1 MAC adresu (susedove PC) a nastavte akciu pri porušení na protect, pripojte si do neho susedove PC (samozrejme zmení si IP adr.)
i. Spravte test: ping na váš smerovač zo susedovho PC, malo by prejsť.
ii. Následne odpojte suseda a zapojte do daného portu svoje PC. Overte či funguje. Čo sa udeje so stavom portu? – nemalo by sa nič `(sh ip int br, sh int f0/x)`. Pribudol nejaký záznam v running-config? – nemal by. Zvýšilo sa počítadlo porušení zabezpečenia na danom porte? – nemalo by. `(sh port-security int f0/x, sh int f0/x status)`
- Zaznamenajte si výsledky svojich experimentov.

iii. Vypnite port, na ktorom ste robili tento druhý experiment, pred tým ako pôjdete na ďalší (zrejme bude potrebné aj zmazať celé port security na tomto porte: `no switchport port-security` -> spravte to ale až keď vám nepôjde nasledujúci scenár, aby ste videli v čom je problém).

c. Na ďalšom porte nastavte dynamické port security +sticky na 1 MAC adresu, a nastavte akciu pri porušení na restrict, pripojte si do neho svoje PC
i. Overte či funguje (požičajte si susedove PC) – ping z PC na smerovač. Čo sa udeje s portom? Pribudol nejaký záznam v running-config? Zvýšilo sa počítadlo porušení zabezpečenia na danom porte? `(sh port-security int f0/x, sh int f0/x status)`

d. Ukončite experimenty s port-security a pripojte PC do portu, kde ste nenastavovali žiadnu L2 ochranu.

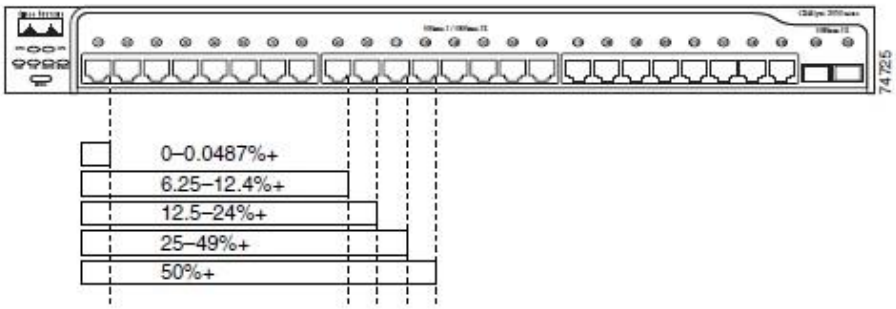
6. **Smerovanie** (na preopakovanie a precvičenie z minula)
a. Rozbehnite RIPv2 tak, aby ste mali konektivitu v celej vašej štvorici
b. K susednej štvorici nastavte statickú cestu cez smerovač R1 zo susednej skupiny a redistribuujte ju do RIPv2 domény
i. IP adresy ostávajú ako minule 10.100.0.#
ii. Skontrolujte obsahy IPv4 smerovacích tabuliek na všetkých smerovačoch, sledujte do akých cieľov existujú viaceré cesty s rovnakou metrikou.
iii. Otestujte konektivitu ku susednej skupine
c. Do internetu nastavte default route cez ISP a šírte ju ostatným smerovačom cez RIP.
i. ISP má 10.100.0.254
ii. Otestujte konektivitu do Internetu z vášho PC v IPv4
iii. Pozn.: Áno, bod b. by sme mohli vynechať, keďže sme vyriešili bod c. ktorý ním rieši konektivitu všade - aj do internetu aj k ostatným skupinám. Bod b. sme si pridali iba pre opakovanie konfigurácie špecifických IPv6 statických ciest.

d. Pokiaľ ste boli rýchli, rozbehnite aj RIPng, aby ste mali konektivitu v celej vašej štvorici, aj do internetu
   i. Adresa ISP je 2001:470:22B3:A::254, vaša je 2001:470:22B3:100::#, dĺžka prefixu /64
   ii. Skontrolujte obsahy IPv6 smerovacích tabuliek na všetkých smerovačoch, sledujte do akých cieľov existujú viaceré cesty s rovnakou metrikou.
   iii. Otestujte konektivitu do Internetu z vášho PC v IPv6, napr. k tejto IPv6 adrese: ping 2001:4860:4860::8888 (google public IPv6 DNS)

Príloha A: Účel módu UTIL pre LEDky na prepínači

Ak napríklad prvé dva porty svietia na zeleno, ďalšie 4 na oranžovo a zvyšné nesvietia vôbec, tak to znamená využitie šírky pásma na prepínači nízke, medzi 6.25% a 12.4%.

Figure 1-21 Bandwidth Utilization on Catalyst 2950-24, 2950C-24, 2950SX-24, and 2950T-24 Switches



If all LEDs on a Catalyst 2950-12, 2950-24, 2950C-24, 2950SX-24, or 2950T-24 switch are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the far-right LED is off, the switch is using more than 25 but less than 50 percent of the total bandwidth, and so on. If only the far-left LED is green, the switch is using less than 0.0488 percent of the total bandwidth. (See Figure 1-20 and Figure 1-21.)

UTIL (utilization)	Green	The current backplane utilization that is displayed over the amber LED background on a logarithmic scale.
	Amber	The maximum backplane utilization since the switch was powered on.
	Green and amber	See Figure 1-20 to Figure 1-24 for details. **Note** If the current utilization exceeds the maximum utilization, the maximum utilization is automatically updated.

Konfigurácia ISP smerovača (pre učiteľa, alebo šikovného študenta):

Ak neostala na smerovači pôvodná/základná konfigurácia (IPv6 tunel a pod.), treba ju nakopírovať z flash: config-2801.txt príkazom v privilegovanom móde:

```
config replace flash:config-2801.txt
```

A k tejto základnej konfigurácii pridať toto (ctrl+c, ctrl+v v globálnom config móde na smerovači):

```
!
hostname ISP
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0/0
 no shut
 ip address 10.100.0.254 255.255.0.0
 ip nat inside
 no ipv6 address 2001:470:22B3::1/64
 ipv6 address 2001:470:22B3:A::254/64
!
interface GigabitEthernet0/0/1
 no shut
 ip nat outside
 ip add dhcp
!
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
!
access-list 1 permit 192.0.0.0 0.255.255.255
access-list 1 permit 10.100.0.0 0.0.255.255
access-list 1 permit 10.200.0.0 0.0.255.255
!
ip route 192.168.1.0 255.255.255.0 10.100.0.1
ip route 192.168.2.0 255.255.255.0 10.100.0.2
ip route 192.168.3.0 255.255.255.0 10.100.0.3
ip route 192.168.4.0 255.255.255.0 10.100.0.4
ip route 192.168.5.0 255.255.255.0 10.100.0.5
ip route 192.168.6.0 255.255.255.0 10.100.0.6
ip route 192.168.7.0 255.255.255.0 10.100.0.7
ip route 192.168.8.0 255.255.255.0 10.100.0.8
ip route 192.168.9.0 255.255.255.0 10.100.0.9
ip route 192.168.10.0 255.255.255.0 10.100.0.10
!
ipv6 route 2001:470:22B3:100::/56 2001:470:22B3:A::1
ipv6 route 2001:470:22B3:200::/56 2001:470:22B3:A::2
ipv6 route 2001:470:22B3:300::/56 2001:470:22B3:A::3
ipv6 route 2001:470:22B3:400::/56 2001:470:22B3:A::4
ipv6 route 2001:470:22B3:500::/56 2001:470:22B3:A::5
ipv6 route 2001:470:22B3:600::/56 2001:470:22B3:A::6
ipv6 route 2001:470:22B3:700::/56 2001:470:22B3:A::7
ipv6 route 2001:470:22B3:800::/56 2001:470:22B3:A::8
ipv6 route 2001:470:22B3:900::/56 2001:470:22B3:A::9
ipv6 route 2001:470:22B3:1000::/56 2001:470:22B3:A::10
```