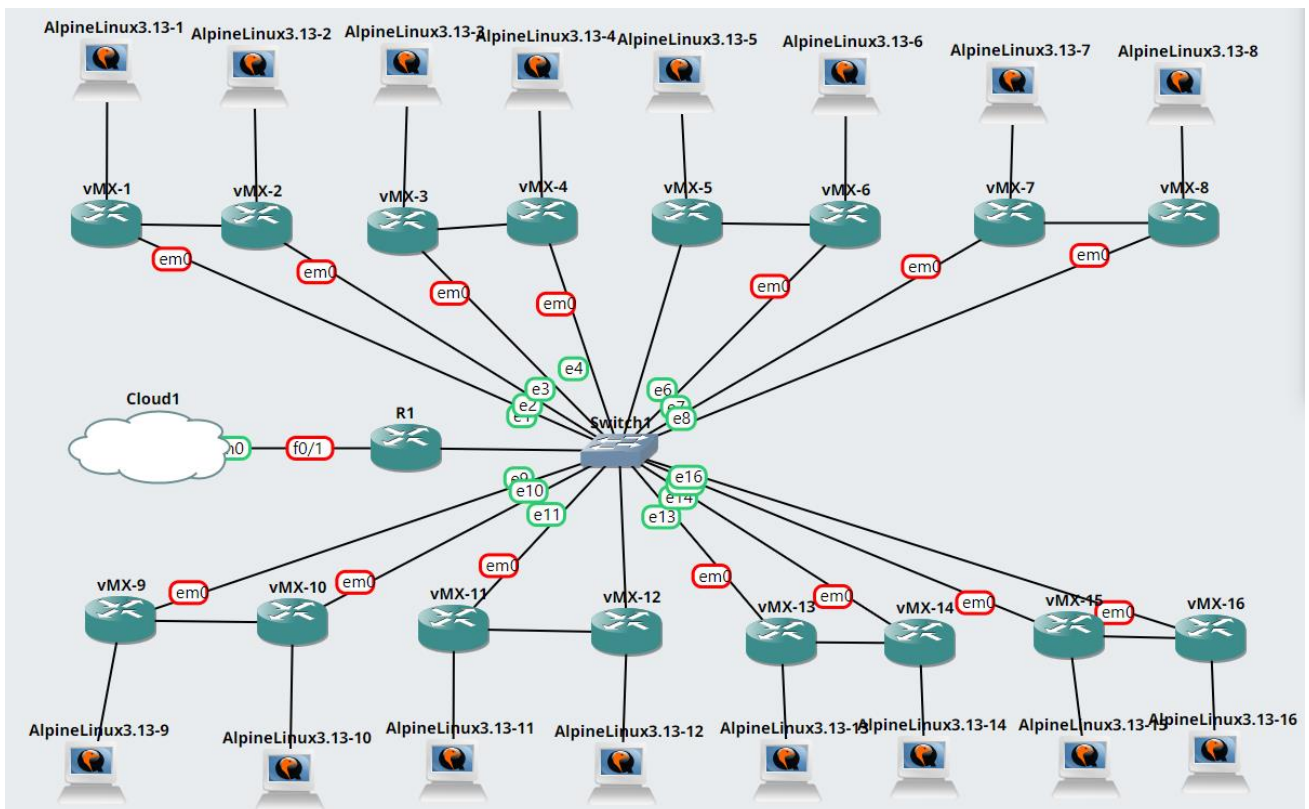
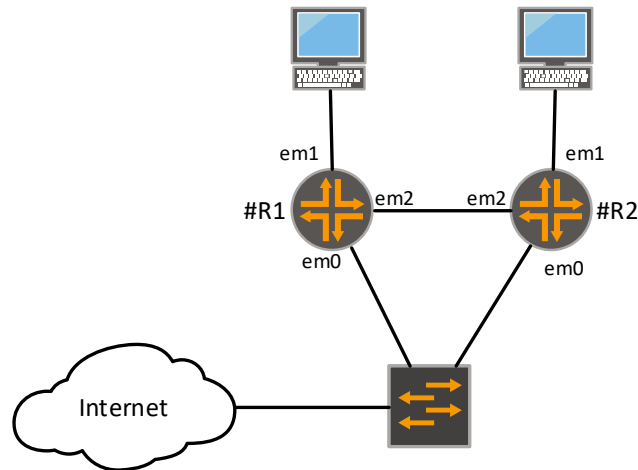


PS2 / Cvičenie 12 / Juniper JunOS

Topológia

Topológia je pripravená v GNS3 pod názvom: **Moravcik-2021-Junos-sablona**, ktorú si treba duplikovať pre daný termín cvičenia, iba 1x, keďže všetci študenti budú pracovať v jednej spoločnej topológii.



Scenár a príprava

Topológiu s 2 smerovačmi rieši **dvojica** študentov, pričom každý študent konfiguruje jeden smerovač.

Základná konfigurácia smerovača

IPv4 adresy

- číslo skupiny (1, 2, 3, ...)

Zariadenie	Rozhranie	IPv4 Adresa	Sieťová maska	Default Gateway
#R1	em0	192.168.1.#1	255.255.255.0	192.168.1.254
	em1	10.#.1.1	255.255.255.0	N/A
	em2	10.#.255.1	255.255.255.252	N/A
	lo0	10.#.10.1	255.255.255.255	N/A
#R2	em0	192.168.1.#2	255.255.255.0	192.168.1.254
	em1	10.#.2.1	255.255.255.0	N/A
	em2	10.#.255.2	255.255.255.252	N/A
	lo0	10.#.10.2	255.255.255.255	N/A
PC-1	eth0	10.#.1.3	255.255.255.0	10.#.1.1
PC-2	eth0	10.#.2.2	255.255.255.0	10.#.2.1

IPv6 adresy

- číslo skupiny (1, 2, 3, ...)

Zariadenie	Rozhranie	IPv6 Adresa	Sieťová maska	Default Gateway
#R1	em0	FE80::#:1	64	FE80::FFFF
	em1	2001:ACAD:#:1::1 FE80::#:1	64 64	N/A
	em2	FE80::#:1	64	N/A
	lo0	2001:ACAD:#:10::1	128	N/A
#R2	em0	FE80::#:2	64	FE80::FFFF
	em1	2001:ACAD:#:2::1 FE80::#:2	64 64	N/A
	em2	FE80::#:2	64	N/A
	lo0	2001:ACAD:#:10::2	128	N/A
PC-1	eth0	2001:ACAD:#:1::ABCD	64	2001:ACAD:#:1::1
PC-2	eth0	2001:ACAD:#:2::ABCD	64	2001:ACAD:#:2::1

Postup

1. Základná konfigurácia

- Nastavenie root hesla, hostname, Router-ID, DNS servera, NTP servera (napr. 158.193.152.3), spustíte telnet a SSH
- Vytvorte používateľa „admin“ ako superpoužívateľa a používateľa „student“, ktorý má práva len na pozieranie
- IPv4 adresy, IPv6 adresy, otestujte konektivitu (smerovače)

- d. Nastavte smerovaču statickú predvolenú cestu cez ISP smerovač (192.168.1.254)
- e. Nastavte PC nech má statické adresy podľa tabuľky. DNS server pre IPv4 nastavte ľubovoľný (1.1.1.1, 8.8.4.4, 8.8.8.8, 9.9.9.9, 158.193.138.7, 158.193.152.4,). V PC je nastavenie v súbore /etc/network/interfaces

2. Nakonfigurujte Single area OSPFv2 (oblasť 0)

- a. Pridajte do OSPFv2 rozhranie em0
- b. Pridajte do OSPFv2 rozhranie em2
 - i. R1 nech je DR
 - ii. Zmeňte časovače na 7/21
 - iii. Spustite MD5 autentifikáciu s heslom „Cisc0isBetter!“. Číslo kľúča zvolíte 54. (pozn. v slove Cisco je nula)
- c. Pridajte do OSPFv2 rozhranie Loopback, ktorý nastavte ako pasívny, typ siete je „point to point“
- d. Pridajte do OSPFv2 rozhranie em1
- e. Overte konektivitu (aj globálnu), popozerajte OSPFv2 databázy

3. Nakonfigurujte Single area OSPFv3 (oblasť 0)

- a. Pridajte do OSPFv3 rozhranie em0
- b. Pridajte do OSPFv3 rozhranie em2
 - i. R2 nech je DR
 - ii. Zmeňte časovače na 9/27
- c. Pridajte do OSPFv3 rozhranie Loopback, ktorý nastavte ako pasívny, typ siete je „point to point“
- d. Pridajte do OSPFv3 rozhranie em1
- e. Overte konektivitu (len lokálnu), popozerajte OSPFv3 databázy

4. Nakonfigurujte prístupový filter (ACL)

- a. Vytvorte filter s názvom „ZiadnyTelnet“, ktorým zakážete protokol telnet pre IPv4 na smerovač odkiaľkoľvek zo sveta. Z vašich vnútorných sietí bude povolený.
- b. Vytvorte filter s názvom „PustiLenUniza“, ktorým do siete kde sa nachádza aj PC povolíte prístup len ak je zdrojom niekto z IPv6 priestoru Uniza (2001:4118:300::/48). Všetko ostatné bude zakázané.