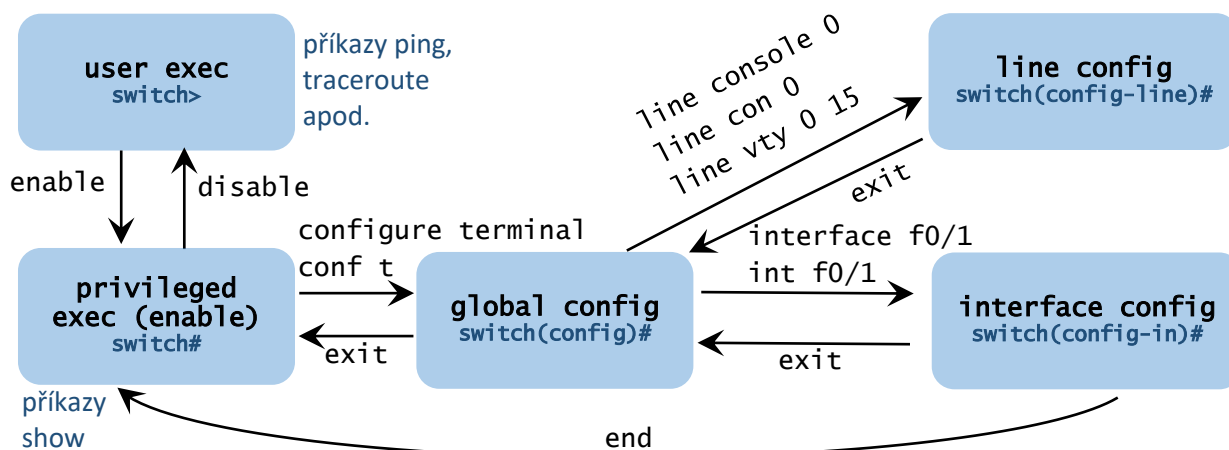
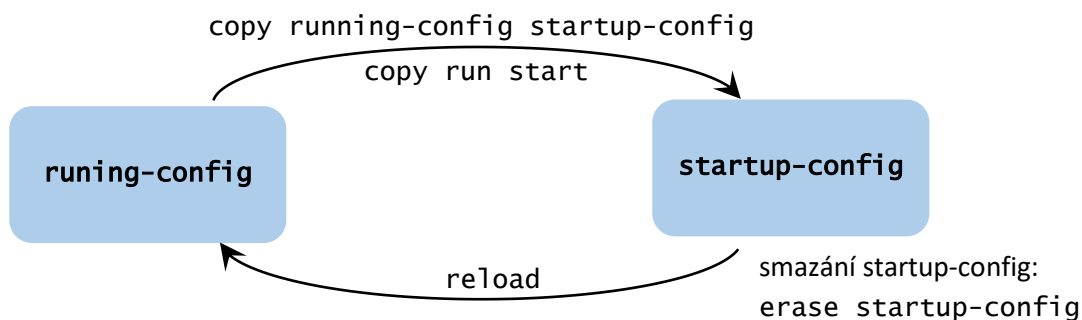


Módy přístupu pro switche a routery



Kam se co ukládá:

- flash: obraz operačního systému IOS, který se používá na Cisco zařízeních
- running-config: konfigurace, která se právě používá; pokud děláme změny pomocí příkazů (například nastavujeme IP adresu, heslo apod.), tyto změny se projeví zde, ale jde o RAM, tedy po restartu je smazaná
- startup-config: odtud se načítá konfigurace při startu systému IOS, je to čip NVRAM (v reálu flash), sem můžeme uložit running-config po provedení změn, aby se neztratily



Čím ukončit dlouhý nebo zaseknutý příkaz:

- někdy funguje Ctrl+C
- obecná ukončující sekvence: Ctrl+Shift+6

Router – pracuje na L3, tedy IP adresy dáváme přímo na jednotlivá rozhraní (interface) pojmenovaná fastethernet 0/1, 0/2,..., zkráceně f0/1 atd., resp. gigabitethernet 0/1,..., zkráceně g0/1 atd.

Switch – pracuje standardně na L2, IP adresu nedáváme na rozhraní f0/něco či g0/něco (jsou to L2 rozhraní), ale kvůli přístupu přes telnet nebo SSH někdy musíme IP adresu dát – dáváme na virtuální rozhraní, které vytvoříme příkazem `interface vlan 1` (nebo jiné číslo VLAN).

Ukázka základní konfigurace switche

```
Switch>enable      ...přejdeme do módu „enabled“ (privileged exec)
Switch#configure terminal      ...přejdeme do globálního konfiguračního módu
Switch(config)#hostname S1     ...nastavíme název switche
S1(config)#enable secret heslo ...nastavíme heslo do enabled módu
S1(config)#line console 0      ...přejdeme do konfigurace konzole
S1(config-line)#password heslo ...nastavíme heslo pro přístup do konzole
S1(config-line)#login          ...vynutíme si, že na konzoli musí uživatel heslo opravdu zadat
S1(config-line)#logging synchronous ...ať na konzoli syslog moc neotravuje
S1(config-line)#exit          ...ukončíme konfiguraci konzole
S1(config)#line vty 0 15      ...přejdeme do konfigurace virtuálních terminálů (telnet, SSH)
S1(config-line)#password heslo ...nastavíme heslo na terminály
S1(config-line)#login          ...vynutíme si, že v terminálech je nutné heslo zadat
S1(config-line)#exit          ...ukončíme konfiguraci virtuálních terminálů
S1(config)#service password-encryption ...heslo se ukládá do running-config, kde je
                                „viditelné“, ale po tomto příkazu tam bude místo hesla
                                jen jeho hash = bezpečnější
S1(config)#banner motd #
neautorizovany pristup je prisne zakazan
#
S1(config)#interface vlan 1    ...přejdeme do konfigurace pro virtuální rozhraní VLAN 1
S1(config-if)#ip address 10.0.10.2 255.255.255.0 ...nastavíme mu IP adresu
S1(config-if)#no shutdown      ...zapneme (tj. negace vypnutí)
S1(config-if)#exit            ...ukončíme konfiguraci rozhraní
S1(config)#ip default-gateway 10.0.10.1 ...nastavíme výchozí bránu
S1(config)#int range f0/4,8-12 ...můžeme pracovat s více rozhraními najednou (rozsah)
S1(config-in)#shutdown        ...vypneme nepoužívaná rozhraní
S1(config-in)#end              ...přeskočíme rovnou do enabled módu
S1#show ip interface brief     ...zobrazíme tabulku rozhraní
S1#show interfaces             ...zobrazíme podrobné informace o rozhraních
S1#show mac address-table      ...zobrazíme tabulku MAC adres
S1#copy running-config startup-config ...uložíme running-config do startup-config
```

Zkracování příkazů: do té míry, aby se příkaz nepletl s jiným (cokoliv zadáváme, musí být jednoznačné). Například:

```
configure terminal      zkrátíme na  conf t
show interface brief    zkrátíme na  sh int br
copy running-config startup-config zkrátíme na  copy run start
```

Příkazy show se zadávají v enable módu, ale pokud chceme takový příkaz zadat v některém konfiguračním módu, taky to jde, jenom musíme před příkaz dát „do“:

```
S1(config-if)#do sh ip int brief
```

Další příkazy show: například sh arp, sh version, sh protocols,
sh cdp, sh cdp neighbors

Ukázka základní konfigurace routeru

Většina je podobná jako u switche, až na počet virtuálních terminálů (u switche obvykle 0 až 15, u routeru obvykle 0 až 4), a samozřejmě konfiguraci L3. U routerů bychom vždy měli dopsat popisek (description) rozhraní. U switche můžeme samozřejmě taky.

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#enable secret heslo
R1(config)#line console 0
R1(config-line)#password heslo
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password heslo
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
Neautorizovaný přístup přísně zakázán
#
R1(config)#interface g0/0                                ...přecházíme do konfigurace rozhraní
R1(config-if)#description linka do site 10              ...popisek rozhraní
R1(config-if)#ip address 10.0.10.1 255.255.255.0...IP adresa rozhraní
R1(config-if)#no shutdown                               ...zapnutí rozhraní
R1(config-if)#interface g0/1                            ...další rozhraní
R1(config-if)#description linka do site 20
R1(config-if)#ip address 10.0.20.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
R1#ping 8.8.8.8
R1#traceroute 8.8.8.8
```

IPv6 adresy:

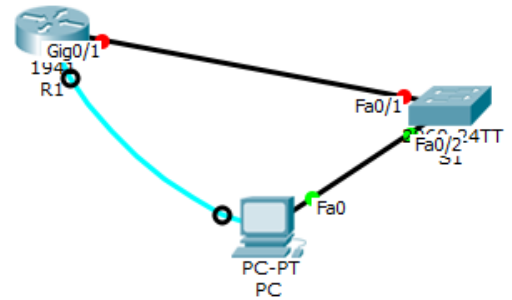
```
R1(config-if)#interface g0/1                            ...další rozhraní
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#end
R1#sh ipv6 int brief
R1#sh ipv6 int g0/1
```

Směrovací tabulka:

```
R1#sh ip route      (pro IPv6: sh ipv6 route) ...zobrazí směrovací tabulku
R1(config)#ipv6 unicast-routing                    ...zapnutí IPv6 směrování
R1(config)#ip route 192.168.20.0 255.255.255.0 209.165.200.225
...přidá do směrovací tabulky statický záznam (zadáváme IP adresu, masku a adresu
sousedního zařízení, přes které vede cesta), místo souseda můžeme zadat rozhraní (naše)
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.64.2 ...default route pro IPv4
R1(config)#ipv6 route ::/0 2001:db8:acad:4::2 ...default route pro IPv6
```

Telnet a SSH

Nejdřív přes konzoli a konzolový kabel zabezpečíme zařízení a přidělíme IP adresu (switch: na virtuální rozhraní; router: na skutečné rozhraní), a až pak lze na zařízení přistupovat přes telnet nebo ssh.



```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#service password-encryption
S1(config)#enable secret heslo
```

```
S1(config)#ip ssh version 2           ...používání verze 2
S1(config)#ip domain-name firma.com  ...pouze pro účely generování klíčů, klidně nesmysl
S1(config)#crypto key generate rsa   ...vygenerujeme klíče, délka min. 1024 (ptá se)
S1(config)#username uzivate11 secret heslo ...vytvoříme uživatele (zde dva)
S1(config)#username uzivate12 secret heslo
```

```
S1(config)#line vty 0 15
S1(config-line)#transport input ssh  ...zakážeme telnet, přes síť pouze SSH
S1(config-line)#login local         ...autentizace proti lokální databázi
S1(config-line)#exit
```

```
S1(config)#line console 0
S1(config-line)#password heslo
S1(config-line)#login local
S1(config-line)#exit
S1(config)#banner motd #
neautorizovany pristup je prisne zakazan
#
S1(config)#interface vlan 1
S1(config-if)#ip address 10.0.10.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 10.0.10.1
S1(config)#exit
```

```
S1#show ssh
S1#show ip ssh
```

Další zabezpečení:

```
R1(config)#no ip domain-lookup      ...aby se router nepokoušel chybně zadaný příkaz
interpretovat jako doménové jméno
```

```
R1(config)#security passwords min-length 10      ...min. délka hesel 10
```

```
R1(config-line)#exec timeout 5          ...pokud se na této lince 5 minut nic neděje,
je uživatel odhlášen
```

```
R1#copy startup-config tftp://....      ...pokud máme na některém počítači
rozběhnutý TFTP server, můžeme si na něj stáhnout do zálohy startup-config tohoto zařízení
```