Laboratorní cvičení: Konfigurace VLAN a

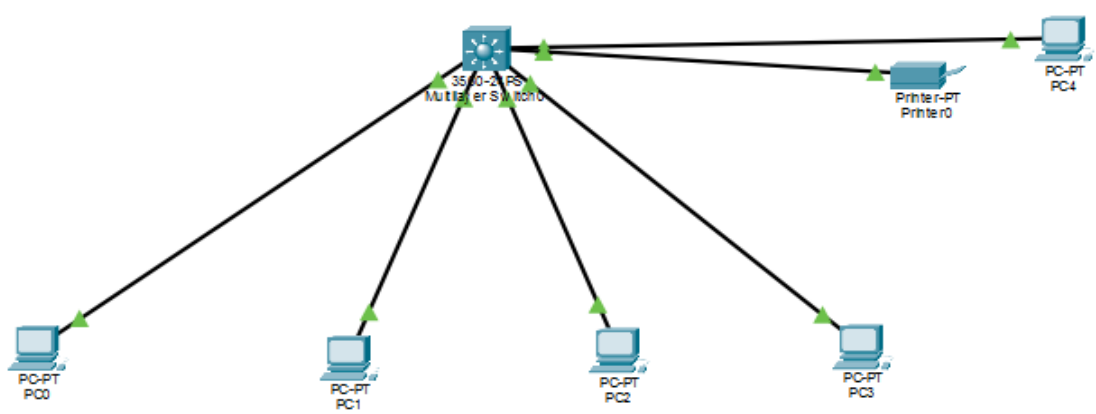
Cíl cvičení: Navrhnout IP adresaci, fyzicky zapojit síť v Cisco Packet Traceru a nakonfigurovat L3 switch tak, aby logicky oddělil počítače studentů od zařízení učitelů pomocí virtuálních sítí (VLAN) a zároveň zajistil jejich směrování.

Krok 1: Fyzická topologie

Otevřete Cisco Packet Tracer a postavte topologii podle následujících požadavků:

- **1x L3 Switch** (Vyberte model **3560-24PS** - naleznete jej ve spodním menu pod ikonkou Multilayer Switches)
- **5x PC** (4 počítače pro studenty, 1 počítač pro učitele)
- **1x Tiskárna** (Printer - zařazena k učitelům)

> ***Důležité:*** *Proč nepoužijeme obyčejný L2 switch (např. 2960)? Běžný přepínač na 2. vrstvě OSI modelu neumí pracovat s IP adresami, nedokáže routovat a nemůže sloužit jako výchozí brána. Nasazením "chytrého" L3 switche spojíme logiku přepínače i routeru do jedné jediné součástky!*



Krok 2: Subnetting a návrh IP adres

Byl vám přidělen celkový síťový rozsah **192.168.0.0 /16**. Vaším úkolem je z něj vytvořit menší, oddělené podsítě s maskou **/24** (tj. maska 255.255.255.0).

Logika rozdělení a výchozích bran:

- **VLAN 10 (Studenti):** Použijte síť `192.168.10.0 /24` (Brána bude: 192.168.10.1)
- **VLAN 20 (Učitelé):** Použijte síť `192.168.20.0 /24` (Brána bude: 192.168.20.1)

- **VLAN 99 (Nativní/Nová zařízení):** Použijte síť `192.168.99.0 /24`

Úkol: Otevřete nastavení každého PC a Tiskárny (Desktop > IP Configuration) a nastavte jim statickou IP adresu z příslušného rozsahu (např. 192.168.10.2 pro studenta). Do pole **Default Gateway** vyplňte přesnou adresu brány pro danou síť!

Krok 3: Vytvoření VLAN na Switchi

Otevřete záložku CLI u L3 switche a vytvořte příslušné virtuální sítě:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Studenti
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name Ucitele
Switch(config-vlan)# exit
Switch(config)# vlan 99
Switch(config-vlan)# name Nativni_Nova
Switch(config-vlan)# exit
```

Krok 4: Přiřazení koncových zařízení do VLAN

Nyní zařadíme fyzické porty do vytvořených sítí. Režim `access` znamená, že na daném portu je připojeno koncové zařízení. *(Upravte čísla portů fa0/1-4 podle vaší reálné topologie)*:

```
! Assign student computers (e.g., ports 1 to 4)
Switch(config)# interface range fastEthernet 0/1-4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

! Assign teacher PC and Printer (e.g., ports 5 and 6)
Switch(config)# interface range fastEthernet 0/5-6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
```

Krok 5: Zabezpečení nepoužitých portů

Jelikož veškeré směrování probíhá přímo uvnitř našeho L3 switche, **nepotřebujeme zakládat Trunk port** pro propojení s externím routerem. Přesto z bezpečnostních důvodů přesuneme všechna nezapojená a budoucí zařízení z výchozí (zranitelné) VLAN 1 do izolované VLAN 99.

```
! Move all remaining unused ports to VLAN 99 (e.g., ports 7 to 24)
Switch(config)# interface range fastEthernet 0/7-24
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 99
Switch(config-if-range)# exit
```

Zkontrolujte svou práci zadáním příkazu: `show vlan brief` (z privilegovaného režimu).

Krok 6: Výchozí brány (Inter-VLAN Routing)

Aby mohly VLANy mezi sebou vůbec komunikovat, musíme L3 switchi aktivovat funkci směrování (routing). Místo nastavování fyzických portů vytvoříme virtuální rozhraní **SVI (Switched Virtual Interface)** pro každou VLAN a přiřadíme jim adresy našich výchozích bran.

```
! Enable global routing (Crucial command on L3 switch!)
Switch(config)# ip routing

! Create SVI gateway for VLAN 10 (Students)
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Create SVI gateway for VLAN 20 (Teachers)
Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# end
```

Krok 7: Analýza ARP a test izolace (Simulace)

Dříve než zavoláte vyučujícího, vyzkoušejte si, jak síť blokuje všesměrový provoz (broadcast). Abychom proces hledání adresy viděli od začátku, vymažte nejprve záznamy z paměti:

- **Na počítačích (Command Prompt):** Zadejte `arp -d` pro smazání lokální cache.
- **Na Switchi (v privilegovaném režimu):** Zadejte `clear arp-cache`.

Závěrečné testování (Příprava na hodnocení)

1. **Úspěšný Unicast (Směrování funguje):** V příkazovém řádku studentského PC zadejte `ping` na IP adresu učitelského PC. Ping projde. Ukázali jste, že díky nakonfigurovaným SVI branám dokáže L3 switch směrovat adresný (unicast) provoz mezi VLANami.
2. **Izolace Broadcastu (Zadržení na L2):** Přepněte Packet Tracer z Realtime do **Simulation módu** (filtr pouze na ICMP a ARP). Ze studentského PC odešlete plošný dotaz – např. ping na broadcast `192.168.10.255`. Pozorujte kroky: switch tento paket rozešle **pouze** na ostatní studentské porty. Učitel ani tiskárna tento zbytečný provoz vůbec neuvidí!

3. **Bezpečnost nového zařízení:** Připojte do switche zbrusu nový počítač s kabelem (např. do portu fa0/10). Zadejte na switchi `show vlan brief` a přesvědčte se, že port nespadá do zranitelné VLAN 1, ale je bezpečně uklizen v Nativní VLAN 99.

Router-on-a-stick

Pokud v síti nemáme moderní L3 switch, musíme k L2 switchi připojit klasický router. Abychom nemuseli pro každou VLAN tahat ze switche do routeru samostatný fyzický kabel, propojíme je pouze jedním kabelem (to je ten "stick" – klacek).

Aby tento jeden kabel dokázal přenést data z více sítí, musí být strana na switchi nastavena jako **Trunk**. Router pak přijímá rámce opatřené 802.1Q tagy a musí je umět správně roztřídit.

Jak to funguje logicky:

1. **Fyzický port** na routeru pouze zapneme, ale nedáme mu **žádnou IP adresu**.
2. Místo toho na něm vytvoříme virtuální podrozhraní (tzv. **subinterfacy**), ideálně pojmenované podle čísla VLAN (např. `g0/0.10`).
3. Každému subinterfacu řekneme, jaký **802.1Q tag** má číst a přiřazovat (zapouzdření).
4. Nakonec subinterfacu přiřadíme IP adresu, která se stane **výchozí bránou** pro danou VLAN.

Konfigurace v Cisco CLI:

```
! 1. Enable main physical interface (no IP address)
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit

! 2. Configure subinterface for VLAN 10 (Students)
Router(config)# interface gigabitEthernet 0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit

! 3. Configure subinterface for VLAN 20 (Teachers)
Router(config)# interface gigabitEthernet 0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
```

Ověření úspěšnosti: Zkuste ping ze studentova PC na učitelovo PC. Rámec opustí PC bez tagu, switch mu přidá tag 10, pošle ho trunkem do routeru. Router ho přijme na `g0/0.10`, podle IP adresy přeroutuje na `g0/0.20`, změní tag na 20 a pošle zpět do switche.