05 - VLAN, návrh podnikové sítě

# Koncept VLAN

* Logické rozdělení sítě na části
* Nemusíme dělat fyzické změny
* Čistě softwarová záležitost
* Výhody:
  + Menší broadcastová doména (menší provoz => lepší výkon)
  + Jednoduché přesunutí zařízení do jiné sítě
* IEEE 802.1Q:
  + Dot1q
  + Síťový standard, který podporuje tagování framů běhen trunkování
* Typy VLAN:
  + Access – výchozí mód, přijímá pouze netagované rámce, může být členem pouze jedné VLAN (untagged port), obsahuje pouze jednu VLAN
  + Trunk – Dokáže přenášet více VLAN mezi jednotlivými switchi (trunk je pojem Cisca, non-cisco pojem je tagger port)
  + Native – Přenáší netagované rámce (zařízení nepodporující VLAN)
  + Management – SSH, Telnet
  + Voice – podpora VoIP (za telefon lze ještě připojit PC)

# VLAN mezi více switchi

* Cisco ISL – Inter-Switch Link – funguje pouze na Cisco zařízeních
* Propojení access portů na obou switchích pro každou VLAN – nepraktické
* Trunkování (IEEE 802.1Q)

# DTP

* Dynamic Trunking Protocol
* Automatické vyjednání nastavení módů na portech
* Možnosti DTP konfigurace: Dynamic Auto, Dynamic Desirable, Trunk, Access
* Dynamic se vždy přizpůsobí
* DA + DA = Access
* DD + DD = Trunk
* DA + DD = Trunk
* Trunk + Access = Limited connectivity
* Představuje bezpečnostní hrozbu

# Port security

* Zabezpečuje přístup do sítě
* Kontroluje, zda pakety přichází z povolené MAC
* Při porušení pravidel máme na výběr ze tří chování:
  + Shutdown: port nepustí danou trafiku, pošle syslog zprávu, zvýší počet porušení a vypne se
  + Restrict: port nepustí danou trafiku, pošle syslog zprávu, zvýší počet porušení, ale nevypne se
  + Protect: pouze nepustí danou trafiku
* Nastavování MAC adres:
  + Static: adresy jsou staticky nastaveny a uloženy do running config
  + Dynamic: adresy se učí z připojených zařízení na portu, jsou uloženy do tabulky s adresami
  + Sticky: učí se dynamicky, jsou ale uloženy do running configurace
* K porušení dojde pokud:
  + Bude na portu více než maximum (nastavené) MAC adres
  + Když je adresa, která již byla na jiném portu, na jiném portu

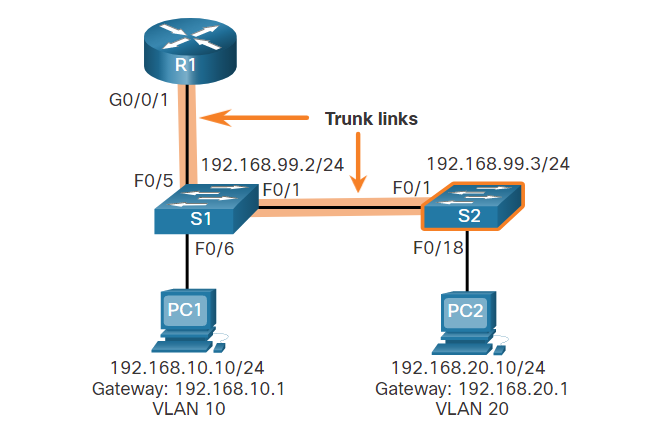
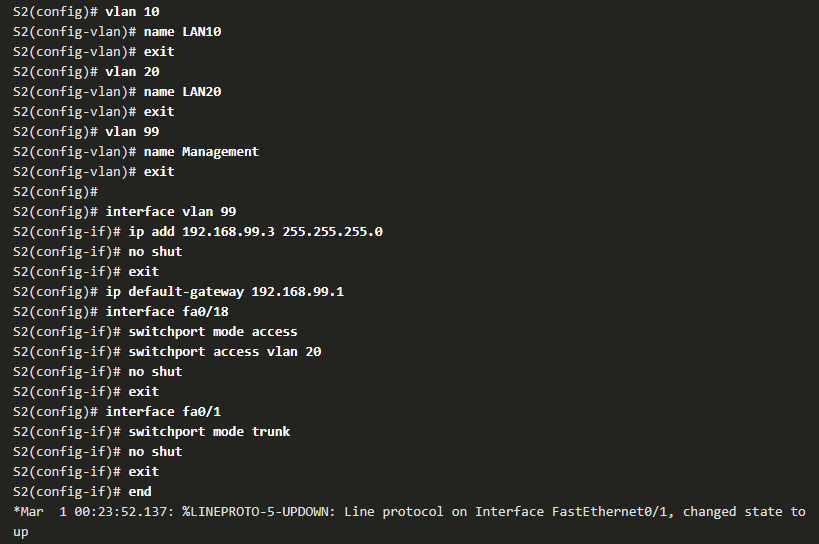
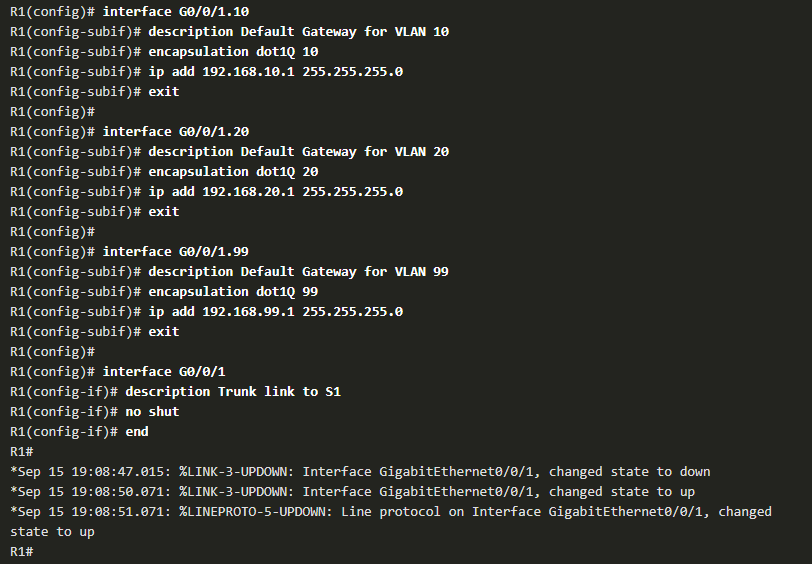
# Inter-VLAN routing

* Routování VLAN

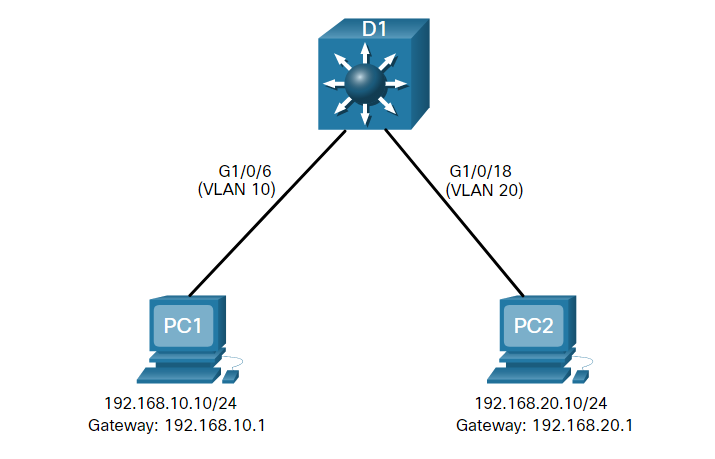
## Legacy Inter-VLAN routing

* Využívá porty na routeru
* Každý port má jinou VLAN
* Využívá příliš mnoho portů

# Router-on-a-stick

* Vyžaduje pouze jedno rozhraní routeru
* Switch se spojí s routerem přes trunk
* Pro každou VLAN je na interface nakonfigurován subinterface

# L3 switch

* Nepotřebujeme switch a router (stačí pouze jedna „krabička“)
* Využití SVI (switch virtual interface) pro každou VLAN
* Rychlejší než Router-on-a-stick
* Dražší
* Na switchi vytvoříme VLAN
  + vlan 10
  + vlan 20
* Vytvoříme SVI VLAN rozhraní
  + interface vlan 10
  + ip address 192.168.10.1 255.255.255.0
  + no shutdown
* Nastavíme access porty
  + interface GigabitEthernet1/0/6
  + switchport mode access
  + switchport mode access vlan 10
* Zapneme routování
  + ip routing