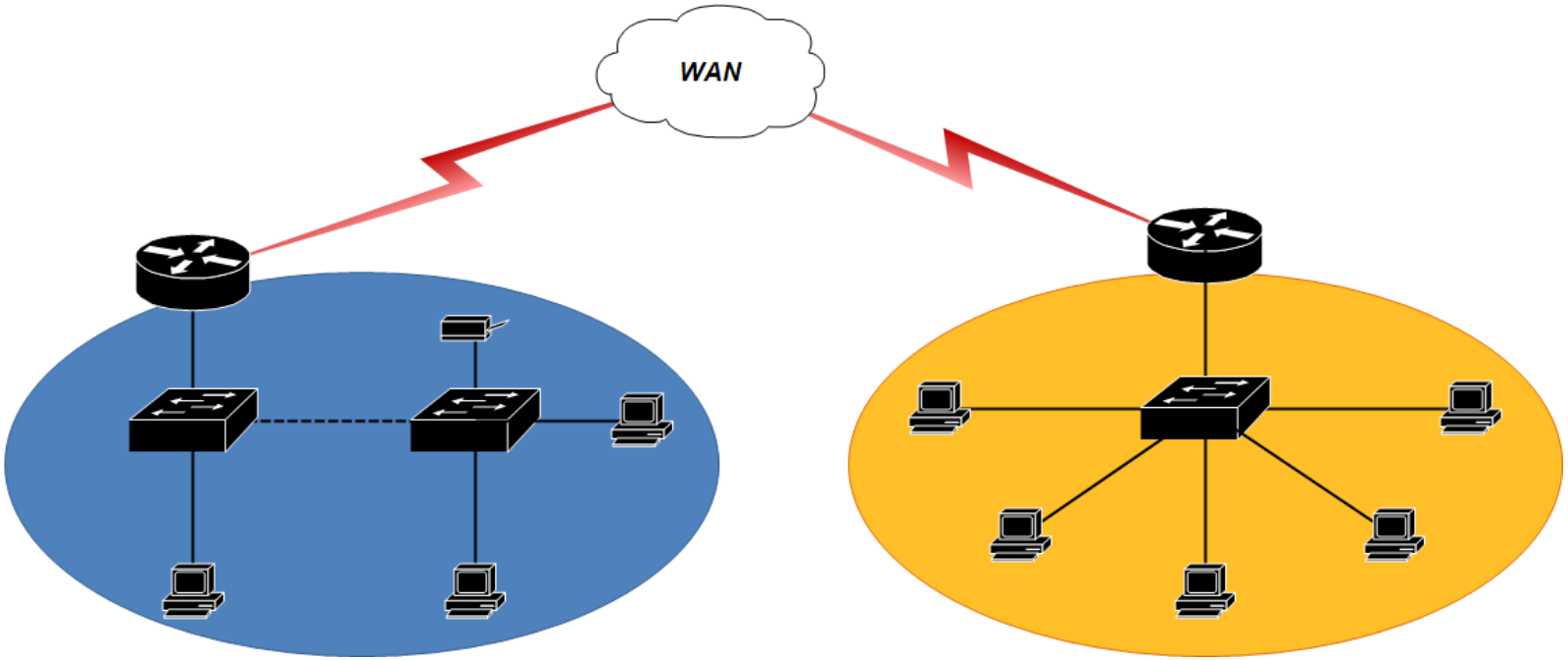
Počítačové sítě 1

Přednáška č.7 – Přepínané LAN sítě

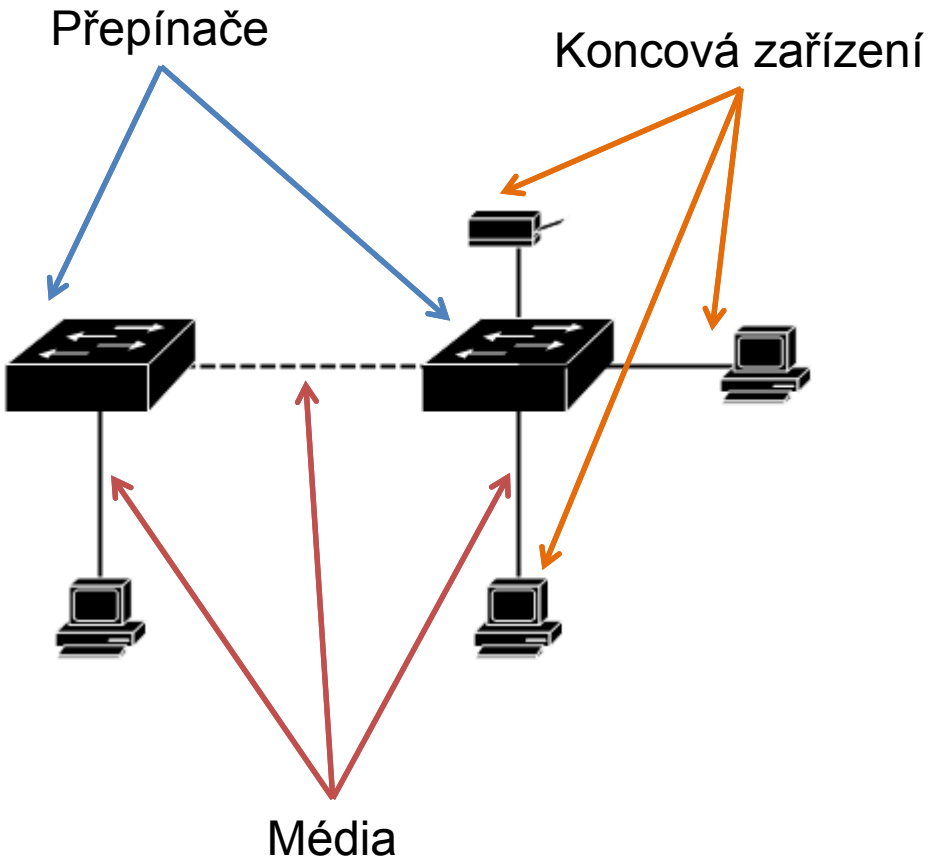
- Přepínané LAN sítě
  - Základní charakteristiky přepínaných sítí
  - Prvky přepínaných sítí
- Přepínač
  - Principy přepínání
  - Typy přepínačů

Přepínané LAN sítě

- Propojení výpočetních systémů do jedné sítě
- Může se odehrávat na různých vrstvách ISO modelu
  - Nejběžněji se však děje na Data-Linkové vrstvě (L2 přepínačing)



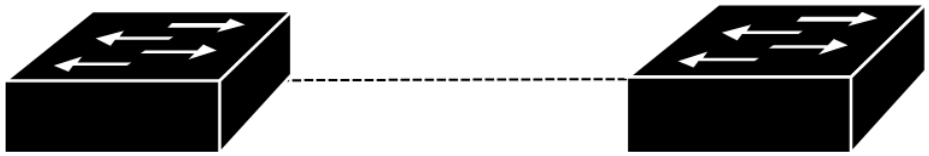
= Zásuvky
= Patch panely
= Konektory
= Racky
= Konvertory
= Síťové karty
= Antény



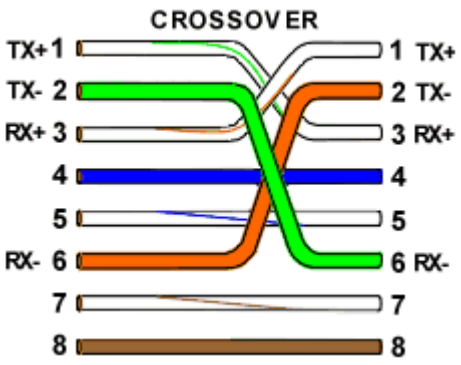
Přepínač - Switch

- Přepíná mezi více připojenými segmenty současně
- Samotné přepínání realizováno hardwarovými prostředky s vysokým stupněm paralelizace
  - Jedná se o velmi rychlý proces
  - Využití ASIC obvodů
- Může si v síti vynutit více deterministické chování
  - Řízení toku dat
  - Quality of Services – podpora priority provozu
- Dělí kolizní domény
- Rámce přeposílá pouze stanicím pro které jsou určeny

- Ethernetové přepínače patří do rodiny tzv. transparentních mostů (transparent bridge)
  - Připojené stanice **nevědí** o jejich existenci
  - Rámec není při průchodu přes switch modifikován
- Přepínač se učí **pasivním čtením zdrojových MAC** adres z přenášených rámců
- Doručování rámců je řízeno **MAC tabulkou**, vytvořenou průběžným učením
  - Rámce pro známé příjemce jsou odeslány **příslušným portem**
  - Rámce pro neznámého příjemce jsou odeslány **všemi ostatními porty**
- Toto plně automatizované chování způsobuje problémy při **redundantním** zapojením přepínané sítě
  - **Broadcast storm**

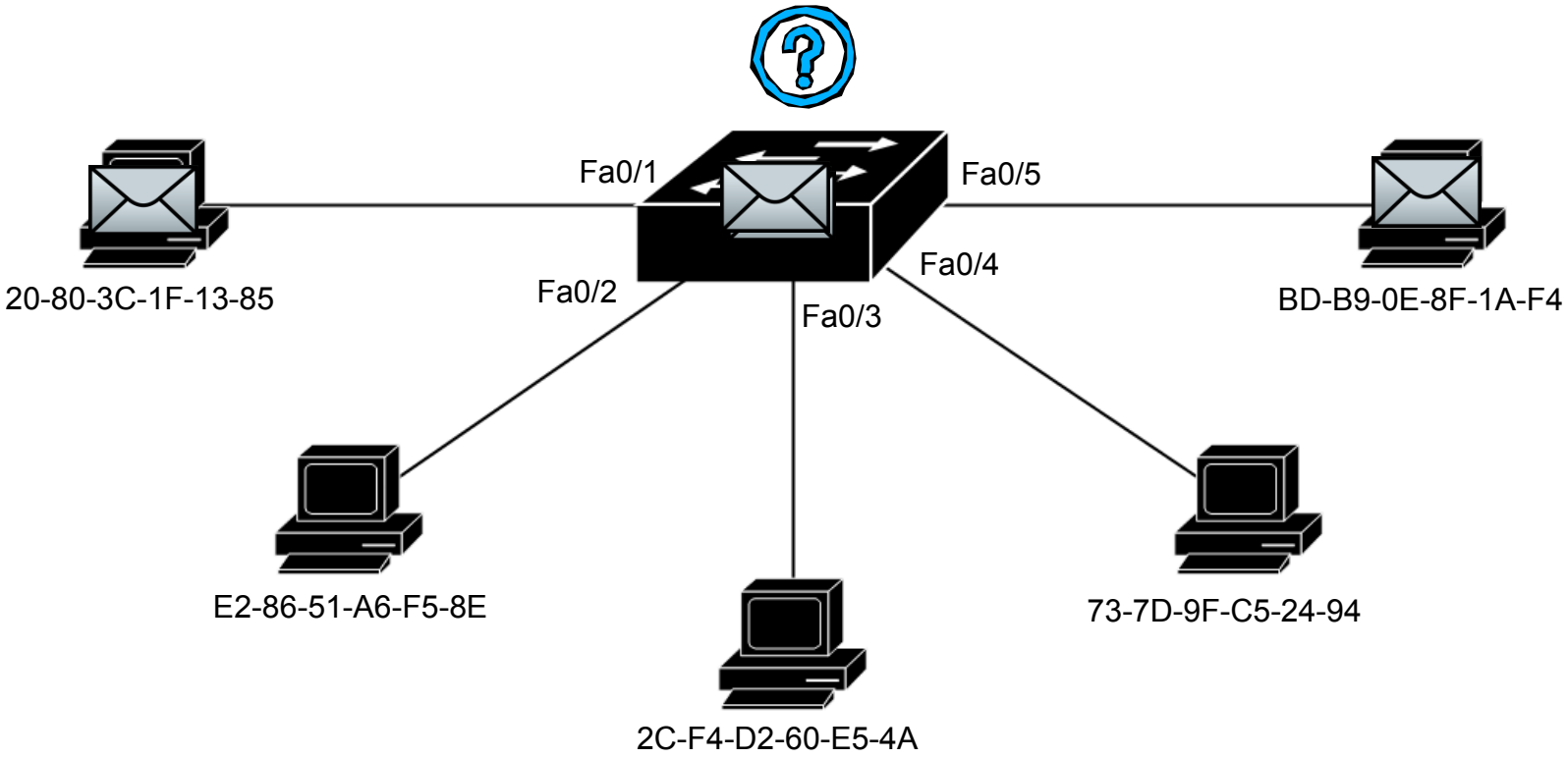


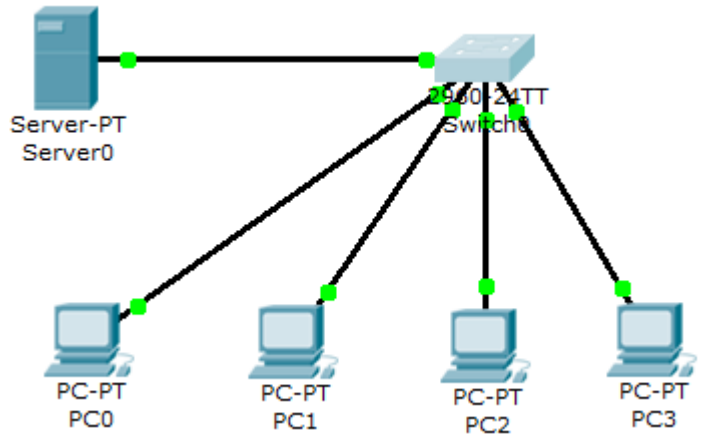
- Médium podle typu portu na přepínači (UTP, optické vlákno)
- Většinou se jedná o **křížený** (crossover) UTP kabel
  - Křížené UTP se obecně používá pro propojení zařízení pracujících na **stejné vrstvě** OSI modelu (switch-switch, router-router, PC-PC)



- Zařízení (switch) může podporovat funkci **auto MDI/MDIX**
  - Takovéto rozhraní dokáže detekovat zda je potřebný crossover kabel a následně se přepnout do takového režimu, ve kterém není vyžadován **křížený** kabel
  - Jinými slovy, pokud zařízení disponuje **auto MDI/MDIX** není třeba se starat jaký typ kabelu použít

Port	MAC adresa	Type
Fa0/1	20-80-3C-1F-13-85	DYNAMIC
Fa0/5	BD-B9-0E-8F-1A-F4	DYNAMIC





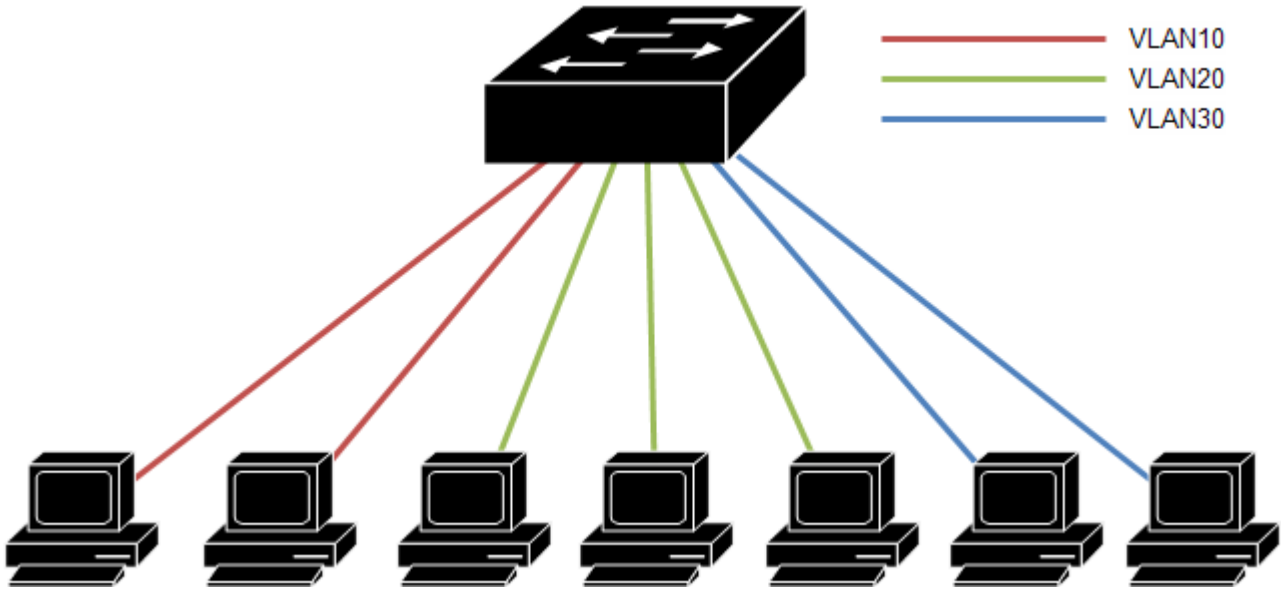

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.969a.b472    DYNAMIC     Gig1/1
   1    0001.97d7.383e    DYNAMIC     Fa0/2
   1    000a.41ac.5dbe    DYNAMIC     Fa0/3
   1    0090.21c3.50db    DYNAMIC     Fa0/4
   1    00d0.9722.7a57    DYNAMIC     Fa0/1
```

- Moduly, počty, rychlosti a typy portů
- Agregovaná propustnost
- Techniky bufferingu
  - Buffery na vstupech a výstupech
  - Sdílený buffer
  - Více bufferů na každém vstupu/výstupu pro různě prioritní traffic
- Počet MAC adres přiřaditelných jednomu portu
- Možnosti přiřazení MAC na port
  - **Statické** – obrana proti možným útokům
  - **Dynamické** – samoučící se pomocí rámců s dosud neznámými adresami
- **SPAN porty** pro duplikaci a analýzu komunikace
- Způsob správy (telnet, ssh, www, SNMP)
- Ochrana proti broadcast-storm (Spanning-tree protocol – STP)
- Zpracovávání multicastů (IGMP snooping)

- **Store-and-forward**
  - Přijatý rámec je nejdříve celý přijat a uložen do bufferu
  - Následně je určen výstupní port, na základě cílové MAC adresy
  - Poté je výsledný rámec odeslán daným portem (porty)
  - Využívá se vždy při asymetrickém přepínačingu
    - **Asymetrický přepínačing** – pokud má příchozí a odchozí port různé rychlosti (např. 100Mbit a 1000Mbit), případně jsou jiného typu (metalický a optický)
- **Cut-through**
  - Po obdržení části hlavičky (s cílovou MAC adresou) je již určován výstupní port
  - Následně je **ihned** odesílán, i v případě že ještě není celý přijat
  - **Výhoda**: vyšší rychlost než store-and-forward
  - **Nevýhoda**: před odesláním nemůže být zkontrolován CRC součet rámce (který je obsažen v patičce)
- **Fragment-free**
  - Kombinace obou výše zmíněných metod

- VLAN (Virtual LAN) je logické rozdělení přepínané sítě do menších podsítí (VLAN) nezávisle na fyzickém rozdělení
  - VLAN je identifikována pomocí **číselného** identifikátoru **VLAN ID**
  - Přístupové porty na přepínači jsou vždy přiděleny do určité VLAN
  - Switch potom hlídá, aby mezi sebou mohly komunikovat pouze zařízení ve **stejné VLAN** síti
  - Výchozí nastavení je takové, že všechny porty switche jsou přiřazeny do defaultní **VLAN 1**
- Pro propojení mezi přepínači je realizováno pomocí tzv. trunk linek
  - Jako jediné dokáží přenášet rámce všech VLAN sítí
  - Aby mohly být rámce na druhé straně opět zařazeny do příslušné VLAN sítě, je potřeba přidat do jeho hlavičky informaci o VLAN ID
  - K tomuto účelu je definován otevřený protokol **IEEE 802.1Q**
  - Cisco Systems vyvinulo vlastní proprietální protokol **ISL**

= Switch kontroluje, že spolu mohou navzájem komunikovat pouze porty zařazené ve stejné VLAN

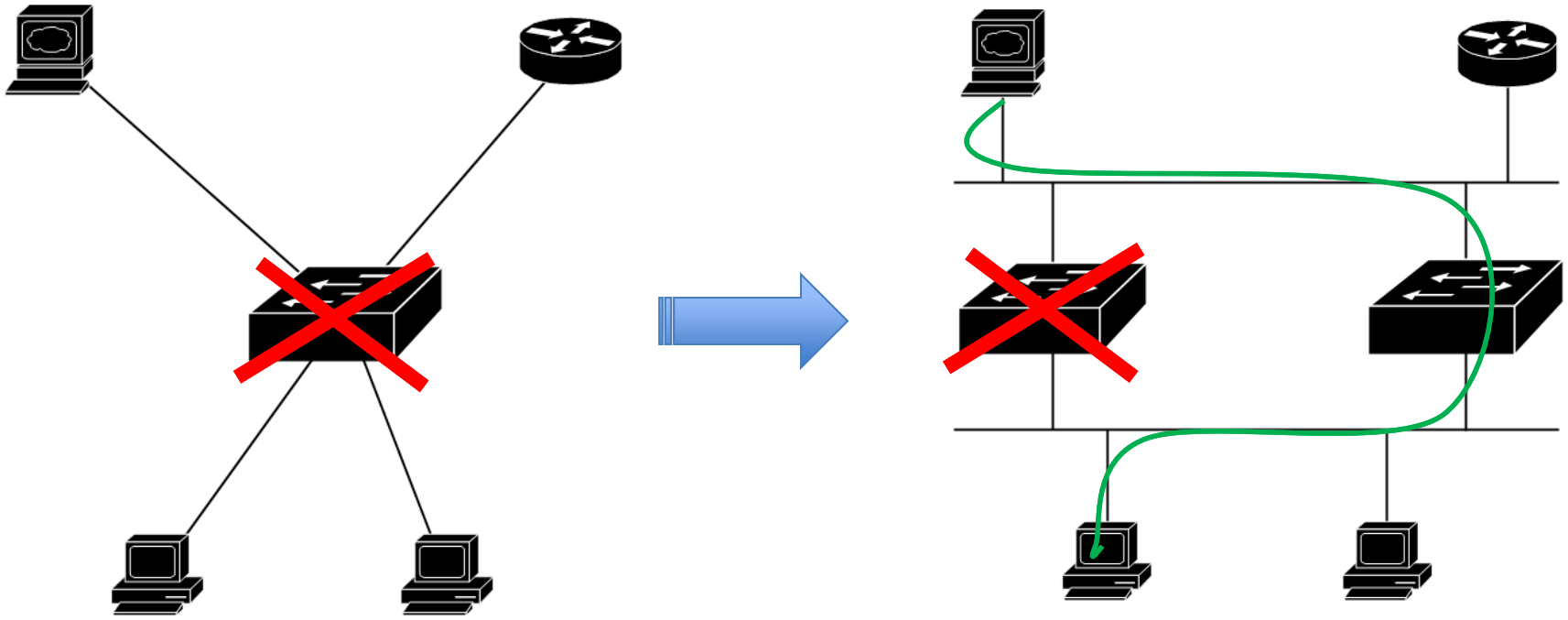


- Switch dělí **kolizní doménu** a vytváří jednu pro každé připojené zařízení
  - Výrazné omezení kolizí v sítí
  - Vetší propustnost sítě

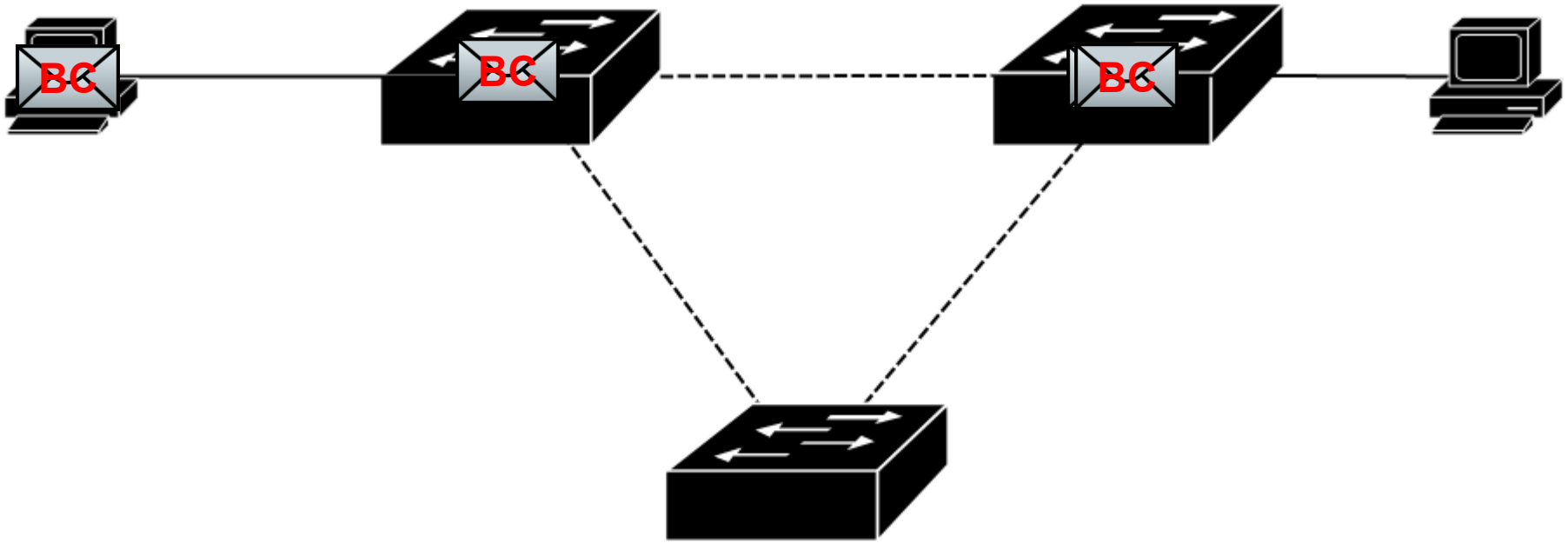
- Switch standardně **nerozděluje broadcastovou doménu**
  - Pokud switch obdrží rámec s broacastovou MAC adresou (FF:FF:FF:FF:FF:FF) odešle tento rámec na všechny ostatní porty (v dané VLAN), kromě portu, kterým rámec obdržel
  - Při použití více VLAN je možné broadcastovou doménu dělit
    - Potom každá VLAN sít tvoří samostatnou broadcastovou doménu

Redundance a Spanning Tree Protocol

- Cílem redundance prvků je eliminovat výpadek centrálního prvku
  - Tím je docíleno existence záložních cest



- Pokud switch obdrží rámec s **broacastovou MAC** adresou (FF:FF:FF:FF:FF:FF) odešle tento rámec na **všechny ostatní porty** (v dané VLAN), kromě portu, kterým rámec obdržel
- Pokud bude odeslán broadcastový rámec a zapojení topologie obsahuje **kruhové redundantní zapojení** mezi přepínači, bude rámec duplikován do nekonečna
  - L2 PDU neobsahuje ve své hlavičce žádnou **TTL hodnotu**
  - **Každý broadcastový** rámec bude putovat po přepínané síti do nekonečna



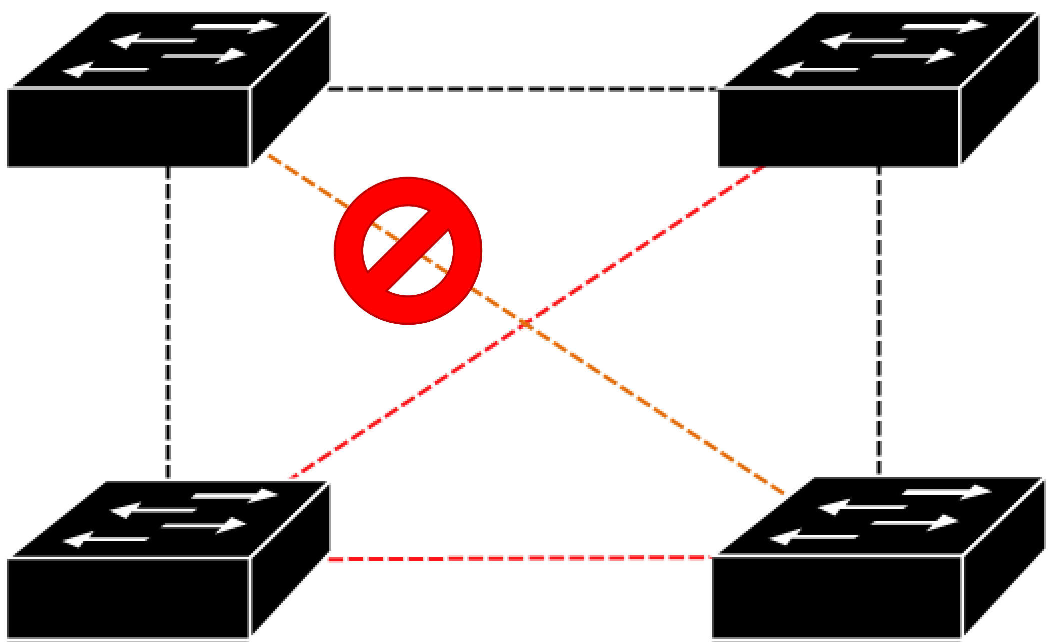
- Fyzické smyčky nevyhnutelné
  - Zajišťují **redundanci prvků** a tím existenci **záložních cest**
- Je zapotřebí eliminovat **L2 smyčky**
  - L2 smyčky = přeposílací smyčky způsobené **logikou činnosti switche**
- Tento problém řeší rodina protokolů **Spanning tree** (STP)
  - Hledá v přepínané síti kostru (maximální acyklický faktorový podgraf)
  - Existuje více variant STP, avšak základní principy mají shodné
  - Kostra vzniká jako **strom nejlepších cest** od každého switche k jednomu referenčnímu bodu (přepínači) – **root bridge**
  - **Metriky jednotlivých cest** jsou dány tak, aby tvořily úplné uspořádání a aby v přepínané síti neexistovaly dvě rovnocenné cesty
  - Tzn. z pohledu jednoho switche existuje vždy jen **jedna nejlepší cesta**, nikdy ne více

- Základní standard STP **IEEE 802.1D**
- Základní verze STP se nazývá **Legacy 802.1D**
  - Ze současné verze standardu IEEE 802.1D je vypuštěná
- Zrychlená verze standardu je Rapid STP (RSTP), **802.1w**
  - V současnosti je součástí standardu IEEE 802.1D
- Verze podporující vícero instancí v jedné přepínané síti se nazývá Multiple Spanning Tree Protocol (MST), **802.1s**
  - V současnosti je součástí standardu IEEE 802.1D
- Cisco Systems má vlastní (proprietální) varianty STP a RSTP
  - Per VLAN STP (**PVST**) a Rapid Per VLAN STP (**RPVST**) pro každou VLAN nad proprietálním Cisco protokolem **ISL**
  - Per VLAN STP (**PVST+**) a Rapid Per VLAN STP (**RPVST+**) pro každou VLAN nad otevřeným protokolem **dot1Q**

V základní topologii existují fyzické smyčky (kružnice)

STP dočasně deaktivuje některé linky, tak aby v topologii smyčky (kružnice) neexistovaly a zároveň byly propojeny všechny přepínače

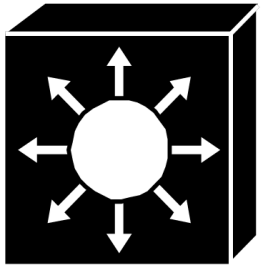
Po kolapsu některé z používaných linek STP přepočítá topologii a nastaví linky tak, aby byly všechny přepínače propojené a nadále neexistovala žádná smyčka



Multilayer přepínačing

- Klasické přepínání probíhá na druhé (L2) vrstvě ISO osi modelu
- Z tohoto pohledu je však možné rozlišovat další typy přepínání
  - Layer 1 přepínačing: Přenos a zesílení signálu
    - Hub, repeater
  - Layer 2 přepínačing: Přenos rámců (rozhodování na základě L2 hlavičky)
    - L2 switch, bridge
  - Layer 3 přepínačing: Přenos paketů (rozhodování na základě L3 hlavička)
    - L3 switch, router s modulem
  - Layer 4 přepínačing: Prenos segmentov (rozhodování na základě L4 hlavička)
    - Firewall s modulem
  - Layer 7 přepínačing: Přenos aplikačních dat (rozhodování na základě obsahu dat)
    - IPS/IDS systémy

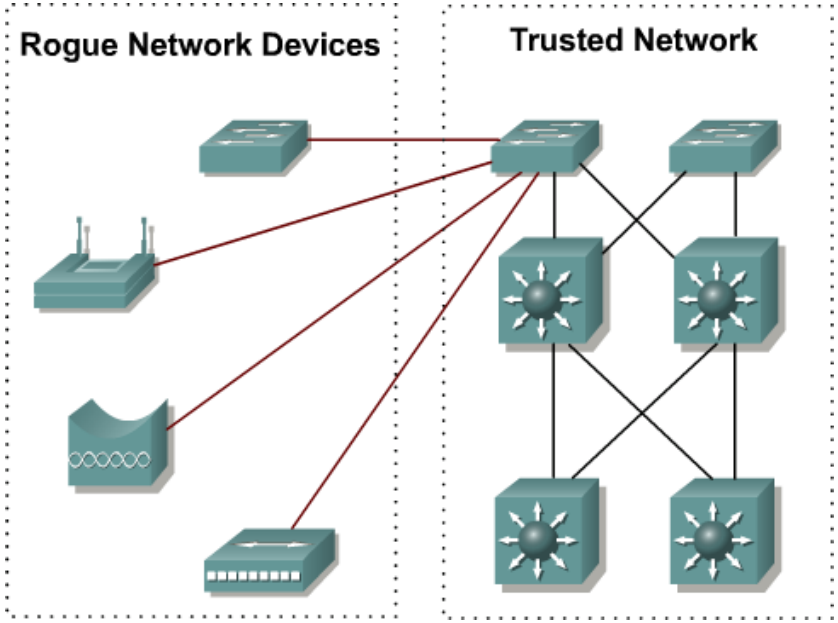
- Rozdíl mezi směrováním a přepínáním?
  - Routing je obvykle zpracováván softwarově
- přepínačing je realizovaný s hardwarovou podporou – ASIC
  - Obchází zpracování pomocí CPU



- Multilayer (L3+) switche
  - Switche s podporou přepínání na více vrstvách současně
  - Využití tzv. TCAM na rychlé procházení směrovací tabulky

Bezpečnost přepínané sítě

- Častým jevem je nekontrolované připojování zařízení k přepínané síti
  - Nové notebooky, PC, Access pointy, routery PDA
- Úkolem přepínačů na přístupové vrstvě je i ochrana přístupu do sítě
- Cisco přepínače nabízejí několik mechanismů pro řízení přístupu k přepínanému portu
  - Port security
  - Autentifikace 802.1X
  - Network Admission Control



- Port security dovoluje na každém portu definovat seznam tzv. bezpečných (**secured**) MAC adres
  - Takto zabezpečený port povolí komunikovat **pouze** těm stanicím, jejichž MAC adresa se nachází **v seznamu**
- Zabezpečené porty mohou být třech druhů:
  - **Static secure MAC** – manuálně nakonfigurovaná adresa
    - Nachází se v konfiguraci i MAC tabulce
    - Po restartu přepínače se z konfigurace opět načte
  - **Dynamic secure MAC** – dynamicky získaná (naučená) adresa
    - Nachází se pouze v MAC tabulce
    - Po odpojení portu nebo po restartu přepínače je ztracena
  - **Sticky secure MAC** – hybrid mezi statickou a dynamickou adresou
    - Je získaná (naučená) dynamicky a přepínač automaticky vygeneruje záznam do běžící konfigurace
    - Nachází se tedy jak v konfiguraci tak v MAC tabulce
    - Po restartu přepínače se opět načítá z konfigurace

- Na portu je možné definovat maximální počet bezpečných adres
  - Statické adresy se započítávají do počtu bezpečných adres
  - Přepínač automaticky přidá každou novou neznámou MAC adresu do seznamu bezpečných adres, jako dynamickou resp. sticky
  - Pokud by přidáním nové adresy překročil maximální počet bezpečných adres, nastává tzv. **porušení bezpečnosti** (security violation)
- Na narušení bezpečnosti lze zareagovat třemi způsoby
  - **Protect** – rámec s nepovolenou MAC adresou se **zahodí**
  - **Restrict** - rámec s nepovolenou MAC adresou se **zahodí** a zároveň je incident **zaznamenán** (hláška na konzolu, SNMP trap, Syslog)
  - **Shutdown** – port se při přijetí rámce s nepovolenou MAC adresou automaticky uvede do stavu **err-disabled**

Děkuji za pozornost