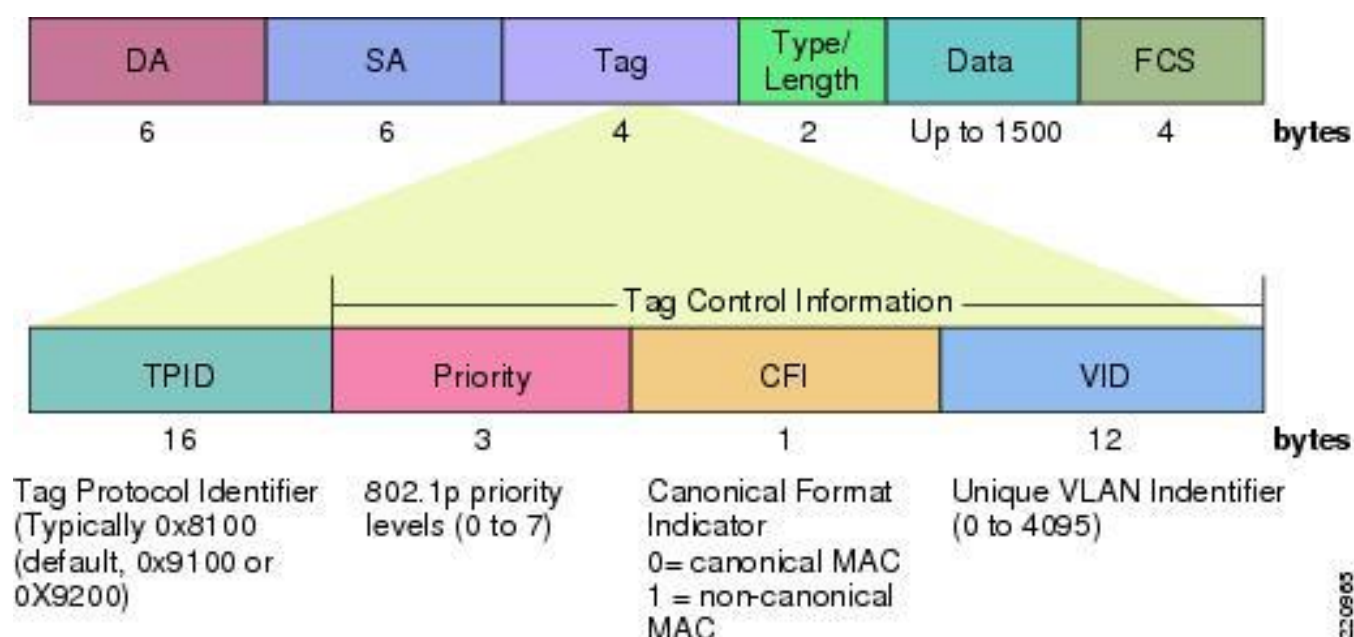


## Virtální lokální síť (VLAN)- pokračování

### IEEE 802.1q tagging

Protokolu IEEE 802.1q se říká také trunking protokol nebo dot1q tagging. Jedná se o standardizovanou metodu, kterou podporují všechny moderní switche s podporou VLAN. Funguje na principu tzv. tagování. Vezmeme originální rámec, jeho hlavičku rozšíříme o 4B informací, z nichž první je značka, že se jedná o protokol 802.1q (hodnota 0x8100). Dále následuje priorita dle protokolu 802.1p, příznak, zda je MAC adresa v kanonickém tvaru a poslední je číslo VLAN. Protože se změnila data, je třeba přepočítat kontrolní součet na konci rámce.



### Originální rámec

6B	6B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	typ nebo délka	data	kontrolní součet (FCS)

### Upravený rámec pomocí 802.1q

6B	6B	4B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	802.1q tag	typ nebo délka	data	kontrolní součet (FCS)

### Tvar 802.1q tagu

2B	3b	1b	12b
0x8100	priorita (802.1p)	Canonical Format Indicator (CFI)	VLAN ID

Tag Protocol ID (TPID) 2B Tag Control Information (TCI) 2B

Native VLAN je termín spojený s protokolem 802.1q. Nastavuje se na trunk portu, u Cisco prvků musíme nativní VLAN vždy nastavit a to shodně na obou stranách trunku. Provoz, který je

zařazen do native VLAN se při přenosu netaguje (zůstává nezměněn) a příchozí provoz, který není tagovaný se zařazuje do native VLAN. Často se jako native VLAN nastavuje management VLAN. Důsledkem také je, že pokud se na trunk port dostane nějaký rámec, který nemá tag, tak je zařazen do nativní VLAN. Jinak řečeno, pokud do portu, který je nakonfigurován jako trunk, připojíme normální stanici (která nepodporuje trunk), tak bude komunikovat v této VLAN. V praxi můžeme využít tuto vlastnost třeba u zapojení, kdy je připojen IP telefon a za ním PC. Native VLAN nastavíme stejně jako VLAN pro PC, potom pokud se odpojí telefon a PC se připojí přímo, tak jeho komunikace stále funguje.

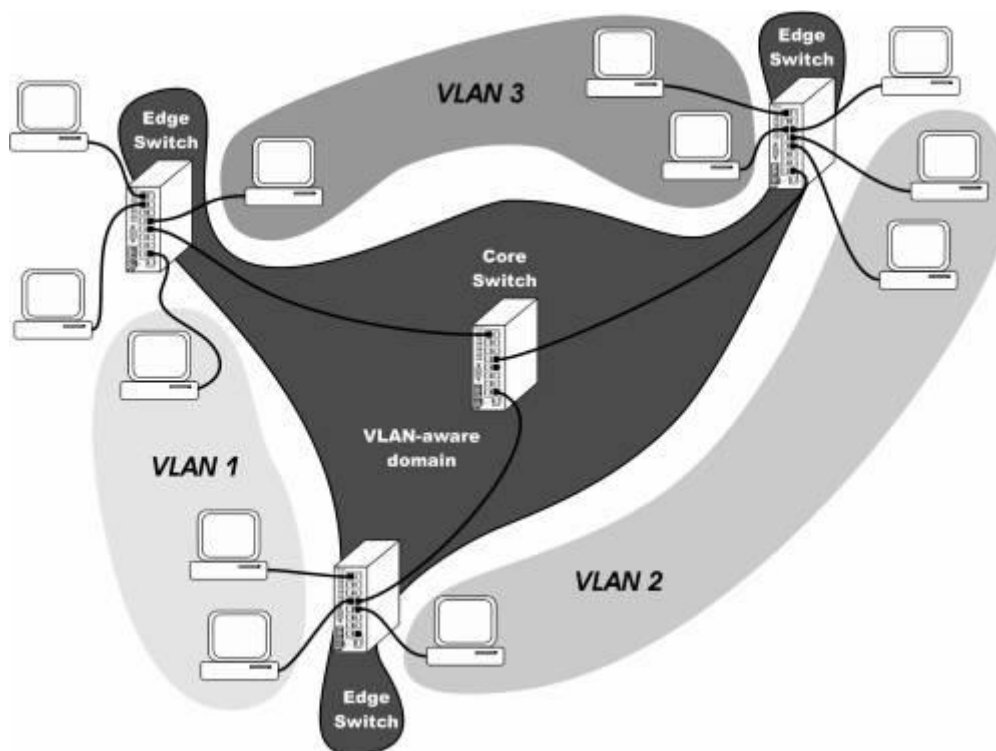
### Cisco ISL encapsulation

ISL znamená Inter-Switch Link, tedy spoj mezi switchi. Cisco vytvořilo svůj protokol ještě v době, kdy neexistoval standard. ISL má výhodu, že funguje nejen pro protokol IP, ale i pro jiné. Stejně jako 802.1q podporuje prioritizaci. Bohužel se jedná o proprietární metodu, kterou používá pouze Cisco a v dnešní době ji nalezneme pouze na switchích vyšší řady (třeba Catalyst 3750). Princip funkce je takový, že se celý rámec zabalí (encapsulate) do nové hlavičky a kontrolního součtu. Z toho plyne nevýhoda, že se více zvětšuje komunikace, každý rámec je o 30B větší.

26B		4B
ISL header	encapsulation frame (originální rámec)	kontrolní součet (FCS)

### Další využití trunků

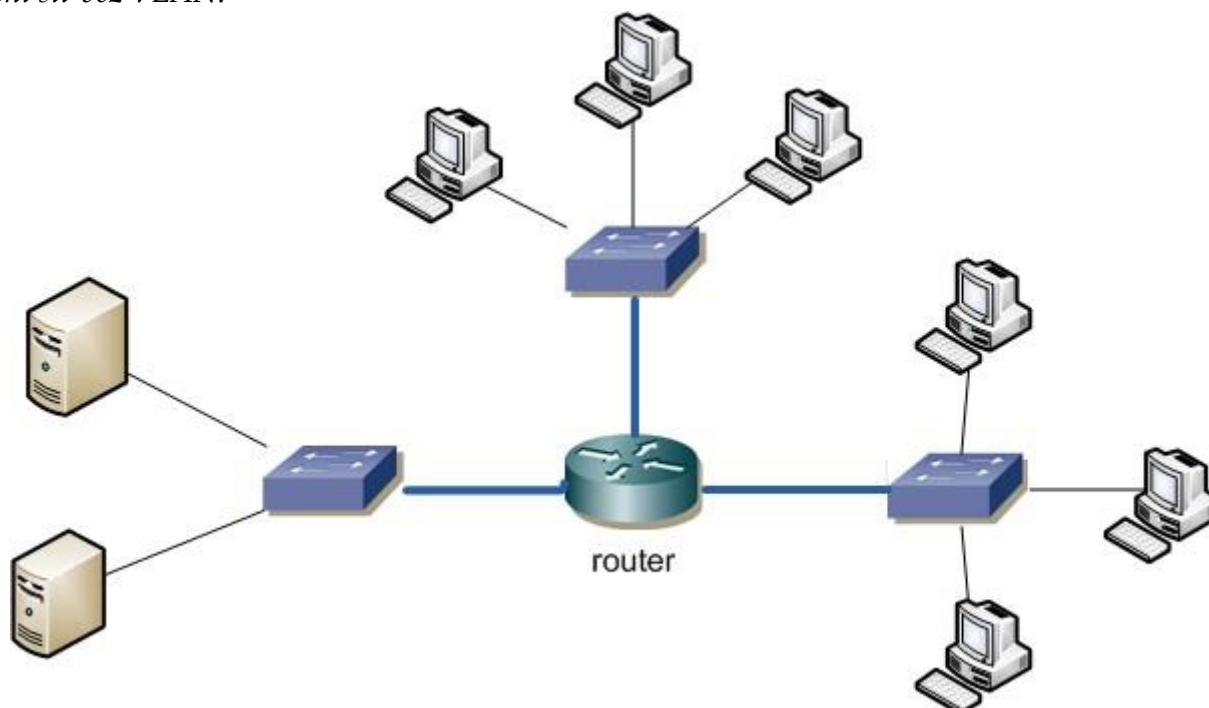
V dnešní době nemusíme používat trunk pouze pro propojení switchů, ale velice účinně jej využít i pro připojení serverů, které potřebujeme mít připojené do více sítí. Operační systém Linux podporuje protokol 802.1q již v jádře, pro Windows potřebujeme ovladač pro síťovou kartu s podporou VLAN (například Intel). Na síťové kartě pak nakonfigurujeme VLAN, které zde přichází a pro každou se vytvoří virtuální síťové spojení, které můžeme používat jako běžnou NIC. Ušetříme tím fyzické síťové karty na serveru, i když se snižuje propustnost. Použít to můžeme třeba na firewallu nebo host serveru pro virtuály. Na druhou stranu je třeba se vždy zamyslet, zda je toto to správné řešení a neexistuje něco jednoduššího (například pro DHCP server nepřipojovali do každé routované podsítě, když lze využít DHCP relay agenta).



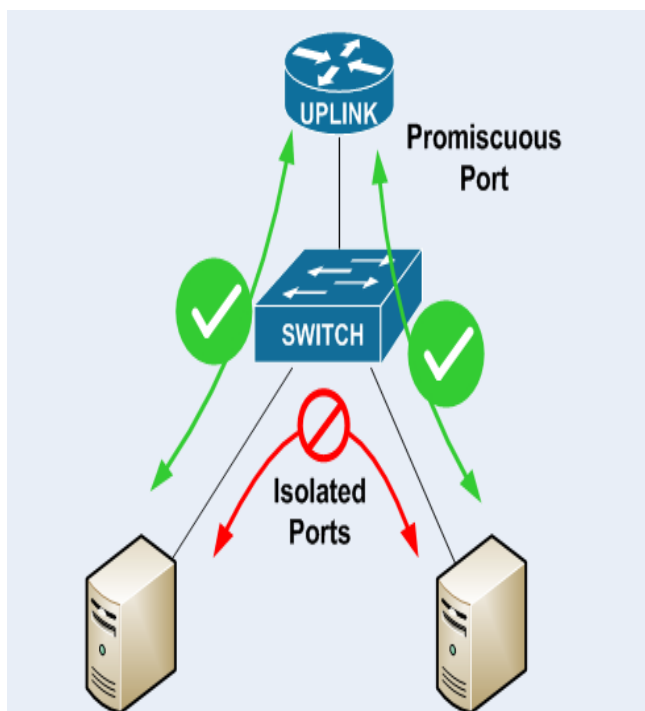
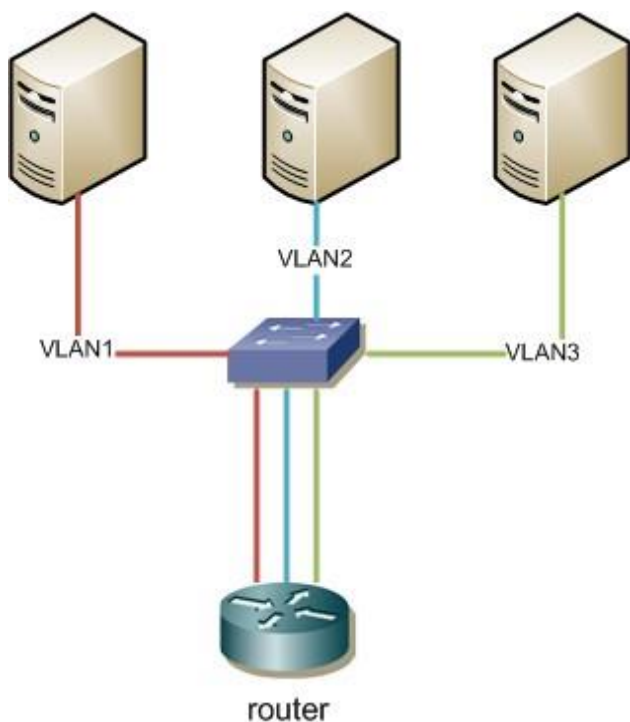
## Routing mezi VLANy

Tradiční routing vypadá tak, že máme několik oddělených sítí a chceme mezi nimi umožnit nějakou komunikaci. Následující obrázek představuje tři samostatné switchce propojené pomocí routeru. Může se jednat například o firemní servery a dvě oddělení, které k nim chceme připojit, ale nechceme, aby mohla komunikovat mezi sebou.

*Tradiční síť bez VLAN:*

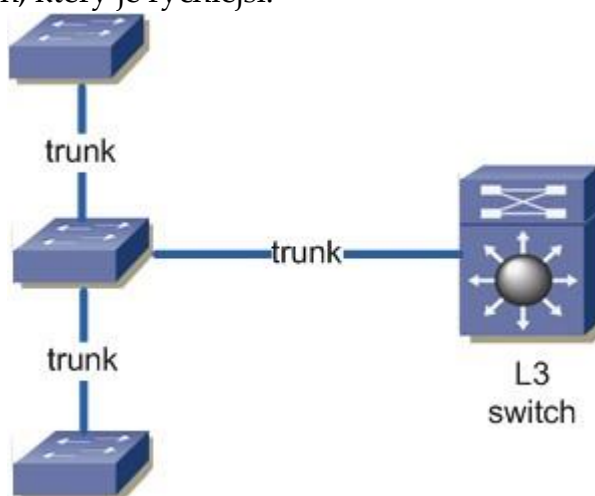
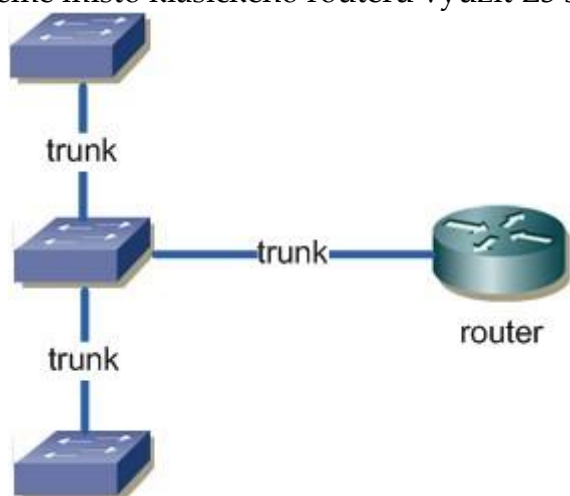


Pokud využíváme VLAN, můžeme se k nim chovat stejně jako k normálním podsítím. Na switchi můžeme jednotlivé VLAN, které chceme routovat, vyvést do samostatných access portů a ty připojit k routeru.



Využití buď samostatných portů na Routeru a nebo 1 port konfigurovaný jako router-on-a stick.

To je však zbytečné plýtvání a výhodnější je použít mezi routrem a switchem trunk. Také můžeme místo klasického routeru využít L3 switch, který je rychlejší.



U Cisco L3 switchů provedeme inter-VLAN routing jednoduše tak, že zapneme routování a na ty VLAN, které mají mezi sebou routovat, nastavíme IP adresu.

