Chapter 3: Architektura sítě kampusu

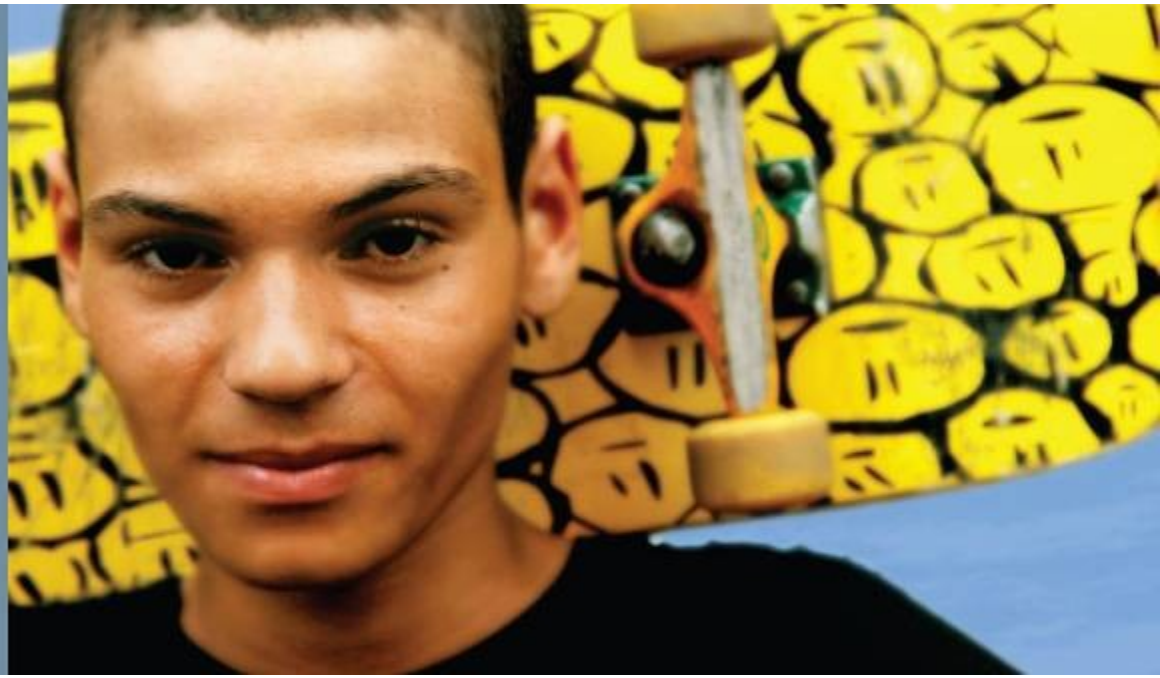
CCNP SWITCH: Implementing Cisco IP Switched Networks

Cisco | Networking Academy®
Mind Wide Open™

Cíle kapitoly 3

- Implementace sítí VLAN a trunků v přepínané architektuře kampusu
- Pochopení pojmu VTP a jeho omezení a konfigurace
- Implementace a konfigurace EtherChannel

Implementace VLAN a trunků v prostředí kampusu



Implementace VLAN a trunků v prostředí kampusu

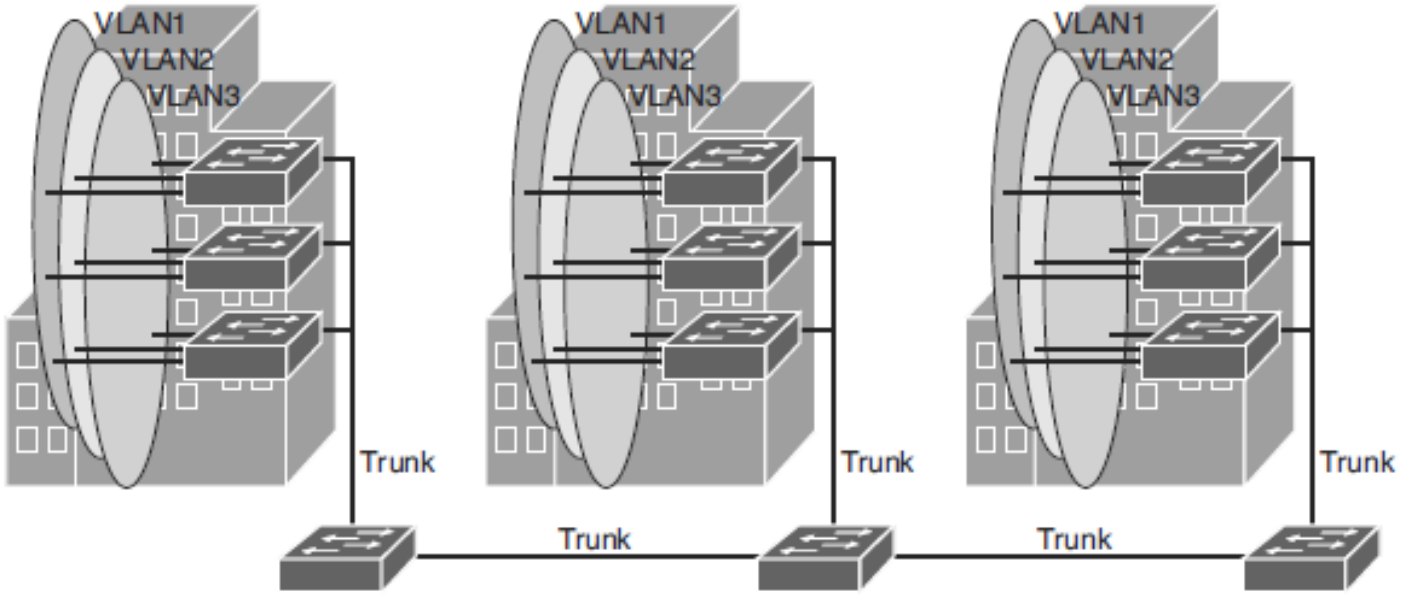
- V rámci komutované sítě poskytují sítě VLAN segmentaci a organizační flexibilitu.
- VLAN pomáhají správcům mít koncový uzel nebo skupinu pracovních stanic, které jsou logicky rozděleny podle funkcí, projektových týmů a aplikací, bez ohledu na fyzické umístění uživatelů.
- Sítě VLAN umožňují implementovat zásady přístupu a zabezpečení pro určité skupiny uživatelů a omezit doménu vysílání.
- Funkce hlasové VLAN umožňuje přístupovým portům přenášet hlasový provoz IP z IP telefonu. Protože kvalita zvuku telefonního hovoru IP se může zhoršit, pokud jsou data odesílána nerovnoměrně, přepínač podporuje kvalitu služeb (QoS).

Segmentace VLAN

- Větší ploché sítě se obvykle skládají z mnoha koncových zařízení, ve kterých jsou na všech portech v síti zaplaveny vysílání a neznámé pakety unicast.
- Jednou z výhod používání sítí VLAN je schopnost segmentovat vysílací doménu vrstvy L2. Všechna zařízení ve VLAN jsou členy stejné vysílací domény. Pokud koncové zařízení generuje vysílání vrstvy L2, přijímají vysílání všichni ostatní členové VLAN.
- Přepínače filtrují vysílání ze všech portů nebo zařízení, které nejsou součástí stejné VLAN.
- Při návrhu kampusu může správce sítě navrhnout síť kampusu s jedním ze dvou modelů:
  - End-to-End VLAN
  - Lokální sítě VLAN.
- Každý model má své výhody a nevýhody.

End-to-End VLANy

- End-to-End VLAN označuje jednu VLAN, která je spojena s porty přepínačů široce rozptýlenými v celé podnikové síti na více přepínačích.

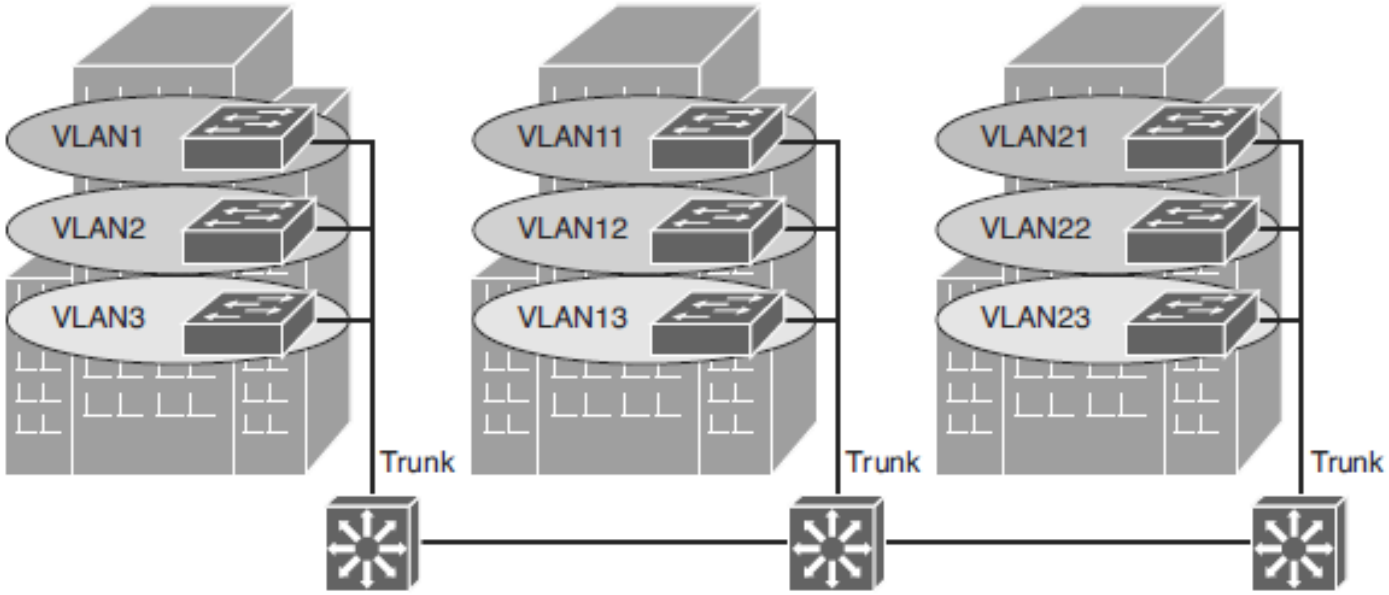


Charakteristika modelu End-to-End VLANy

- Každá síť VLAN je geograficky rozptýlena po celé síti.
- Uživatelé jsou seskupeni do každé VLAN bez ohledu na fyzické umístění.
- Když se uživatel pohybuje po areálu, členství VLAN tohoto uživatele zůstává stejné, bez ohledu na fyzický přepínač, ke kterému se tento uživatel připojuje.
- Uživatelé jsou obvykle spojeni s danou sítí VLAN z důvodů správy sítě. To je důvod, proč jsou udržovány ve stejné síti VLAN, tedy ve stejné skupině, když se pohybují kampusem.
- Všechna zařízení v dané VLAN mají obvykle adresy ve stejné podsíti IP.
- Přepínače běžně pracují v režimu VTP serveru/klienta.

Local VLANs

- V lokálním modelu VLAN jsou všichni uživatelé sady geograficky běžných přepínačů seskupeni do jediné VLAN, bez ohledu na organizační funkci těchto uživatelů.



Charakteristiky modelu Local VLANy

- Správce sítě by měl vytvořit lokální sítě VLAN s ohledem na fyzické hranice, nikoli na funkce úloh uživatelů na koncových zařízeních.
- Obecně existují lokální VLAN mezi přístupovou a distribuční úrovní.
- Provoz z místní sítě VLAN je směrován na úrovni distribuce a jádra, aby bylo dosaženo cílů v jiných sítích.
- Nakonfigurujte režim VTP v transparentním režimu, protože **sítě VLAN na daném přepínači přístupu by neměly být inzerovány na všechny ostatní přepínače v síti**, ani není nutné je vytvářet ručně v jiných databázích VLAN přepínačů.
- Síť, která se skládá výhradně z lokálních sítí VLAN, může těžit ze zvýšených časů konvergence nabízených prostřednictvím směrovacích protokolů namísto překlenovacího stromu pro sítě vrstvy 2. Obvykle se doporučuje mít jeden až tři VLAN na přepínač přístupové vrstvy.

Porovnání VLAN End-to-End a Local

Důvody pro implementaci návrhu end-to-end:

- **Seskupení uživatelů**
  - Uživatelé mohou být seskupeni do společného segmentu IP, i když jsou geograficky rozptýleni.
- **Bezpečnostní**
  - VLAN může obsahovat prostředky, které by neměly být přístupné všem uživatelům v síti, nebo může existovat důvod omezit určitý provoz na konkrétní VLAN.
- **Uplatňování kvality služeb (QoS)**
  - Provoz může být prioritou s vyšším nebo nižším přístupem k síťovým prostředkům z dané sítě VLAN.

Porovnání VLAN End-to-End a Local

Další důvody pro implementaci návrhu end-to-end:

- **Vyhýbání se směrování**
  - Pokud je většina provozu uživatelů VLAN určena pro zařízení na stejné VLAN.
- **Speciální síť VLAN**
  - Někdy je poskytována síť VLAN pro přenos jednoho typu provozu, který musí být rozptýlen po celém kampusu (například vícesměrové vysílání, hlasové nebo návštěvnické sítě VLAN).
- **Špatný design**
  - Pro jasný účel jsou uživatelé umístěny do VLAN, které pokrývají areál nebo dokonce WAN. Někdy, když je síť již nakonfigurována a spuštěna, organizace váhají s vylepšením návrhu z důvodu prostojů nebo z jiných politických důvodů.

Porovnání VLAN End-to-End a Local

Důvody pro implementaci návrhu Local:

- **Deterministický tok provozu**
  - Jednoduché rozvržení poskytuje předvídatelnou trasu vrstvy 2 a vrstvy 3.
- **Aktivní redundantní cesty**
  - Při implementaci per-VLAN Spanning Tree (PVST) nebo Multiple Spanning Tree (MST) lze využít redundantní cesty, protože není k dispozici žádná smyčka.
- **Vysoká dostupnost**
  - Redundantní cesty existují na všech úrovních infrastruktury.
- **Konečná doména selhání**
  - Pokud jsou VLAN lokální pro přepínací blok a počet zařízení v každé VLAN je udržován malý, poruchy ve vrstvě 2 jsou omezeny na malou podmnožinu uživatelů.
- **Škálovatelný design**
  - V návaznosti na návrh architektury podnikového kampusu lze snadno začlenit nové přepínače přístupu a v případě potřeby přidat nové dílčí moduly.

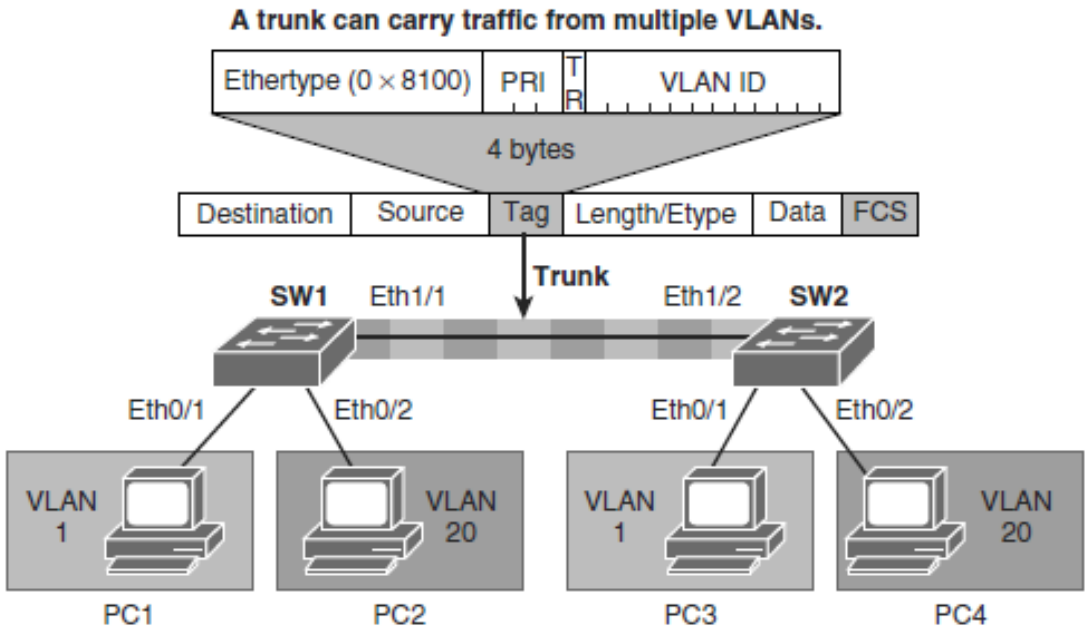
Porovnání VLAN End-to-End a Local

Nevýhody End-to-End VLAN:

- Porty přepínačů jsou poskytovány každému uživateli a jsou spojeny s danou sítí VLAN. Protože uživatelé na komplexní VLAN mohou být kdekoli v síti, všechny přepínače si musí být vědomy této VLAN. To znamená, že u všech přepínačů přenášejících provoz pro end-to-end VLAN **je nutné mít tyto specifické VLAN definovány v databázi VLAN každého přepínače.**
- Zaplavený provoz pro VLAN je ve výchozím nastavení předáván každému přepínači, i když v současné době nemá žádné aktivní porty v konkrétním VLAN typu end-to-end.
- Odstraňování problémů se zařízeními v kampusu s koncovými sítěmi VLAN může být náročné, protože provoz jedné sítě VLAN může procházet několika přepínači ve velké části kampusu, což může snadno způsobit potenciální problémy v rámci Spanning Tree.

Implementace trunku v prostředí kampusu

- Trunk je spojení point-to-point, které přenáší provoz pro více VLAN přes jediné fyzické spojení mezi dvěma přepínači nebo jakýmkoli dvěma zařízeními.
- Trunking se používá k rozšíření operací vrstvy 2 v celé síti.

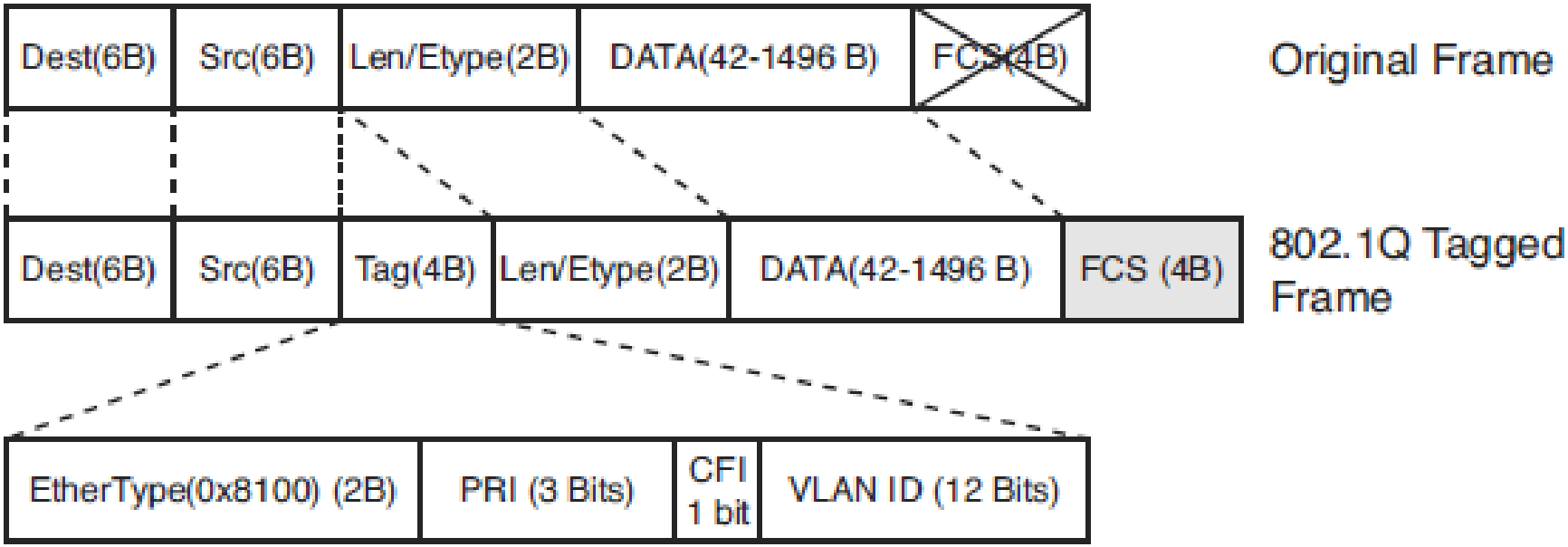


Protokoly Trunkingu

- Pro přenos více sítí VLAN přes jediné spojení mezi dvěma zařízeními se používá speciální protokol.
- Existují dvě trunkové technologie:
  - Inter-Switch Link (ISL): Proprietární trunking zapouzdření Cisco

    zapomeňme na něj
  - IEEE 802.1Q: Standardní průmyslová metoda vedení

802.1Q Frame

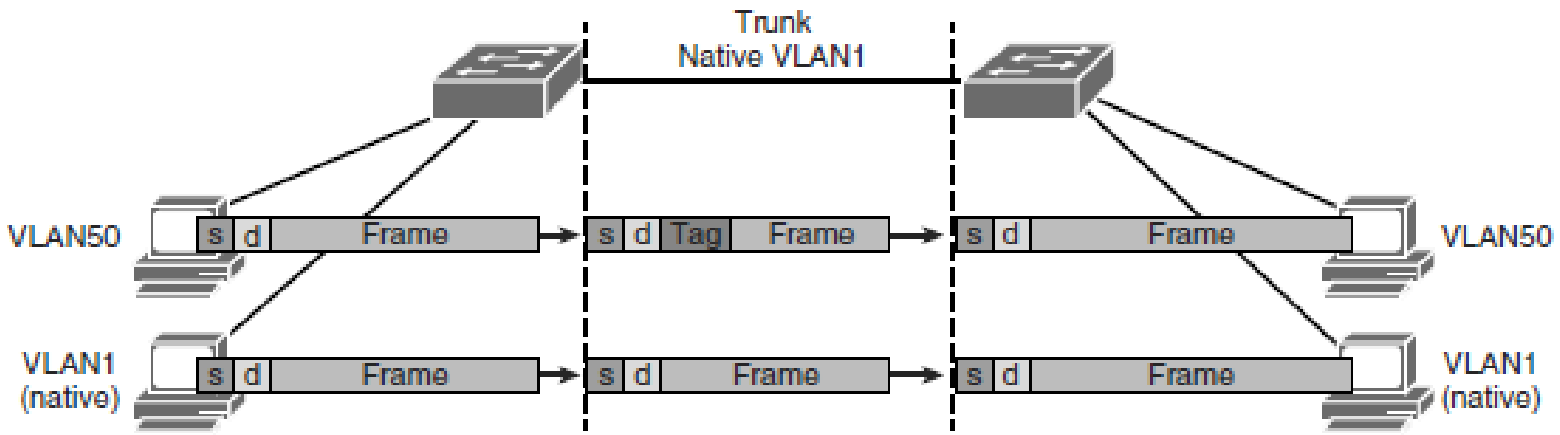

Dest(6B)
Src(6B)
Len/Etype(2B)
DATA(42-1496 B)
FCS(4B)
Original Frame
Dest(6B)
Src(6B)
Tag(4B)
Len/Etype(2B)
DATA(42-1496 B)
FCS (4B)
802.1Q Tagged Frame
EtherType(0x8100) (2B)
PRI (3 Bits)
CFI 1 bit
VLAN ID (12 Bits)

802.1Q tag

- **EtherType(TPID):** 0x8100 pro Ethernet.
- **PRI:** 3-bit 802.1p priorita.
- **CFI:** Canonical Format Identifier 0 for Ethernet switches.
- **VLAN ID:** 12-bit VLAN field. Max. 4094. 0 indikuje prioritní rámec, a hodnota 4095 (FFF) is rezervována.

- MTU je 1522 byte.

Native VLAN



- Častou chybou konfigurace jsou různé nativní sítě VLAN. Nativní síť VLAN, která je nakonfigurována na každém konci kufru 802.1Q, musí být stejná.
- Přepínače Cisco používají protokol Cisco Discovery Protocol (CDP) k upozornění na nativní nesoulad VLAN.
- Ve výchozím nastavení bude nativní VLAN VLAN 1.

```
Switch(config-if)# switchport trunk native vlan vlan-id
```

DTP

Mode in Cisco IOS	Function
Access	Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.
Trunk	Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.
Nonegotiate	Prevents the interface from generating DTP frames. You must configure the local and neighboring interface manually as a trunk interface to establish a trunk link. Use this mode when connecting to a device that does not support DTP.
Dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.
Dynamic auto	Makes the interface willing to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. This is the default mode for all Ethernet interfaces in Cisco IOS.

Kombinace módů DTP

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Čísla VLAN

VLAN Range	Range Usage	Propagated via VTP
0, 4095	Reserved for system use only. You cannot see or use these VLANs.	—
1	Normal Cisco default. You can use this VLAN, but you cannot delete it.	Yes
2–1001	Normal For Ethernet VLANs. You can create, use, and delete these VLANs.	Yes
1002–1005	Normal Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.	Yes
1006–1024	Reserved for system use only. You cannot see or use these VLANS.	—
1025–4094	Extended for Ethernet VLANs only.	Not supported in VTP Versions 1 and 2. The switch must be in VTP transparent mode to configure extended-range VLANS. This range is only supported in Version 3.

Konfigurace, verifikace a troubleshooting VLAN a Trunks

Step 1.

- `Switch# configure terminal`

Step 2. Vytvoření nové VLAN s jejím ID:

- `Switch(config)# vlan vlan-id` *je nutný*

Step 3. (volitelné) Název VLAN:

- `Switch(config-vlan)# name vlan-name` *není nezbytný*

```
Switch# configure terminal
Switch(config)# vlan 5
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit
```

```
Switch# configure terminal
Switch(config)# no vlan 3
Switch(config)# end
```

Přiřazení Access portu k VLAN

Krok 1. V režimu globální konfigurace zadejte režim konfigurace pro konkrétní port, který chcete přidat do VLAN:

- `Switch(config)# interface interface-id`

Krok 2. Určete port jako přístupový port:

- `Switch(config-if)# switchport mode access`
- `Switch(config-if)# switchport host`

Krok 3. Odstraňte nebo umístěte port do konkrétní VLAN:

- `Switch(config-if)# [ no ] switchport access vlan vlan-id`

host zapne spanning-tree PortFast and vypne EtherChanneling

Přiřazení Access portu k VLAN

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet 5/6
Switch(config-if)# description PC A
Switch(config-if)# switchport
Switch(config-if)# switchport host
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 200
Switch(configif)# no shutdown
Switch(config-if)# end
```

Výpis podle čísla či jména VLANy

```
SW1#show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active    Et1/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

SW1#
```

```
SW1# show vlan name VLAN0003

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active    Et1/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

SW1#
```

Nezapomenout na kontrolu správnosti

```
Switch# show running-config interface FastEthernet 5/6
Building configuration... !
Current configuration :33 bytes
interface FastEthernet 5/6
switchport access vlan 200
switchport mode access
end
```

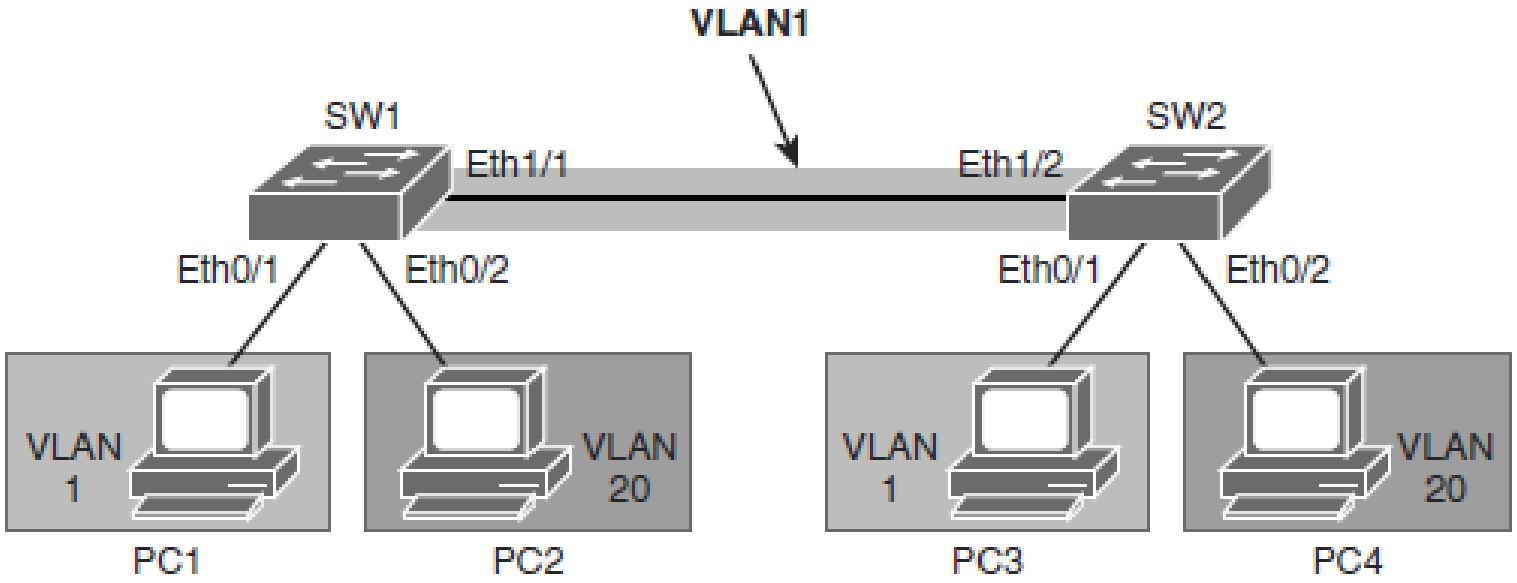
Kontrola informací na portu

```
BXB-6500-10:8A# SW1# show int ethernet 4/1 switchport
Name: Et4/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Operational Dotlq Ethertype:  0x8100
Negotiation of Trunking: Off
Access Mode VLAN: 200 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Operational Native VLAN tagging: disabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Voice VLAN: none (Inactive)
Appliance trust: none
```

Zobrazení tabulky MAC Address

```
Switch# show mac-address-table interface GigabitEthernet 0/1 vlan 1
SW1# show mac address-table interface Gigabitethernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aabb.cc01.0600    DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 1
```

Výchozí topologie příkladu



Device	Device IP	Device Interface	Device Neighbor	Interface on the Neighbor
PC1	192.168.1.100	Eth0/0	SW1	Eth0/1
PC2	192.168.20.101	Eth0/0	SW1	Eth0/2
PC3	192.168.1.110	Eth0/0	SW2	Eth0/1
PC4	192.168.20.110	Eth0/0	SW2	Eth0/2

Konfigurace VLAN a trunků

Krok 1. Konfigurace VLAN 20 na obou stranách.

- `SW1(config)# vlan 20`
- `SW1(config-vlan)# exit`
- `% Applying VLAN changes may take few minutes. Please wait...`

Krok 2. Na SW1/2 konfigurace Ethernet 0/2 coby access portu a přiřazení k VLAN 20

- `SW1(config)# interface ethernet 0/2`
- `SW1(config-if)# switchport mode access`
- `SW1(config-if)# switchport access vlan 20`

Krok 3. Konfigurace trunku na SW1 a SW2. dot1Q encapsulation.

- Trunk configuration on SW1:
- `SW1(config)# interface Ethernet 1/1`
- `SW1(config-if)# switchport trunk encapsulation dot1q`
- `SW1(config-if)# switchport trunk allowed vlan 1,20`
- `SW1(config-if)# switchport mode trunk`
- Trunk configuration on SW2:
- `SW2(config)# interface Ethernet 1/2`
- `SW2(config-if)# switchport trunk encapsulation dot1q`
- `SW2(config-if)# switchport trunk allowed vlan 1,20`
- `SW2(config-if)# switchport mode trunk`

Verifikace trunkingu

```
SW1# show interfaces trunk

Port            Mode         Encapsulation  Status        Native vlan
Et1/1           on           802.1q         trunking      1

Port            Vlans allowed on trunk
Et1/1           1,20

Port            Vlans allowed and active in management domain
Et1/1           1,20

Port            Vlans in spanning tree forwarding state and not pruned
Et1/1           1,20
```

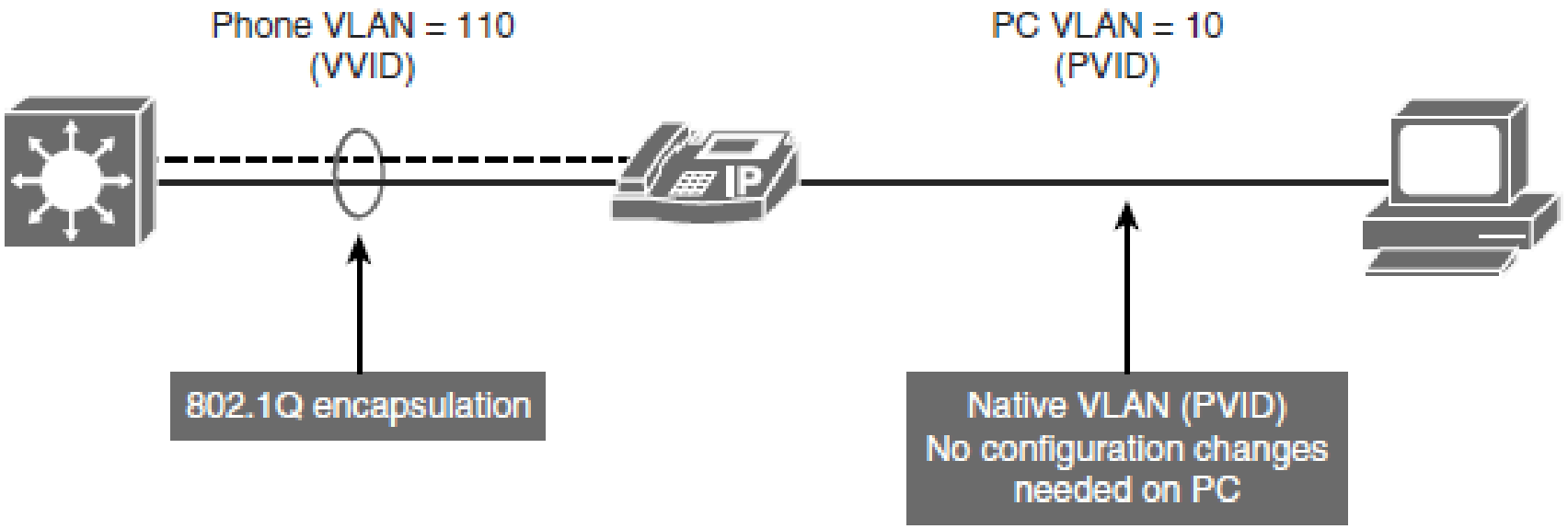
Praktické rady pro VLANs a Trunkingu

- Pro model Local VLAN se obvykle doporučuje mít pouze jednu až tři VLAN na přístupový modul.
- V lokálním modelu VLAN se vyhněte VTP.
- Nepoužívejte VLAN 1 jako černou díru pro všechny nepoužívané porty.
- Snažte se mít vždy samostatné hlasové sítě VLAN, datové sítě VLAN, sítě VLAN pro správu, nativní sítě VLAN, sítě VLAN s černou dírou a výchozí sítě VLAN (VLAN 1).
- Zabraňte veškerému datovému provozu z VLAN 1; povolují pouze řídicí protokoly, aby fungovaly na VLAN 1 (DTP, VTP, BPDU, Port Aggregation Protocol [PAgP], Link Aggregation Control Protocol [LACP], Cisco Discovery Protocol [CDP] atd.).

Best Practices for VLANs and Trunking

- DTP je užitečný, když je stav přepínače na druhém konci propojení nejistý nebo se může časem měnit. Když má být spojení nastaveno na trunk stabilním způsobem, změna obou konců na trunk nonegotiate urychluje konvergenční čas, což ušetří až 2 sekundy po spuštění. Tento režim doporučujeme na stabilních propojeních mezi přepínači, které jsou součástí stejné základní infrastruktury.
- Na trunkových linkách se doporučuje ručně odříznout (prune) VLANy, které se nepoužívají.
- Je také dobré mít nepoužitou VLAN jako nativní VLAN na trunkových spojích, aby se zabránilo **spoofingu DTP. Na access portu ne trunk nebo "dynamic desirable", "dynamic auto"**.
- https://gist.github.com/mgeeky/7ff9bb1dcf8aa093d3a157b3c22432a0
- Pokud na portu nepoužíváte trunking, můžete jej deaktivovat pomocí příkazu **switchport host**.

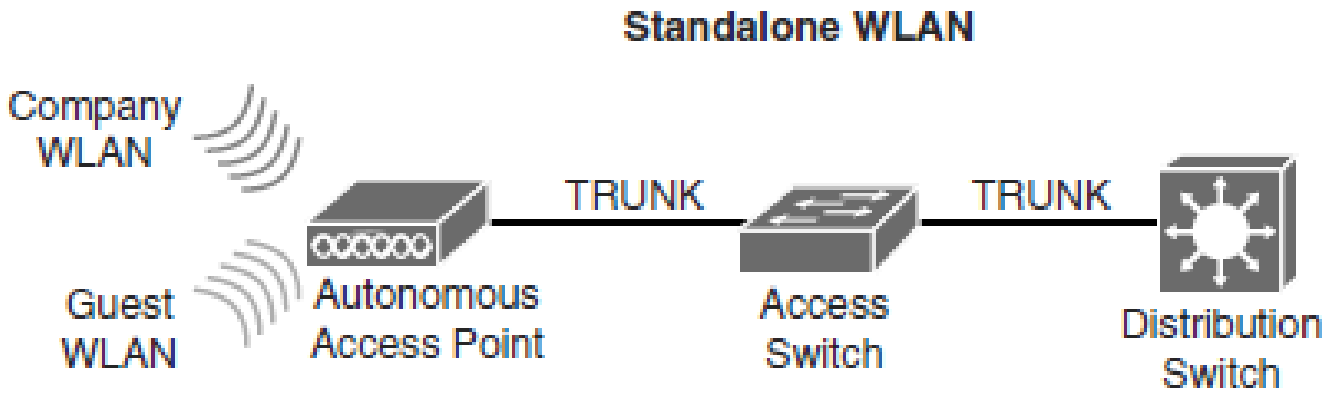
Voice VLAN



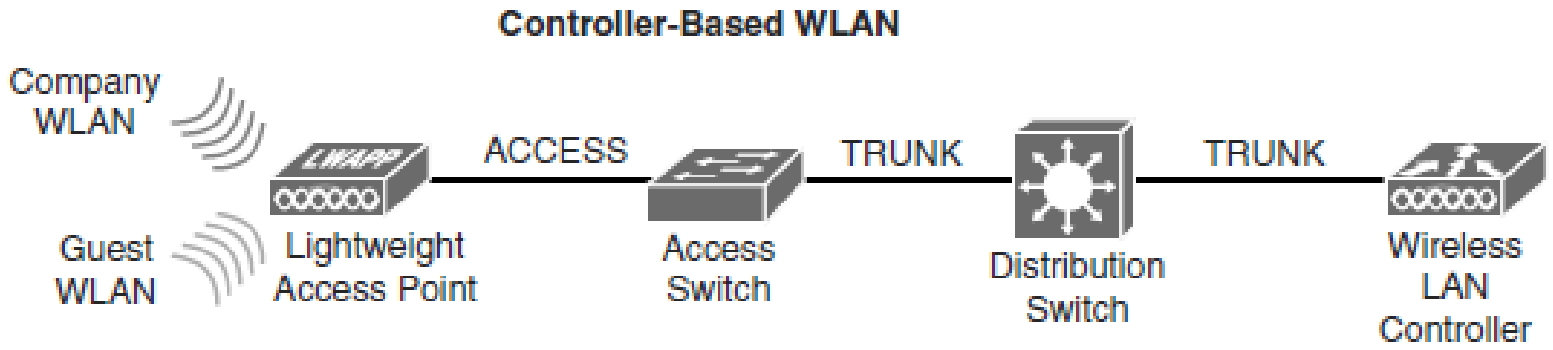

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport voice vlan 110
```

Autonomní WLANy

- V autonomním (nebo samostatném) řešení pracuje každý přístupový bod samostatně a funguje jako přechodový bod mezi bezdrátovým médiem a médiem 802.3.
- Datový přenos mezi dvěma klienty teče přes přepínač Layer 2, když je ve stejné podsíti z jiné AP infrastruktury. Když AP převádí rámec IEEE 802.11 na rámec 802.3, MAC adresa bezdrátového klienta je přenesena do záhlaví 802.3 a zobrazuje se jako zdroj pro přepínač.
- Bezdrátový klient se zobrazí jako cílová adresa MAC.



Controller-Based WLANy



- U řešení controller-based jsou funkce správy, řízení, nasazení a zabezpečení přesunuty do centrálního bodu: **wireless con**troller.
- K implementaci bezdrátové sítě je třeba nakonfigurovat přístupové body a přepínače. AP lze konfigurovat přímo (autonomní AP) nebo prostřednictvím ovladače (**lightweiht A**P).

VLAN Trunking Protocol

Charakteristika proprietárního protokolu VTP

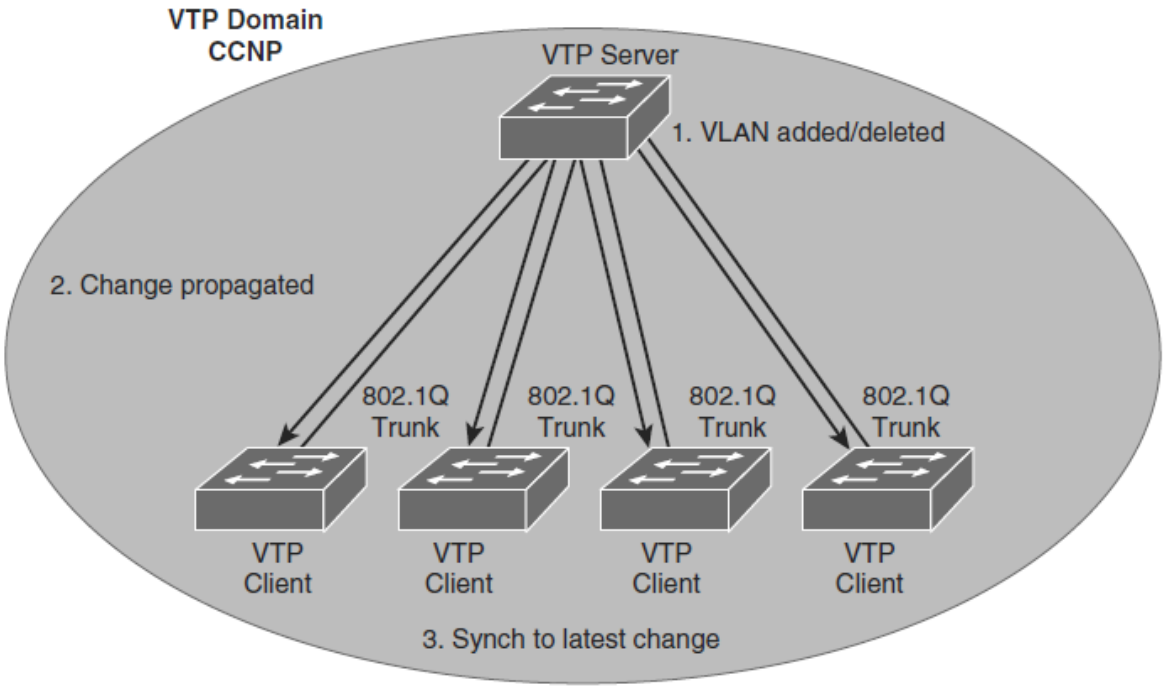
- VTP je protokol Layer 2, který udržuje konzistenci konfigurace VLAN pomocí **správy přidávání, mazání a změn názvů** VLAN v sítích.
- Přepínače Cisco přenášejí souhrnné reklamy VTP přes správu VLAN (ve výchozím nastavení VLAN 1) pomocí rámce vícesměrového vysílání vrstvy 2 každých **5 minut**.
- Doména VTP je jeden přepínač nebo několik propojených přepínačů sdílejících stejné prostředí VTP, ale přepínač může být kdykoli pouze v jedné doméně VTP.
- Ve výchozím nastavení je přepínač Cisco Catalyst ve stavu domény bez správy nebo <null>, dokud neobdrží advertisement na doménu přes trunkové propojení nebo dokud nenakonfigurujete doménu správy.
- Konfigurace, které jsou vytvořeny na jednom serveru VTP, jsou šířeny přes trunkové odkazy na všechny připojené přepínače v síti.
- Konfigurace jsou považovány za vyměněny, pokud se shodují doména VTP a hesla VTP.

Šíření VTP

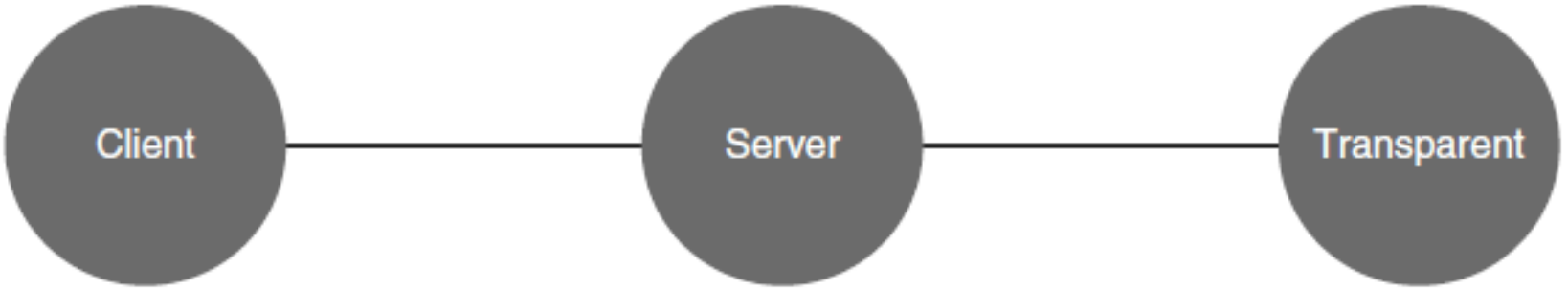
Krok 1. Správce přidá novou definici VLAN.

Krok 2. VTP šíří informace VLAN na všechny přepínače v doméně VTP.

Krok 3. Každý přepínač synchronizuje svou konfiguraci tak, aby obsahoval nová data VLAN.



Módy VTP



- Cannot create, modify, or delete VLANs
- Sends and forwards advertisements
- Synchronizes VLAN configurations

- Creates, modifies, and deletes VLANs
- Sends and forwards advertisements
- Synchronizes VLAN configurations

- Creates, modifies, and deletes local VLANs only
- Forwards advertisements
- Does not synchronize VLAN configurations

Operace VTP

- Servery a klienti CTP IOS VTP ve výchozím nastavení ukládají sítě VLAN do souboru vlan.dat v paměti Flash, což jim umožňuje uchovávat **tabulku VLAN a číslo revize**.
- Příkaz *erase startup-config* neovlivní soubor vlan.dat na přepínačích v režimech VTP klient a server.
- Přepínače, které jsou v transparentním režimu VTP, zobrazují konfigurace VLAN a VTP ve výstupu příkazu *show running-config*, protože tyto informace jsou uloženy v konfiguračním textovém souboru.
- Pokud provedete *erase start-config* na transparentním přepínači VTP, odstraníte jeho VLAN.

Verze VTP

- Přepínače Cisco Catalyst podporují tři různé verze VTP: 1, 2 a 3.
- Je důležité rozhodnout, kterou verzi použít, protože nejsou interoperabilní.
- Společnost Cisco doporučuje provozovat pouze jednu verzi VTP, aby byla zajištěna stabilita sítě.
- Výchozí verze VTP, která je povolena u přepínače Cisco, je verze 1.
- Pokud potřebujete změnit verzi VTP v doméně, jedinou věcí, kterou musíte udělat, je povolit ji na serveru VTP; změna se bude šířit po celé síti.

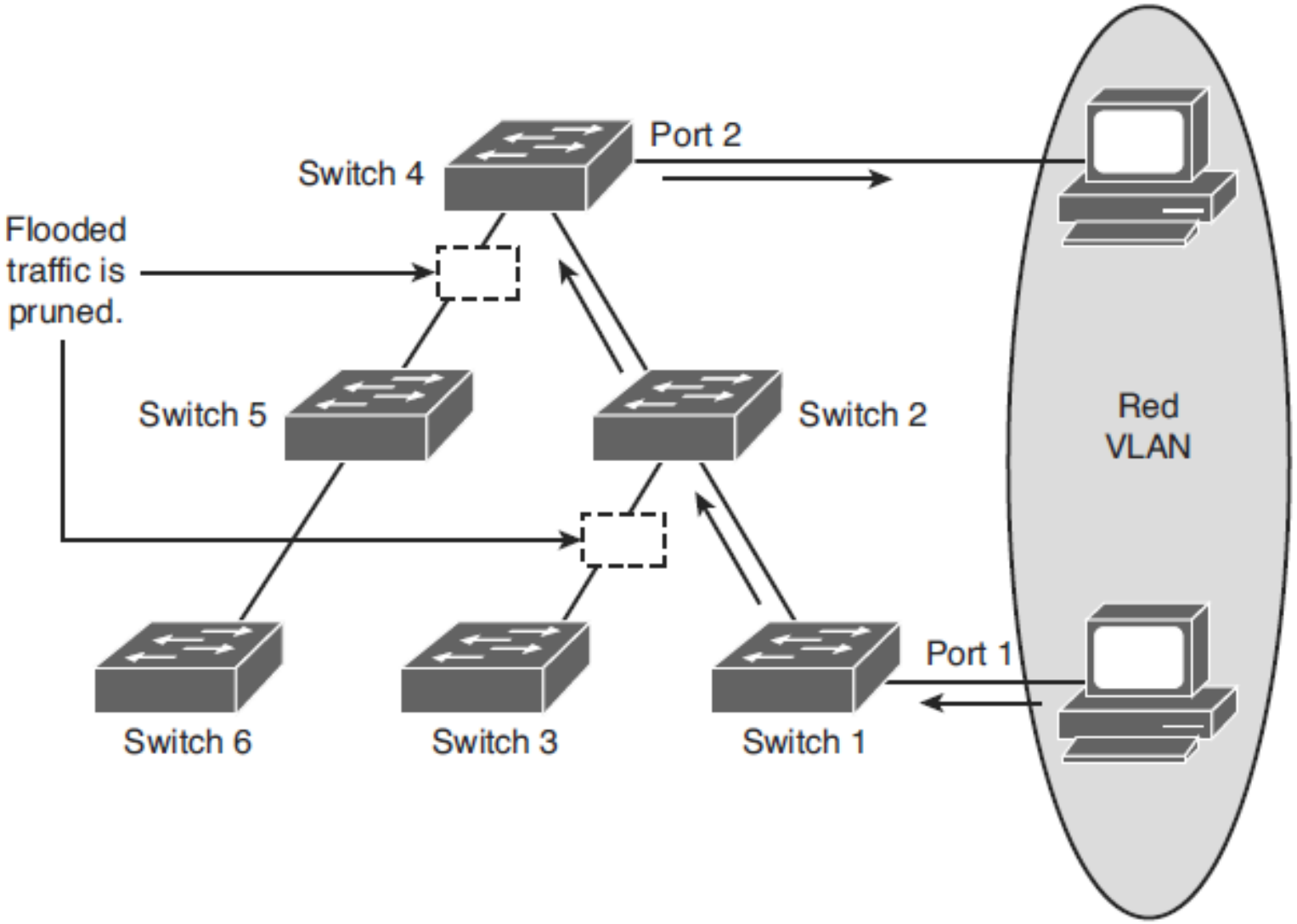
VTP Verze 1 a 2

- **Transparentní režim závislý na verzi**
  - VTP verze 1, transparentní síťové zařízení VTP kontroluje zprávy VTP na název domény a verzi
  - VTP verze 2 přeposílá zprávy VTP v transparentním režimu, aniž by zkontrolovala verzi.
- **Kontrola konzistence**
  - Ve verzi VTP 2 jsou prováděny kontroly konzistence VLAN, jako jsou názvy a hodnoty VLAN.
- **Podpora Token Ring**
  - VTP verze 2 podporuje přepínání Token Ring LAN a VLAN.
- **Nerozpoznaná podpora typu value-length-value**
  - Přepínače VTP verze 2 šíří přijaté zprávy o změně konfigurace mimo jiné odkazy na trunk, i když nejsou schopni zprávě porozumět.

VTP Version 3

- **Rozšířená podpora VLAN**
  - VTP lze také použít k propagaci rozšířených VLAN
- **Název domény se automaticky nenaučí**
  - U VTPv2 bude výchozí tovární přepínač, který přijímá zprávu VTP, upravovat nový název domény VTP.
- **Lepší zabezpečení**
  - Heslo domény VTP je bezpečné během přenosu a v databázi přepínače.
- **Lepší propagace databáze**
  - Jiná zařízení mohou aktualizovat pouze primární server a tuto roli může mít pouze jeden server na doménu VTP.
- **Podpora více Spanning Tree (MST)**
  - VTPv3 přidává podporu pro propagaci instancí MST.

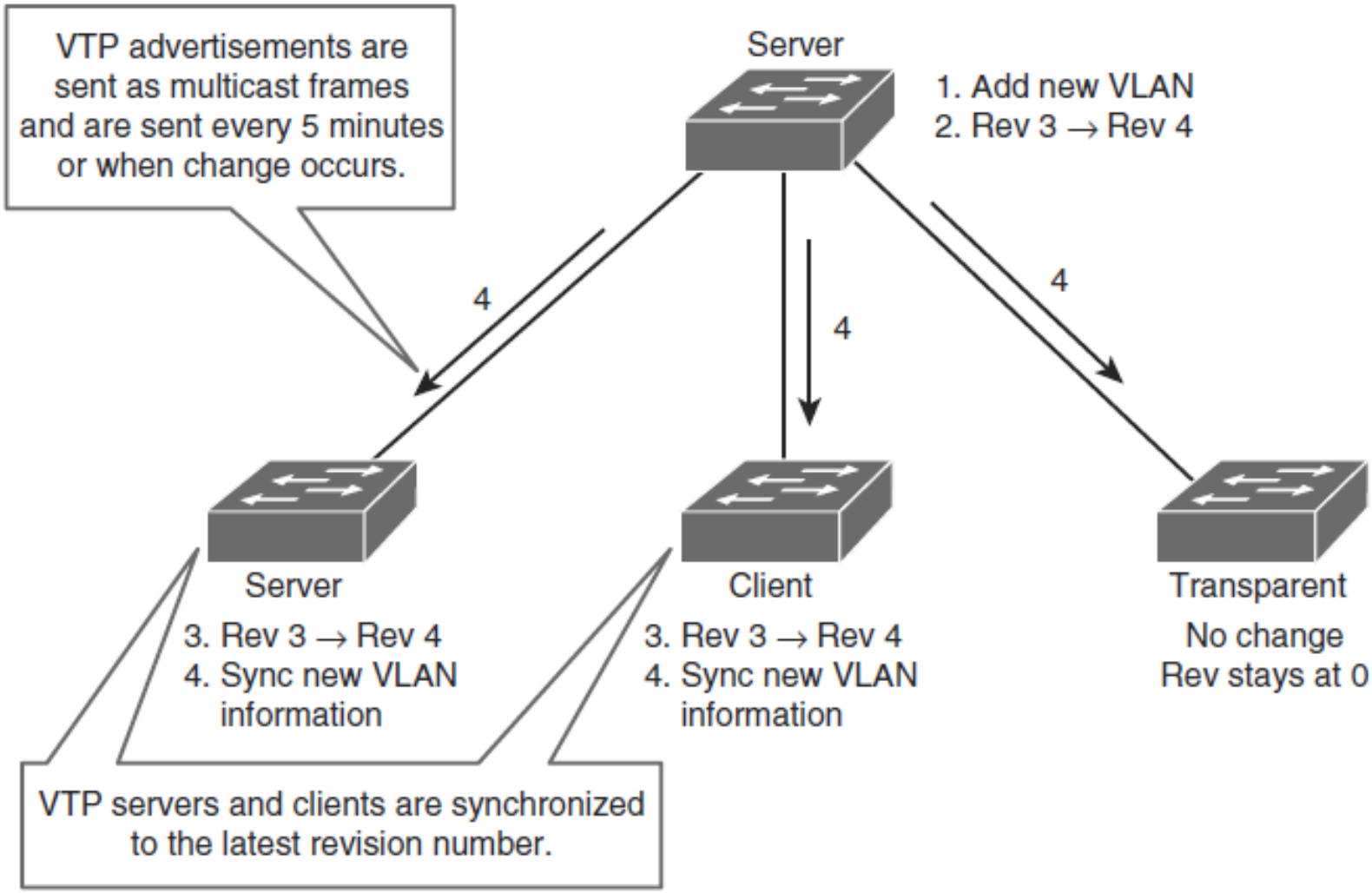
VTP Pruning


Port 2
Switch 4
Flooded
traffic is
pruned.
Switch 5
Switch 2
Red
VLAN
Port 1
Switch 6
Switch 3
Switch 1

VTP Authentizace

- Domény VTP lze zabezpečit pomocí funkce hesla VTP.
- Je důležité zajistit, aby všechny přepínače v doméně VTP měly stejné heslo a název domény; jinak se přepínač nestane členem domény VTP.
- Přepínače Cisco používají algoritmus digest 5 (MD5) pro kódování hesel v 16bajtových slovech.
- Tato hesla se šíří uvnitř souhrnných reklam VTP.
- Ve VTP hesla rozlišují velká a malá písmena a mohou mít délku 8 až 64 znaků.

Nabídky (advertisements) VTP



Typy zpráv VTP

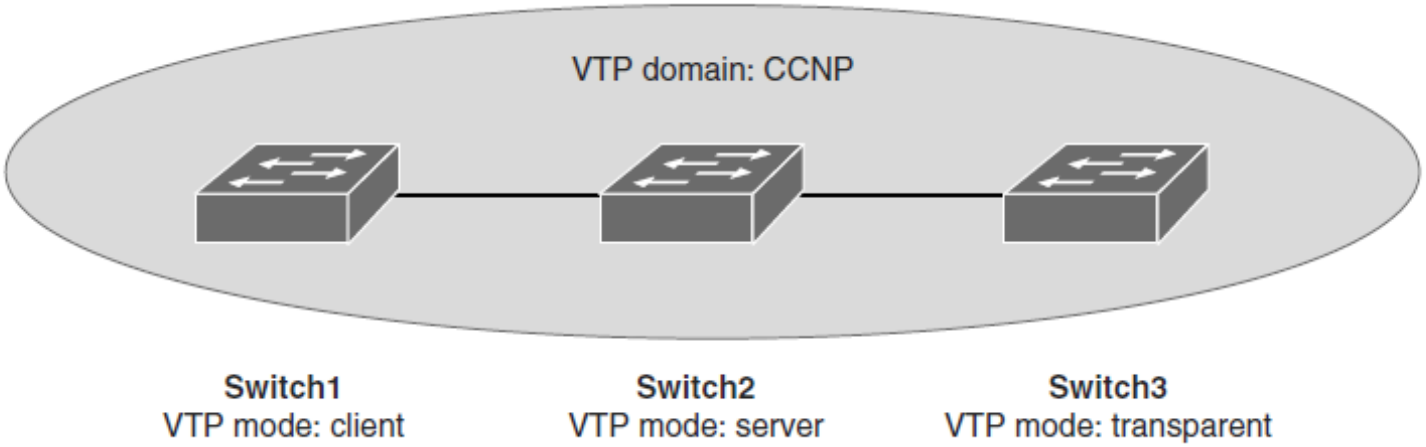
- **Summary Advertisements**
  - Ve výchozím nastavení přepínače Catalyst vydávají souhrnné reklamy v 5minutových krocích. *Summary Advertisement* informují sousední přepínače o aktuálním názvu domény VTP a čísle revize konfigurace.
  - Když přepínač obdrží paket *Summary Advertisement*, přepínač porovná název domény VTP s vlastním názvem domény VTP.
  - Pokud se název liší, přepínač jednoduše ignoruje paket.
  - Pokud je název stejný, přepínač pak porovná revizi konfigurace s vlastní revizí.
  - Pokud je jeho vlastní revize konfigurace vyšší nebo stejná, paket je ignorován. Pokud je nižší, je odeslán *Avertisement Request*.

Typy zpráv VTP

- **Subset Advertisements**
  - Když přidáte, odstraníte nebo změníte VLAN na serveru Catalyst, server Catalyst, na kterém jsou provedeny změny, zvýší revizi konfigurace a vydá souhrnnou reklamu.
  - Po *Summary Advertisements* následuje jedna nebo několik *Subset Advertisementů*.
  - *Subset advertisement* obsahuje seznam informací VLAN.

- **Advertisement Requests** je poslán když**:**
  - Přepínač byl resetován.
  - Název domény VTP byl změněn.
  - Přepínač obdržel *Summary Advertisements* VTP s vyšší revizí konfigurace, než její vlastní.
  - Po přijetí žádosti o reklamu pošle zařízení VTP *Summary Advertisements*. Po *Summary Advertisements* následuje jedna nebo více *Subset Advertisementů*.

Konfigurace a verifikace VTP



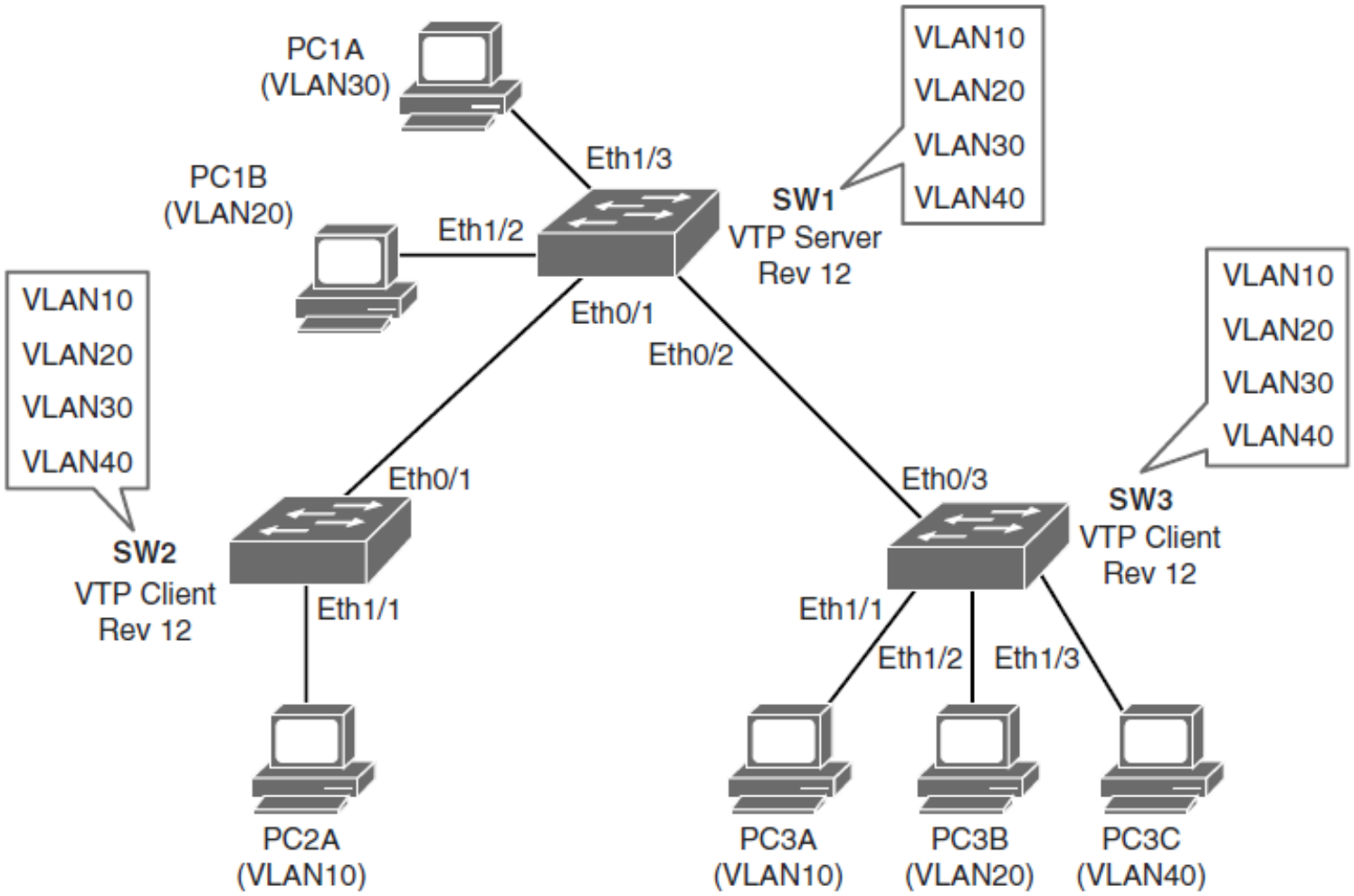
- **Krok 1.** Konfigurace VTP na všech přepínačích, Switch 1 and Switch 3 jsou klienti a Switch2 server

```
Switch1(config)# vtp password Cisco
Switch1(config)#vtp mode client
Switch1(config)#vtp domain CCNP
Switch1(config)#vtp version 1
```

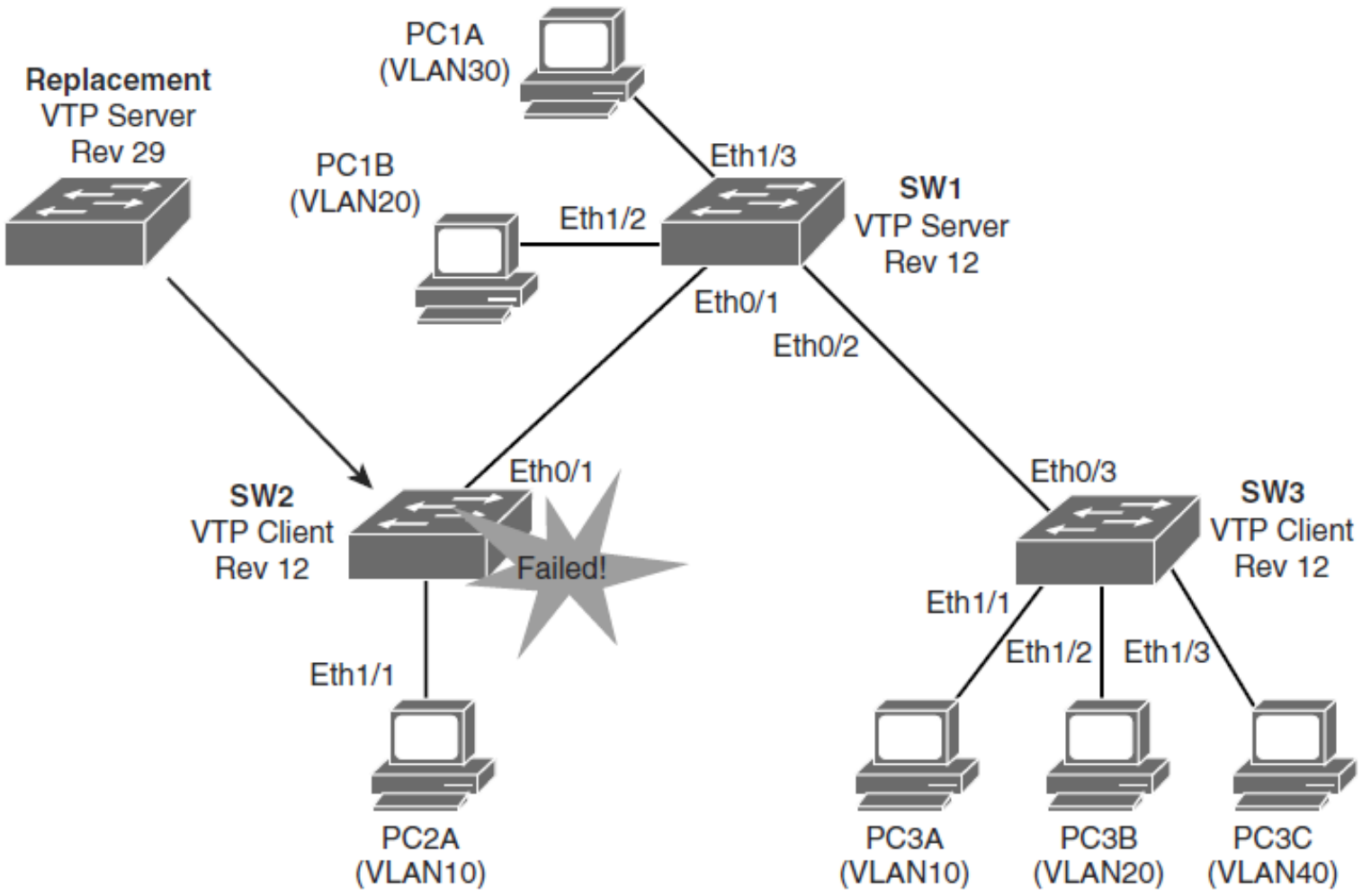
```
Switch3(config)# vtp password Cisco
Switch3(config)#vtp mode client
Switch3(config)#vtp domain CCNP
Switch3(config)#vtp version 1
```

```
Switch2(config)# vtp password Cisco
Switch2(config)#vtp mode server
Switch2(config)#vtp domain CCNP
Switch2(config)#vtp version 1
```

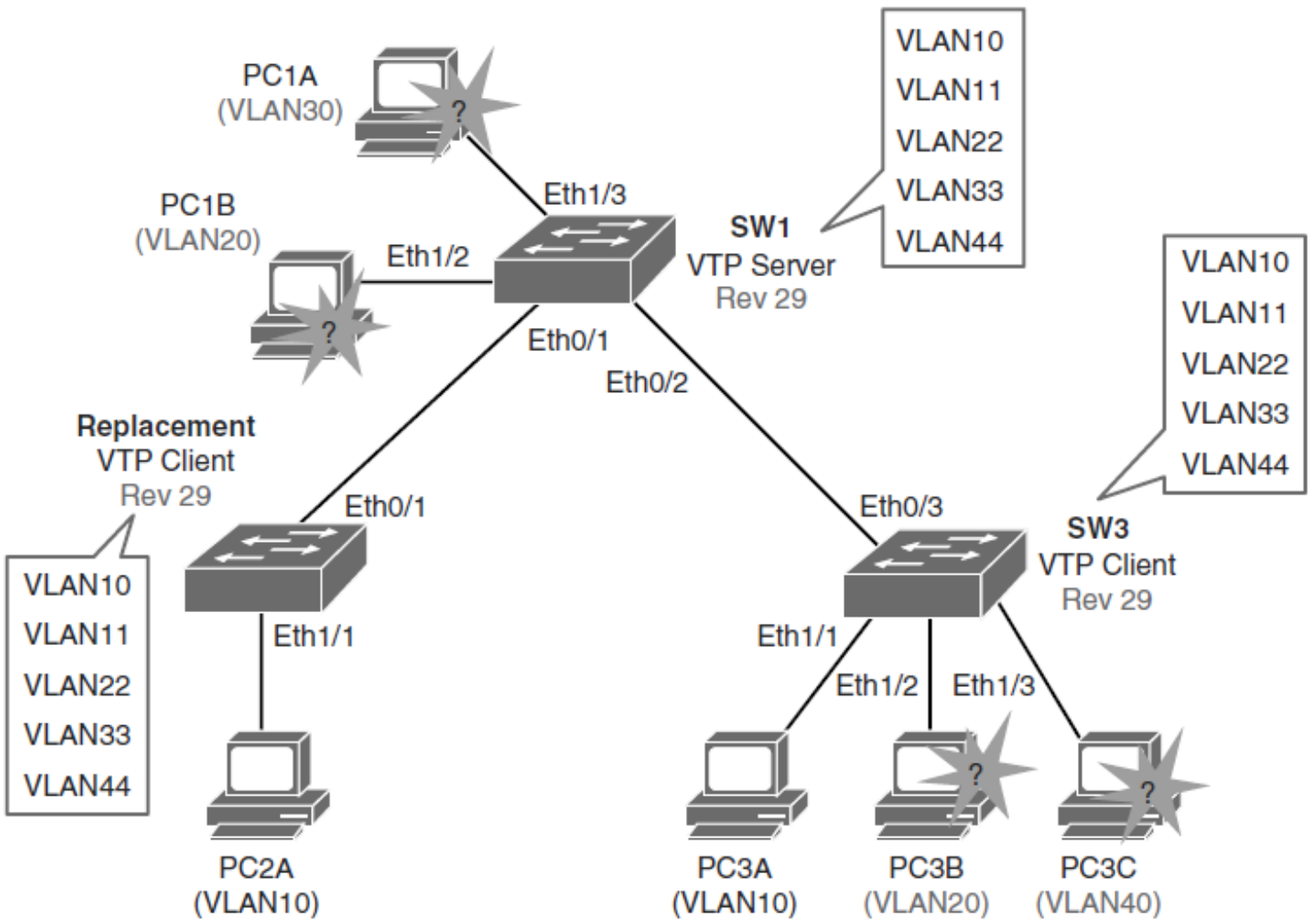
Přepis konfigurace VTP



Přepis konfigurace VTP



Přepis konfigurace VTP



Klíčové body VTP

- Pokud je to možné, vyhýbejte se VLAN, které pokrývají celou síť.
- Číslo revize VTP je uloženo v NVRAM a není resetováno, pokud vymažete konfiguraci přepínače a znovu ji načtete. Chcete-li obnovit číslo revize VTP na nulu, použijte následující dvě možnosti:
  - Změňte doménu VTP přepínače na neexistující doménu VTP a poté doménu změňte zpět na původní název.
  - Změňte režim VTP přepínače na transparentní a poté zpět do předchozího režimu VTP.

Praxe implementace VTP

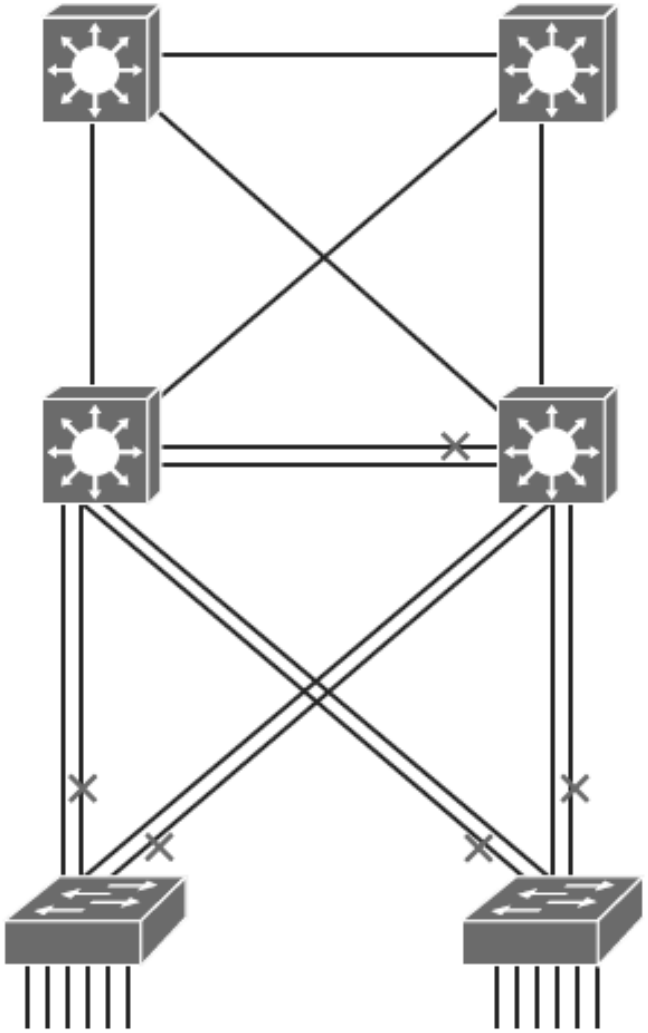
- VTP se často používá v nové síti k usnadnění implementace VLAN.
- S rostoucí sítí se však tato výhoda může proměnit v odpovědnost.
- Pokud je síť VLAN odstraněna náhodou na jednom serveru, bude odstraněna v celé síti.
- Pokud je do sítě vložen přepínač, který již má definovanou databázi VLAN, může databázi VLAN ohrozit odstraněním přidaných VLAN.
- Z tohoto důvodu je doporučeno nakonfigurovat všechny přepínače do transparentního režimu VTP a ručně přidat sítě VLAN podle potřeby, zejména ve větší síti kampusu.
- Konfigurace VTP je obvykle vhodná pro malé firmy.

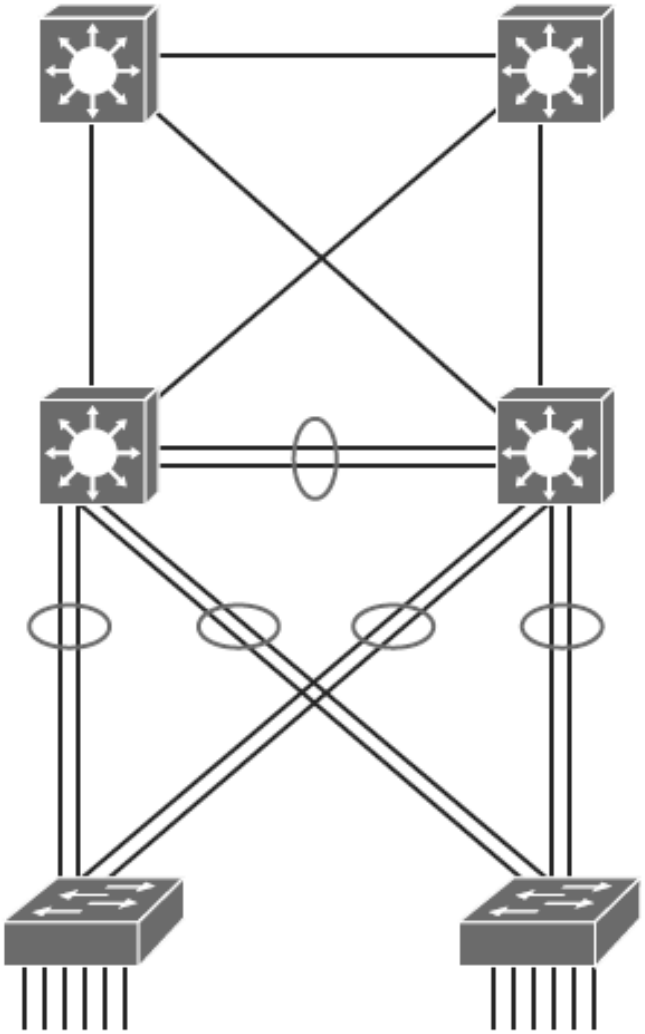
Implementace EtherChannelu v přepínané síti

Implementace EtherChannelu

- Potřeba technologie EtherChannel
- Protokoly vyjednávání agregace portů
- Kroky konfigurace pro sdružování rozhraní do vrstvy 2 EtherChannel
- Konfigurace EtherChannel
- Změna chování vyrovnávání zátěže EtherChannel
- Jak funguje vyrovnávání zátěže EtherChannel
- Role EtherChannel Guardu

Potřeba EtherChannel





EtherChannel Overview

- EtherChannel je technologie, která byla původně vyvinuta společností Cisco jako technika přepínání LAN, při které se seskupuje několik rychlých nebo gigabitových ethernetových portů do jednoho logického kanálu.
- Tato technologie má mnoho výhod:
  - Spoléhá se na existující přepínací porty. Není nutné upgradovat propojení typu switch-to-switch na rychlejší a dražší připojení.
  - Většinu konfiguračních úkolů lze provádět na rozhraní EtherChannel namísto na každém jednotlivém portu, čímž je zajištěna konzistence konfigurace v rámci propojení typu switch-to-switch.
  - Vyrovnávání zatížení je možné mezi odkazy, které jsou součástí stejného EtherChannel. V závislosti na hardwarové platformě můžete implementovat jednu nebo několik metod, například vyvažování zátěže zdroj-MAC k cíli-MAC nebo vyvážení zdroje-IP k cílové-IP přes fyzické odkazy.

Mechanismy EtherChannelu

- **LACP:** IEEE's negotiation protocol
- **PAgP:** Cisco's negotiation protocol
- **Static persistence:** No negotiation protocol
  (statická vytrvalost – žádné vyjednávání)

LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

Static Persistance

	On
On	Yes

LACP

- Link Aggregation Control Protocol (LACP) je součástí specifikace IEEE (802.3ad), která umožňuje sdružovat několik fyzických portů do jediného logického kanálu. LACP umožňuje přepínači vyjednat automatický balíček zasláním LACP paketů partnerovi.
- Zajišťuje, že při vytvoření EtherChannel mají všechny porty stejný typ **rychlosti konfigurace, nastavení duplexu a informace VLAN**. Jakákoli úprava portu po vytvoření kanálu změní také všechny ostatní porty kanálu.
- Přepínač s nejnižší prioritou systému může rozhodovat o tom, které porty se aktivně účastní EtherChannel.

LACP

- Porty se stanou aktivními podle jejich priority portů.
- Nižší číslo znamená vyšší prioritu.
- EtherChannel lze obvykle přiřadit až 16 linek, ale současně může být aktivní pouze 8.
- Neaktivní odkazy jsou umístěny do pohotovostního stavu a jsou povoleny, pokud jeden z aktivních odkazů vypadne.
- Maximální počet aktivních linek v EtherChannel se mezi přepínači liší.

Typy LACP Operací

- **Active:** Nastavení LACP
- **Passive:** Nastavení LACP pouze když je detekováno LACP zařízení

- Dodatečné parametry LACP:
- **System priority**
  - Každý přepínač, na kterém běží LACP, musí mít prioritu systému. Prioritu systému lze zadat automaticky nebo prostřednictvím CLI. Přepínač používá MAC adresu a prioritu systému k vytvoření ID systému.
- **Port priority**
  - Každý port přepínače musí mít prioritu portu. Prioritu portu lze zadat automaticky nebo prostřednictvím CLI.
- **Administrative key**
  - Každý port přepínače musí mít administrativní hodnotu klíče, kterou lze zadat automaticky nebo prostřednictvím CLI. Administrativní klíč definuje schopnost portu agregovat se s jinými porty a je **určen fyzickými vlastnostmi portu**, jako je rychlost přenosu, duplexní schopnost a médium typu point-to-point **anebo tím, že jde o sdílené médium**.

PAgP

- Port Aggregation Protocol (PAgP) poskytuje stejné výhody při vyjednávání jako LACP.
- PAgP je patentovaný protokol Cisco a bude fungovat pouze na zařízeních Cisco.
- Pakety PAgP jsou vyměňovány mezi přepínači přes porty podporující EtherChannel.
- Sousedé jsou identifikováni a schopnosti jsou učeny a porovnávány s lokálními schopnostmi přepínáče.
- Porty, které mají stejné schopnosti, jsou spojeny do EtherChannelu.
- PAgP tvoří EtherChannel pouze na portech, které jsou konfigurovány pro identické VLAN nebo trunking.
- PAgP automaticky změní parametry EtherChannel, pokud se změní jeden z portů ve svazku.
- PAgP a LACP nejsou kompatibilní.

Typy operací PAgP

Typy PAgP operací:

- ■ **Desirable:** Nastavit PAgP
- ■ **Auto:** Enable PAgP pouze když je detekováno PAgP zařízení

Statically Bundle Links

- Dohadování na bázi LACP nebo PAgP zavádějí režii a zpoždění v inicializaci.
- Alternativně lze staticky sdružovat odkazy do EtherChannel.
- Tato metoda nezavádí žádné zpoždění, ale může způsobit problémy, pokud není správně nakonfigurována na obou koncích.

Konfigurační průvodce Layer 2 EtherChannel

Před implementací EtherChannel do sítě naplánujte následující kroky nezbytné k dosažení úspěchu:

- Prvním krokem je identifikace portů, které budete používat pro EtherChannel na obou přepínačích.
- Každé rozhraní by mělo mít identifikovaný příslušný protokol (PAgP nebo LACP), mělo by mít číslo skupiny kanálů pro přiřazení všech daných rozhraní ke skupině portů a mělo by být nakonfigurováno, zda by mělo dojít k vyjednávání.
- Po navázání spojení se ujistěte, že se vytvořily obě strany EtherChannel a poskytují agregovanou šířku pásma.

Konfigurační průvodce Layer 2 EtherChannel

Při konfiguraci rozhraní EtherChannelu:

- **Podpora EtherChannelu**
  - Všechna rozhraní Ethernet na všech modulech podporují EtherChannel, aniž by bylo nutné, aby rozhraní byla fyzicky sousedící nebo na stejném modulu.
- **Rychlost a duplex**
  - Nakonfigurujte všechna rozhraní v EtherChannel tak, aby fungovala **stejnou rychlostí a ve stejném duplexním režimu**.
- **Soulad VLAN** Všechna rozhraní v balíčku EtherChannel musí být přiřazena ke stejné VLAN nebo musí být nakonfigurována jako kmen.
- **Rozsah VLAN**
  - EtherChannel podporuje stejný povolený rozsah VLAN na všech rozhraních v kanálu EtherChannel Layer 2.

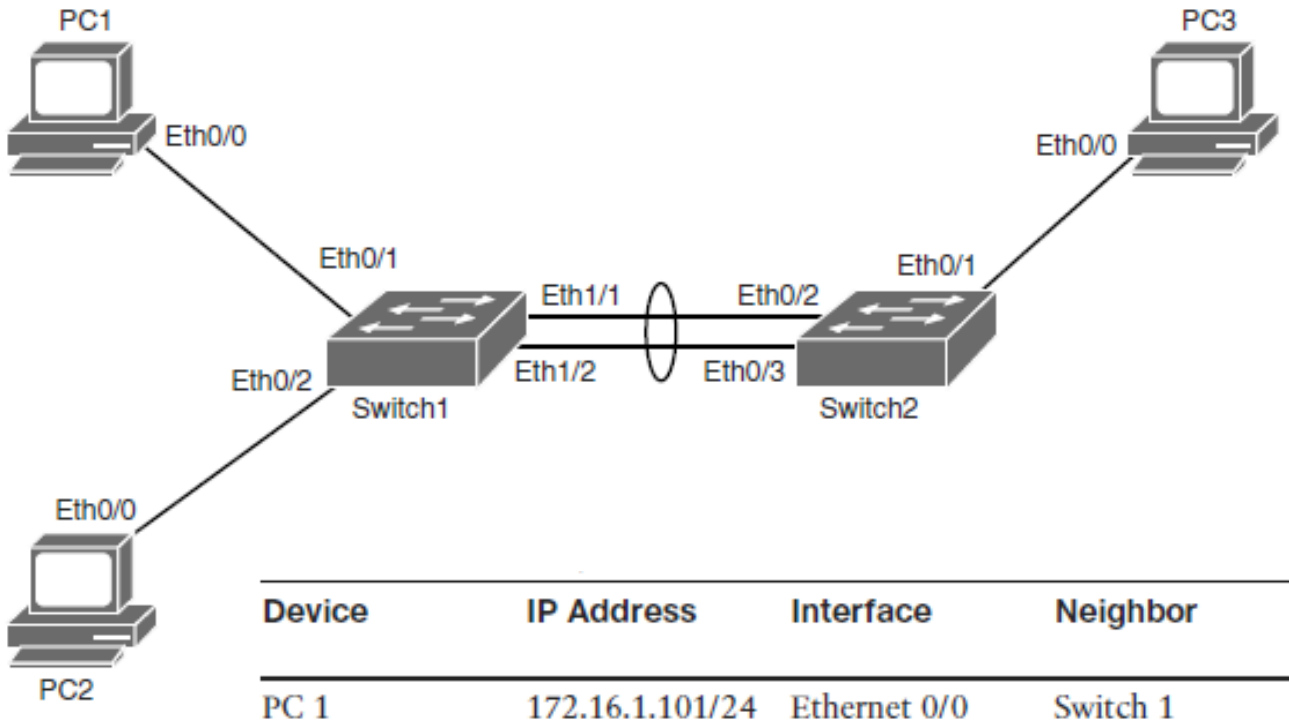
Konfigurační průvodce Layer 2 EtherChannel

- **Náklady na cestu STP**
  - Rozhraní s různými náklady na cestu portem STP mohou tvořit EtherChannel, pokud jsou kompatibilně nakonfigurována.
  - Nastavení různých nákladů na cestu k portu STP samo o sobě nezpůsobuje nekompatibilitu rozhraní pro vytvoření EtherChannel.
- **Portový kanál versus konfigurace rozhraní**
  - Po konfiguraci EtherChannel ovlivní EtherChannel jakákoli konfigurace, kterou aplikujete na rozhraní portu kanálu.
  - Jakákoli konfigurace, kterou použijete na fyzická rozhraní, ovlivní pouze konkrétní rozhraní, které jste nakonfigurovali.

Volby EtherChannel Load-Balancingu

Hash Input Code	Hash Input Decision	Switch Model
dst-ip	Destination IP address	All models
dst-mac	Destination MAC address	All models
src-dst-ip	Source and destination IP address	All models
src-dst-mac	Source and destination MAC address	All models
src-ip	Source IP address	All models
src-mac	Source MAC address	All models
src-port	Source port number	4500, 6500
dst-port	Destination port number	4500, 6500
src-dst-port	Source and destination port number	4500, 6500

Příklad konfigurace EtherChannelu 1 ze 4



Device	IP Address	Interface	Neighbor	Interface on the Neighbor
PC 1	172.16.1.101/24	Ethernet 0/0	Switch 1	Ethernet 0/1
PC 2	172.16.1.102/24	Ethernet 0/0	Switch 1	Ethernet 0/2
PC 3	172.16.1.203/24	Ethernet 0/0	Switch 2	Ethernet 0/1
Switch 1	*No IP address*	Ethernet 1/1	Switch 2	Ethernet 0/2
Switch 1	*No IP address*	Ethernet 1/2	Switch 2	Ethernet 0/3

Příklad konfigurace EtherChannelu

Krok 1.

- `Switch1# configure terminal`
- `Switch1(config)# interface range Ethernet 1/1-2`
- `Switch1(config-if-range)# channel-group 1 mode active`

Krok 2.

- `Switch1(config)# interface port-channel 1`
- `Switch1(config-if)# switchport trunk encapsulation dot1q`
- `Switch1(config-if)# switchport mode trunk`

Příklad konfigurace EtherChannelu 3

Krok 3.

Switch 1:`show etherchannel summary`

```
Switch1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
1      Po1(SU)         LACP      Et1/1(P)    Et1/2(P)
```

Příklad konfigurace EtherChannelu 4

Krok 4.

- **show etherchannel load-balance**

```
Switch1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
```

Souhrn kapitoly 3

- Implementace sítí VLAN a trunků v přepínané architektuře kampusu
  Pochopení pojmu VTP a jeho omezení a konfigurace
  Implementace a konfigurace EtherChannel

Chapter 3 Labs

- **CCNPv7.1 SWITCH Lab3.1 VLAN TRUNK VTP**
- **CCNPv7.1 SWITCH Lab3.2 ETHERCHANNEL**

Acknowledgment

- *Some of the images and texts are from Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: (CCNP SWITCH 300-115)* by Richard Froom and Erum Frahim (1587206641)

- Special Thanks to *Bruno Silva*