Modul 3 Virtuální LAN (VLAN)

3.0 Úvod

Jedním z faktorů, které ovlivňují výkon sítě, je velikost broadcastových domén. Pomocí konfigurace VLAN je možné tyto broadcastové domény omezit.

Tato kapitola popisuje

- význam VLAN
- význam trunk VLAN
- konfiguraci VLAN na switchích
- řešení obvyklých problémů s konfigurací VLAN

3.1 Úvod do VLAN

3.1.1 Úvod do VLAN

Pokud jsou stanice patřící do jedné sítě v jednom místě, nejsou VLAN potřeba. Ale pokud máme několik budov a v každé z nich stanice patřící do různých skupin, museli bychom vytvořit jednu velikou síť. V tom případě se ale špatně řeší zabezpečení jednotlivých skupin, sdílení (a oddělení) síťových zdrojů. V tom mohou pomoci VLAN – vytvoříme fyzicky jednu velkou síť a na úrovni switchů ji rozdělíme do několika VLAN (podle skupin). Tyto VLAN pak mohou sdružovat různé počítače z různých budov, jejichž příslušnost k dané VLAN určuje konfigurace jejich IP adresy a portu switche, na který jsou připojeny.

Vlastnosti VLAN

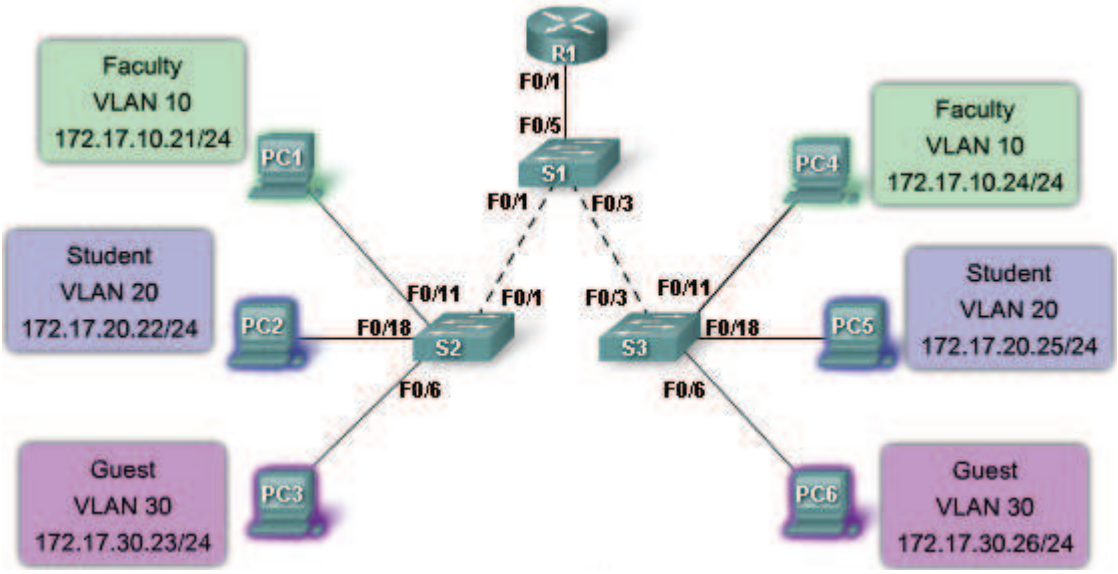
Přehled

- VLAN je nezávislá síť
- VLAN umožňuje oddělit různé stanice, ačkoliv jsou fyzicky v jedné LAN
- VLAN je určena primárně číslem (VLAN ID), ale může být pro snadnější identifikaci pojmenována

Detailněji

- stanice patřící do stejné VLAN musí mít IP adresy v jedné IP (pod)síti
- na switchi musí být VLAN nakonfigurována
- všechny porty switche připojující stanice z jedné VLAN musí být do této VLAN zařazeny
- port switche, který je nakonfigurován pouze pro jednu LAN, se nazývá „access port“

Příklad použití VLAN ilustruje obrázek – switche S1 a S3 mohou být fyzicky v různých budovách a přestože jsou fyzicky (na úrovni linkové vrstvy) všechny stanice v jedné síti, správně nakonfigurované switche je dokážou oddělit.



Výhody VLAN

- zabezpečení – síťový provoz jednotlivých VLAN je od sebe striktně oddělen, což snižuje riziko útoků
- úspory nákladů – díky efektivnímu využití poskytovaného přenosového pásma můžeme snížit případné náklady při upgradu
- výkon – rozdělení sítě na úrovni L2 na několik broadcastových domén redukuje zbytečné zatížení sítě příliš rozsáhlými broadcasty
- redukce „broadcast storm“ – díky rozdělení do více broadcastových domén se případné „bouře broadcastů“ bude účastnit méně stanic
- efektivita práce IT zaměstnanců – při rozšiřování sítě stačí správně přidělit porty do odpovídajících VLAN a tím jsou automaticky nastaveny politiky těchto portů; navíc jednotlivé VLAN lze pojmenovat pro snadnější identifikaci – viz obrázek – VLAN 10 pro zaměstnance, VLAN 20 pro studenty a VLAN 30 pro „hosty“

Rozsahy VLAN ID

Standardní rozsah VLAN ID

- čísla od 1 do 1005
- 1002 až 1005 jsou určeny pro Token Ring a FDDI VLAN
- ID 1 a 1002 až 1005 jsou vytvářeny automaticky a nemohou být odstraněny
- konfigurace VLAN jsou uloženy v souboru vlan.dat ve flash paměti switche
- VTP (VLAN trunking protocol) pracuje pouze s tímto rozsahem ID

Rozšířený rozsah VLAN ID

- čísla od 1006 do 4094
- používaný zejména poskytovateli
- poskytují méně funkcí oproti standardním
- ukládají se do „running-config“
- VTP je nepodporuje

Například Cisco Catalyst 2960 switch podporuje až 255 konfigurovaných VLAN.

3.1.2 Typy VLAN

Ačkoliv existuje v podstatě jediná možnost, jak vytvářet strukturu VLAN – na základě konfigurace portů, používají se některé pojmy pro obvyklé VLAN:

- datová VLAN – zpravidla pouze pro přenos uživatelských dat (kromě hlasových služeb a managementu switchů), někdy se také označuje jako „uživatelská VLAN“
- výchozí (default) VLAN – při prvním startu switche jsou všechny porty zařazeny do výchozí VLAN s ID 1 – to umožňuje vzájemně komunikovat všem připojeným zařízením; tato VLAN nemůže být ani přejmenována, ani smazána – některé protokoly (CDP, STP) používají vždy tuto VLAN; proto je vhodné porty zařadit do jiné „výchozí“ VLAN sítě – např. 100; na obrázku je vidět, že spoje mezi S1-S2 a S1-S3 musí být schopny přenášet data pro různé VLAN – takové porty se nazývají „trunk porty“ (používají protokol 802.1Q)
- nativní VLAN – jsou přidělovány na 802.1Q trunk porty – ty podporují jak komunikaci z různých VLAN (tagged – označenou), tak komunikaci nepocházející z žádné VLAN (untagged – pro zpětnou kompatibilitu s klasickými LAN sítěmi bez VLAN); komunikaci bez VLAN označení je přidělena právě nativní VLAN; nativní VLAN by měla být různá od VLAN 1
- management VLAN – je jakákoliv VLAN, která umožňuje přístup ke vzdálené správě zařízení (ve výchozím nastavení je to VLAN 1) – switch může být spravován pomocí HTTP, telnet, SSH nebo SNMP; je vhodné tuto VLAN oddělit od VLAN 1 – nastavit například VLAN 99
- hlasová (voice) VLAN – pokud potřebujeme, abychom měli vždy plynulé hlasové služby, musíme tomu přizpůsobit konfiguraci celé sítě (např. aby tato data prošla i jinak zahlcenou částí sítě); požadavky = zajištěná šířka pásma, priorita dat, zpoždění méně než 150 ms

Protože VLAN je vlastně totéž, co LAN, musí být schopna přenášet stejné typy datového provozu – správa zařízení (CDP, SNMP, RMON), IP telefonii, IP multicast, standardní data a ostatní (např. hry apod.).

3.1.3 Režimy přidělení portu k VLAN

Při konfiguraci VLAN je povinné nastavení VLAN ID (čísla) a volitelně můžeme VLAN přidělit také jméno. Poté nastavíme jednotlivým portům příslušnost k daným VLAN. Port může patřit do:

- statické VLAN – v CLI, nebo jiném konfiguračním nástroji, nastavíme ručně příslušnost k zadané VLAN; pokud v CLI zadáme neexistující VLAN ID, switch tuto VLAN založí; ukázka konfigurace příslušnost portu Fa0/18 k VLAN 20:

```
S1#configure terminal
S1(config)#interface fastEthernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

- dynamické VLAN – nevyužívá se často; příslušnost k VLAN je definována na serveru (VMPS), který portu přidělí VLAN na základě MAC adresy zařízení připojeného k portu; výhodou je možnost přepojit zařízení do jiného portu (nebi i switche) bez nutnosti další rekonfigurace
- hlasové (voice) VLAN – předpokládá se připojený IP telefon (patřící do voice VLAN – např. 150) a přes něj stanice (patřící do jiné VLAN – např. 20); ukázka konfigurace (příkaz **`mls qos trust cos`** nastavuje prioritu hlasových služeb – musí být nastaveno v celé síti):

```
S1(config)#interface fastEthernet 0/18
S1(config-if)#mls qos trust cos
S1(config-if)#switchport voice vlan 150
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 20
```

3.1.4 Broadcasty ve VLAN sítích

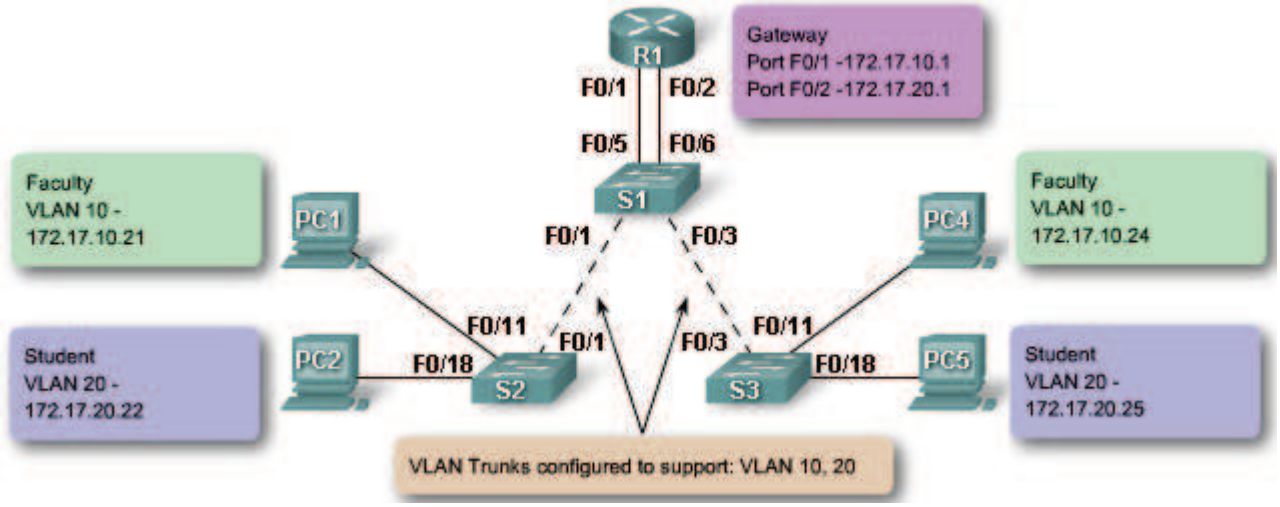
Pokud v síti nejsou nakonfigurovány VLAN, přeposílají switche broadcastové rámce na všechny své porty (kromě příchozího) – bez ohledu na to, jakou IP adresu může mít stanice připojená k těmto portům. To nemusí být nutné – řešením jsou VLAN.

Na obrázku výše (v odstavci 3.1.1) jsou 3 VLAN. Jestliže PC1 pošle ARP dotaz (=broadcast), přepošle jej S2 pouze na port F0/1 → S1 opět pouze přes F0/3 → S3 a ten pouze na F0/11 směrem k PC4. Zbytek sítě tuto zprávu nevidí!

Bez konfigurovaných VLAN by tuto zprávu dostaly všechny stanice.

Broadcastové domény – switche, routery

Broadcastové domény jsou standardně oddělovány routery. Zde jsme si ukázali, že je možné je oddělit také pomocí switchů. Nicméně pro komunikaci mezi jednotlivými VLAN je vždy potřeba zařízení, které funguje jako router – viz obrázek:



Komunikace v rámci jedné VLAN

PC1 posílá zprávu PC4:

- PC1 pošle ARP dotaz (broadcast) na adresu PC4 → S2 – přes F0/1→ S1 přes F0/5 (R1) a F0/3 → S3 přes F0/11 → PC4
    - R1 musí také tuto zprávu dostat, protože má své F0/1 nakonfigurované také v dané VLAN (Faculty = VLAN 10)
- PC4 odpoví (unicast ARP) přes S3, S1, S2 na PC1
- PC4 posílá zprávu (unicast) na PC1 (přes S2, S1, S3 – nikdo jiný ji nedostane)

Komunikace mezi VLAN

PC1 posílá zprávu PC5:

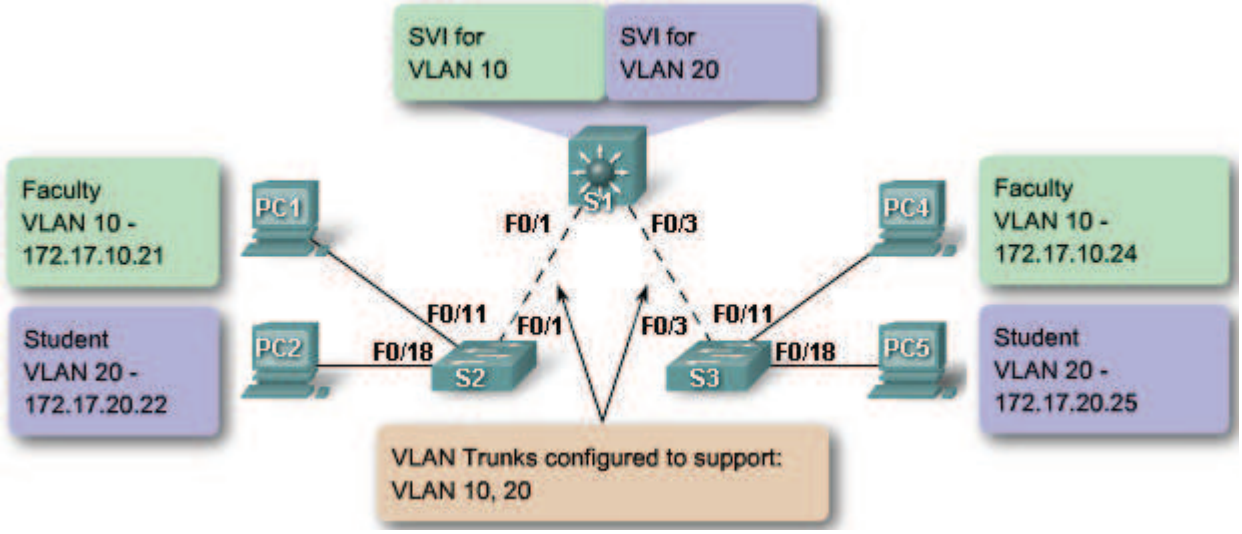
- PC1 pošle ARP dotaz (broadcast) na adresu R1 → S2 – přes F0/1→ S1 přes F0/3 (S3 a poté přes F0/11 na PC4) a F0/5 → R1
    - stanice komunikuje s jinou sítí, takže musí jít přes bránu (gateway) – tj. přes R1
- R1 odpoví (unicast ARP) přes S1, S2 na PC1
- PC4 posílá zprávu (unicast) na PC5 (fyzicky na R1)
- R1 přijme zprávu, pošle ARP dotaz na adresu PC5 – přes F0/2 → S1 přes F0/1 (S2 a poté přes F0/18 na PC2) a F0/3 → S3 přes F0/18 → PC5

- switch S1 musí tento dotaz poslat na S2 i S3, protože obě spojení (F0/1 i F0/3) jsou konfigurovány jako trunk spoje s VLAN 10 a 20

- PC5 odpoví (unicast ARP) přes S3, S1 na R1
- R1 přepošle zprávu přijatou od PC1 (unicast) na PC5 (přes S1, S3 – nikdo jiný ji nedostane)

Broadcastové domény – L3 switche

Některé Cisco switche podporují také směrování na úrovni třetí vrstvy – tyto switche se označují jako L3 switche – na obrázku – S1.



V předchozím odstavci řešil směrování mezi VLAN 10 a VLAN 20 router R1. Zde jeho funkci nahradí S1, kterému nakonfigurujeme dvě SVI (switch virtual interface), která „zastoupí“ rozhraní F0/1 a F0/2 routeru R1.

SVI je virtuální logické rozhraní konfigurované pro danou VLAN, které je nutné, pokud chceme mezi VLAN směrovat (na L3 switchi). Defaultně je SVI vytvářeno pro výchozí VLAN (VLAN 1) kvůli vzdálené správě switche.

Postup při odesílání zprávy mezi PC1 (VLAN 10) a PC5 (VLAN 20) je tedy podobný jako v předchozím odstavci – pouze roli R1 a jeho rozhraní F0/1 a F0/2 nahrazuje switch S1 a rozhraní SVI pro VLAN 10 a SVI pro VLAN 20.

3.2 Propojování VLAN – trunk spoje

3.2.1 VLAN – trunk

Trunk = spoj mezi dvěma zařízeními, který má přenášet komunikaci několika různých VLAN. Na Cisco zařízeních je proto pro Fast Ethernet a Gigabit Ethernet rozhraní podporován protokol 802.1Q. Trunk nepatří do konkrétní VLAN – je to propojení mezi částmi VLAN přes switche a routery. Viz spoje mezi S1-S2 a S1-S3 na předchozích obrázcích.

Teoreticky by trunk linky nemusely být potřeba – propojení částí VLAN je možno řešit samostatnými porty pro každou VLAN. Pak by ale pro spojení dvou switchů s podporou 4 VLAN byly na každém switchi potřeba 4 porty.

Pomocí trunk spoje je možné využít jediný port na každém switchi, který bude nastaven jako trunk a nakonfigurován pro všechny potřebné VLAN.

Obrázek: vlevo – 4 linky pro 4 různé VLAN; vpravo – jeden trunk spoj pro 4 různé VLAN

Označování rámců – 802.1Q

Switche jsou standardně L2 zařízení, ale nyní potřebujeme, aby předávané rámce obsahovaly informace o příslušnosti rámce k dané VLAN – což standardní ethernetové rámce nemají. Proto jsou ke klasickému rámci přidávány 802.1Q hlavičky, které toto řeší.

Přidávání hlaviček – pokud switch přijme rámec na access mode portu s definovanou statickou VLAN, vloží do rámce VLAN tag (hlavičky), přepočítá FCS a předá rámec na trunk port.

Součástí hlaviček jsou pole

- EtherType – hodnota 0x8100 znamená, že switch má kontrolovat následující pole pro doplňující informace
- Tag control information field – priorita (3 bity), CFI (1 bit) = podpora Token Ringu, VID = VLAN ID (12 bitů)
- FCS – kontrolní součet, který musí být přepočítán

Poznámka – zprávy, přicházející od stanic na porty, které jsou v nativní VLAN, zůstávají neoznačené a měly by být předány na trunk.

Nativní VLAN a 802.1Q trunky

Řídící zprávy přicházející na porty nativní VLAN by měly být neoznačené (untagged). Pokud switch dostane na trunk port označený rámec (tagged – s označením VLAN), zahodí jej. Pokud chceme k takovému portu připojit zařízení, které standardně odesílá označené rámce, je potřeba je nakonfigurovat.

V okamžiku, kdy nakonfigurujeme 802.1Q trunk port, je nastaven výchozí Port VLAN ID (PVID) na hodnotu nativní VLAN – například, pokud je VLAN 99 označena jako nativní, je PVID=99.

Pokud Cisco switch dostane na trunk port neoznačený rámec, předá jej do nativní VLAN – podle PVID. Poznámka – výchozí nastavení nativní PVID je VLAN 1. Ukázka konfigurace nativní VLAN a trunk portu:

```
S1(config)#interface F0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

Nejprve se nastaví režim portu na trunk a poté se přidělí do VLAN 99, která se vytvoří a je označena jako nativní. Ověření konfigurace – viz zvýrazněné části výpisu:

```
S1#show interfaces F0/1 switchport
Name: F0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enables
...
Administrative private-vlan trunk Native VLAN tagging: enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
...
Trunking VLANs Enabled: ALL
```

3.2.2 Funkce trunku

Funkce trunku při předávání rámců – viz obrázek v odstavci 3.1.4 – PC 1 posílá broadcast:

S2 dostane na port F0/11 (access port) neoznačený (untagged) rámec, který má být předán na trunk port - proto jej označí VLAN ID 10. Následně jej přepošle přes trunk port F0/1 na S1, který si přečte VLAN ID a přepošle jej na všechny porty příslušející VLAN 10 (takže i na F0/3). Switch S3 si přečte VLAN ID, odstraní hlavičky a neoznačený (untagged) rámec předá na všechny porty ve VLAN 10 – tj. na F0/11 pro PC4.

3.2.3 Režimy trunku

Existují dva typy trunk portů – ISL (interswitch link), který již není požívaný, a IEEE 802.1Q

IEEE 802.1Q podporuje označené i neoznačené rámce. 802.1Q trunk portu je přiděleno výchozí PVID, na které se přeposílá všechna komunikace neoznačená nebo označená VLAN ID 0. Paket s VLAN ID odchozího portu rovným výchozímu PVID je odeslán neoznačený, vše ostatní je odesíláno označené.

ISL trunk port předpokládá veškerou komunikaci označenou (zabalenou do ISL hlaviček). Neoznačené (nativní) rámce jsou zahazovány. ISL není doporučováno a mnoho Cisco switchů jej ani nepodporuje.

DTP

DTP (Dynamic Trunking Protocol) je Cisco protokol, switche jiných výrobců jej neznají. DTP řeší nastavení trunk režimu, pokud je port druhého switche v trunk režimu, který podporuje DTP. DTP není nutné, některé Cisco switche a routery jej ani nepodporují.

Trunk režimy

Port switche může být nakonfigurován jedním z několika trunk režimů. To, a také režim portu na druhé straně spoje, poté určí, jestli spoj bude trunk nebo ne.

- „on“=zapnuto (výchozí) – **`switchport mode trunk`**
  Port stále odesílá DTP rámce („advertisements“) vzdálenému portu, že je v trunk režimu (bez ohledu na odpověď vzdáleného portu).
- „auto“=automatický režim – **`switchport mode dynamic auto`**
  Port oznamuje, že je schopen být trunk, ale není to nutné, výsledný stav záleží na režimu vzdáleného portu – pokud je „on“ nebo „auto“, výsledkem bude trunk, jinak ne.
- „desirable“=požadovaný režim – **`switchport mode dynamic desirable`**
  Port oznamuje, že chce být trunk, pokud to půjde. Jestliže vzdálený režim je „on“, „auto“ nebo „desirable“, výsledkem je trunk, jinak ne.
- „DTP off“=vypnuté DTP - **`switchport nonegotiate`**
  Port neoznamuje svůj stav a nerozhoduje o něm dynamicky – je vhodné pro trunk spojení se switchi jiných výrobců než Cisco.

Souhrn možností a výsledný stav popisuje tabulka:

S1 \ S2	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Nedoporučováno
Access	Access	Access	Nedoporučováno	Access

Ke zjištění aktuálního stavu portu můžeme použít příkaz **`show dtp interface`**.

3.3 Konfigurace VLAN a trunk spojů

3.3.1 Konfigurace VLAN a trunk spojů – přehled

Většina potřebné teorie už byla popsána v předchozích odstavcích – zde si ukážeme praktické postupy a příklady základní konfigurace VLAN a trunk spojů. Použité příkazy mají většinou další nepovinné parametry – ty zde neuvádíme.

Obecný postup při konfiguraci VLAN:

- vytvořit VLANy
- staticky přiřadit porty do VLAN
- ověřit konfiguraci VLAN
- povolit trunk na spojích mezi switchi
- ověřit konfiguraci trunků

3.3.2 Konfigurace VLAN

Přidání nové VLAN a pojmenování – příklad:

```
S1(config)#vlan 20
S1(config-vlan)#name student
```

Pokud bychom VLAN nepojmenovali, má výchozí jméno podle čísla (doplněné zleva nulami) – „VLAN0020“.

Ověření konfigurace VLAN – příkaz **`show vlan brief`** – zobrazí seznam všech VLAN, jejich stav a porty, které do nich patří.

Nastavení režimu portu „access“ (staticky) a přiřazení portu do VLAN – příklad:

```
S1(config)#interface fastEthernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

Ověření – opět příkazem **`show vlan brief.`** Poznámka – „access“ port může být zařazen pouze v jedné VLAN. Ukázka:

```
S1#sh vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24
20   student             active    Fa0/18
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

3.3.3 Správa VLAN

Ověření nastavení VLAN – příklady:

- **`show vlan brief`** – pro každou VLAN jednořádkové shrnutí (viz. výše)
- **`show vlan id`** `20` – podrobnější informace o VLAN určené pomocí ID
- **`show vlan name`** `student` – podrobnější informace o VLAN určené pomocí jména

- **show vlan summary** – souhrnné informace o počtu a typu konfigurovaných VLAN

Ověření nastavení přidělení portů – příklady:

- **show interfaces** Fa0/18 – informace o rozhraní
- **show interfaces vlan** 20 – stav VLAN („up“/“down“) a další podrobné informace
- **show interfaces** Fa0/18 s**witchport** – informace o rozhraní – příslušnost k VLAN, nativní VLAN, režim portu, stav zabezpečení portu, …

Vyřazení portu z VLAN, zařazení do jiné – příklady:

- (config-if)#**no switchport access vlan 20** – vyřadí daný port z VLAN 20
- (config-if)#**switchport access vlan 100** – zařadí daný port do VLAN 100, pokud byl předtím port v jiné VLAN, automaticky se z ní vyřadí (protože statický port může být maximálně v jedné VLAN)

Odstranění VLAN – příklady:

- #**no vlan** 100 – odstraní VLAN s číslem 100; POZOR! – před odstraněním VLAN je nutné její porty přiřadit do jiných VLAN, jinak poté nebudou funkční
- #**delete flash:vlan.dat** – odstraní informace o všech definovaných VLAN, takže po reloadu switche budou VLAN ve výchozím stavu (od výrobce)

3.3.4 Konfigurace trunku

V rámci tohoto kurzu budeme ke konfiguraci trunk spoje používat pouze statické nastavení příkazem **switchport mode trunk**. Tj. switch bude tuto linku brát vždy jako trunk, bez ohledu na nastavení portu na druhém konci. Příklad konfigurace trunk spoje:

```
S1(config)#interface F0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

Poslední příkaz zároveň změní nativní VLAN na číslo 99.

Ověření konfigurace trunku – příklad:

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Voice VLAN: none
...
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
...
```

Další konfigurace trunku – příklady:

- (config-if)#**no switchport trunk allowed vlan** – odstraní všechny VLAN konfigurované na tomto rozhraní
- (config-if)#**no switchport trunk native vlan** – vrátí zpět konfiguraci nativní VLAN na výchozí hodnotu (tj. 1)
- (config-if)#**switchport mode access** – vrátí port na režim „access“

3.4 Řešení problémů s VLAN a trunky

3.4.1 Obvyklé problémy s trunk spoji

Obvyklé problémy a jejich příčiny:

- chybná konfigurace nativní VLAN („Native VLAN mismatches“) – na dvou různých trunk portech jsou definovány různé nativní VLAN
    - příklad: S1 nativní VLAN 99 a S3 nativní VLAN 100
- chybná konfigurace trunků („Trunk mode mismatches“) – jeden konec spoje je „trunk mode on“, druhý „trunk mode off“
    - příklad – oba porty, které mají být na koncích trunku, jsou v režimu „dynamic auto“
- VLAN a IP podsítě – počítač se špatnou IP adresou ztratí spojení v síti; zařízení v jedné VLAN musí mít odpovídající IP adresy
    - příklad – při konfiguraci PC zadáme špatnou IP adresu (např. překlepem), která nespadá do rozsahu dané VLAN
- povolené VLAN sítě na trunk spojích – pokud seznam povolených VLAN ještě nebyl aktualizován, může být síťový provoz zpracováván chybně
    - příklad: nepovolená (třeba 1 z několika) VLAN na trunk spoji