Ethernet – protokol VLAN

Tato prezentace se zaměřuje na koncept virtuálních lokálních sítí (VLAN), které umožňují logické rozdělení fyzické sítě Ethernet do menších, samostatných segmentů. Cílem je představit, jak VLAN fungují, jak se značí a přenášejí v rámci standardu IEEE 802.1Q, k čemu slouží trunky a jaké jsou přínosy VLAN z hlediska bezpečnosti a organizace sítě.

Úvod do problematiky VLAN

Co je VLAN

- Virtuální LAN, tedy logické rozdělení fyzické sítě do menších segmentů.
- Každá VLAN působí jako samostatná síť (různé broadcast domény).

Proč VLAN

- Zlepšení škálovatelnosti (správa velké sítě v logických celcích).
- Zvýšení bezpečnosti (oddělení citlivých částí sítě).
- Lepší segmentace provozu (snížení broadcastů v rámci VLAN).

Základní principy VLAN

Broadcast doména

- Každá VLAN tvoří vlastní broadcast doménu (nepropustí broadcasty do jiných VLAN).

Rozdělení sítě bez nutnosti fyzického dělení

- Dříve bylo nutné používat více switchů nebo fyzicky oddělené segmenty.
- VLAN dovolují využít jeden (či několik) přepínačů a přitom vytvořit „logické“ oddělení.

Komunikace mezi VLAN

- Aby spolu mohly VLAN komunikovat, je potřeba směrování (router, L3 switch).

Výhody VLAN

1. **Bezpečnost**
   - Citlivé systémy (např. účetní) v samostatné VLAN, oddělené od ostatních.
2. **Správa a přehlednost**
   - Možnost vytvářet VLAN dle oddělení ve firmě (účtárna, marketing, IT, atd.).
3. **Efektivní využití sítě**
   - Snížení počtu broadcastů v rámci jedné fyzické sítě.
4. **Snadné rozšiřování**
   - Přidání další VLAN se obejde bez větších změn kabeláže či topologie.

Standard IEEE 802.1Q (VLAN Tagging)

Tagování rámců

- Při průchodu trunk portem se do Ethernetového rámce vkládá VLAN tag (4 bajty), který nese informaci o VLAN ID.

Ethernetový rámec s 802.1Q

- Obsahuje pole pro TPID (Tag Protocol Identifier = 0x8100) a TCI (Tag Control Information: 12 bitů pro VLAN ID).

Výchozí VLAN (Native VLAN)

- Na trunk portu se určuje tzv. Native VLAN, jejíž rámce nejsou (nebo mohou být) tagovány.

Rozsah VLAN ID

- 0–4095 (praktické použití 1–4094, VLAN 1 je výchozí, VLANy 1002–1005 se historicky používaly pro FDDI/Token Ring).

Access port vs. Trunk port

Access port

- Port na switchi, který je přiřazen do konkrétní VLAN.
- Koncové zařízení (PC, tiskárna) neví o VLAN značkách; komunikace je „neoznačená“.

Trunk port

- Přenáší provoz více VLAN mezi switche (případně switch ↔ router).
- Rámce obsahují VLAN tag 802.1Q, aby bylo možné rozlišit VLAN.

Typy VLAN a členství

Statické VLAN

- Přiřazování portů manuálně správcem (např. port 1 patří do VLAN 10, port 2 do VLAN 20).

Dynamické VLAN

- Přiřazování dle MAC adresy, uživatele nebo dalších kritérií (vyžaduje speciální software či server).

Voice VLAN

- Využívá se pro VoIP telefony, často je definována vedle datové VLAN.

Příklad konfigurace VLAN (obecný přehled)

Příklad: Switch Cisco

- vlan 10
  - name Sales
- vlan 20
  - name IT
- Port pro oddělení prodeje (Sales) → VLAN 10:
  - interface FastEthernet0/1
  - switchport mode access
  - switchport access vlan 10

Trunk port

- interface FastEthernet0/24
  - switchport mode trunk
  - switchport trunk native vlan 1
  - switchport trunk allowed vlan 10,20

(Detailní příkazy závisí na konkrétním výrobci.)

Routing mezi VLAN (Inter-VLAN Routing)

Potřeba směrování

- Zařízení v různých VLAN si vzájemně nevyměňují data, pokud není nasazeno L3 zařízení.

Možnosti

1. **Router-on-a-Stick** – VLAN trunk připojený na router, který směruje mezi VLAN ID.
2. **L3 Switch** – přepínač s routingovou funkcí; virtuální rozhraní SVI (Switched Virtual Interface).

Příklady použití

- Větší sítě, kde je třeba oddělit např. účtárnu a marketing, ale povolit jim bezpečnou komunikaci.

Best Practices a časté chyby

Bezpečnost

- Nepoužívat VLAN 1 jako produkční VLAN (je výchozí a často zneužitelná).
- Oddělit management VLAN (pro správu) od uživatelských VLAN.

Organizace čísel

- Udržovat VLAN ID a názvy VLAN tak, aby odrážely reálnou strukturu (např. VLAN 10 = Sales).

Trunk vs. Access

- Důsledně rozlišovat porty pro koncová zařízení (Access) a pro spojení mezi switche (Trunk).

Nesprávné tagování

- Dejte pozor na **native VLAN mismatch** (různě nastavené native VLAN na stranách trunku).

Shrnutí

VLAN

- Logické rozdělení jedné fyzické sítě do více oddělených segmentů.

Hlavní výhody

- Lepší bezpečnost, správa, snížení broadcast provozu, flexibilita při změnách.

IEEE 802.1Q

- Standardní protokol pro VLAN tagování (4bajtová vložka do Ethernetového rámce).

Access vs. Trunk

- Access port slouží konkrétní VLAN, trunk přenáší více VLAN s označenými rámci.

Routing mezi VLAN

- Potřeba L3 funkce (router či L3 switch), jinak se VLAN navzájem nevidí.

Kontrolní otázky

1. Vysvětlete rozdíl mezi Access portem a Trunk portem.
2. Jaký je hlavní význam VLAN a jak se liší od fyzického rozdělení sítě?
3. Co je to VLAN tag (802.1Q) a k čemu slouží?
4. Proč potřebujeme L3 prvek (router nebo L3 switch) pro komunikaci mezi různými VLAN?
5. Uveďte příklad, jak byste logicky rozdělili školní počítačovou síť (které VLAN byste navrhli?).
6. Jaké bezpečnostní a organizační výhody přináší nasazení VLAN ve firmě či škole?

Kontrolní otázky

1. **Tanenbaum, A. S., Wetherall, D.**: *Počítačové sítě*, 5. vydání (česky) – Kapitoly o LAN a VLAN.
2. **Kurose, J. F., Ross, K. W.**: *Computer Networking: A Top-Down Approach* – Základy síťových technologií, vč. LAN.
3. **Cisco Networking Academy – CCNA**: Oficiální výukové materiály (kapitoly o VLAN, 802.1Q).
4. **IEEE 802.1Q Standard**: Technické detaily VLAN tagování (dostupné online).
5. **Oficiální dokumentace výrobců síťových zařízení** (např. Cisco, HPE, MikroTik), které popisují konfiguraci VLAN v praxi.