**21. Správa VLAN ve středně velkých a velkých sítích**

**Princip hierarchického návrhu sítě a jeho vlastnosti**

* Tento způsob umožňuje **zlepšit výkon** a **dostupnost sítě**, **zvýšit bezpečnost** a **efektivně spravovat** středně velké a velké sítě.

Tuto hierarchii můžeme rozdělit do tří vrstev:

1. Access — Nejblíže k koncovým uzlům
2. Distribution — Mezi Access a Core, spojuje
3. Core — Vysokorychlostní backbone připojení

**Vrstvy**

**Access**

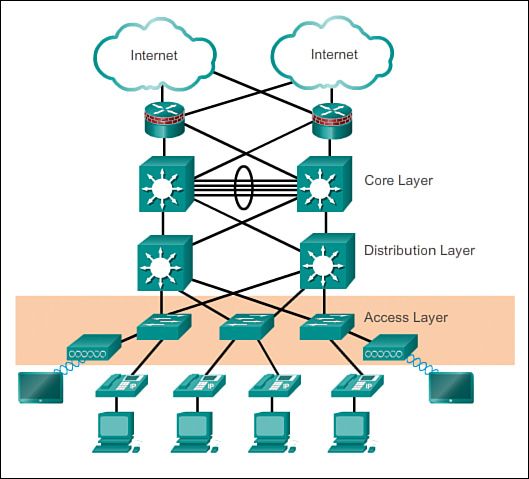
* Nejblíže k uživatelům
* Jejím **úkolem je poskytnout připojení pro koncová zařízení** (např. počítače, tiskárny) přes kabely nebo bezdrátové spojení.
* Má také za úkol **poskytnout zabezpečení připojení** pro koncová zařízení.
* V této vrstvě mohou být také implementovány technologie pro **řízení toku dat a kontroly přístupu, např. port security**.

**Distribution**

* Vrstva umístěna mezi Access a Core vrstvou
* Připojuje jednotlivé Access vrstvy k sobě
  + Zajišťuje tím přenos dat mezi jednotlivými Access vrstvami, např. přesměroávní datového provozu do správného segmentu sítě
* Implementace technologií pro zvýšení dostupnosti, např. STP

**Core**

* **Nejblíže k jádru** sítě a **poskytuje vysokorychlostní spojení mezi distribučními vrstvami**
* Jejím úkolem je především zajištění rychlého a spolehlivého přenosu dat mezi jednotlivými částmi sítě
* Implementace technologií pro zajištění minimálních prodlev (latence) a zajištění vysoké dostupnosti sítě, např. **Link Aggregation (EtherChannel)**



**Strukturovaný návrh kabeláže**

* Návrh kabeláže do budovy **ještě bez aktivních prvků**
* Návrh kde bude optika, drát, atd.
* Návrh kde se všechno bude zakončovat - serverovna
* Návrh kolik zásuvek kde, .. atd.
  + Když se vám zákazník řekne, že tady chce mít 32 zásuvek, tak jich uděláte 64
* Braní vpotaz pro budoucí aktivní prvky jako access pointy, …
* OZNAČOVÁNÍ KABELŮ štítkama
* Dokumentace kde co a kam jede
* **VŽDY, když se dělá zásuvka, tak nejdříve kabel jde ze zásuvky do PATCH PANELU, odkuď se to teprve připojuje patch kabelem ke switchi**
  + Pokud toto řeknete Mullerové, tak se z vás posere a dá vám hned 1

**Správa VLAN na Cisco switchích**

**VLAN**

* Virtual Local Area Network — Logická část sítě, která umožňuje rozdělit zařízení do skupin na základně jejich usmíštění, funkce a jiných kritérií
* Umožňuje segmentovat fyzickou síť do logických sítí
* Přináší větší kontrolu nad tokem dat mezi zařízeními a prvky

**Rozdíl mezi VLAN a fyzickou sítí**

* **Fyzická síť** — Tvořená fyzickými kabely, aktivními prvky, atd.
* **VLAN** — Logická část sítě, nezávisle implementována na fyzické infrastruktuře (částečně.. nějaké porty musí být access, atd.)

**Výhody VLAN**

* Segmentace sítě — Rozděluje síť na menší logické celky, což usnadňuje správu a diagnostiku problémů
* Zvýšení bezpečnosti — Umožňuje oddělit kritické zařízení od ostatních v síti a tak omezit přístup neoprávněných osob k nim
* Snadná správa — Umožňuje správci lépe kontrolovat a spravovat tok dat

**Vytváření a následná správa VLAN**

**Definujte potřebné VLAN podle topologie sítě a požadavků na segmentaci:**

* Počet, jména, jejich funkce
* zvážení, jak se mezi VLANy bude komunikovat, pokud by bylo potřeba
* Např. VLAN pro učitelské počítače ve škole

**Přidělení VLAN k jednotlivým portům — access porty**

* Nastavení VLAN na jednotlivé porty → na access porty, budou do nich zapojeny např. uživatelské počítače
* Např. Připojený učitelský počítač k switchy

**Trunking mezi jednotlivými switchemi**

* “Svázání” komunikace z vícero VLAN do jednoho připojení (ať logického či fyzického):
  + IEEE 802.1Q — Umožňuje tagovat jednotlivé rámce do svých specifických VLAN
* Např. Propojení dvou učitelských kabinetů

**Zabezpečení VLAN proti neoprávněnému přístupu**

* Nastavení příslušných ACL k omezení přístupu, atd.
* Např. studentské počítače nebudou moct do učitelské VLAN, ale budou moct do VLAN, kde se nachází lab server

**Otestování a správa VLAN**

* Monitorování síťového provozu a zda všechno funguje správně
* Případná záloha konfigurací switchů, kdyby došlo ke katastrofě

**Protokol DTP a jeho dopady na bezpečnost sítě**

* DTP — Dynamic Trunking Protocol — je protokol využívány na Cisco switchých pro dynamické nastavení trunk portů mezi switchemi
* Switche dokáží rozpoznat, zda má být port nastaven jako trunk port či access port

**Výchozí nastavení**

* Povolené na všech portech
* Pokud se na portu vyskytne DTP komunikace, switche se snaží port nastavit jako trunk port

**Dopad na bezpečnost sítě**

* Neoprávnění uživatelé můžou zasílat DTP komunikaci do námi zamýšleného access portu → tím si umožnit přístup do VLAN, do kterých by neměl mít přístup
* Útok, např. VLAN hopping

**Vypnutí DTP či změna nastavení**

* Vypnutí na konkrétním portu pomocí **"switchport nonegotiate"**
* Alternativně, nastavení access portů staticky — switchport mode access

**Alternativy k DTP**

* Nastavení trunk portů a jednotlivých VLAN na nich manuálně
* Tím správe přesně určí, jaké VLANs můžou procházet trunk připojením

**Jak omezit riziko neoprávněného připojení přes trunk porty na switchích:**

* Použití funkcí Port Security a (BPDU Guard)
* Nastavení trunk portů pouze na stranách spojení mezi switchi, nikoliv na portech napojených na koncová zařízení
* Omezení počtu aktivních trunk
* portů
* Použití autentizace u trunk portů (např. 802.1x)

**Layer 3 Switching — vlastnosti a způsoby nasazení**

L3 Switch je prvek, který umí routovat mezi sítěmi, ale pracovat i jako L2 switch.

* Routing mezi samostatnými sítěmi
  + Ale i mezi VLANy, atd.

**Rozdíl mezi L2 a L3 switchem**

* L2 switch zpracovává komunikaci výhradně na druhé vrstvě OSI modelu — linková vrstva
  + Pracuje hlavně s MAC, atd.
* L3 switch dokáže zpracovávat i komunikaci na třetí vrstvě OSI modelu — síťová vrstva
  + Routing, atd.

**Výhody L3 switche**

* Více portů (rozhraní) jak na routeru
* Mnohem rychlejší než router (Rounting a forwarding probíhá na úrovni interface – rychlé)???
* Větší flexibilita
* Umožňuje lepší zabezpečení sítě díky využití ACL pro kontrolu přístupu mezi sítěmi.

**Způsoby nasazení L3 switche**

* Routing mezi VLAN pomocí L3 switchingu:
  + Umožňuje připojení více logických sítích k jednomu L3 switch a provádění routingu mezi VLANami na jednom fyzickém zařízení
* Inter-VLAN routing
  + Klasicky, routing VLAN na jednom fyzickém rozhraní
* Využití L3 switchingu jako brány mezi sítěmi
  + Umožňuje připojení více sítí na jedno fyzické rozhraní a provádět mezi nimi routing jenom na L3 - stejně jako router

**SVI — Switch Virtual Interface**

* Nutný nastavit pro každou VLAN
* SVI umí routovat mezi VLANy, jelikož vidí do L3 hlavičky paketu

**Routed porty**

* Porty switche, které se chovají stejně, jako fyzické rozhraní na routeru
* Routed port není součástí žádné VLAN
* Vytváříme ho pomocí no switchport
* Nekomunikace s subinterfaces a neumí STP

**Konfigurace Layer 3 Switchingu na Cisco switchích:**

* **Konfigurace IP rozhraní:** nastavení IP adresy na Layer 3 Switchi pro každé fyzické rozhraní.
* **Vytvoření VLAN rozhraní:** nastavení virtuálního rozhraní pro každou VLAN.
* **Nastavení statických rout:** přiřazení statických cest pro routování mezi sítěmi.
* **Konfigurace dynamického routovacího protokolu (RIP, OSPF, BGP):** automatické vyhledávání nejlepších cest pro routování mezi sítěmi.

**Bezpečnostní zvážení při používání Layer 3 Switchingu**

* **Kontrola přístupu (ACL):** Access Control Lists umožňují definovat, které typy provozu jsou povoleny nebo zakázány na daném rozhraní. ACL se používají k omezení přístupu k určitým zdrojům v síti.
* **Nastavení port security:** Port security slouží k omezení počtu připojených zařízení na daný port. Tím se minimalizuje riziko útoků typu MAC flooding nebo MAC spoofing.
* **Omezení počtu protokolů pro routování:** Omezení počtu používaných routovacích protokolů minimalizuje riziko útoků, které se zaměřují na exploitace těchto protokolů.
* **Monitorování sítě a detekce neoprávněného přístupu:** Pro aktivní monitorování sítě lze použít různé nástroje, například SNMP. Detekce neoprávněného přístupu se provádí pomocí systémů IDS/IPS nebo firewalls.