IT doupě

# Jak funguje Internet – VLAN

Zdravím vás u dalšího dílu této internetové ságy. Má dojná kráva jménem Sítě stále nevyschla a ba naopak se zdá, že je větší, než jsem si býval myslel. Dnes si ukážeme jednu z nejdůležitějších věcí, co budete jako správce sítě potřebovat, a to konkrétně segmentaci sítě nikoliv podle lokace (jako to normálně dělají routery a switche), ale podle funkce.

Dejme si příklad. Máme tří patrovou firmu a v ní několik oddělení, z nichž každé by mělo mít svoji vlastní síť. Proč neudělat jen jednu síť, ptáte se? Už jen z toho důvodu, že každé zařízení jednou za čas pošle všem ostatním na síti broadcast, a kdyby takových bylo více, celá síť by se ucpala. Můžeme tedy zkusit více sítí a použít routery – ani to není úplně ideální. Routery jsou drahé, ale hlavně spojit například část oddělení z prvního a část ze třetího patra bude logisticky docela náročné a dlouhodobě neudržitelné řešení. Je tu ale ještě jedna možnost.

VLAN je schopná vyřešit všechny naše stávající problémy. Funguje na té nejnižší vrstvě, takže nám k její funkci stačí obyčejný switch, jednoduše se škáluje, je bezpečná (komunikovat mohou jen uživatelé se stejnou VLAN, o „interVLAN“ se zmíním později) a hlavně není závislá na lokaci – i přes to, že je každá z jiné sítě, mohou z prvního až třeba do stého patra putovat všechny současně na jednom kabelu.

To, z jaké VLAN frame pochází, zjistí switch podle jeho hlavičky. V praxi se používají ty s ID od jedné do tisíce, i když ta první bývá často nastavená jako defaultní pro všechny sítě. Kromě toho je v hlavičce i priorita, používaná hlavně u hlasových komunikací. Pro každý port switche se dá nastavit konkrétní VLAN (access port), a podle toho potom daný frame přesměruje. To platí i pro broadcasty, které konečně nezahltí celou síť.

S jedním switchem je nastavení celkem snadné. Pokud se ale chce dostat do sítě, kde je stejná VLAN, ale úplně jiný switch než ten váš, musíte vytvořit trunk. Tak se označuje spojení mezi dvěma switchi/routerem, které funguje jako bílá listina a můžete na něm nastavit, která VLAN projde a která se od tohoto switche nehne ani na krok.

A tímto se dostáváme k poslednímu problému. Doteď totiž nemohly různé VLAN komunikovat mezi sebou, protože je switch nepustil. Tady už potřebujeme podporu IP adres a zároveň zajistit, že všechna zařízení ve stejné VLAN mají stejnou IP sítě. Nejstarší z metod pro interVLAN routing používá pro směrování router, do kterého vede z každé VLAN jeden kabel. Protože je ale fyzických portů na routeru jako šafránu, tato metoda se prakticky nepoužívá. Mnohem efektivnější je tzv. Router-on-a-Stick, který získal své jméno díky tomu, že je v diagramech na okraji. Místo fyzických portů používá ty virtuální (subinterface), z nichž každý může mít jinou ip adresu. K routeru tak stačí jeden jediný kabel a on už vše přesměruje. Poslední dobou se ale velice uchytily Layer 3 Switche, které oproti těm normálním zvládají i IP adresy a protože je čtou hardwarově, jsou dokonce rychlejší než samotný router.

Tak, a za mě nejtěžší problematiku z celého CCNA máte za sebou. Nicméně pro správné pochopení je třeba také praxe. K té se dostanete, pokud úspěšně splníte CCNA1 a zapíšete se do dvojky. Tam se naučíte nejen vše možné i nemožné o VLAN, ale i o STP, Etherchannelech, DHCP, FHRP, WLAN a dalších. Umělá inteligence sice pomalu nahrazuje programování, ale správu sítě jen tak neovládne. Informatice Zdar!

Jan Dlabaja, 3L

//img1