JAK SE NESPÁLIT

Vybíráme switch pro firemní sítě

Jakým způsobem nově vybudovat, případně rozšířit již existující síť obsahující switche tak, aby vyhovovala stále vyšším nárokům firemních aplikací a operačních systémů? Jaké jsou klíčové výhody a nevýhody možných řešení? Které vlastnosti jsou důležité pro bezproblémovou funkčnost sítě a aplikací?

Na začátku je dobré odpovědět si na několik klíčových otázek, které souvisí s volbou vhodného zařízení. Nechť má přesně ty funkce, které potřebujete a žádnou nechtěnou (či placenou) nad vaše požadavky, budete schopni docílit onoho klišé, a to kvality za rozumnou cenu.

Budou v síti používány multimediální aplikace? Budou někteří uživatelé mobilní, tj. budou používat při práci bezdrátový přenos? Budou v síti použity aplikace citlivé na krátkodobé výpadky? Pak není příliš vhodné použít standardní Wi-Fi, ale Enterprise Wi-Fi, řešení 4. generace. Takové řešení nabízí možnost minimálního až nulového roamingu mezi přístupovými body. Technologie Wi-Fi je z pohledu kapacity datového toku velmi limitující, proto platí: Čím více sítě se podaří dostat do optického či metalického kabelu, tím lépe!

Trápí vás náklady? Pak použijte optiku jen na páteři, případně tam, kde hrozí rušení. Pro rozvod sítě k počítači využijte levnější metalický kabel. Než přejdeme k volbě vhodného switche, stojí za zmínku pohled na zabezpečení celé sítě proti vnějším útokům i vnitřnímu přetížení – například přílišným stahováním nejrůznějších aplikací z internetu. Možností je využití proprietárního řešení nejčastěji na bázi Unixu, nebo využití služeb některého z výrobců tzv. L7 shaperů, kde se nyní mezi nejprodávanějšími v Česku drží izraelský Allot. Taková zařízení zvládají veškerý příchozí i odchozí provoz monitorovat, vyhodnocovat a případné nevhodné aplikace blokovat či omezovat.

AUTOR

Martin Doušek
Pracuje na pozici produktového manažera společnosti Intelek, specializuje se na síťová řešení a služby.

Na počátku koupě

Kritérií pro výběr toho správného síťového přepínače je celá řada. Na první pohled nejvíce patrné jsou hardwarové parametry jako počet portů a jejich rychlost. Z pohledu budoucího rozvoje firemní sítě je ideálním obsazení 60 % portů. Zbylých 40 % zůstává připraveno k případným změnám v obsazení kanceláří či zvýšení počtu zaměstnanců. Nejpoužívanější rychlostí připojení pracovní stanice je v případě Ethernetu stále 100 Mbit/s, páteř by pak měla být gigabitová.

Jak celou síť spravovat? Zde se velmi často používá protokol **SNMP** (Simple Network Management Protokol), který dokáže zajistit komunikaci mezi switchem a monitorovací aplikací. Samozřejmě za předpokladu, že switch podporuje tento protokol a máte k dispozici aplikaci, která dokáže SNMP zpracovat. Takových je celá řada: od placených software až po freeware aplikace. Pro bezproblémovou práci se SNMP by měl výrobce uvést kompatibilní MIB tabulku, případně pokud má switch speciální funkci, musí dát výrobce MIB tabulku s těmito funkcemi k dispozici.

Z pohledu budoucího rozvoje sítě činí ideální obsazení portů 60 %

Množství a kvalita funkcí, a tedy samotného switche, je pak přímo ovlivňována čipovou sadou, kterou zařízení používá. Dalším kritériem volby budiž technická podpora. Část výrobců nabízí poprodejní podporu jako dodatečnou službu, za kterou zákazník platí, druhá část výrobců tuto podporu zahrnuje již do prodejní ceny. Poprodejní podporou je myšlena hlavně budoucí

úprava firmware switche, do kterého dodává výrobce nové funkce, případně upravuje chyby z předešlých verzí. Funkce v přepínačích lze rozdělit do několika logických skupin: ovlivňující bezpečnost, topologii a kvalitu služeb.

Bezpečnostní stránka switche

Prvním krokem v zabezpečení je situace, kdy se do sítě chce připojit nové zařízení. Ideální volbou je řízení přístupu dle standardu 802.1x společně s Radius serverem. Možností je zabezpečení pomocí výše uvedeného L7 shaperu. Switch však v rámci managementu obsahuje vlastní možnosti zabezpečení. K nejčastějšímu způsobu patří funkce **ACL** (Access Control List). Využití takové funkce znamená, že má do sítě přístup pouze zařízení s definovanou MAC adresou (možnost Allow či Permit), nebo naopak lze nastavit seznam zařízení, která mají zákaz připojení (možnost DENY).

Zesílením tohoto zabezpečení je využití IP adresy místo MAC adresy, případně párování MAC i IP adresy. V takovém případě jde o funkci IP-MAC binding a do sítě přistoupí pouze zařízení s odpovídající MAC i IP adresou. Využívání takové funkce může výrazněji zatížit hardware switche, což může mít v případě volby nekvalitního switche přímý vliv na nestabilitu sítě.

Některé L3 switche umožňují nastavit i blokaci určitých portů (http, ftp) pro blokování nechtěné komunikace, hlavně pak P2P provozu, který dokáže dramaticky ovlivnit datovou průchodnost sítě. Většina P2P aplikací ale využívá šifrované komunikace a bez **DPI** (Deep Packet Inspection) je nerozlišitelná.

Funkce ovlivňující topologii sítě

Nastavení téměř každé sítě je spojeno s použitím Virtuálních sítí jako 2 úrovňové sítě (hardwarová a softwarová úroveň). Spojuje skupiny uživatelů, které mají něco společného (prioritu, omezení, rychlost připojení atd.). Switche s označením WebSmart nebo Lite management jsou nejčastějším označením pro jednoduchý management obsahující pouze základní množství funkcí a také pouze tzv. portové VLAN. VLAN skupiny lze tedy nastavit pouze v rámci jednoho zařízení. Častějším je ale použití VLAN mezi více počítači – pak jde o tzv. značené nebo tagované VLAN.

Pro případ zajištění redundance páteře sítě je možné využít tzv. dvojité páteře. V takovém případě musí mít přepínače na páteřní lince L2 funkci **LACP** (Link Aggregation Control Protocol), která v případě poruchy prvního kruhu automaticky přesměruje datový stream na redundandní trasu. Nejčastěji je páteř budována na optických portech s rychlostí 1 Gbit/s. Switche ale umožňují pro páteřní připojení použití páru portů, kdy při zapojení jednoho se automaticky deaktivuje párovaný port, tzv. Combo porty. Jde o kombinaci portu metalického RJ45 a optického SFP.

Další nezbytnou funkcí je **STA** (Spanning Tree Algorithm), respektive jeho rychlá varianta **Rapid STA** dle 802.1w. Jestliže jsou v síti využity VLAN, je možné nastavit speciální parametrizaci RSTA pro každou VLAN. Tuto funkcionalitu zajistí podpora **Multiple Spanning Tree** dle 802.1s. Pro případ, kdy je nutné ve skupině VLAN definovat ještě další úroveň, je možné využít tzv. VLAN ve VLAN označované výrobci jako Q-in-Q.

Další uvažovanou vlastností switche je i případná podpora **PoE** (Power over Ethernet) dle 802.3af. Jde o možnost vzdáleného napájení po metalickém kabelu. Použití je pak v situaci, kdy některé zařízení nelze připojit k silové síti a je nutné přivést napájení k zařízení spolu s daty. Existují 2 verze těchto zařízení tzv. **PSE** (Power Source Equipment) a **PD** (Powered Device). První umí napájet, tj. „slučovat" data a napájení do jednoho metalického kabelu, druhé pak dokáže toto napájení zpracovat a nechat se jím napájet.

Průmyslový switch musí odolat extrémním teplotám, také vyšší prašnosti či vlhkosti.

Od multimédií k průmyslu

Třetí skupinou důležitých funkcí switche jsou ty, které ovlivňují kvalitu služeb. V případě využití multimedií v síti je nutné, aby dokázal plnohodnotně pracovat s Multicast/Unicast přenosem. Zařízení pak musí podporovat **IGMP** (Internet Group Management Protocol) funkce (IGMP snoopong, leaving, join). IGMP Snooping má na starosti tvorbu skupin pro multicast komunikaci. Další užitečnou funkcí je i DHCP Option 82, který se používá k předávání DHCP dotazu ze sítí bez DHCP serveru do sítí s DHCP serverem. Neméně důležitou je i MVR (Multicast VLAN Registration) zajišťující bezpečné šíření multicastu mezi více VLANy.

Kvalita **QoS** se dá definovat pomocí následujících parametrů: ztracené pakety (Dropped packets), zpoždění (Delay) nebo rozptyl zpoždění (Jitter). Parametrem pro zabezpečení ještě vyšší kvality služeb je i počet front na port switche (minimem jsou 4 fronty). Zde mohou být použita různá pravidla zpracování, např. WRR (Weighted Round Robin). Nejvyšší prioritu pro odeslání pak mají kontrolní zprávy 2. vrstvy následované kontrolními zprávami 3. vrstvy a dále multimediální tok. Nejnižší prioritu má běžný datový tok tzv. **best effort**.

Síťový přepínač L3 Signamax.

V případě využití L3 switchů lze využít některý z routovacích protokolů. Varianty jsou dvě: **RIP** (Routing Information Protokol) nebo **OSFP** (Open Shortest Path First). Prvně zmiňovaný je vhodnější spíše pro použití v menších sítích, ten druhý pak v rozlehlejších sítích.

V případě umístění switche do prostředí s možným výskytem extrémních teplot (–40 °C až 80 °C) je nutné vybrat průmyslový switch – zařízení, které těmto teplotám odolá. Nepřemohou jej ani vyšší prašnost či vlhkost např. s IP krytím 67. Rozhraní pro napájení je v tomto případě nejčastěji ve formě terminal bloku. Další zajímavostí pak může být zasílání informací o nestabilitě spoje či chybě napájení přímo ke správci IT. Kromě toho může zařízení obsahovat i např. management či možnost redundadního zdroje napájení. ❑