Univerzitní počítačová síť v roce 2010

Vašek Lorenc, David Rohleder,
ÚVT MU

Pro úspěšné studium, výzkum či provozní práci na naší univerzitě poskytují různá oddělení celou řadu služeb, jež mají za úkol buď umožnit nebo alespoň usnadnit zmiňované činnosti.

Některé nabízené služby jsou přímo viditelné – často tím, že je všichni používají každý den, přihlašují se k nim a řeší vlastní agendu (informační systémy IS či Inet). Jiné činnosti možná nejsou tak často využívané, přesto však stále trochu na očích (tiskové úlohy, účtování tisků). Postupně se tak můžeme dostat až ke skupině, která je svým způsobem zvláštní – ke službám týkajícím se infrastruktury. K nim patří například přístupové systémy, dohledy budov, podpůrné databázové či DNS servery… nebo datová síť univerzity, díky které jsou počítače připojené k Internetu.

Takovéto provozní služby trpí z pohledu svých správců nepříjemnou konkurenční nevýhodou – jsou vidět zejména tehdy, když nefungují. Aby však univerzitní síť fungovala neustále, spolehlivě a aby poskytovala celou řadu funkcí, které uživatelé požadují, je třeba nejen její udržování při životě, ale také vývoj do budoucna, předvídání růstu a požadavků, přizpůsobování se trendům.

Pojďme se společně podívat, co za změny se objevilo v datových sítích Masarykovy univerzity v posledních měsících. Možná jste tyto změny ani nepostřehli…

1 Nová páteřní síť

Nejdůležitější z pohledu nás, správců sítě, a přitom nejméně viditelnou z pohledu uživatelů, je kompletní změna technologií páteřních prvků. Ta se neudála najednou, ale z technických důvodů musela probíhat postupně, při současném zachování provozu.

Takový požadavek rozhodně není nemožný, přesto se však proti postupu, kdy je možné si celou technologii ověřit a vyladit, vyznačuje vyšším rizikem výskytu chyb, o nichž bude zmínka později.

Jaké byly důvody k přechodu na nové technologie? Asi nejznatelnějším pro všechny je to možnost dodat fakultám vyšší přenosové rychlosti, až do 10 Gb/s, a to včetně zálohování spojení proti výpadku jednoho prvku.

Posílení proti výpadkům jednotlivých uzlů se ostatně v dohledné době podaří i směrem k síti CESNET, kdy bude univerzita připojena k dosud nejvýkonnějšímu páteřnímu směrovači Cisco CRS-1 umístěnému v serverovně na VUT Brno. Spojení se světem tedy bude realizováno *dvěma nezávislými okruhy* do dvou míst sítě CESNET. Dlouhodobý výpadek napájení v jedné části Brna by proto nemusel ohrozit provoz datových sítí jiných částí.

Změna páteřních prvků s sebou přinesla i změnu technologie propojování jednotlivých sítí. Dřívější použití *spanning tree* protokolu na L2 vrstvě bylo nahrazeno *MPLS*, což zaručuje vyšší stabilitu sítě. MPLS rovněž umožňuje vybudování nezávislých routovaných VPN sítí pro potřeby některých univerzitních aplikací, mezi které paří například Celouniverzitní počítačové studovny. To celé dohromady pak slouží jako základ lépe spravovatelné a udržovatelné sítě.

S novou technologií je dostupná i novější verze IP protokolu, *IPv6*, přímo na páteřních směrovačích, tedy bez nutnosti komplikovaných obcházení technických nedokonalostí starších prvků za pomoci špatně spravovatelných výjimek. Zatím je na IPv6 připravena hlavně síťová infrastruktura, nemáme k dispozici některé nadstavbové služby k čistě IPv6 sítové konektivitě potřebné, jako třeba DNS servery nebo poštovní servery běžící na IPv6. Každá fakulta má však možnost už nyní vyzkoušet připojení i pomocí IPv6 a připravit se tak na budoucnost s IPv6 jako novým standardem v IP sítích.

Další zajímavou službou, kterou univerzitní síť poskytuje, je *IPv4 multicast*, čehož se dá využít např. při videopřenosech přednášek. Multicastové vysílání umožňuje přenášet datový tok pouze jednou pro mnoho uživatelů současně. Dochází tak ke značné úspoře datového pásma a

zátěže serverů poskytujících datové přenosy tohoto typu.

Nu a v neposlední řadě je to i podpora IP telefonie, poskytování dostatečného pásma pro videopřenosy, lepší zabezpečení celé sítě a do budoucna i rychlejší reakce na případné zavirované stroje.

2 Monitoring

I sebelépe připravený přechod na nové prvky není schopen zabránit přinejmenším dvěma věcem – chybám softwaru na straně jedné a lidským na straně druhé. Zatímco chyby druhého typu se dají poměrně často rychle odhalit a opravit, záludnosti v softwaru způsobily během loňského a začátkem letošního roku několik nemilých výpadků.

Aby správci sítě i serverů byli informováni o nastalých chybách včas, existuje na Ústavu výpočetní techniky MU pracoviště monitorující stav sítě. To má za úkol nejen dohled nad jednotlivými prvky v síti, ale i nad jejím logickým fungováním.

V dalších úrovních, funguje-li síť, nastupují komplexnější dohledové systémy sledující provoz, např. vytížení webových serverů, odezvy jednotlivých částí sítě, případně dostupnost a kvalita poskytovaných služeb.

Uživatelé, kteří pociťují problémy s počítačovou sítí, by se měli obracet na své lokální správce, kteří následně kontaktují naše dohledové centrum pro počítačovou síť na telefonním čísle (+420) 549 49 4241.

3 Bezdrátové sítě

V posledních dvou letech se udály i zásadní změny v organizaci bezdrátových sítí na MU. A pro většinu uživatelů opět spíše neviditelně.

Z původních několika málo ostrůvků na technicky vyspělých fakultách, které se na vlastní náklady vybavily bezdrátovými přístupovými body a jejichž správci se museli vypořádat se všemi požadavky uživatelů svépomocí, se postupně na většině lokalit zavedl systém Eduroam [4]. Tím se uživatelům umožnilo připojovat se do bezdrátových sítí jednotně nejen napříč univerzitou, ale i v partnerských organizacích v zahraničí [3].

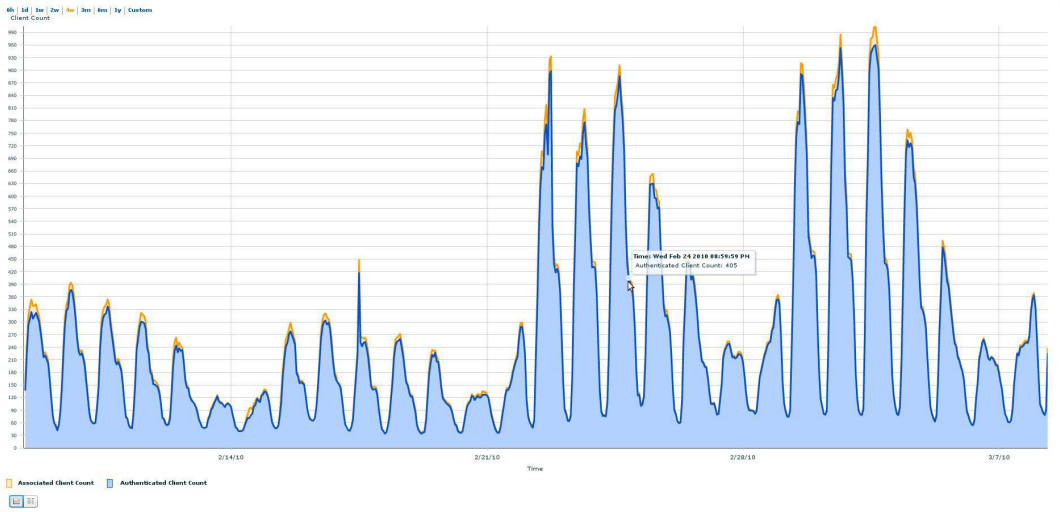
Z pohledu správy bezdrátové sítě se však až donedávna jednalo o izolované body, mezi kterými šlo jen velmi obtížně přecházet bez ztráty spojení, navíc vyžadovalo určité zásahy do infrastruktury na fakultách. Z několika jednotek až desítek bezdrátových přístupových bodů jich máme v současnosti více než 300. V takovém měřítku by ruční nastavování parametrů v jednotlivých lokalitách připomínalo noční můru mnoha správců a následně i uživatelů.

Proto byly pořízeny tzv. „wireless controllery“ [1], řídící prvky pro bezdrátové sítě, které umožňují elegantně a přehledně spravovat jednotlivé lokality, monitorovat je a řešit chyby vzniklé přetížením jednotlivých pracovišť. Navíc již díky tomuto zařízení nevynucuje připojení AP v nových lokalitách zásahy ze strany fakulty, naopak – stačí vyhradit nějakou IP adresu, která se na centrálních prvcích zaregistruje…, a je to!

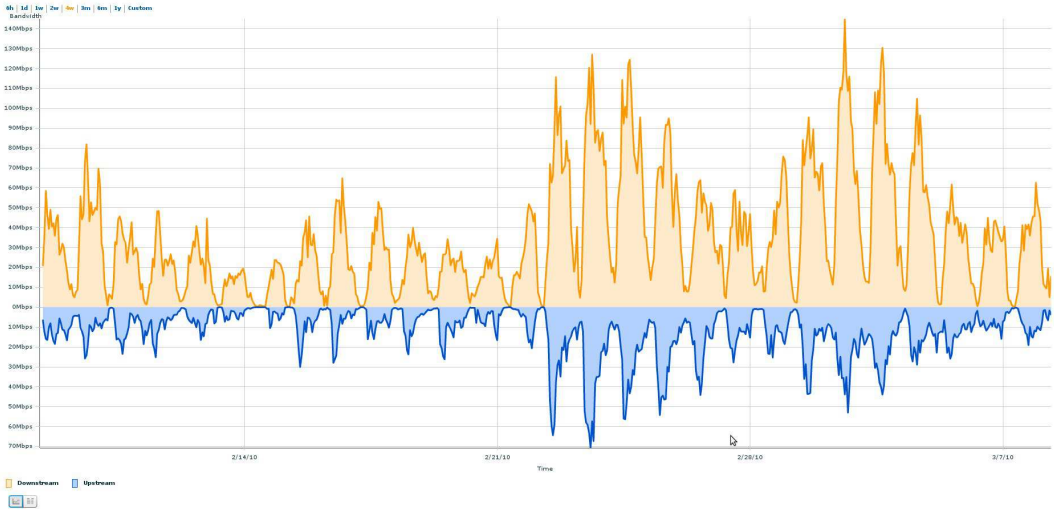
Ani tento přechod se nevyhnul určitým problémům s vylaďováním technologie. Přesto však díky přehlednějším statistikám a dohledu na jednotlivé přípojené body dochází k řešení problémů lokalit, které jsou odkázány výhradně na bezdrátové připojení a bývá obtížné zajistit tam stabilní a dostatečně rychlé připojení.

V současnosti se k bezdrátové síti připojuje až 1.100 uživatelů současně a tento počet nadále roste (největší nárůsty je obvykle vidět po Vánocích a na začátku nového školního roku), hlavně díky stále lepší dostupnosti notebooků a dalších zařízení s bezdrátovým připojením (např. mobilní telefony či mp3 přehrávače).

Přínos centralizovaného řešení správy bezdrátové sítě spočívá jak v přehledném znázornění aktuálních provozních parametrů bezdrátové sítě, tak i jejího zatížení v čase – je tak možno vysledovat exponované měsíce, dny a týdny a pomocí nich plánovat další kroky k vylepšování pokrytí. Na obrázku 1 je možno v polovině grafu vidět, jak se na počtu připojených klientů projeví začátek jarního semestru, obrázek 2 pak ukazuje totéž, ale z pohledu datových přenosů – nahoře (žlutě) je znázorněn směr ke klientům, dole (modře) od nich.



Obrázek 1: Počty bezdrátových klientů, začátek semestru



Obrázek 2: Přenosy v bezdrátových sítích, začátek semestru

4 Studentské notebooky

V souvislosti s rostoucími počty notebooků se objevily i požadavky na jejich připojení ke klasickým drátěným zásuvkám s dostupným Internetem.

Teoreticky vzato se nejedná o obtížný úkol, vždyť pro notebooky stačí vyhradit speciální blok adres a některé síťové zásuvky. Co ale dělat v případě nevhodného chování takto připojených účastníků? Tedy v okamžicích, kdy stahují nelegální obsah, útočí na servery či nevědomky svým zavirovaným notebookem obtěžují ostatní v síti? Pro takové situace je nutné evidovat, kdo byl v který čas kam připojený.

S řešením tohoto problému pomáhá stejná technologie, jaká je nasazena pro bezdrátové sítě – protokol 802.1x [2] a autentizační infrastruktura Eduroam. Celé řešení naštěstí není vázané jen na aktivní prvky jediného dodavatele, jsme tak schopni poradit s provozem na jednotlivých fakultách a nastavit celou škálu přepínačů, jež podporují standard 802.1x v dostatečné míře.

V pilotním provozu se tyto zásuvky objevily v celouniverzitní počítačové studovně na Komen-

ského náměstí, nově je jich pár nastaveno i na Pedagogické fakultě MU a uvažuje se o jejich zprovoznění i v prostorách fakulty filozofické. V kombinaci s gigabitovými přepínači je tak studentům umožněn přístup k datům uloženým na Internetu velice komfortním způsobem.

5 Bezpečnost

Celou sadu vlastností nové páteřní sítě uzavírají i nové bezpečnostní prvky, které by měly umožnit snazší a rychlejší řešení incidentů, které stěžují případné útoky nejen z vnějších sítí, ale zejména z prostředí mnohem zranitelnějšího, zevnitř univerzity.

Z toho důvodu již několik let probíhá poměrně intenzívní spolupráce s jednotlivými fakultami, z pilotního projektu univerzitních firewallů jsou již některé několik let v provozu, před kritické síťové segmenty se plánuje nasazení systémů na prevenci útoků.

Nemalou sadu konfigurací a návrhů síťových infrastruktur řešíme i pro projekt celouniverzitních počítačových studoven. Jejich rozmístění mezi různými částmi univerzity, uvnitř sítí fakult a kolejí, vynucuje celou řadu netypických bezpečnostních opatření pro zajištění stabilního provozu a bezpečnosti uživatelských dat.

Konzultace a úpravy konfigurací aktivních síťových prvků poskytujeme i pro fakulty, které nás o podobný druh spolupráce požádaly.

V neposlední řadě pak připravujeme také nástroje pro další oddělení Ústavu výpočetní techniky MU – např. pro rychlejší odezvy na hlášení o bezpečnostních incidentech, které detekuje a zpracovává Oddělení bezpečnosti datových sítí.

6 Závěr

Ač stěží viditelná, přesto klíčová – proto „páteřní“.

Oddělení, které se o tuto část univerzity stará, možná není největší, ani nejznámější. Přesto se snaží odvádět práci tak, aby ostatní univerzitní složky, které síť vyžadují, mohly poskytovat své služby těm, kteří je využívají.

Literatura

[1] D. Rohleder, M. Saitl. *Univerzitní bezdrátová síť – nové perspektivy*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2009, roč. XIX, č. 4, s. 9–11.

[2] D. Rohleder, V. Lorenc. *802.1x – autentizace v počítačových sítích*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2008, roč. XIX, č. 1, s. 2–4.

[3] E. Hladká, L. Matyska. *Mobilita napříč sítěmi*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XV, č. 4, s. 13–16.

[4] M. Procházka. *Všichni chceme Eduroam!*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVII, č. 2, s. 4–6. □