Gigabitová páteř univerzitní počítačové sítě

David Rohleder, ÚVT MU

Masarykova univerzita se vždy snažila svým studentům a zaměstnancům poskytnout v oblasti počítačových sítí co nejlepší možnosti. Postupně se zlepšovalo počítačové vybavení jednotlivých fakult, bohužel páteřní infrastruktura poněkud zaostávala. V poslední době rostly nároky na provoz počítačové sítě takovým způsobem, že bylo obtížné dosahovat požadovaných parametrů se stávajícím vybavením. Proto bylo počátkem roku 2002 rozhodnuto, že existující, již morálně zastarávající, vybavení bude nahrazeno modernějšími technologiemi na bázi gigabitového ethernetu. Zavedení gigabitového ethernetu umožnilo mimo jiné zvýšit přistupovou rychlost ze 155 Mbit/s, které používala stará ATM síť na 1 Gbit/s. Univerzitní síť se tak vydala směrem k větší stabilitě a vyššímu výkonu.

Když kolega Slavíček před rokem a půl popisoval naši ideu nové univerzitní počítačové sítě (Zpravodaj ÚVT, ročník XII, č.3), ještě nebylo jasné, kdy se budeme moci pochlubit jejím dokončením. Záleželo hlavně na způsobu financování celé výstavby. Díky kombinovanému financování z vlastních zdrojů univerzity a grantu z programu MŠMT Transormační a rozvojové programy VVŠ na rok 2003 bylo možné výstavbu výrazně urychlit. V současnosti již páteřní síť odpovídá představám, které jsme si vytvořili při jejím navrhování.

Ve výběrovém řízení na dodávku prvků pro gigabitovou síť vyhrály síťové technologie firmy Cisco, která je největším světovým výrobcem těchto zařízení. Konkrétně se jedná o typy Cisco Catalyst 6506 pro jádro sítě (v celkovém počtu 5 ks) a L3 přepínače Cisco 3550 pro každý bod distribuční vrstvy sítě. V rámci dodávky byly také vyjednány podmínky pro opravy v případě poruchy. Protože nebylo finančně výhodné pořizovat servisní smlouvu s krátkou reakční dobou servisní organizace, je na ÚVT umístěn vždy náhradní prvek od každého typu aktivního prvku (s výjimkou 6506). Pracovníci ÚVT tedy mohou případnou poruchu aktivního prvku vyřešit jeho výměnou a udržet tak minimální dobu trvání poruchy.

Aktivní prvky

Pro jádro sítě byl vybrán modulární přepínač Cisco Catalyst 6506. Tento přepínač má k dispozici celkem 6 slotů na zasunutí různých druhů modulů. Všechny přepínače jsou vybaveny Supervisor engine 2 se směrovací kartou MFCS2. Na dvou strojích umístěných na sále ÚVT jsou navíc umístěny analyzační karty pro vyhodnocování provozu.

Distribuční část sítě tvoří přepínače Cisco Catalyst 3550-12T nebo 3550-12G podle místních podmínek (vybaven buď deseti 10/100/1000 Mbit porty a dvěma GBIC zásuvkami v případě 3550-12T nebo v opačném poměru v případě 3550-12G). Jedná se o kombinovaný L2-L3 přepínač s neblokující architekturou.

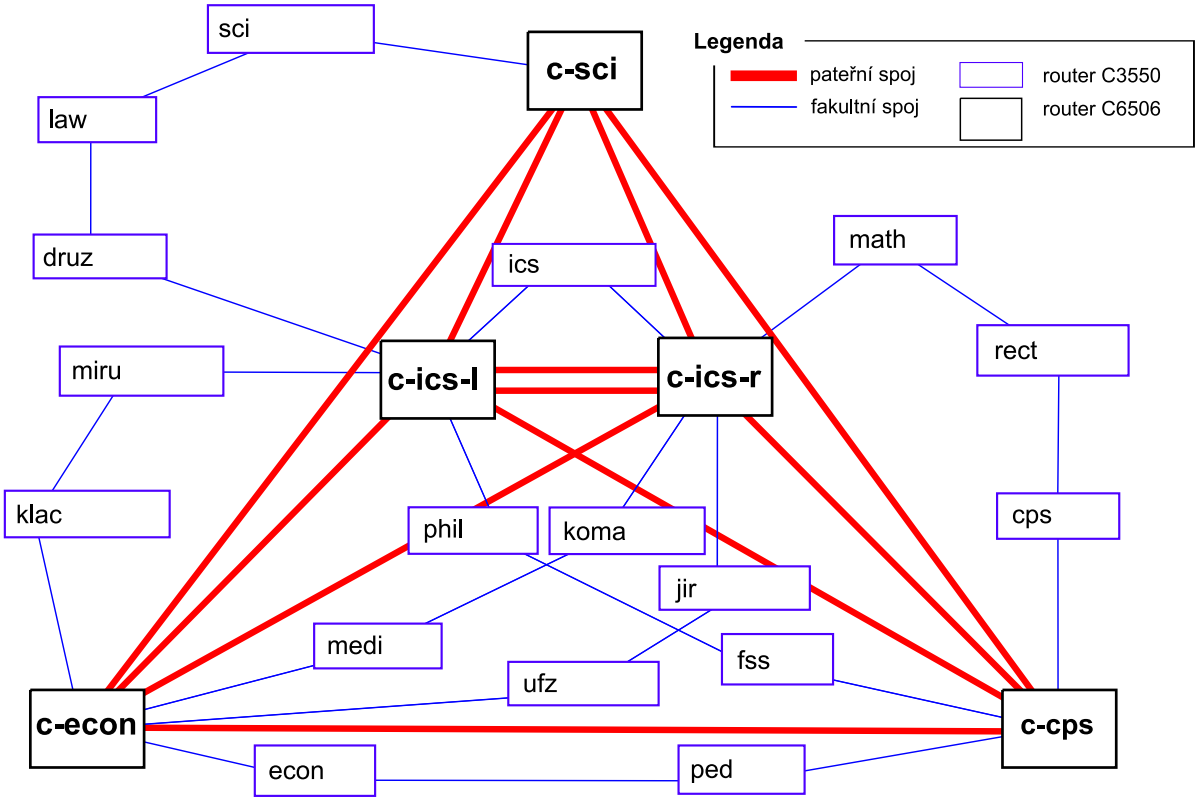
Vybavení jednotlivých bodů sítě

Každý bod sítě je vybaven rackem, ve které jsou aktivní prvky umístěny většinou spolu s UPS, která je schopna překlenout výpadek elektrické energie na několik desítek minut (závisí na odběru).

Struktura sítě

Síť je tvořena tzv. jádrem a distribuční vrstvou. Každý bod jádra je vybaven přepínačem Catalyst 6506 a jedním přepínačem distribuční vrstvy. Pro umístění přepínačů byly vybrány důležité body univerzitní sítě (např. z pohledu umístění koncových bodů optické kabeláže). Tyto přepínače jsou tedy umístěny na počítačovém sále ÚVT, v areálu Přírodovědecké fakulty, Ekonomicko-správní fakulty a v Celouniverzitní počítačové studovně na Komenského náměstí.

Přepínače distribuční vrstvy jsou umístěny v místech připojení dané části univerzity. Každá samostatná organizační jednotka má k dispozici jeden port na přepínači distribuční vrstvy. Tento port je připraven na připojení rychlostí 10, 100 nebo 1000 MBit/s v závislosti na možnostech připojované instituce. Některé fakulty už 1 Gbit přípojkou disponují, jiné jsou připojeny 100 MBit/s



Topologie nové gigabitové sítě

přípojkou. Postupně by i tyto instituce měly přejít na gigabitovou rychlost.

Celá síť (viz obrázek) je navržena tím způsobem, aby připojení bylo zálohované tak, a bylo tak odolné proti výpadku jednoho (libovolného) aktivního prvku sítě. Každý prvek je tedy připojen minimálně ke dvěma dalším aktivním prvkům, které mohou přesměrovat provoz přes sebe. Taková topologie je rovněž odolná proti případnému přerušení optického kabelu mezi jednotlivými lokalitami.

Páteřní a distribuční síť používá pro směrování směrovací protokol OSPF, přičemž jednotlivé sítě jsou k distribuční síti připojeny pomocí nastavených statických cest.

Centrální servery

Snaha o co nejvyšší procento dostupnosti prostředků počítačové sítě, hlavně centrálních serverů umístěných v počítačových sálech ÚVT, nás vedla ke zdvojení aktivních prvků. Největší překážkou v dosažení co nejvyšší dostupnosti centrálních serverů už tedy není počítačová síť, ale častěji nepřipravenost existujících serverů na zálohované připojení (např. pomocí AFT síťových karet).

Bezpečnost sítě

Protože páteřní síť má sloužit především k rychlému přesunu dat, není příliš vhodné řešit bezpečnost počítačové sítě na tomto místě. Navíc k obsluze přepínačů mají přístup pouze zaměstnanci ÚVT. Bezpečnostní politika jednotlivých přístupových bodů je plně v kompetenci správců připojené lokality. Jediné systémové omezení je takové, že z lokálních sítí mohou odcházet pakety pouze se zdrojovou adresou z místní sítě. To zabraňuje většině typů útoků se zfalšovanou IP adresou (typicky distribuovaný útok na zahlcení některé z cizích sítí DDoS – Distributed Denial of Service).

Sledování sítě

Jednou z nejdůležitějších činností při správě sítě je sledování jejího chování. K tomuto účelu jsou k dispozici dvě karty pro analýzu síťového provozu. Tyto karty nám poskytují cenné informace o provozu v síti a umožnují nám reagovat na aktuální situaci.

V poslední době se „urodila“ celá řada nedostatků v zabezpečení operačního systému Microsoft Windows (zejména chyba RPC DCOM a populární červ Blaster a jeho mutace). Tyto nákazy se díky většinovému zastoupení tohoto operačního systému mezi koncovými uživateli šíří lavinovitým způsobem po celém Internetu. Tento provoz je v univerzitní síti monitorován a nakaženým počítačům je blokován přístup k síti na nejbližším aktivním prvku distribuční vrstvy.

Díky zmíněným monitorovacím kartám je také možné sledovat anomální chování sítě. Monitorovací karty umožňují poměrně jednoduchým způsobem vysledovat příčiny vzniklé situace. Často se jedná o nelegální poskytování obsahu podléhajícího autorskému zákonu (distribuce hudby nebo filmů). Obvykle se distributorem tohoto nelegálního obsahu stává uživatel bez svého vědomí (jeho počítač byl napaden červem nebo došlo k úspěšnému útoku na jeho počítač). Na počítači se pak většinou usídlí některý z programů peer to peer sítí a počítač je zneužit jako překladiště nelegálního materiálu.

Tyto a podobné aktivity jsou sledovány a ve spolupráci s LVT jednotlivých fakult průběžně řešeny.

Poskytované služby

Páteřní univerzitní síť postkytuje čistou IPv4 konektivitu připojeným uzlům. Nasazení nových technologií umožnilo také zprovoznit standardní skupinové vysílání (native IP multicast) až na hranice distribuční vrstvy sítě a umožnit fakultám příjem těchto dat. Skupinové vysílání může najít uplatnění například u přenosu videokonferencí nebo u e-learningu.

V budoucnosti uvažujeme o možnosti experimentálního provozování IPv6 konektivity. Nové technologie nám také umožní nasazení QoS (Quality of Service) pro aplikace, které takové služby vyžadují. Jedná se především o IP telefonii a podobné aplikace.

Další plány

Vybudováním páteřní sítě naše práce na univerzitní síti samozřejmě nekončí. Je před námi celá řada úkolů jako zlepšení možností sledování sítě, vyhodnocování bezpečnostních rizik a situací a také zakomponování bezdrátových sítí pro připojení už poměrně hodně rozšířených notebooků s wireless kartami. K tomuto tématu se jistě dostaneme v některém z příštích čísel Zpravodaje, protože se jedná o téma, které je zajímavé pro poměrně širokou množinu budoucích uživatelů. □