DUM 16 téma: Protokoly vyšších řádů

ze sady: 3 **tematický okruh sady:** III. Ostatní služby internetu
ze šablony: 8 - Internet **určeno pro:** 4. ročník
vzdělávací obor: 26-41-M/01 Elektrotechnika - Elektronické počítačové systémy
vzdělávací oblast: odborné vzdělávání
metodický list/anotace: viz VY_32_INOVACE_08316ml.pdf

Vyšší vrstvy modelu

Za vyšší vrstvy referenčních modelů považujeme většinou L3 u modelu ISO/OSI, případně vrstva Síťová a vyšší u modelu „TCP/IP“. Jedná se o vrstvy, kdy již upozaďujeme samotné technické provedení komponentů sítě a využíváme již její komplexní služby doručování zpráv mezi jednotlivými účastníky. Jak to síť zajistí, necháváme z větší části na ní samotné – respektive na její vnitřní inteligenci.

Síť jako služba

Můžeme zde oddělit subjekt provozující síť a subjekty, jí využívající. Odtud je již logicky cesta k tématu zpoplatnění a přímému prodeji síťové kapacity. Typickým představitelem takového rozdělení je přístup k síti internet, kdy komerční poskytovatel připojení (ISP) zajišťuje provoz nižších vrstev, a jak je koncový zákazník využije je již zcela v jeho režii. Nebo by alespoň mělo být, takovému přístupu říkáme „síťová neutralita“. Při jejím dodržování, nesmí poskytovatel přenosové cesty nijak omezovat služby, které na vyšších vrstvách uživatel hodlá provozovat.

V praxi je to třeba omezení služeb VoIP (telefonování po síti) u poskytovatelů mobilního internetu.

Služby přenosu

Základní vyšší službou jsou služby přenosu dat mezi koncovými uzly, u kterých je znám jejich identifikátor (IP adresa či DNS název). S využitím prostředků nižších vrstev pak taková služba přenáší packety („pakety“) – balíčky dat, které jsou označeny v hlavičce řadou pomocných informací o odesilateli, příjemci, pořadí ve skupině, účelu a podobně. Jakoukoliv zprávu, kterou chce uživatel nebo aplikace odeslat, nejprve rozdělí odesílající strana (resp. její „IP stack“) na konečný počet dostatečně malých packetů (velikosti řádově jednotek kByte) a označí je sekvenčními čísly. To proto, že k příjemci mohou dorazit v jiném pořadí a on je musí znovu sestavit ve správné konstelaci.

Spojovaný a nespojovaný přenos

Z oboru telekomunikací vychází klasická myšlenka spojovaného přenosu. U něj lze rozdělit fáze zahajování spojení, průběh a jeho ukončení. Tedy jako u běžného telefonního přístroje. Před samotným přenosem dat, musí být speciálním postupem spojení navázáno (u telefonu například vytočením čísla, kterým se v ústředně fyzicky propojí vodiče od telefonu

na jiné vodiče směrem k cílové stanici), což trvá nenulovou dobu a přenos dat musí na navázání spojení počkat. Druhá strana také musí spojení přijmout a být ochotna se ho účastnit. Dokud není spojení navázáno, není možné odesílat data.

Na druhou stranu, jednou navázané spojení je k dispozici bez čekání a s jistotou, že druhá strana je zapnuta a data očekává. V době, kdy nejsou žádná data přenášena, je komunikační kanál blokován a většinou je za jeho provoz účtován i poplatek. Jednou navázané spojení je také nutné po skončení řádně rozpojit, v opačném případě jej rozpojí až infrastruktura sítě, či protistrana, ale až po uplynutí časového limitu, během kterého je stále linka blokována.

V telekomunikacích pak hovoříme o principu přepínání okruhů, v počítačových sítích lze využitím protokolu spojovaného přenosu takový virtuální „okruh“ úspěšně emulovat („předstírat“) i s využitím sítě na bázi přepínání paketů.

Druhou variantou jsou formy přenosu nespojovaného, kdy odesilatel pouští do sítě pakety s vyznačeným cílem a pouze statisticky předpokládá, že se k příjemci dostanou, bez poškození, v rozumném čase a že příjemce bude vůbec schopen data přijímat. Tento způsob komunikace se dá úspěšně přirovnat k posílání vzkazů v láhvi z opuštěného ostrova.

Spolehlivý a nespolehlivý přenos

Dalším možným pohledem na komunikační protokoly vyšších řádů je sledování spolehlivosti. Spolehlivost v tomto případě chápeme tak, že data jsou příjemci doručena, nebo se odesilatel dozví, že se doručení nepodařilo.

Naproti tomu nespolehlivý přenos pouze data odesílá a nezdržuje se ověřováním, zda data došla, a nepokouší se je odeslat znovu, pokud nebyl přenos úspěšný. Tím dochází k dramatickému zvýšení výkonnosti sítě, protože na potvrzování a případné opakování jednotlivých paketů se u spolehlivého přenosu spotřebovává nemalou část přenosové kapacity, která je u nespolehlivého přenosu k dispozici uživatelským datům. V situaci nepřetížené a relativně fyzicky spolehlivé sítě může být nespolehlivý komunikační protokol velmi výkonný.

Typickými představiteli těchto kombinací jsou protokoly:

- UDP – User Datagram Packet … protokol nespojovaného nespolehlivého přenosu
- TCP – Transmission Control Protocol … protokol spolehlivého spojovaného přenosu

Někdy bývá protokol TCP označován jako „TCP/IP“, což ale není technicky zcela správně. TCP je L4 protokol, využívající služby L3 protokolu IP, tato vazba ale není povinná. UDP také využívá IP služby. Obdobně, je označení „TCP/IP“ nevhodné, pokud hovoříme o samotném IP protokolu.

Rozhodnutí, který protokol zvolit, je většinou na autorovi aplikace, mnohdy si uživatel může i sám vybrat. Jsou třídy aplikací, u kterých je použití TCP jasnou volbou – typicky při přenosech binárních dat, souborů a šifrogramů. Zde je samozřejmě nepřípustná jakákoliv ztráta dat a přenosový protokol se musí snažit zprávu doručit bez chyb a kompletní, případně potvrdit že přenos není možný.

Nespolehlivý přenos pak najde uplatnění v situacích, kdy malá ztrátovost dat není na závadu a naopak využijeme výhody okamžitého přenosu, bez čekání na jeho zahájení a zdržování při opakovaném doručování poškozených paketů. Takovou aplikací je třeba on-line streaming (vysílání/přenos) videa, či audia. Koncovému uživateli rozhodně méně vadí výpadek několika pixelů obrázku, než zastavení přenosu na několik sekund, aby se třeba 20x tento úsek dat opakovaně přenášel, dokud nebude snímek dokonalý.

Další vyšší protokoly

Již využívají některé ze zmíněných variant, pro své konkrétní potřeba, uvedeme je ve stručném přehledu:

- http – hyper text transfer protocol – protokol pro přenos stránek formátu html u služby www
- ftp – file transfer protocol – protokol pro přenos souborů libovolného typu
- ssh – secure shell – protokol textového terminálu, který obsahuje šifrovací mezivrstvu pro ověření identity protistrany a zamezení odposlechu přenášených dat
- rpc – remote procedure call – protokol vzdáleného spouštění procedur a programů, z jiného nebo na jiném počítači; v systémech Windows často bezpečnostně velmi riziková funkce

- nfs – network file system – protokol vzdáleného přístupu k souborovému systému, na rozdíl od ftp uživateli skrývá rozdíl mezi místním a vzdáleným diskem, i se vzdáleným může pracovat jako by byl lokální
- dns – domain name system – protokol služby doménových názvů
- dhcp/bootp – dynamic host configuration protocol – protokol pro vzdálenou konfiguraci síťových uzlů a nastavování jejich základních IP parametrů
- imap/smtp/pop3 – různé poštovní protokoly
- ospf/rip – protokoly automatické konfigurace směrování v síti

Úkoly pro samostatnou práci

- V laboratoři pomocí diagnostického SW pozorujte TCP a UDP komunikaci.
- Vyhledejte informace o protokolu NTP.
- Zjistěte, jaký L4 protokol využívají nadřazené protokoly FTP a http.
- V čem spočívá rozšíření HTTPs?

- Zdroje:

- Archiv autora