IT doupě

# Jak funguje Internet – Aplikační vrstva a protokoly

V zářijovém dílu jsem vás provedl transportní vrstvou zodpovědnou za přenos dat. Pokud ale chcete mezi aplikacemi komunikovat, potřebujete jít ještě výš, a to až k té aplikační. Dnes se vám proto pokusím popsat její funkci a ukážu i pár základních protokolů, se kterými se setkáváte denně.

Stejně jako ty předchozí se i tato vrstva dá rozdělit na více podvrstev. Nejnižší relační se stará o komunikaci mezi aplikacemi, obnovuje nebo ukončuje relace. Ta nad ní, prezentační, umí formátovat, kompresovat a šifrovat data a zaručuje, že si budou obě aplikace rozumět. A na úplné špičce pomyslné TCP/IP pyramidy sedí aplikační vrstva, která slouží jako rozhraní mezi uživatelem a sítí. Tady se nachází všechny webové prohlížeče, emailové klienty a CLI aplikace využívající protokoly, z nichž si dnes pár z těch nejznámějších probereme.

Nejznámější ze všech je bezpochyby HTTP a jeho šifrovaná verze HTTPS, která ho postupně nahradila. Pomocí metody GET můžete z webového serveru stahovat HTML dokumenty, které se následně zobrazí ve vašem prohlížeči jako webové stránky. Přes POST můžete odesílat formuláře nebo data na server a PUT umožňuje posílat soubory.

Takový email má protokoly hned tři. Pro odeslání se ustálil SMTP. Ten email nejdříve odešle na server odesílatele (vás) a potom na server příjemce, který si ho uloží. Pokud není server příjemce nalezen, vrátí zprávu zpět a dá vám o tom vědět. Pro získání emailu pak záleží, zda si chcete na serveru nechat kopii (IMAP) a nebo ne (POP3).

Dalším důležitým protokolem je SSH. Stejně jako jeho předchůdce Telnet se umí připojit na vzdálený počítač a přes textové rozhraní v něm vykonávat příkazy shellu. Problém Telnetu byl, že všechna data včetně hesel posílal v plaintextu, na což doplatila například univerzita v Helsinkách. Díky SSH je celá komunikace zašifrovaná a vy už se nemusíte ničeho bát (za předpokladu, že vám někdo neukradne privátní klíč).

Důvod, proč nepotřebujete znát IP adresu 195.113.190.106 k tomu, abyste se dostali na stránky naší školy, tkví v DNS – protokolu překládající IP adresy na doménová jména a naopak. Jeho požadavek vypadá zhruba takto – Prohlížeč se nejdříve zeptá počítače, zda nemá IP adresu k této doméně uloženou v paměti. Pokud ne, pošle požadavek vašemu poskytovateli internetu. Ani ten ji ale nemá, a tak se musí zeptat výš. Najde nejbližší kořenový server (kterých je na světě 13) a zeptá se ho, zda doménu nezná. Bohužel ne, ale protože poznává .cz (doména nejvyšší úrovně), dá mu adresu serveru spravujícího všechny .cz domény. Ten poznává doménu druhého řádu spseol a dá mu IP školního DNS serveru. Až na něm jsou uloženy informace o subdoménách a veškeré IP adresy, díky kterým si můžeme webovou stránku zobrazit. Je to trochu složitější, takže vám tu nechávám [video](https://youtu.be/J44jvmoDxzo) přímo od NIC.cz, správce cz domény, a také malý ilustrační obrázek

//img 1, nezapomeň na hyperlink o řádek výš

A jako poslední vám řeknu něco o DHCP, protože i to určitě používáte denně. Ve zkratce je to služba, která vám automaticky přidělí IP adresu, DNS server i default gateway pro komunikaci se vnějškem. Tyto údaje jsou časově omezené a po vypršení platnosti si musíte zažádat o nové. Využití je možné všude, kde se vám nechce konfigurovat tyto údaje ručně, například při používání WiFi.

A to je vše, došli jsme až na samý vrchol internetové pyramidy. Pokud vám to ale nestačí a chcete se ponořit do tajů králičí nory, nezoufejte – i letos je otevřený Cisco CCNA1 kroužek, kde se dozvíte vše, o čem jsem za těch několik měsíců napsal a ještě mnohem víc. Také si budete moc zapojit switch, navrhnout vlastní síť nebo připravit UTP kabel, a k tomu dostanete i certifikaci uplatnitelnou v pracovním životě. V příštím a posledním dílu bych to chtěl všechno trochu shrnout a podívat se na zabezpečení sítě a další témata, na která zatím nebyl prostor. No a do té doby, jako vždy, informatice Zdar!

Jan Dlabaja, 3L