NEJPOPULÁRNĚJŠÍ SNIFFER NAPLNO VYUŽITÝ V DESÍTKÁCH REÁLNÝCH SCÉNÁŘŮ

ANALÝZA SÍTÍ
A ŘEŠENÍ PROBLÉMŮ V PROGRAMU
WIRESHARK

CHRIS SANDERS

computer press

no starch press

Chris Sanders

Analýza sítí a řešení problémů v programu Wireshark

Computer Press
Brno
2012

Analýza sítí a řešení problémů v programu Wireshark

Chris Sanders

Překlad: Jakub Goner
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek

Objednávky knih:
http://knihy.cpress.cz
www.albatrosmedia.cz
eshop@albatrosmedia.cz
bezplatná linka 800 555 513
ISBN 978-80-251-3718-5

Vydalo nakladatelství Computer Press v Brně roku 2012 ve společnosti Albatros Media a. s. se sídlem Na Pankráci 30, Praha 4. Číslo publikace 15 946.

1. vydání

ALBATROS MEDIA a.s.

Obsah

Poděkování

Tato kniha mohla vzniknout díky přímým i nepřímým příspěvkům mnoha různých lidí.

V prvé řadě všechna sláva patří Bohu. Při psaní knihy se projevuje mnoho pozitivních i negativních emocí. Když jsem nervózní, uklidňuje mě. Když jsem zklamaný, utěšuje mě. Když jsem zmatený, dává mi odhodlání. Když jsem unavený, přináší mi odpočinek. Když jsem pyšný, zachovává moji rozvážnost. Za tuto knihu, svou kariéru i vlastní existenci vděčím pouze Bohu a jeho synu Ježíši Kristu.

Táto, svou motivaci jsem čerpal z mnoha zdrojů. Nic mě však nepotěší tolik, jako když mi říkáš, že jsi na mě pyšný. Nemůžu Ti dostatečně poděkovat za to, že mi to dáváš najevo.

Mami, druhé vydání této knihy se objeví přímo před desátým výročím Tvého odchodu. Vím, že mě sleduješ a že jsi na mě hrdá. Doufám, že v dalších letech budeš ještě více.

Teto Debi a strýci Randy, od prvního dne jste mě maximálně podporovali. Moje rodina není velká, ale velmi si cením těch příbuzných, které mám – především vás. Nesetkáváme se sice tak často, jak bych si přál, ale nemohu vám dostatečně poděkovat za to, že jste pro mě byli druhými rodiči.

Tino Nance, sice už spolu nemluvíme tak často jako dříve, ale vždy Tě budu považovat za náhradní mámu. Bez Tvé podpory a důvěry bych nedělal to, co dnes dělám.

Jasone Smithi, musel jsi vyslechnout více mých tirád než kdokoli jiný, ale díky tomu jsem si zachoval zdravý rozum. Jsem rád, že mám v Tobě dobrého kamaráda a spolupracovníka, který mi pomáhá s různými projekty. Dodatečně Ti ještě děkuji za to, žes mi tehdy na půl roku půjčil svou garáž.

Co se týče mých spolupracovníků (minulých i současných): vždy jsem věřil tomu, že pokud se člověk obklopí dobrými lidmi, sám se stane lepším. Mám štěstí, že spo-

lupracuji s mnoha skvělými lidmi, kteří patří mezi nejlepší a nechytřejší v branži. Počítám vás do své rodiny.

Mike Poor je bez diskuze mým idolem v oboru analýzy paketů. Tvoje práce a přístup mě inspirují a pomáhají mi v tom, co sám dělám.

Tylerovi Regulymu děkuji za odborné korektury této knihy. Určitě to nebyla žádná zábava, ale bylo to nezbytné a moc si toho vážím.

Děkuji také Geraldu Combsovi a vývojářskému týmu programu Wireshark. Díky Geraldovi a stovkám jiných vývojářů je program Wireshark vynikající analytickou platformou. Nebýt jejich úsilí, tato knihy by neexistovala… nebo pokud by přece jen vznikla, popisovala by program tcpdump a to by nikoho nebavilo.

Bill a zaměstnanci nakladatelství No Starch Press dali šanci klukovi z Kentucky, a to nejen jednou, ale dvakrát. Děkuji za vaši důvěru a trpělivost a za to, že jsem si mohl splnit své sny.

Úvod

Druhé vydání knihy *Analýza sítí a řešení problémů v programu Wireshark* vzniklo během jednoho a půl roku od sklonku roku 2009 do poloviny roku 2011, tj. asi čtyři roky poté, co se objevilo vydání první (pouze v anglickém jazyce).

Cíle knihy

Možná přemýšlíte nad tím, proč byste si měli koupit zrovna tuto knihu o analýze paketů, a ne nějakou jinou. Odpověď se skrývá v titulu: *Analýza sítí a řešení problémů v programu Wireshark*. Není nad praktické zkušenosti a v knize lze tyto zkušenosti nejlépe nahradit díky praktickým příkladům analýzy paketů a reálným scénářům.

První polovina této knihy přináší nezbytné znalosti, které potřebujete k analýze paketů a práci v programu Wireshark. Druhá polovina knihy je věnována výhradně praktickým příkladům, se kterými se můžete běžně setkat při každodenní správě sítě.

Nehledě na to, zda pracujete jako síťový technik, správce sítě, šéf oddělení IT, správce pracovních stanic, nebo dokonce síťový bezpečnostní analytik, mohou vám značně pomoci metody analýzy paketů, které jsou popsány v této knize.

Koncepce a přístup

Obecně se můžu označit za pohodáře. Při výuce se tedy snažím postupovat neformálním způsobem. Tento přístup se projevuje i v jazyce této knihy. Při rozboru technických koncepcí je snadné zapadnout do technického žargonu, ale vyvinul jsem maximální úsilí, abych výklad udržel na konverzační rovině. Všechny definice jsem psal jasně, přímo a věcně, bez zbytečné vaty.

Pokud to s učením analýzy paketů myslíte vážně, měli byste si osvojit koncepce v prvních několika kapitolách, protože bez nich nemůžete porozumět zbytku

knihy. Druhá polovina knihy je zcela praktická. Ve své práci se sice nemusíte setkat s přesně stejnými scénáři, ale měli byste umět příslušné koncepce aplikovat v situacích, které budete řešit.

Následuje stručný přehled obsahu kapitol této knihy:

Kapitola 1: Úvod do analýzy paketů a sítí

Co to je analýza paketů? Jak funguje? Jak se provádí? Tato kapitola se zabývá základy síťové komunikace a analýzy paketů.

Kapitola 2: Napíchnutí linky

V této kapitole si ukážeme různé metody, jak lze do sítě připojit paketový sniffer.

Kapitola 3: Úvod do programu Wireshark

Tato kapitola obsahuje základní informace o programu Wireshark – kde jej získat, jak jej používat, co dělá, proč je skvělý a další užitečné podrobnosti.

Kapitola 4: Zpracování zachycených paketů

Po instalaci a zprovoznění programu Wireshark se musíte naučit, jak zachycené pakety zpracovávat. V této kapitole získáte základy.

Kapitola 5: Pokročilé funkce programu Wireshark

Jakmile se naučíte lézt, je čas s výukou chození. V této kapitole se pustíme do pokročilých funkcí programu Wireshark a podíváme se mu pod kapotu, abychom mohli využít některé méně triviální funkce.

Kapitola 6: Běžné protokoly nižších vrstev

Tato kapitola ukazuje, jak na úrovni paketů vypadají některé běžné síťové komunikační protokoly nižších vrstev, např. TCP, UDP a IP. Chcete-li porozumět možným chybám těchto protokolů, musíte nejdříve chápat, jak správně fungují.

Kapitola 7: Běžné protokoly vyšší vrstvy

Tato kapitola pokračuje v rozboru protokolů a představuje na úrovni paketů nejrozšířenější síťové komunikační protokoly vyšší vrstvy: HTTP, DNS a DHCP.

Kapitola 8: Běžné scénáře z praxe

V této kapitole naleznete rozbor některých běžných vzorů provozu a první sadu praktických scénářů. Všechny scénáře mají přehledný formát, který postupuje od problému přes jeho analýzu k řešení. Tyto základní scénáře se týkají pouze několika počítačů a nevyžadují rozsáhlou analýzu – pouze do té míry, abyste získali základní přehled problematiky.

Kapitola 9: Zrychlení pomalé sítě

Síťoví technici nejčastěji řeší stížnosti, které se týkají nedostatečného výkonu sítě. Devátá kapitola je věnována řešení tohoto typu problémů.

Kapitola 10: Analýza paketů a zabezpečení

Zabezpečení sítě patří mezi nejsledovanější témata z oblasti IT. Kapitola 10 představuje některé scénáře, které se týkají řešení bezpečnostních potíží metodami analýzy paketů.

Kapitola 11: Analýza bezdrátových paketů

Tato kapitola slouží jako úvod do analýzy bezdrátových paketů. Rozebírá rozdíly mezi analýzou v bezdrátových a kabelových sítích a uvádí některé příklady provozu v bezdrátových sítích.

Příloha: Další informace

Příloha knihy doporučuje některé další referenční nástroje a weby, které se vám mohou hodit při rozvíjení postupů analýzy paketů, s nimiž jste se seznámili v předchozí části knihy.

Jak s knihou pracovat

Tuto knihu lze používat dvěma způsoby:

- Jako výukový text, který můžete přečíst po jednotlivých kapitolách od začátku do konce a který vám umožní porozumět základům analýzy paketů. Přitom je vhodné věnovat zvláštní pozornost praktickým scénářům v posledních několika kapitolách.
- Jako referenční zdroj. Některé funkce programu Wireshark se nepoužívají příliš často, takže můžete zapomenout, jak pracují. Knihu *Analýza sítí a řešení problémů v programu Wireshark* je vhodné mít po ruce, potřebujete-li si rychle osvěžit, jak se určitá funkce používá. Kniha také obsahuje unikátní grafy, diagramy a postupy, které se mohou při praktické analýze paketů hodit.

Ukázkové zachycené soubory

Všechny zachycené soubory v této knize jsou k dispozici na stránce nakladatelství No Starch Press: `http://www.nostarch.com/packet2.htm` po klepnutí na odkaz „Download the capture files for this book“. Chcete-li z knihy vytěžit maximum, rozhodně doporučuji, abyste si tyto soubory stáhli a používali je při čtení příslušných příkladů.

Nadace Rural Technology Fund

V tomto úvodu nesmí chybět zmínka o velkém přínosu originálního vydání knihy *Analýza sítí a řešení problémů v programu Wireshark*. Krátce po prvním vydání této knihy jsem založil neziskovou organizaci typu 501(c)(3), která završuje mé největší sny.

Studenti z venkova, i když mají výborné známky, mívají často méně příležitostí k seznámení s technologiemi než jejich kolegové z měst. Nadace Rural Technology Fund (RTF), založená roku 2008, se snaží vyrovnat digitální příkop mezi venkovskými komunitami a jejich městskými a předměstskými protějšky. Přitom se využívají cílené stipendijní programy, komunitní práce a obecná propagace technologií ve venkovských oblastech.

Naše stipendia jsou zaměřena na studenty žijící ve vesnických komunitách, kteří se zajímají o počítačové technologie a plánují se v tomto oboru dále vzdělávat. S potěšením oznamuji, že 100 procent autorských honorářů z této knihy směřuje přímo do nadace Rural Technology Fund, která bude poskytovat tato stipendia. Chcete-li získat další informace o nadaci Rural Technology Fund nebo o tom, jak můžete sami přispět, navštivte náš web na adrese `http://www.ruraltechfund.org/`.

Kontakt s autorem

Pokaždé jsem nadšený, když dostanu zpětnou vazbu od svých čtenářů. Pokud byste mě chtěli z jakéhokoli důvodu kontaktovat, můžete posílat libovolné otázky, komentáře, hrozby a návrhy k sňatku přímo na moji adresu `chris@chrissanders.org`. Pravidelně také píši blog na adrese `http://www.chrissanders.org/` a můžete mě následovat na účtu Twitter @chrissanders88.

Zpětná vazba od čtenářů

Nakladatelství a vydavatelství Computer Press, které pro vás tuto knihu přeložilo, stojí také o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

redakce PC literatury
Computer Press
Spielberk Office Centre
Holandská 3
639 00 Brno

nebo

sefredaktor.pc@cpress.cz

Computer Press neposkytuje rady ani jakýkoli servis pro aplikace třetích stran. Pokud budete mít dotaz k programu, obraťte se prosím na jeho tvůrce.

Errata

Přestože jsme udělali maximum pro to, abychom zajistili přesnost a správnost obsahu, chybám se úplně vyhnout nelze. Pokud v některé z našich knih najdete chybu, ať už chybu v textu nebo v kódu, budeme rádi, pokud nám ji oznámíte. Ostatní uživatele tak můžete ušetřit frustrace a nám můžete pomoci zlepšit následující vydání této knihy.

Veškerá existující errata zobrazíte na adrese `http://knihy.cpress.cz/K1986` po klepnutí na odkaz Soubory ke stažení.

KAPITOLA 1

Úvod do analýzy paketů a sítí

V každé počítačové síti se může denně vyskytnout spousta problémů: od prosté infekce spywarem po složitou chybu konfigurace směrovače. Některé potíže přitom nelze vyřešit okamžitě. Můžeme nanejvýš doufat, že jsme na problémy plně připraveni a máme dostatečné znalosti a potřebné nástroje, abychom dokázali vhodně reagovat.

Všechny síťové problémy začínají na úrovni paketů, kde se může ukázat, že i nejpřitažlivější aplikace má zcela neefektivní implementaci a zdánlivě spolehlivé protokoly obsahují bezpečnostní díry. Chceme-li síťovým problémům lépe porozumět, musíme přejít na úroveň paketů. Zde je vidět úplně vše – nic neschovají matoucí struktury nabídek, vizuálně atraktivní uživatelské rozhraní ani nespolehliví zaměstnanci. Na této úrovni neexistují žádná skutečná tajemství (pouze ta šifrovaná). Čím více toho zvládneme na úrovni paketů, tím lépe dokážeme kontrolovat svou síť a řešit síťové potíže. To je doménou analýzy paketů.

V této knize se do světa analýzy paketů pustíme okamžitě. Na praktických příkladech ukážeme, jak zrychlit síťovou komunikaci, identifikovat úzká hrdla aplikací, nebo dokonce stopovat hackery. Po přečtení této knihy dokážete implementovat pokročilé postupy analýzy paketů, které vám pomohou vyřešit i ty nejobtížnější síťové potíže.

V této kapitole začneme od základů a zaměříme se na síťovou komunikaci. S využitím těchto základních informací pak analyzujeme různé scénáře.

Analýza paketů a nástroje pro sledování paketů

Analýza paketů, která se často označuje jako *sledování paketů* (packet sniffing) nebo *analýza protokolů*, popisuje proces zachytávání a interpretace aktuálních dat přenášených po síti. Díky tomu lze lépe porozumět fungování dané sítě. K analýze paketů se obvykle používá *paketový sniffer* (packet sniffer – nástroj pro sledování paketů), který umožňuje zachytávat neformátovaná síťová data při jejich přenosu.

Analýza paketů poskytuje následující možnosti:

- Seznámení s vlastnostmi sítě
- Zjištění uživatelů sítě
- Zjištění, kdo nebo co spotřebovává dostupnou šířku pásma
- Identifikace časů špičkového využití sítě
- Identifikace možných útoků nebo škodlivé aktivity
- Vyhledání nezabezpečených a neefektivních aplikací

K dispozici jsou paketové sniffery různých typů včetně bezplatných a komerčních. Každý program je navržen k odlišným účelům. Mezi oblíbené programy na analýzu paketů patří tcpdump, OmniPeek a Wireshark (v této knize se budeme zabývat pouze posledním uvedeným programem). tcpdump je program pro příkazový řádek. OmniPeek a Wireshark mají grafická uživatelská rozhraní (GUI).

Hodnocení paketového snifferu

Při výběru paketového snifferu je nutné zohlednit několik faktorů, mj.:

- **Podporované protokoly** – všechny paketové sniffery umožňují interpretovat více protokolů. Většina z nich dokáže interpretovat běžné síťové protokoly (např. IPv4 a ICMP), protokoly transportní vrstvy (např. TCP a UDP), a dokonce protokoly aplikační vrstvy (mezi něž patří DNS a HTTP). Nemusí však podporovat netradiční nebo novější protokoly (třeba IPv6, SMBv2 či SIP). Před nasazením snifferu byste měli ověřit, zda je kompatibilní s protokoly, které chcete analyzovat.
- **Snadné používání** – vezměte v úvahu uspořádání ovládacích prvků programu, snadnost instalace a celkové postupy standardních operací. Zvolený program by měl odpovídat úrovni vašich znalostí. Pokud nemáte s analýzou paketů delší praxi, raději se vyhněte pokročilejším paketovým snifferům pro příkazový řádek, jako je tcpdump. Na druhou stranu máte-li bohaté zkušenosti, můžete dát pokročilejšímu programu přednost. Když získáte v oblasti analýzy paketů více praxe, můžete v některých případech dokonce s výhodou kombinovat více paketových snifferů.
- **Náklady** – na paketových snifferech je potěšující, že existuje mnoho bezplatných programů tohoto typu, které jsou srovnatelné s kterýmkoli komerčním

produktem. Komerční produkty a jejich bezplatně dostupné alternativy se liší zejména svými vykazovacími moduly. Komerční programy obvykle obsahují nějaký modul na generování složitých výkazů, který má u bezplatných aplikací často jen omezené možnosti nebo úplně chybí.

- **Podpora programu –** i když postupně zvládnete základy používání paketového snifferu, můžete příležitostně potřebovat pomoc při řešení nových problémů. Když porovnáváte dostupnou podporu, všímejte si vývojářské dokumentace, veřejných fór a e-mailových konferencí. Bezplatně dostupné programy na sledování paketů jako Wireshark sice obvykle nenabízejí podporu vývojářů, ale tuto mezeru často zaplňují komunity uživatelů těchto aplikací. Tyto komunity uživatelů a přispěvatelů provozují diskuzní fóra, wiki a blogy, kde můžete získat dostatek informací, abyste svůj paketový sniffer lépe využili.
- **Podpora operačních systémů –** některé paketové sniffery bohužel nejsou kompatibilní se všemi operačními systémy. Zvolte si ten program, který bude fungovat ve všech operačních systémech, které potřebujete používat. Pracujete-li jako konzultant, často musíte zachytávat a analyzovat pakety v různých operačních systémech. Hledejte proto nástroj, který funguje ve většině systémů. Pamatujte také na to, že někdy je nutné zachytávat pakety v jednom počítači a analyzovat je v jiném. Kvůli rozdílům mezi operačními systémy může být potřeba použít v každém zařízení jinou aplikaci.

Principy paketových snifferů

Proces sledování paketů vyžaduje spolupráci softwaru a hardwaru. Celý proces lze rozdělit na tři fáze:

- **Shromažďování –** v prvním kroku paketový sniffer sbírá neformátovaná binární data, která putují po síti. Přitom se vybrané síťové rozhraní obvykle přepíná do *promiskuitního režimu*. V tomto režimu dokáže síťová karta naslouchat veškerému provozu v síťovém segmentu, nikoli pouze datům, která jsou jí adresována.
- **Konverze –** v tomto kroku jsou zachycená binární data převedena do čitelného tvaru. Zde končí možnosti většiny pokročilých paketových snifferů pro příkazový řádek. V této fázi mají síťová data podobu, kterou lze interpretovat pouze na zcela základní úrovni. Větší část analýzy zůstává na koncovém uživateli.
- **Analýza –** třetí a závěrečný krok zahrnuje vlastní analýzu zachycených a konvertovaných dat. Paketový sniffer načte zachycená síťová data, na základě extrahovaných informací zkontroluje síťové protokoly a zahájí analýzu konkrétních vlastností příslušného protokolu.

Principy komunikace počítačů

Chcete-li plně pochopit analýzu paketů, musíte přesně rozumět tomu, jak počítače komunikují. V této části prozkoumáme základy síťových protokolů, model OSI (Open Systems Interconnections), síťové datové rámce a hardware, který činnost sítí umožňuje.

Protokoly

Moderní sítě jsou tvořeny různými systémy, které fungují na mnoha odlišných platformách. Jejich komunikaci usnadňuje sada společných jazyků, které se označují jako *protokoly*. K běžným protokolům patří TCP (Transmission Control Protocol), IP (Internet Protocol), ARP (Address Resolution Protocol) a DHCP (Dynamic Host Configuration Protocol). *Sada protokolů* (protocol stack) je logické seskupení protokolů, které fungují společně.

Princip protokolů nejlépe přiblížíme, když je přirovnáme k pravidlům, která řídí ústní nebo písemnou komunikaci mezi lidmi. Každý jazyk má pravidla, která například řídí časování sloves nebo způsob, jakým někoho pozdravit či mu poděkovat. Protokoly fungují podobně a umožňují mj. definovat, jakým způsobem budou směrovány pakety, jak lze inicializovat připojení a jak se potvrzuje přijetí dat.

V závislosti na své funkci může být protokol mimořádně jednoduchý, nebo značně složitý. Různé protokoly se sice často zásadně liší, ale mnohé z nich řeší podobné aspekty:

- **Inicializace připojení** – inicializuje připojení klient nebo server? Které informace je nutné před zahájením komunikace vyměnit?
- **Vyjednání vlastností připojení** – je komunikace protokolu šifrována? Jak se mezi komunikujícími hostiteli přenášejí šifrovací klíče?
- **Formátování dat** – jak jsou uspořádána data v paketu? V jakém pořadí probíhá zpracování dat u přijímajících zařízení?
- **Detekce a oprava chyb** – co se stane v případě, že doručení paketu do cíle trvá příliš dlouho? Jak probíhá zotavení klienta, pokud nemůže krátkodobě navázat komunikaci se serverem?
- **Ukončení připojení** – jak jeden z hostitelů druhému sděluje, že komunikace skončila? Jaké závěrečné informace je nutné přenést, aby byla konverzace uzavřena správně?

Model OSI se sedmi vrstvami

Protokoly se dělí podle svých funkcí na základě referenčního modelu OSI, který představuje oborový standard. Model OSI dělí síťové komunikační procesy do sedmi samostatných vrstev (viz obrázek 1.1). Tento hierarchický model značně zjedno-

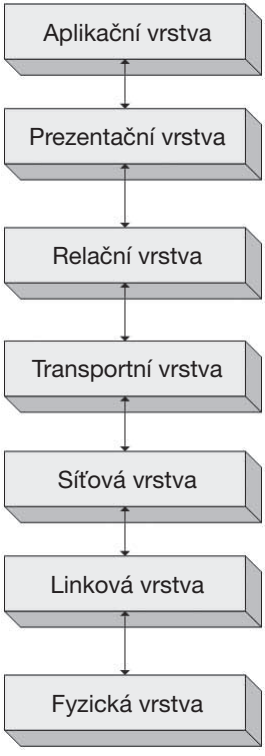
dušuje popis síťové komunikace. Aplikační vrstva nahoře představuje vlastní programy, které slouží pro přístup k síťovým prostředkům. Vespod se nachází fyzická vrstva, jejímž úkolem je přenášet síťová data po médiu. Díky spolupráci protokolů na sousedních vrstvách je zajištěno správné zpracování dat.

POZNÁMKA

Model OSI původně roku 1983 publikovala organizace ISO (International Organization for Standardization) jako svůj dokument označený ISO 7498. Model OSI je pouze doporučený oborový standard. Vývojáři protokolů nemají povinnost se jím přesně řídit. Síťový model OSI navíc nemá monopol. Někteří odborníci dávají přednost modelu amerického Ministerstva obrany (Department of Defense – DoD), který je také znám jako model TCP/IP.

Každá vrstva modelu OSI symbolizuje určitou funkci (viz dále):

- **Aplikační vrstva (vrstva 7)** – vrchní vrstva modelu OSI poskytuje uživatelům přístup k síťovým prostředkům. Koncoví uživatelé se obvykle setkávají pouze s touto vrstvou, která představuje rozhraní pro všechny jejich síťové činnosti.
- **Prezentační vrstva (vrstva 6)** – tato vrstva převádí přijatá data do formátu, který je čitelný pro aplikační vrstvu. Kódování a dekódování dat na této vrstvě závisí na protokolu aplikační vrstvy, který data odesílá nebo přijímá. Prezentační vrstva také obsluhuje některé metody šifrování a dešifrování, které slouží k zabezpečení dat.
- **Relační vrstva (vrstva 5)** – tato vrstva zajišťuje *dialog* neboli relaci mezi dvěma počítači. Navazuje, řídí a ukončuje toto připojení mezi všemi komunikujícími zařízeními. Relační vrstva také rozhoduje o tom, zda vzniká duplexní nebo poloduplexní připojení, a stará se, aby komunikace mezi hostiteli nebyla náhle přerušena, ale spořádaně ukončena.
- **Transportní vrstva (vrstva 4)** – primárním účelem transportní vrstvy je zajistit spolehlivé služby přenosu dat pro nižší vrstvy. Díky řízení toku, segmentaci a zpětnému spojování a kontrole chyb transportní vrstva zajišťuje, že se data dostanou do cíle bez chyb. Zabezpečení spolehlivého přenosu dat je značně složité, takže mu model OSI



Obrázek 1.1: Hierarchický pohled na sedm vrstev modelu OSI

věnuje celou vrstvu. Transportní vrstva využívá spojované i nespojované protokoly. Na této vrstvě fungují některé firewally a proxy servery.

- **Síťová vrstva (vrstva 3)** – tato vrstva odpovídá za směrování dat mezi fyzickými sítěmi a jedná se o jednu z nejkomplikovanějších vrstev modelu OSI. Jejím úkolem je logické adresování síťových hostitelů (např. pomocí IP adres). Obsluhuje také fragmentaci paketů a v některých případech i detekci chyb. Na této vrstvě fungují směrovače.
- **Linková vrstva (vrstva 2)** – tato vrstva umožňuje přenášet data po fyzické síti. Jejím hlavním úkolem je poskytnout adresní schéma, které umožní identifikovat fyzická zařízení (např. pomocí MAC adres). Mezi fyzická zařízení, které pracují na linkové vrstvě, se řadí mosty a přepínače.
- **Fyzická vrstva (vrstva 1)** – vrstva v základně modelu OSI symbolizuje fyzické médium, přes které se síťová data přenášejí. Tato vrstva definuje fyzické a elektrické vlastnosti veškerého použitého hardwaru, včetně hodnot napětí, rozbočovačů, síťových adaptérů, opakovačů a parametrů kabelů. Fyzická vrstva navazuje a ukončuje připojení, umožňuje sdílet komunikační prostředky a převádí digitální signály na analogové a naopak.

Tabulka 1.1 uvádí některé rozšířenější protokoly, které se používají na každé z jednotlivých vrstev modelu OSI.

Tabulka 1.1: Typické protokoly, které se používají na jednotlivých vrstvách modelu OSI

Vrstva	Protokol
Aplikační vrstva	HTTP, SMTP, FTP, Telnet
Prezentační vrstva	ASCII, MPEG, JPEG, MIDI
Relační vrstva	NetBIOS, SAP, SDP, NWLink
Transportní vrstva	TCP, UDP, SPX
Síťová vrstva	IP, IPX
Linková vrstva	Ethernet, Token Ring, FDDI, AppleTalk

Model OSI je sice pouze doporučeným standardem, ale měli byste jej znát zpaměti. V dalších kapitolách této knihy zjistíte, že na interakci protokolů různých vrstev závisí postup řešení síťových problémů. Potíže se směrovačem budete brzy označovat jako „problémy na vrstvě 3“ a chyby softwaru budou patřit do kategorie „problémy na vrstvě 7“.

POZNÁMKA

Když jsme diskutovali o své práci, zmínil se kolega o uživateli, který si stěžoval, že se nemůže připojit k síťovému prostředku. Problém spočíval v tom, že uživatel zadával chybné heslo. Kolega to komentoval jako „problém na vrstvě 8“. Vrstva 8 je neoficiální uživatelská vrstva. Odborníci, kteří pracují na úrovni paketů, tento termín často používají.

Jak se v modelu OSI přenášejí data? Přenos dat v síti začíná na aplikační vrstvě vysílajícího systému. Data postupují přes sedm vrstev modelu OSI směrem dolů, dokud se nedostanou na fyzickou vrstvu. V této fázi fyzická vrstva vysílajícího systému odešle data přijímajícímu systému. Přijímající systém vyzvedne data na své fyzické vrstvě a data postupují zbývajícími vrstvami tohoto systému až do aplikační vrstvy zcela nahoře.

Služby, které poskytují různé protokoly na jednotlivých vrstvách modelu OSI, nejsou redundantní. Pokud například protokol jedné vrstvy zajišťuje konkrétní službu, pak stejnou službu nemůže poskytovat žádný jiný protokol na libovolné jiné vrstvě. Protokoly na různých vrstvách sice mohou mít podobné vlastnosti, ale fungují poněkud odlišně.

Protokoly na odpovídající vrstvách odesílajících a přijímajících počítačů se vzájemně doplňují. Jestliže například za šifrování přenášených dat odpovídá protokol na vrstvě 7 odesílajícího počítače, očekává se, že data bude dešifrovat odpovídající protokol na vrstvě 7 přijímajícího počítače.

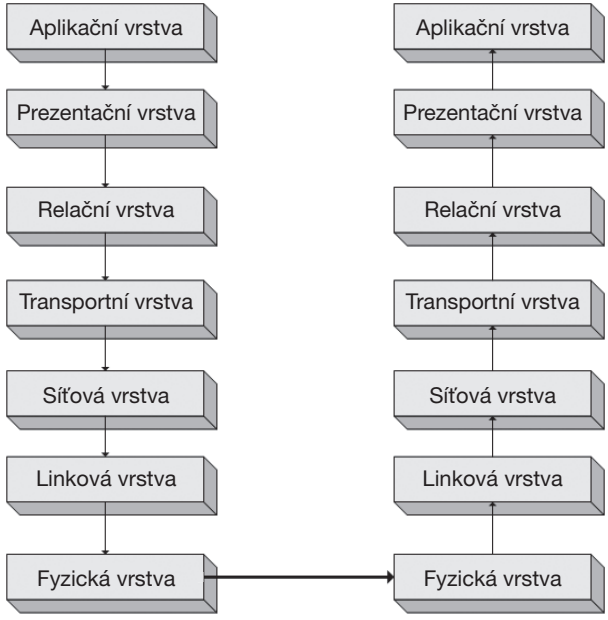
Obrázek 1.2 představuje grafické znázornění modelu OSI při komunikaci mezi dvěma klienty. Je zřejmé, že komunikace na straně jednoho klienta směřuje shora dolů a po dosažení druhého klienta postupuje opačným směrem zdola nahoru.

Každá vrstva modelu OSI dokáže komunikovat pouze s vrstvou přímo nad sebou a pod sebou. Vrstva 2 může například odesílat a přijímat pouze data z vrstev 1 a 3.

Zapouzdření dat

Protokoly na různých vrstvách modelu OSI komunikují pomocí *zapouzdření dat* (data encapsulation). Každá vrstva v sadě protokolů doplňuje k přenášeným datům hlavičku nebo patičku – dodatečné informační bity, které umožňují komunikaci mezi vrstvami. Když například transportní vrstva přijme data z relační vrstvy, přidá k těmto datům vlastní informace hlavičky a poté je předá další vrstvě.

Proces zapouzdření vytváří *datovou jednotku protokolu* (protocol data unit – PDU), která obsahuje odesílaná data a všechny doplňkové informace hlaviček a patiček. Když data postupují v modelu OSI směrem dolů, datová jednotka protokolu se



Obrázek 1.2: Protokoly fungují na stejných vrstvách odesílajícího i přijímajícího systému

postupně mění a zvětšuje, jak k ní jednotlivé protokoly přidávají vlastní hlavičky a patičky. Svou výslednou formu získává datová jednotka protokolu po dosažení fyzické vrstvy, kdy je odeslána cílovému počítači. Přijímající počítač pak z datové jednotky protokolu postupně odstraňuje hlavičky a patičky tak, jak data procházejí vrstvami modelu OSI směrem vzhůru. Když jednotka dosáhne vrchní vrstvy modelu OSI, zbývají z ní pouze původní data.

POZNÁMKA

Termín *paket* (packet) označuje úplnou datovou jednotku protokolu, která obsahuje informace hlaviček a patiček ze všech vrstev modelu OSI.

Pochopení principu zapouzdření nemusí být snadné. Podíváme se tedy na praktický příklad, který popisuje vznik, přenos a příjem paketu ve vztahu k modelu OSI. Pamatujte, že analytici se obvykle nezabývají relační ani prezentační vrstvou, takže budeme uvedené vrstvy v tomto příkladu (a zbývající části knihy) ignorovat.

V tomto scénáři se ze svého počítače pokoušíme zobrazit stránku `http://www.google.com/`. Aby bylo možné tuto akci provést, je nutné generovat paket s požadavkem, který je ze zdrojového klientského počítače odeslán cílovému serveru. Tento

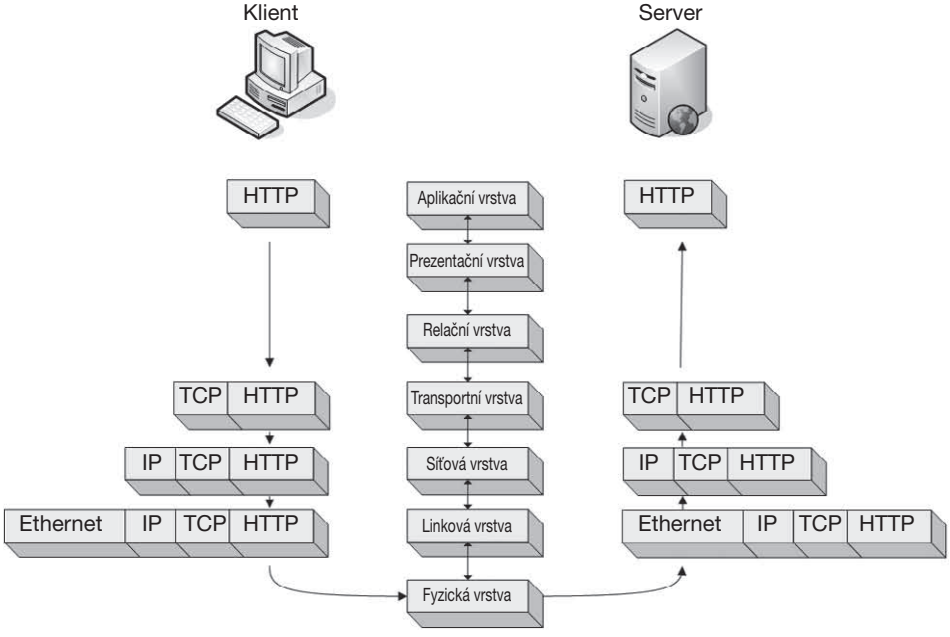
scénář předpokládá, že komunikační relace protokolu TCP/IP je již navázána. Proces zapouzdření dat v tomto příkladu je znázorněn na obrázku 1.3.

Začínáme na aplikační vrstvě svého klientského počítače. Prohlížíme si web a přitom používáme protokol aplikační vrstvy HTTP, který vydá příkaz ke stažení souboru `index.html` z adresy `google.com`.

Když protokol aplikační vrstvy definuje požadovanou akci, je potřeba zajistit přenos paketu do jeho cíle. Data v paketu jsou předána dolů zásobníku protokolů transportní vrstvy. HTTP je protokol aplikační vrstvy, který využívá protokolu TCP (je umístěn nad ním). TCP tedy slouží jako protokol transportní vrstvy, který zajišťuje spolehlivé doručení paketu. V souvislosti s tím je generována hlavička TCP. Tato hlavička TCP obsahuje pořadová čísla a další data připojená k paketu. Hlavička odpovídá za doručení paketu do cílového umístění.

POZNÁMKA

S ohledem na hierarchický návrh modelu OSI se často uvádí, že jeden protokol „leží“ na jiném. Aplikační protokol jako HTTP poskytuje určitou službu a přitom se spoléhá na protokol TCP. Na dalších stranách se dostaneme k tomu, že protokol DNS leží na protokolu UDP a protokol TCP na IP.



Obrázek 1.3: Grafické schéma zapouzdření dat mezi klientem a serverem

Když protokol TCP splní svou úlohu, předá paket protokolu IP, což je protokol vrstvy 3 odpovědný za logické adresování paketů. Protokol IP vytvoří hlavičku, která obsahuje logické adresní informace, a předá ji protokolu Ethernet na linkové vrstvě. V hlavičce protokolu Ethernet jsou uvedeny fyzické adresy sítě Ethernet. Paket je nyní kompletní a dostává se na fyzickou vrstvu, která jej po síti přenáší ve formě nul a jedniček.

Kompletní paket prochází kabely globální sítě a nakonec je doručen webovému serveru Google. Webový server postupuje při čtení paketu od spodních vrstev. Nejdříve tedy přečte data na linkové vrstvě, kde jsou k dispozici fyzické adresní informace sítě Ethernetu. Síťová karta pomocí nich zjistí, že je paket určen pro konkrétní server. Po svém zpracování jsou tyto informace vrstvy 2 odstraněny a nastává zpracování informací vrstvy 3.

Stejným způsobem jako u vrstvy 2 proběhne čtení adresních informací protokolu IP, které zajišťují správné adresování paketu a zabraňují jeho fragmentaci. Tato data jsou opět odstraněna, aby bylo možné pokračovat ve zpracování na další vrstvě.

Nyní jsou přečteny informace protokolu TCP vrstvy 4, které dovolují zjistit správné pořadí doručených paketů. Následně dojde k oddělení informací hlavičky vrstvy 4 a zůstanou pouze data aplikační vrstvy, která lze předat aplikaci webového serveru zajišťující činnost daného webu. V odpovědi na tento paket od klienta by měl server vyslat paket TCP s potvrzením, který klienta informuje o správném doručení jeho požadavku, a následně soubor `index.html`.

Bez ohledu na použité protokoly se všechny pakety vytvářejí a zpracovávají stejným způsobem jako v tomto příkladu. Zároveň však pamatujte, že některé síťové pakety jsou generovány protokoly jiné než aplikační vrstvy. Můžete se tedy setkat s pakety, které obsahují pouze informace protokolů vrstev 2, 3 a 4.

Síťový hardware

Podívejme se nyní na síťový hardware, který zajišťuje fungování sítě. Zaměříme se pouze na některé běžnější prvky síťového hardwaru: rozbočovače, přepínače a směrovače.

Rozbočovače

Rozbočovač (hub) obvykle vypadá jako krabice s více porty RJ-45, podobně jako zařízení NETGEAR na obrázku 1.4. Počet portů rozbočovačů se pohybuje od čtyř u malých zařízení až po 48 portů u velkého hardwaru pro umístění do racků v prostředí podnikových sítí.

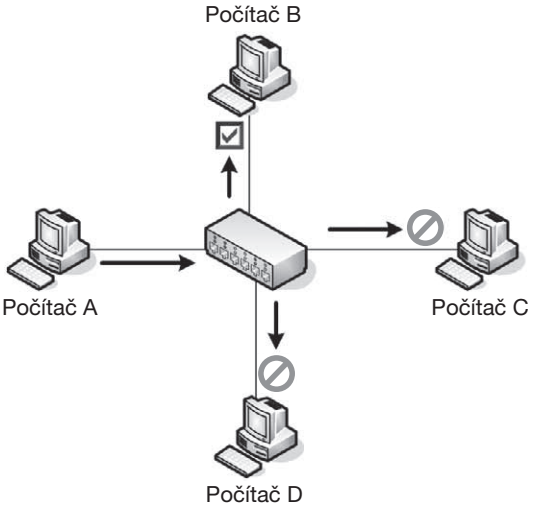
Vzhledem k tomu, že rozbočovače mohou generovat značný objem zbytečného síťového provozu a dokáží fungovat pouze v *poloduplexním režimu* (nemohou data sou-

časně odesílat i přijímat), obvykle se s nimi ve většině moderních či komplikovaných sítích nesetkáte (používají se místo nich přepínače). Přesto byste měli vědět, jak rozbočovače fungují, protože jsou velmi důležité při analýze paketů metodou „rozbočování" (hubbing out), kterou popíšeme v kapitole 2.

Obrázek 1.4: Typický ethernetový rozbočovač se 4 porty

Rozbočovač není nic jiného než *opakovací zařízení*, které funguje na fyzické vrstvě modelu OSI. Přebírá pakety odeslané z jednoho portu a vysílá je (opakuje) na všechny ostatní porty. Pokud například počítač připojený k portu 1 čtyřportového rozbočovače potřebuje odeslat data počítači na portu 2, rozbočovač tyto pakety odešle na porty 1, 2, 3 i 4. Klienti připojení k portům 3 a 4 analyzují pole MAC adresy (Media Access Control) v ethernetové hlavičce paketu a zjistí, že daný paket není určen pro ně, takže jej *zahodí* (drop). Obrázek 1.5 znázorňuje příklad, ve kterém počítač A vysílá data počítači B. Když počítač A vyšle tato data, přijmou je všechny počítače připojené k rozbočovači. Data však v praxi přijme pouze počítač B a ostatní počítače je ignorují.

Můžeme to přirovnat k situaci, kdy byste odeslali e-mail s předmětem „Určeno pro všechny zaměstnance oddělení marketingu" každému zaměstnanci podniku, a nikoli pouze těm, kteří skutečně pracují v příslušném oddělení. Pracovníci v oddělení marketingu by věděli, že e-mail je určen jim, a pravděpodobně by jej otevřeli. Jiní zaměstnanci by zjistili, že není pro ně, a nejspíš by jej smazali. Sami vidíte, že se přitom hodně zpráv přenáší zbytečně a plýtvá se časem na jejich zpracování. Právě tak ale rozbočovače fungují.



Obrázek 1.5: Síťový provoz při vysílání dat z počítače A počítači B pomocí rozbočovače

Nejlepší alternativu rozbočovačů v produkčních a hodně vytížených sítích představují *přepínače* (switch), což jsou *plně duplexní* zařízení, která mohou odesílat a přijímat data synchronně.