Obsah

Předmluva

Možná jste tím člověkem, který sedí před monitorem počítače, diví se, proč je připojení k Internetu pomalé jako hlemýžď, a touží proniknout bariérou výmluv, kterou před něj staví poskytovatel. Nebo jste možná počítačovým samoukem, který dostal práci v menší firmě proto, že zná rozdíl mezi rozbočovačem (hub) a přepínačem (switch), a očekává, že teď zodpovíme všechny jeho dotazy. Možná se ale skutečně zajímáte o síťování a chcete se dozvědět o tomto tématu něco víc, nebo se dokonce v tomto oboru stát specialistou. Nebo snad v oboru síťování platíte za uznávaného odborníka, který si chce jen doplnit něco málo, co mu ještě uniklo. V každém případě jste nejspíš zjistili, že materiály, z nichž byste mohli uceleně čerpat znalosti z oblasti síťování, často bohužel nejsou nijak utříděny, takže než se dozvíte, co v nějaké situaci v síti provést, musíte prostudovat hory papírů.

A aby síťování bylo ještě zajímavější, pak určitě budete mít k tomu všemu síť s klienty využívajícími jak Windows, tak Linux. Jestliže jako pomocníka hledáte knihu, jež vám k většině nejdůležitějších situací a problémů navrhne možná řešení, která vám navíc jasně vysvětlí všechny použitelné příkazy a možnosti konfigurace a navíc vás nebude příliš zatěžovat nekonečným teoretizováním a nesrozumitelnými dokumenty RFC, pak jste peníze za tuto knihu neutratili zbytečně.

Jak by měl vypadat typický čtenář?

V ideálním případě by měl mít čtenář této knihy alespoň nějaké zkušenosti s operačním systémem Linux. Měl by vědět, jak v Linuxu instalovat a odinstalovat programy, dále by měl zvládat procházení soubory a složkami na discích, spravovat oprávnění k souborům a složkám a vytvářet uživatele a skupiny. Dále se předpokládají zvládnuté základy protokolu TCP/IP a Ethernetu, znalost pojmů IPv4, IPv6, LAN, WAN, maska podsítě, směrovač (router), firewall, brána, přepínač (switch) a rozbočovač (hub). Pokud patříte mezi úplné začátečníky, doporučujeme prostudovat několik knih, které vám základní pojmy v oblasti síťování vysvětlí.

Pokud nemáte ani minimální znalosti Linuxu, pak vám doporučíme knihu *Ubuntu Příručka uživatele Linuxu* (Computer Press, 2008). Je sice zaměřena na konkrétní distribuci, ale vzhledem k tomu, že právě tato distribuce je určena úplným linuxovým začátečníkům, lze ji doporučit právě vám.[1]

[1] Poznámka českého vydavatele: Autorka publikace *Linux Kuchařka administrátora sítě*, Carla Schroder, se zde odkazuje na jinou svou knihu: *Linux Cookbook*. Protože v češtině bohužel nevyšla, dovolili jsme si nahradit ji jiným titulem, který stejně jako *Linux Cookbook* učí čtenáře používat systém Linux zcela od základu. Kromě navrženého titulu mohou začátečníci vzít do rukou knihu *Mandriva Linux Instalační a uživatelská příručka* od Ivana Bíbra. Dále velmi doporučujeme podívat se na adresu `http://knihy.cpress.cz/knihy/pocitacovaliteratura/linux/`, kde najdete seznam všech linuxových publikací nakladatelství Computer Press.

V této knize, kterou právě čtete, si přijdou na své nejen správci sítě nějaké firmy, ale i domácí uživatelé. Každý, kdo bude chtít proniknout do síťování v Linuxu, si bude moci vše v této knize vyzkoušet s několika obyčejnými počítači a cenově dostupným síťovým hardwarem.

Obsah knihy

Tato kniha obsahuje 19 kapitol a 3 přílohy.

Kapitola 1: Úvod do síťování v Linuxu

Tato kapitola nabídne na skutečně vysoké úrovni pohled na síťování počítačů, včetně kabeláže, směrování a přepínání, síťových rozhraní, různých typů internetových služeb a základů síťové architektury a výkonnosti sítě.

Kapitola 2: Vytvoření internetové brány na jednodeskovém počítači s operačním systémem Linux

V této kapitole vám představíme neuvěřitelně fascinující a adaptabilní svět Linuxu na routerboardech. V naší knize budeme používat výrobky od firem Soekris a PC Engines. Také vám ukážeme, jak Linux na těchto malých deskách poskytne daleko větší výkon a flexibilitu než komerční řešení, která jsou několikanásobně dražší.

Kapitola 3: Vytvoření firewallu v počítači s operačním systémem Linux

Zde se naučíte pro ochranu vaší sítě používat nejmocnější paketový filtr v Linuxu – iptables. Najdete zde úplné návody pro vytvoření hraničního firewallu, firewallu pro jeden počítač (single-host firewall), poskytování služeb prostřednictvím NAT (Network Address Translation – překlad síťových adres), blokování vnějšího přístupu k vnitřním službám, zabezpečený vzdálený přístup přes firewall a návod pro bezpečné testování nových firewallů před jejich nasazením v reálných podmínkách.

Kapitola 4: Vytvoření bezdrátového přístupového bodu v počítači s operačním systémem Linux

Linux a routerboard (či jiný klasický počítačový hardware) můžete použít i pro vytvoření bezpečného, výkonného, plně funkčního bezdrátového přístupového bodu upraveného podle vašich potřeb – včetně nejmodernějších metod pro ověřování a šifrování dat, názvových služeb, směrování a přemostění.

Kapitola 5: Vytvoření serveru VoIP využívajícího ústřednu Asterisk

Tato kapitola se snaží proniknout do základů zcela revolučního a velmi oblíbeného řešení – VoIP serveru Asterisk. Dnes samozřejmě není pro nikoho žádný problém pořídit si hezké a snadno ovladatelné grafické prostředí pro správu vašich systémů iPBX, ale možná vás bude zajímat, co se za těmito prostředími skrývá a jak to všechno funguje. V této kapitole se dozvíte, jak Asterisk nainstalujete a od základů nakonfigurujete. Popíšeme, jak vytvoříte uživatelská rozšíření a hlasovou poštu, jak spravovat vlastní pozdravy a zprávy, jak vysílat hlasovou poštu, poskytovat telefony, nastavit digitálního recepčního, provést integraci PSTN (Public Switched Telephone Network), vytvořit čisté VoIP, spravovat připojení „road warrior“ a mnoho dalšího.

Kapitola 6:
Směrování v Linuxu

Možnosti síťování v Linuxu jsou skutečně na vysoké úrovni, takže se nelze divit, že v něm najdete i podporu pro pokročilé směrování. Najdete zde návody pro vytvoření směrovačů postavených na Linuxu, návody pro výpočty podsítí (přesné a bezbolestné), blokování nevítaných návštěvníků pomocí „blackholingu“, používání statického a dynamického směrování a pro sledování vašich těžce pracujících směrovačů.

Kapitola 7:
Vzdálená správa zabezpečená pomocí SSH

OpenSSH je úžasná a velmi užitečná implementace velmi bezpečného protokolu SSH. Podporuje tradiční přihlašování pomocí hesel či hesel v kombinaci s veřejným klíčem a bezpečně přenáší data i přes nedůvěryhodné sítě. V této kapitole se dozvíte, jak toto všechno provést a navíc, jak se do systémů přihlásit ze vzdáleného počítače a jak chránit a posílit samo OpenSSH.

Kapitola 8:
Používání vzdálených ploch napříč platformami

OpenSSH je rychlé a uhlazené, navíc nabízí jak textovou konzolu, tak zabezpečený tunel X Windows pro spouštění grafických aplikací. Existuje několik skvělých aplikací (FreeNX, rdesktop či VNC), které nabízejí další možnosti, jako například vzdálenou pomoc, možnost výběru vzdálených ploch nebo použití Linuxu jako klienta služby Windows Terminal Server. Díky těmto nástrojům lze pomocí jedné klávesnice a myši ovládat několik počítačů, popřípadě třeba řídit třídu, kde stejnou vzdálenou relaci může pozorovat nebo podílet se na ní více uživatelů.

Kapitola 9:
Vytvoření virtuálních privátních sítí s OpenVPN napříč platformami

Určitě každému by se pozdávala bezpečná a uživatelsky přívětivá virtuální privátní síť (VPN). Okolo toho, co vlastně VPN je, existuje spousta omylů a nedorozumění. Řada komerčně dostupných produktů ve skutečnosti vůbec nejsou VPN, ale pouze portály SSL využívající omezené množství služeb. OpenVPN je skutečná VPN založená na SSL, která potřebuje, aby všechny koncové body byly důvěryhodné a která pro zabezpečení připojení a jeho udržování jako bezpečného a zašifrovaného používá pokročilé metody. OpenVPN obsahuje klienty pro Linux, Solaris, Mac OS X, OpenBSD, FreeBSD a NetBSD. V této kapitole se naučíte vytvořit a spravovat vaši vlastní PKI (Public Key Infrastructure – infrastrukturu veřejného klíče), která je pro bezbolestnou správu OpenVPN zcela zásadní. Také se dozvíte, jak bezpečně OpenVPN testovat, jak nastavit server a připojit klienty.

Kapitola 10:
Vytvoření serveru PPTP VPN v Linuxu

Tato kapitola obsahuje návod pro vytvoření a konfiguraci linuxového serveru PPTP VPN pro klienty využívající operační systémy Windows a Linux. Dozvíte se, jak upravit klienty Windows tak, aby dosáhli nezbytné úrovně podpory šifrování, jak tento server integrovat s Active Directory a jak dostat PPTP přes *iptables* firewall.

Kapitola 11:
Nasazení Samby ve smíšených Linux/Windows LAN

Použití Samby jako řadiče domény ve stylu Windows NT4 vám poskytne flexibilní, spolehlivý a levný prostředek pro ověření vašich klientů přihlašujících se do sítě. Naučíte se, jak provést migraci

z řadiče domény Windows na Sambu v Linuxu, jak provést migraci uživatelských účtů z Windows do Samby, dále jak integrovat klienty využívající Linux s Active Directory a jak klienty vůbec připojit.

Kapitola 12:
Centralizovaný síťový adresář s OpenLDAP

Adresář LDAP představuje skvělý mechanismus, na němž jsou založeny vaše síťové adresářové služby. Tato kapitola vám ukáže, jak od samotného začátku vytvořit adresář OpenLDAP, jak jej otestovat, jak v něm provádět změny, jak v něm hledat, jak urychlit vyhledávání pomocí inteligentního indexování a jak adresář OpenLDAP vyladit na maximální výkon.

Kapitola 13:
Sledování sítě pomocí systému Nagios

Nagios je skvělý systém na sledování sítě, jenž chytře využívá standardních příkazů Linuxu pro sledování služeb a hostů. V případě, když se vyskytnou problémy, tak vás okamžitě varuje. Výsledky vypovídající o stavu sítě jsou vyobrazeny v líbivých barevných grafech na stránkách ve formátu HTML, takže je můžete prohlížet v libovolném internetovém prohlížeči. V této kapitole se naučíte monitorovat základní stav systému a běžné servery, jako je DNS, webový a poštovní server. Také se dozvíte, jak bezpečně provádět vzdálenou správu systému Nagios.

Kapitola 14:
Sledování sítě pomocí MRTG

MRTG je sledování sítě využívající protokol SNMP, takže teoreticky může sledovat jakákoliv zařízení nebo služby, jež dokážou prostřednictvím tohoto protokolu komunikovat. V této kapitole se dozvíte, jak sledovat zařízení nebo služby a jak nalézt všechny potřebné informace pro vytvoření vlastních monitorů.

Kapitola 15:
Seznámení s protokolem IPv6

Ať chcete nebo ne, IPv6 je tady a možná již brzy nahradí protokol IPv4. Jděte s dobou a připravte se na použití protokolu IPv6 ve vaší síti a na Internetu. V této kapitole se dozvíte, proč jsou tyto tak dlouhé IP adresy protokolu IPv6 daleko jednodušší na správu než IP adresy protokolu IPv4, naučíte se, jak v IPv6 použít SSH a jak nastavit automatickou konfiguraci pro klienty, když nelze použít DHCP.

Kapitola 16:
Nastavení automatické síťové instalace nových operačních systémů

Fedora Linux a všechny jí příbuzné distribuce (Red Hat, CentOS, Mandriva, PC Linux OS atd.), dále Debian Linux a všichni jeho následovníci (Ubuntu, Mepis, Knoppix aj.), všechny tyto distribuce obsahují nástroje pro vytvoření a následné klonování vlastních instalací a pro poskytnutí nových operačních systémů prostřednictvím sítě. Stačí jen zapnout počítač a za několik minut máte hotovou instalaci, kterou můžete okamžitě používat. Tato kapitola popisuje, jak použít pro síťovou instalaci Fedory běžné obrazy ISO a jak vytvořit a účinně spravovat úplná místní zrcadla Debianu.

Kapitola 17:
Správa linuxového serveru pomocí sériové konzoly

Pokud se v síti Ethernet něco porouchá, pak nastává čas pro nasazení sériové konzoly. Ta vám ušetří spoustu času, ať už mluvíme o vzdálené nebo místní sériové konzole. Navíc pomocí sériové konzoly jsou často spravovány takové síťové prvky, jako jsou rozbočovače či přepínače. V této kapitole se dozvíte, jak nastavit počítač s operačním systémem Linux tak, aby dokázal přijímat sériová připojení, a jak používat jako terminál pro sériové připojení počítače s operačními systémy

Linux, Mac OS X či Windows. Zároveň se také naučíte, jak provádět správu serveru přes vytáčené připojení a jak přes sériovou linku posílat na server soubory.

Kapitola 18:
Spuštění serveru pro vytáčené připojení s operačním systémem Linux

Vytáčené připojení k serveru má svoje místo i v dnešním světě – a to i přesto, že svět za tu dobu urazil poměrně značný kus cesty směrem k připojení širokopásmovému (broadband connection). Nastavení sdílení připojení k Internetu přes vytáčené připojení, vytáčení na požádání, použití démona cron pro časové rozvržení při vytvoření relací vytáčeného připojení a nastavení většího počtu přihlašovacích účtů pro tento typ připojení – to vše je obsahem právě této kapitoly.

Kapitola 19:
Problémy se sítí a jejich řešení

Pro diagnostiku a řešení problémů v počítačových sítích najdete v Linuxu slušnou zásobu výkonných nástrojů. V této kapitole odhalíte všechny možnosti příkazu ping, naučíte se používat příkaz tcpdump a program Whireshark pro sledování provozu v síti a dozvíte se, jak vyřešit problémy s názvovým a poštovním serverem. Bezpochyby vás bude rovněž zajímat, jak zjistit, kteří uživatelé jsou k síti právě připojeni, jak vystopovat původ problémů v síti a jak nastavit zabezpečený centrální server pro přihlašování uživatelů. Představíme vám spoustu méně známých, ale schopných utilit – fping, httping, arping či mtr a prozradíme vám, jak přeměnit starý notebook na levného a přenosného pomocníka pro diagnostiku a opravu problémů v síti.

Příloha A:
Další literatura

Problematika počítačových sítí je tak rozsáhlá a široká, že rozhodně budete potřebovat pro ještě hlubší načerpání znalostí další literaturu. V této příloze najdete spoustu knih a dalších zdrojů, které vás seznámí se vším, co byste z této oblasti měli znát.

Příloha B:
Slovníček pojmů z oblasti počítačových sítí

Nevíte, co který pojem znamená? Pak se podívejte sem.

Příloha C:
Návod pro kompilaci vlastního jádra Linuxu

I jádro operačního systému Linux se neustále vyvíjí a rozšiřuje o další funkce. Není se tedy co divit, že může nastat potřeba zkompilovat si jádro vlastní, které bude obsahovat vše, co potřebujete. V této příloze se naučíte zkompilovat jádro v linuxových distribucích Fedora, Debian a vanilkové jádro.

Více k obsahu knihy

Budeme se zabývat jak staršími, tak novějšími technikami. Ke starším technikám bude patřit správa systému pomocí sériové konzoly, vytáčené připojení k síti, vybudování internetové brány, sítě VLAN, způsoby zabezpečeného vzdáleného připojení, směrování a sledování provozu v síti. Co se týče novějších technik, ty zahrnují vytvoření vlastního iPBX s využitím ústředny Asterisk, bezdrátové připojení, používání vzdálených ploch napříč platformami, bezobslužná síťová instalace nových operačních systémů, zjednodušené přihlašování v počítačových sítích s klienty na bázi Linuxu a Windows a konečně základy protokolu IPv6. Zároveň v knize najdete i kapitoly týkající se sledování, varování a řešení problémů.

Linuxové distribuce použité v této knize

Na světě existují stovky, ne-li tisíce linuxových distribucí. Mezi ně se řadí tzv. live distribuce, které jsou distribuovány na všech možných druzích bootovatelných médií – počínaje firemními CD disky a vyměnitelnými disky USB, až po standardní CD či DVD. K tomu existuje celá řada distribucí pro běžné použití, dále specializované distribuce určené pro firewally, směrovače či staré počítače a nesmíme zapomenout na distribuce zaměřující se na multimédia, vědce, klastrové (nebo clusterové, podle vkusu) distribuce, distribuce, které dokážou spustit aplikace určené pro Windows, a v neposlední řadě distribuce pro zabezpečení počítačů a dat. Není v našich silách se o všech těchto distribucích rozepisovat. Naštěstí se svět linuxových distribucí dá zhruba rozdělit do dvou táborů – Red Hat Linux a Debian Linux. Tyto distribuce jsou považovány za základní a slouží jako inspirace pro vytváření další spousty odvozenin či klonů.

V této knize bude oblast Red Hatu zastupovat distribuce Fedora, což je distribuce vyvíjená zdarma skupinou vývojářů a je sponzorována Red Hatem. Fedora je dostupná zdarma a jádro distribuce obsahuje pouze volně šiřitelný software. Navíc má daleko kratší interval vydávání nových verzí než třeba Red Hat Enterprise Linux (RHEL). RHEL má v současnosti interval vydávání nových distribucí 18 měsíců, je navržen tak, aby byl stabilní a předvídatelný, a nemá žádnou zdarma šířenou balíčkovou verzi, ačkoliv existuje spousta klonů vytvořených právě z této distribuce. Tyto klony se vytváří z balíčků RHEL SRPM, z nichž se odstraní obchodní značka Red Hat. Mezi linuxové distribuce založené na RHEL patří kupříkladu CentOS, White Box Linux, Lineox, White Box Enterprise Linux, Tao Linux či Pie Box Linux.

Kromě toho se dá vybírat ještě z poměrně slušného množství distribucí odvozených od Red Hatu – klasickými zástupci jsou distribuce Mandriva či PCLinuxOS. Všechny návody pro Fedoru budou tedy fungovat i v těchto distribucích, i když u názvů souborů, jejich umístění či názvů balíčků je možné očekávat drobné odchylky.

Linuxových distribucí založených na Debianu je jako hub po dešti – Ubuntu, Kubuntu, Edubuntu, Xandros, Mepis, Knoppix, Kanotix či Linspire. A to je jen několik z nich. Všechny sice mají svoje vlastní vylepšení a modifikace, nicméně správa balíčků pomocí příkazu `aptitude` nebo Synaptic funguje ve všech.

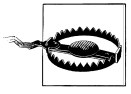
Distribuce Novell/SUSE je podobně jako Red Hat založená na RPM, nicméně vždy šla svou vlastní cestou. Své vlastní místečko na slunci mají i Gentoo a Slackware. Nemá ani smysl pokoušet se vyjmenovat všechny distribuce, nicméně k naprosté většině distribucí existuje poměrně slušná dokumentace a také aktivní a ochotné komunity uživatelů a obecně se od sebe nijak výrazně neliší.

Konvence použité v knize

- *Kurziva* – Kurzivou v knize budeme vyznačovat cesty, názvy souborů, programů a internetové adresy (adresy URL i názvy domén). Stejně budeme označovat i nové pojmy, které budeme definovat.
- `Neproporcionální písmo` – Toto písmo použijeme pro výstup z programů a pro názvy a klíčová slova v příkladech.
- *`Neproporcionální písmo s kurzivou`* – Toto písmo použijeme pro volitelné parametry či prvky v okamžiku, kdy budeme popisovat syntaxi příkazu.
- Neproporcionální písmo vyznačené tučně – Toto písmo použijeme pro příkazy, které by měly být psány doslovně, a také pro zvýraznění ve zdrojovém kódu programu či konfiguračních souborech.

U příkazů Unixu/Linuxu, které budou zadávány aktuálně přihlášeným uživatelem, bude příkazový řádek obsahovat přihlašovací jméno tohoto uživatele ukončené znakem dolaru (`$`). Příkazy, které se musí zadat pod uživatelem `root`, budou na příkazovém řádku obsahovat slovo root ukončené mřížkou (#). V praxi doporučujeme pro příkazy, které mají být vykonány pod uživatelským účtem `root`, použít příkaz `sudo` zadaný pod uživatelem se standardním oprávněním. Je to jednodušší, než kdybyste se museli odhlašovat a pak přihlašovat jako `root`. Ve všech případech bude příkazový řádek obsahovat uživatelské jméno, název počítače a aktuální pracovní adresář, v němž se právě pohybujete (například `root@xena:/var/llibftpboot #`).

Tato ikonka ukazuje na tip, upozornění nebo poznámku.



Tato ikonka označuje upozornění nebo varování.

Použití ukázkových příkladů

Tato kniha je tu od toho, aby vám usnadnila práci. Obecně vzato můžete ve svých programech a dokumentaci použít zdrojový kód, který v této knize najdete. Není nutno nás ani žádat o povolení použít tyto kódy, pokud se ovšem nechystáte kopírovat většinu zdrojového kódu. Konkrétně pro psaní programu, v němž použijete několik řádků kódu z naší knihy, nemusíte žádat o povolení. Naopak prodej a distribuce disku CD-ROM, který by obsahoval příklady z této knihy, však již povolení vyžaduje. Podobně při odpovědi na nějakou otázku, kde použijete citaci z této knihy a kód programu, se povolení nevyžaduje. Na druhou stranu použití většího počtu příkladů z této knihy, třeba v dokumentaci k vašemu produktu, již povolení *vyžaduje*.

Budeme vám velmi vděčni, pokud použijete přesný název knihy. Takový název obvykle obsahuje titul knihy, autora, vydavatele a ISBN. Pro tuto knihu by tedy přesný název byl: *„Linux Networking Cookbook*, Carla Schroder. Copyright 2008 O'Reilly Media, Inc., 978-0-596-10249-7".

Pokud nebudete mít jasno, v jakém rozsahu platí naše povolení o dalším šíření příkladů v této knize, pak nás neváhejte kontaktovat na adrese `permissions@oreilly.com`.

Materiály a poznámky ke knize

Tato kniha i přes velmi pečlivou korekturu provedenou jak autorem, tak redaktory z nakladatelství O'Reilly, může obsahovat chyby, nepřesnosti či nesrovnalosti. Pokud některé z nich objevíte, budeme velmi rádi, pokud nám o nich dáte vědět e-mailem na adresu `netcookbook@bratgrrl.com`. Na stejné adrese přivítáme i vaše náměty. Vše pak zahrneme do případného dalšího vydání. Aktualizace, opravy chyb a všechny skripty použité v knize pak naleznete na internetové adrese `http://www.oreilly.com/catalog/9780596102487`.

Připomínky a dotazy

Připomínky a dotazy týkající se této knihy prosím zasílejte vydavateli na adresu:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (USA a Kanada)
707-829-0515 (ostatní státy)
707-829-0104 (fax)

Tato kniha má i svoje internetové stánky, na nichž najdete příklady, nalezené chyby a další informace. Internetové stránky najdete na adrese:

`http://www.oreilly.com/catalog/9780596102487`

Připomínky nebo otázky technického charakteru prosím směrujte na e-mailovou adresu:

`bookquestions@oreilly.com`

Další informace o knihách vydávaných naším vydavatelstvím, o konferencích a síti O'Reilly Network najdete na internetové adrese:

`http://www.oreilly.com`

Poznámka redakce českého vydání

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

Computer Press
redakce PC literatury
Holandská 8
639 00 Brno

nebo

`knihy@cpress.cz`

Další informace a případné opravy českého vydání knihy najdete na internetové adrese `http://knihy.cpress.cz/K1590`. Prostřednictvím uvedené adresy můžete též naší redakci zaslat komentář nebo dotaz týkající se knihy. Na vaše reakce se srdečně těšíme.