

<b>Předmluva</b>	<b>13</b>
Jak by měl vypadat typický čtenář?	13
Obsah knihy	14
Více k obsahu knihy	17
Linuxové distribuce použité v této knize	18
Konvence použité v knize	18
Použití ukázkových příkladů	19
Materiály a poznámky ke knize	19
Připomínky a dotazy	20
Poznámka redakce českého vydání	20
<b>1. Úvod do síťování v Linuxu</b>	<b>21</b>
<b>2. Vytvoření internetové brány na jednodeskovém počítači s operačním systémem Linux</b>	<b>31</b>
2.1 Seznámení s jednodeskovým počítačem Soekris 4521	33
2.2 Konfigurace většího počtu profilů v programu Minicom	36
2.3 Instalace Pyramid Linuxu na kartu Compact Flash	36
2.4 Síťová instalace Pyramid Linuxu pomocí serveru s Debianem	37
2.5 Síťová instalace Pyramid Linuxu pomocí serveru s Fedorou	40
2.6 Spuštění linuxové distribuce Pyramid	42
2.7 Vyhledání a úprava souborů distribuce Pyramid Linux	44
2.8 Zabezpečení nainstalovaného Pyramid Linuxu	45
2.9 Získání a instalace nejnovější verze Pyramid Linuxu	46
2.10 Přidání dalšího softwaru do Pyramid Linuxu	47
2.11 Instalace ovladačů pro nový hardware	50
2.12 Úprava jádra Pyramid Linuxu	50
2.13 Aktualizace comBIOSu Soekrisu	51
<b>3. Vytvoření firewallu v počítači s operačním systémem Linux</b>	<b>55</b>
3.1 Sestavení zařízení fungujícího jako firewall s operačním systémem Linux	61

3.2	Konfigurace síťových adaptérů v Debianu	63
3.3	Konfigurace síťových adaptérů ve Fedoře	65
3.4	Identifikace síťového adaptéru	67
3.5	Nastavení sdílení internetového připojení na firewallu s dynamickou IP adresou na rozhraní WAN	68
3.6	Nastavení sdílení internetového připojení na firewallu se statickou IP adresou na rozhraní WAN	72
3.7	Zobrazení stavu firewallu	73
3.8	Vypnutí iptables firewallu	74
3.9	Spuštění iptables při startu systému a manuální zapínání a vypínání firewallu	76
3.10	Testování firewallu	78
3.11	Konfigurace firewallu pro vzdálenou správu přes SSH	81
3.12	Povolení vzdálené SSH správy přes NAT firewall	82
3.13	Získání více hostitelských SSH klíčů za firewallem využívajícím službu NAT	84
3.14	Spuštění veřejných služeb na zařízeních s privátními IP adresami	85
3.15	Nastavení firewallu na jednom počítači	87
3.16	Nastavení firewallu na serveru	91
3.17	Konfigurace protokolování iptables	94
3.18	Zadávání pravidel pro odchozí síťový provoz	95

## **4. Vytvoření bezdrátového přístupového bodu v počítači s operačním systémem Linux**

**99**

4.1	Vybudování bezdrátového přístupového bodu postaveného na Linuxu	103
4.2	Přemostění z bezdrátového připojení do drátového připojení	104
4.3	Nastavení názvových služeb	106
4.4	Nastavení statických IP adres ze serveru DHCP	109
4.5	Konfigurace klientů v Linuxu a ve Windows – klienti používají statické IP adresy nastavené přes DHCP	110
4.6	Přidání poštovního serveru do dnsmasq	112
4.7	Jak předělat WPA2-Personal tak, aby byl stejně výkonný jako WPA-Enterprise	113
4.8	Ověřování pomocí serveru RADIUS na úrovni Enterprise	116
4.9	Konfigurace bezdrátového přístupového bodu pro použití se serverem FreeRADIUS	120
4.10	Ověřování klientů na FreeRADIUS	121
4.11	Připojení k Internetu a používání firewallu	122
4.12	Používání směrování namísto přemostění	123
4.13	Testování bezdrátového síťového adaptéru	128
4.14	Změna názvu směrovače s Pyramid Linuxem	129
4.15	Vypnutí režimu diverzity u antény	130
4.16	Správa vyrovnávací paměti DNS nástroje dnsmasq	131
4.17	Správa vyrovnávací paměti ve Windows	134
4.18	Aktualizace času při spuštění systému	136

## **5. Vytvoření serveru VoIP využívajícího ústřednu Asterisk 137**

---

5.1	Instalace Asterisku ze zdrojového kódu	141
5.2	Instalace Asterisku v Debianu	144
5.3	Spuštění a ukončení Asterisku	146
5.4	Testování serveru Asterisk	148
5.5	Přidání rozšíření pro telefonování do Asterisku a zahajování hovorů	149
5.6	Nastavení softwarových telefonů	155
5.7	Začínáme volat přes VoIP	157
5.8	Připojení pobočkové telefonní ústředny Asterisk k analogovým telefonním linkám	160
5.9	Vytvoření digitálního recepčního	162
5.10	Nahrávání vlastních hlášení	164
5.11	Udržování „Zprávy dne“	167
5.12	Předávání hovorů	169
5.13	Směrování hovorů do telefonních skupin	169
5.14	Parkování hovorů	170
5.15	Nastavení hudby při čekání na spojení	171
5.16	Přehrávání souborů ve formátu MP3 v Asterisku	172
5.17	Rozesílání hlasových zpráv uživatelům	172
5.18	Používání konferencí v Asterisku	174
5.19	Sledování konferencí	175
5.20	Průchod síťového provozu využívajícího protokol SIP přes iptables NAT firewallly	176
5.21	Průchod síťového provozu využívajícího protokol IAX přes iptables NAT firewallly	178
5.22	Nasazení AsteriskNOW neboli „Asterisk za 30 minut“	179
5.23	Instalace a odstranění balíčků v AsteriskNOW	180
5.24	Připojení vzdálených uživatelů a zaměstnanců, kteří jsou neustále na cestách	181

## **6. Směrování v Linuxu 183**

---

6.1	Počítání podsítí pomocí nástroje ipcalc	185
6.2	Nastavení výchozí brány	187
6.3	Konfigurace jednoduchého místního směrovače	190
6.4	Konfigurace nejjednodušší varianty sdílení internetového připojení	192
6.5	Konfigurace statického směrování přes několik podsítí	194
6.6	Trvalé nastavení statických cest	195
6.7	Používání dynamického směrování pomocí protokolu RIP v Debianu	196
6.8	Používání dynamického směrování pomocí protokolu RIP ve Fedoře	200
6.9	Použití příkazového řádku Quagga	200
6.10	Vzdálené přihlašování do démonů Quagga	202
6.11	Spouštění démonů Quagga z příkazového řádku	204
6.12	Sledování RIPD	205
6.13	Odpojení cest pomocí démonu Zebra	206
6.14	Používání protokolu OSPF pro jednoduché dynamické směrování	207

6.15	Zvýšení zabezpečení při používání protokolů RIP a OSPF	209
6.16	Sledování OSPFD	210

## **7. Vzdálená správa zabezpečená pomocí SSH** **213**

7.1	Spuštění a zastavení OpenSSH	215
7.2	Vytváření silných hesel	216
7.3	Nastavení hostitelského klíče pro nejjednodušší způsob ověření	217
7.4	Vytvoření a kopírování klíčů SSH	219
7.5	Použití ověření pomocí veřejného klíče na ochranu hesel pro přihlášení do systému	221
7.6	Správa většího počtu klíčů identity	222
7.7	Zvýšení zabezpečení OpenSSH	223
7.8	Změna hesla	224
7.9	Získání otisku klíče	224
7.10	Kontrola syntaxe pro soubor s konfigurací	225
7.11	Použití konfiguračních souborů klienta OpenSSH pro snadnější přihlašování	225
7.12	Bezpečné tunelování X Windows přes SSH	227
7.13	Spuštění příkazů bez otevření příkazového řádku na vzdáleném počítači	228
7.14	Používání popisků pro označení klíčů	229
7.15	Použití DenyHosts jako ochrany proti útokům na SSH	229
7.16	Vytvoření spouštěcího souboru pro DenyHosts	231
7.17	Připojení celých vzdálených souborových systémů pomocí nástroje sshfs	232

## **8. Používání vzdálených ploch napříč platformami** **235**

8.1	Připojení k Windows z Linuxu pomocí nástroje rdesktop	237
8.2	Vytváření a správa SSH klíčů pro FreeNX	239
8.3	Použití aplikace FreeNX pro připojení k počítači s Linuxem z počítače s Windows	240
8.4	Použití FreeNX pro přístup k počítači s Linuxem z operačních systémů Solaris, Mac OS X nebo Linux	244
8.5	Správa uživatelů FreeNX	245
8.6	Sledování uživatelů Nxclient ze serveru FreeNX	246
8.7	Spuštění a zastavení serveru FreeNX	247
8.8	Nastavení vlastní pracovní plochy	248
8.9	Vytváření dalších relací Nxclient	250
8.10	Sledování relací Nxclient pomocí NX Session Administrator	251
8.11	Povolení sdílení souborů a tiskáren, použití a povolení multimédií v aplikaci Nxclient	251
8.12	Jak zabránit uložení hesla v Nxclientovi	252
8.13	Řešení problémů s FreeNX	253
8.14	Použití VNC pro připojení k počítači s Windows z počítače s Linuxem	254
8.15	Využití VNC pro současné ovládání počítačů s Windows a Linuxem	255
8.16	Použití VNC pro vzdálenou správu počítače s Linuxem z počítače se stejným operačním systémem	257
8.17	Zobrazení stejné pracovní plochy Windows více vzdáleným uživatelům	259

8.18	Změna hesla pro server VNC v Linuxu	261
8.19	Úprava pracovní plochy pro vzdálené připojení přes VNC	261
8.20	Nastavení velikosti vzdálené plochy u VNC	263
8.21	Připojení VNC k existující relaci X	264
8.22	Bezpečné tunelování x11vnc přes SSH	265
8.23	Tunelování TightVNC mezi počítači s Linuxem a Windows	266

## **9. Vytvoření virtuálních privátních sítí s OpenVPN napříč platformami** **269**

---

9.1	Vytvoření bezpečného testovacího prostředí pro OpenVPN	271
9.2	Spuštění a testování OpenVPN	274
9.3	Testování šifrování pomocí statických klíčů	276
9.4	Připojení vzdáleného klienta s operačním systémem Linux pomocí statických klíčů	278
9.5	Vytvoření vlastního PKI pro OpenVPN	280
9.6	Konfigurace serveru OpenVPN pro více klientů	282
9.7	Nastavení OpenVPN tak, aby se spouštělo při startu	284
9.8	Odvolání certifikátů	285
9.9	Nastavení serveru OpenVPN v režimu mostu	287
9.10	Spuštění OpenVPN uživatelem bez oprávnění	288
9.11	Připojení klientů s operačním systémem Windows	289

## **10.Vytvoření serveru PPTP VPN v Linuxu** **291**

---

10.1	Instalace serveru Poptop v linuxové distribuci Debian	294
10.2	Aktualizace jádra Debianu pro integraci podpory MPPE	295
10.3	Instalace serveru Poptop v linuxové distribuci Fedora	296
10.4	Aktualizace jádra Fedory pro integraci podpory MPPE	297
10.5	Konfigurace samostatného serveru PPTP VPN	298
10.6	Přidání serveru Poptop do Active Directory	301
10.7	Připojení klientů s operačním systémem Linux k serveru PPTP	302
10.8	Konfigurace iptables firewallu pro použití se serverem PPTP	303
10.9	Sledování činnosti serveru PPTP	304
10.10	Řešení potíží s PPTP	305

## **11.Nasazení Samby ve smíšených Linux/Windows LAN** **309**

---

11.1	Ověření, že máte připraveno vše potřebné	311
11.2	Kompilace Samby ze zdrojového kódu	313
11.3	Spuštění a zastavení Samby	315
11.4	Použití Samby jako primárního řadiče domény	316
11.5	Migrace z primárního řadiče domény ve Windows NT4 na primární řadič domény v Sambě	320
11.6	Přidání počítače s Linuxem do domény Active Directory	322
11.7	Připojení počítače s Windows 95/98/ME do domény Samby	325

11.8	Připojení počítače s Windows NT4 do domény Samby	326
11.9	Připojení Windows NT/2000 k doméně Samba	327
11.10	Připojení Windows XP k doméně Samba	327
11.11	Připojení počítačů s Linuxem k doméně Samba pomocí programů pracujících na příkazovém řádku	328
11.12	Připojení počítačů s Linuxem k doméně Samba pomocí programů pracujících v grafickém rozhraní	331

---

## **12. Centralizovaný síťový adresář s OpenLDAP** **335**

12.1	Instalace OpenLDAP v Debianu	341
12.2	Instalace OpenLDAP ve Fedoře	343
12.3	Nastavení a testování serveru OpenLDAP	344
12.4	Vytvoření nové databáze ve Fedoře	346
12.5	Přidání dalších uživatelů do adresáře	349
12.6	Oprava záznamů v adresáři	351
12.7	Připojení ke vzdálenému serveru OpenLDAP	354
12.8	Hledání v adresáři OpenLDAP	354
12.9	Indexování vaší databáze	356
12.10	Správa adresáře v grafickém rozhraní	358
12.11	Konfigurace Berkeley DB (BDB)	360
12.12	Nastavení protokolování v OpenLDAP	364
12.13	Zálohování adresáře a jeho obnovení ze zálohy	365
12.14	Vylepšování řízení přístupu	367
12.15	Změna hesla	370

---

## **13. Sledování sítě pomocí systému Nagios** **373**

13.1	Instalace Nagiosu ze zdrojových souborů	374
13.2	Konfigurace Apache pro Nagios	377
13.3	Rozumná organizace konfiguračních souborů Nagiosu	380
13.4	Konfigurace Nagiosu pro monitorování počítače localhost	381
13.5	Nastavení oprávnění CGI pro úplný přístup ke všem položkám webového rozhraní	390
13.6	Spuštění Nagiosu při startu systému	392
13.7	Přidání dalších uživatelů Nagiosu	392
13.8	Urychlení Nagiosu pomocí check_icmp	393
13.9	Sledování SSHD	394
13.10	Sledování webového serveru	397
13.11	Sledování poštovního serveru	400
13.12	Používání skupin služeb (servicegroups) pro seskupení příbuzných služeb	402
13.13	Sledování názvových služeb	403
13.14	Konfigurace vzdálené zabezpečené správy Nagiosu pomocí OpenSSH	404
13.15	Konfigurace vzdálené zabezpečené správy Nagiosu pomocí OpenSSL	405

## **14.Sledování sítě pomocí MRTG**

**407**

---

14.1	Instalace MRTG	408
14.2	Konfigurace SNMP v Debianu	409
14.3	Konfigurace SNMP ve Fedoře	411
14.4	Konfigurace služby HTTP pro nasazení MRTG	412
14.5	Konfigurace a spuštění MRTG v Debianu	413
14.6	Konfigurace a spuštění MRTG ve Fedoře	415
14.7	Sledování zatížení aktivního CPU	416
14.8	Sledování nevyužitého času procesoru nebo času využitého uživatelem	419
14.9	Sledování fyzické paměti	421
14.10	Sledování odkládacího souboru a paměti	422
14.11	Sledování využití disku	423
14.12	Sledování připojení TCP	424
14.13	Vyhledávání a testování MIB a OID	425
14.14	Testování vzdálených dotazů SNMP	427
14.15	Sledování vzdálených klientů	428
14.16	Vytvoření většího počtu indexových stránek MRTG	429
14.17	Spuštění MRTG jako démona	430

## **15.Seznámení s protokolem IPv6**

**433**

---

15.1	Testování podpory IPv6 na počítači s Linuxem	438
15.2	Použití příkazu ping pro zařízení připojená v síti využívající IPv6	439
15.3	Nastavení adres typu Unique Local Unicast na jednotlivých síťových rozhraních	440
15.4	Použití SSH v kombinaci s IPv6	441
15.5	Kopírování souborů příkazem scp přes protokol IPv6	442
15.6	Automatická konfigurace adres IPv6	443
15.7	Výpočet adres IPv6	444
15.8	Použití IPv6 v Internetu	445

## **16.Nastavení automatické síťové instalace nových operačních systémů**

**447**

---

16.1	Vytvoření spouštěcího disku pro síťovou instalaci linuxové distribuce Fedora	448
16.2	Síťová instalace Fedory za použití spouštěcího média	450
16.3	Konfigurace serveru pro instalaci Fedory založeného na HTTP	452
16.4	Konfigurace serveru pro instalaci Fedory založeného na FTP	453
16.5	Vytvoření vlastní instalace Fedory	455
16.6	Použití souboru Kickstart pro bezobslužnou instalaci Fedora Linuxu	457
16.7	Síťová instalace Fedory s využitím PXE Netboot	458
16.8	Síťová instalace Debianu	460
16.9	Vytvoření úplného zrcadla Debianu pomocí příkazu apt-mirror	461
16.10	Vytvoření částečného zrcadla Debianu pomocí příkazu apt-proxy	463

---

16.11	Nastavení běžných počítačů tak, aby mohly používat vaše místní zrcadlo	465
16.12	Konfigurace Debian PXE Netboot serveru	466
16.13	Instalace operačních systémů na počítače z místního zrcadla Debianu	467
16.14	Automatizace instalace Debianu pomocí souborů preseed	468

## **17. Správa linuxového serveru pomocí sériové konzoly** **471**

---

17.1	Příprava serveru pro správu přes sériovou konzolu	472
17.2	Konfigurace serveru bez klávesnice a monitoru se zavaděčem LILO	475
17.3	Konfigurace serveru bez klávesnice a monitoru se zavaděčem GRUB	478
17.4	Spuštění Debianu v textovém režimu	480
17.5	Konfigurace sériové konzoly	481
17.6	Konfigurace serveru pro správu pomocí vytáčeného připojení	484
17.7	Navázání spojení se serverem pomocí vytáčeného připojení	486
17.8	Nastavení zabezpečení	488
17.9	Konfigurace protokolování	489
17.10	Ukládání souborů na server	490

## **18. Spuštění serveru pro vytáčené připojení s operačním systémem Linux** **493**

---

18.1	Konfigurace jednoho účtu pro vytáčené připojení pomocí nástroje WvDial	493
18.2	Konfigurace více účtů v programu WvDial	496
18.3	Konfigurace oprávnění pro vytáčené připojení u běžných uživatelů	497
18.4	Vytvoření účtů běžných uživatelů pro program WvDial	498
18.5	Sdílení účtu pro vytáčené připojení	499
18.6	Konfigurace vytáčení na požádání	500
18.7	Nastavení dostupnosti vytáčeného připojení příkazem cron	502
18.8	Vytáčení přes přerušované tóny hlasové pošty	503
18.9	Potlačení funkce čekání hovorů	504
18.10	Umístění hesla mimo konfigurační soubor	504
18.11	Vytvoření zvláštního souboru protokolu pppd	505

## **19. Problémy se sítí a jejich řešení** **507**

---

19.1	Vytvoření notebooku pro diagnostiku a opravy sítě	508
19.2	Testování konektivity pomocí nástroje ping	510
19.3	Zjišťování struktury sítě pomocí nástrojů Fping a Nmap	512
19.4	Vyhledávání duplicitních IP adres pomocí nástroje arping	514
19.5	Testování propustnosti a zpoždění nástrojem httpping	515
19.6	Používání nástrojů traceroute, tcptraceroute a mtr pro zjišťování problémů v sítích	517
19.7	Použití nástroje tcpdump pro zachycení a analýzu síťového provozu	520
19.8	Sledování příznaků TCP (TCP Flags) pomocí utility tcpdump	523
19.9	Měření propustnosti, kolísání a ztráty paketů pomocí nástroje iperf	525
19.10	Používání utility ngrep pro pokročilé sledování paketů	528



19.11	Používání nástroje ntop pro rychlé sledování sítě v barevném provedení	530
19.12	Řešení problémů se servery DNS	532
19.13	Řešení problémů s klienty DNS	535
19.14	Řešení problémů se servery SMTP	536
19.15	Řešení problémů se servery POP3, POP3s a IMAP	538
19.16	Vytvoření klíčů SSL pro server Syslog-ng v Debianu	541
19.17	Vytvoření klíčů SSL pro server Syslog-ng ve Fedoře	546
19.18	Nastavení nástroje stunnel pro Syslog-ng	547
19.19	Vytvoření serveru Syslog	549

---

**A. Další literatura** **553**

---

	Česky psaná nebo do češtiny přeložená literatura	556
--	--	-----

---

**B. Slovníček pojmů z oblasti počítačových sítí** **557**

---

**C. Návod pro kompilaci vlastního jádra Linuxu** **579**

---

	Kompilace vlastního jádra	579
--	---------------------------	-----

---

**Rejstřík** **587**

---



---

# Předmluva

Možná jste tím člověkem, který sedí před monitorem počítače, dívá 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 souborů 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.<sup>1</sup>

---

<sup>1</sup> 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 prostředím 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 nevíтанých 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 systému 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 chytrě 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. Svě vlastní místočko 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

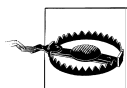
- *Kurziva* – Kurzivou v knize budeme vyznačovat cesty, názvy souborů, programů a internetové adresy (adresy URL i názvy domén). Stejně budeme označovat i nové pojmy, které budeme definovat.
- *Neproporcionální písmo* – Toto písmo použijeme pro výstup z programů a pro názvy a klíčová slova v příkladech.
- *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 vděční, 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](mailto: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](mailto: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 stránky, 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](mailto: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](mailto: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.