

Obsah

Předmluva

13

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

1. Úvod do síťování v Linuxu

21

2. Vytvoření internetové brány na jednodeskovém počítači s operačním systémem Linux

31

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

3. Vytvoření firewallu v počítači s operačním systémem Linux

55

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 předčítat 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 spouštění 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	Přechod síťového provozu využívajícího protokol SIP přes iptables NAT firewally	176
5.21	Přechod síťového provozu využívajícího protokol IAX přes iptables NAT firewally	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 popisů 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 Samba	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 preseeds	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 httping	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**

A aby síťování bylo ještě zajímavější, pak určitě budete mít k tomu všemu i – bližně vyznírající – jak Windows, tak Linux. Jestliže jako pomocníka hledáte knihu, mě vám k vlastnímu řešení různých situací a problémů navrhne mnohá řešení, která vám navíc jasně vysvětlí všechny potřebné příkazy a možnosti konfigurace a navíc vás nebude příliš zatěžovat nekonečným množství z nerozumitelnými dokumenty RFC, pak jste peníze za tuto knihu nezmarnili zbytečně.

Jak by měl vypadat typický čtenář?

V ideálním případě by měl mít čtenář této knihy alespoň nějaké zkušenosti s provozem systému Linux. Měl by vědět, jak v Linuxu instalovat a odinstalovat programy, měl by mít základní pochopení souborů a složek na diskách, spravovat oprávnění k souborům a složkám a vytvářet uživatele a skupiny. Dále se předpokládají základní základy protokolu TCP/IP a Ethernet, znalost pojmů IPv4, IPv6, LAN, WAN, maska podsítě, směrovač (router), firewall, brána, přepínač (switch) a rozbočovač (hub). Požaduje se tedy mezi úplně začátečníky, doplněnými postupováním několika knih, které vám základní pojmy v oblasti síťování vysvětlí.

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

Poznámka českého vydavatele: Autorka publikace *Linux: Světová administrace* sň. Cade Schindler se zde odkazuje na jinou svou knihu *Linux: Co děláte. Průvodce v číselné oblasti* nevyšla, dovolili jsme si náhoda ji jiným titulem, který snad jako *Linux: Co děláte* už čtenáře používající systém Linux odvede od zbludu. Kromě navrženoho titulu možná začátečníci vezí do rukou knihu *Manuál Linux: nastavení a administrace příručka* od stejné firmy. Další vám doporučujeme p. dívat se na adresu <http://www.cpress.cz/knihy/pocitacova-literatura/linux/>, kde najdete seznam všech linuxových publikací nakladatelství Computer Press.