

# Obsah

<b>1 Počítačové sítě</b>	<b>21</b>
1.1 Moderní technologie přepínaných lokálních sítí	21
1.1.1 Přepínání a přepínače	21
1.1.1.1 Funkce přepínače	21
1.1.1.2 Automatické učení přepínací tabulky	21
1.1.2 Virtuální lokální sítě	22
1.1.2.1 Trunk spoje a standard IEEE 802.1q	22
1.1.2.2 Přiřazování stanic do virtuální sítě	25
1.1.2.3 Další použití trunk spojů	26
1.1.3 Protokol Spanning Tree	27
1.1.3.1 Problém smyček v přepínané síti	27
1.1.3.2 Základní funkce protokolu Spanning Tree	28
1.1.3.3 Rapid Spanning Tree (IEEE 802.1w)	29
1.1.3.4 Spanning Tree v prostředí s virtuálními sítěmi	30
1.1.4 Přepínání na více vrstvách	30
1.1.4.1 Princip přepínání na více vrstvách	30
1.1.4.2 Modely použití VLAN v prostředí s přepínači na 3. vrstvě	33
1.2 Protokol IP verze 6	33
1.2.1 Nedostatky protokolu IPv4	33
1.2.2 Adresování v IPv6	34
1.2.2.1 Typy adres v IPv6	34
1.2.2.2 Zápis adres	36
1.2.2.3 Automatická konfigurace	37
1.2.3 Paket IPv6	37
1.2.3.1 Hlavička paketu	37
1.2.3.2 Řetězení hlaviček	39
1.2.4 Podpůrné protokoly IPv6	39
1.2.4.1 ICMPv6	39
1.2.4.2 DNS a IPv6 adresy	40
1.2.5 Pokročilé vlastnosti protokolu IPv6	40
1.2.5.1 Bezpečnost	40
1.2.5.2 Mobilita	40
1.2.5.3 Podpora zabezpečení kvality služby	41
1.2.6 Směrování a protokol IPv6	42
1.2.7 Současný stav podpory protokolu IPv6	42
1.2.7.1 Možnosti přechodu z protokolu IPv4	42
1.3 Směrování v počítačových sítích a v Internetu	43
1.3.1 Hierarchické směrování, autonomní systémy	43
1.3.1.1 Vnitřní a vnější směrovací protokoly	44
1.3.2 Vnitřní směrovací protokoly	45
1.3.2.1 Klasifikace vnitřních směrovacích protokolů	45
1.3.2.2 Standardizované vnitřní směrovací protokoly používané v Internetu	47
1.3.2.2.1 RIP	47
1.3.2.2.2 OSPF	48

1.3.3 Vnější směrovací protokoly.....	51
1.3.3.1 Charakteristika vnějších směrovacích protokolů.....	51
1.3.3.2 Směrovací protokol BGP.....	52
1.3.3.2.1 Optimalizace směrování v protokolu BGP.....	53
1.4 Podpora multimediálních aplikací v Internetu.....	55
1.4.1 Požadavky multimediálních aplikací na kvalitu služby (QoS).....	55
1.4.1.1 Parametry QoS v paketových sítích.....	56
1.4.1.1.1 Omezování a tvarování provozu.....	56
1.4.1.2 Intserv a Diffserv - modely integrovaných a rozlišovaných služeb.....	57
1.4.1.3 Intserv.....	57
1.4.1.3.1 Rezervace zdrojů a protokol RSVP.....	57
1.4.1.4 Diffserv.....	58
1.4.1.4.1 Klasifikace provozu.....	58
1.4.1.4.2 Mechanismy prioritizace provozu.....	59
1.4.1.4.3 Mechanismy předcházení zahlcení.....	60
1.4.1.5 Nasazování mechanismů řízení kvality služby.....	62
1.4.2 Skupinové vysílání v sítích s protokolem IP.....	62
1.4.2.1 Použití skupinového vysílání.....	63
1.4.2.2 Skupinové adresy na 2. a 3. vrstvě modelu OSI RM.....	63
1.4.2.2.1 Skupinové MAC adresy.....	63
1.4.2.2.2 Skupinové adresy v IPv4 a IPv6, výběrové adresy.....	63
1.4.2.2.3 Mapování skupinových IP adres na MAC adresy.....	64
1.4.2.3 Skupinové vysílání v LAN.....	65
1.4.2.3.1 Protokol IGMP.....	65
1.4.2.4 Skupinové vysílání ve WAN.....	65
1.4.2.4.1 Distribuční stromy.....	66
1.4.2.4.2 Reverse Path Forwarding.....	67
1.5 Bezpečnost počítačových sítí.....	70
1.5.1 Základní pojmy.....	70
1.5.1.1 Utajení, integrita a autentizace.....	71
1.5.1.2 Symetrický a asymetrický kryptografický systém.....	71
1.5.1.2.1 Autentizace v symetrickém a asymetrickém systému.....	72
1.5.2 Bezestavová a stavová filtrace provozu.....	73
1.5.2.1 Bezestavová filtrace pomocí ACL.....	74
1.5.2.2 Stavová filtrace pomocí firewallu.....	77
1.5.3 Virtuální privátní sítě (VPN).....	78
1.5.3.1 Použití VPN.....	78
1.5.3.2 Technologie VPN na 3. a 4. vrstvě modelu OSI RM.....	79
1.5.3.2.1 IPsec.....	80
1.5.3.2.2 SSL VPN.....	81
1.5.4 Útoky na počítačové sítě.....	83
1.5.4.1 Útoky typu Denial of Service.....	83
1.5.4.2 Detekce útoků a obrana proti průnikům.....	83
1.5.5 Bezpečnostní mechanismy přepínaných a směrovaných sítí.....	83
1.5.5.1 Možnosti zabezpečení v přepínaných sítích LAN.....	84
1.5.5.2 Základní zabezpečení v intranetech a WAN s protokolem IP.....	85

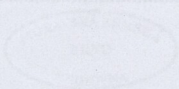
<b>2 Informační systémy a databáze</b> .....	93
2.1 Úvod do databázových technologií.....	93
2.1.1 Úvod.....	93
2.1.2 Historický vývoj.....	93
2.1.3 SRBD.....	93
2.1.4 Architektura SRBD.....	94
2.2 Konceptuální model.....	95
2.2.1 Úvod do konceptuálního modelování.....	95
2.2.2 Konceptuální model Entity Relationship (ER).....	97
2.2.2.1 Úvod.....	97
2.2.2.2 Vazby a integritní omezení.....	97
2.2.2.3 Enhanced ERD.....	97
2.2.3 Konceptuální model UML.....	98
2.2.3.1 Úvod.....	98
2.2.3.2 Třídy, atributy a metody.....	98
2.2.3.3 Zobecnění a specializace.....	100
2.2.3.4 Asociace a role.....	100
2.3 Datový model.....	102
2.3.1 Relační datový model.....	102
2.3.1.1 Úvod.....	102
2.3.1.2 Základní pojmy.....	102
2.3.1.3 Od konceptuálního modelu k modelu relačnímu.....	103
2.3.1.4 Funkční závislosti.....	105
2.3.1.5 Návrh relačního schématu.....	109
2.3.2 Objektový a objektově-relační datový model.....	114
2.3.3 Datový model XML.....	115
2.3.3.1 Úvod.....	115
2.3.3.2 Schéma XML dokumentu.....	116
2.3.3.3 Model XML.....	117
2.3.3.4 Nativní XML databáze.....	118
2.3.4 Cvičení.....	118
2.4 Dotazovací jazyky.....	119
2.4.1 Historický vývoj.....	119
2.4.2 Relační algebra.....	119
2.4.2.1 Operace.....	120
2.4.2 Structured Query Language (SQL).....	121
2.4.2.1 Datové typy v SQL.....	122
2.4.2.2 Definice dat v SQL.....	122
2.4.2.3 Manipulace s daty v SQL.....	125
2.4.3 Dotazovací jazyky pro XML.....	130
2.5 Fyzická implementace uložení dat.....	130
2.5.1 Úvod.....	130
2.5.2 Perzistentní datové struktury.....	130
2.5.3 Datové struktury a algoritmy.....	131
2.5.4 Stromové datové struktury.....	132
2.5.4.1 Binární vyhledávací strom.....	132

2.5.4.2 B-strom	134
2.5.5 Vícerozměrné datové struktury	136
2.5.5.1 R-strom	136
2.5.6 Cvičení	138
2.6 Rozšiřující databázové technologie	138
2.6.1 Paralelní přístup k SRBD	138
2.6.1.1 Transakce	138
2.6.1.2 Plánování transakcí	139
2.6.1.3 Transakce v SQL	141
2.6.2 Distribuované báze dat	142
2.6.3 Datové sklady a dolování dat	143
2.7 Tvorba informačních systémů v prostředí WWW	143
2.7.1 Architektury Informačních systémů	143
2.7.2 Platformy .NET a Java	144
2.7.2.1 .NET	144
2.7.2.2 Java2EE	144
2.7.3 Datová vrstva IS	145

<b>3 Počítačová grafika</b>	151
3.1 Vykreslování základních grafických prvků	151
3.1.2 Generování úseček (DDA), Bresenhamův algoritmus	151
3.1.3 Princip vyplňování a šrafování obrazců	154
3.2 Reprezentace barev a výpočet osvětlení	157
3.2.1 Barevné modely používané v počítačové grafice RGB, CMY, CMYK	157
3.2.2 Intenzita osvětlení	159
3.2.3 Stínování	162
3.3 Afinní a projektivní prostory a jejich aplikace v grafických systémech	165
3.3.1 Afinní prostor a afinní transformace	165
3.3.1.1 Změna souřadné soustavy	166
3.3.1.2 Ortonormalita afinní transformace	168
3.3.2 Projektivní prostor a projektivní transformace	169
3.3.3 Stanovení matice zobrazovací transformace	173
3.4 Standardní zobrazovací řetězec	175
3.4.1 Popis scény, osvětlení a požadovaného zobrazení	175
3.4.2 Posloupnost kroků standardního řetězce	176
3.4.3 Generování plošek aproximujících povrchy těles scény	177
3.4.4 Předběžné odstranění určitě neviditelných ploch	179
3.4.5 Výpočet osvětlení	179
3.4.6 Promítání	182
3.4.7 Ořezání zorným objemem	182
3.4.8 Přejechod od homogenních k afinním souřadnicím a transformace do souřadné soustavy zařízení	184
3.4.9 Vykreslení na rastrové výstupní zařízení a řešení viditelnosti	184
3.4.10 Realizace řetězce při použití Phongova stínování	187
3.5 Zobrazování metodou rekurzivního sledování paprsku	188
3.6 Zobrazování vyzařovací metodou	193
3.7 Programování v OpenGL	198
3.7.1 Syntaxe příkazů OpenGL (a jiné)	199
3.7.2 Kreslení základních geometrických útvarů	200
3.7.3 Geometrické transformace	204
3.7.4 První program v OpenGL	208
3.7.5 Definice osvětlení a materiálů	211

<b>4 Operační systémy a internetové technologie</b> .....	<b>217</b>
4.1 Operační systémy.....	217
4.1.1 Historie.....	218
4.1.2 Program.....	218
4.1.3 Proces.....	219
4.1.3.1 Životní cyklus procesu.....	219
4.1.3.2 Blok řízení procesu.....	220
4.1.4 Správa paměti.....	222
4.1.5 Mapování paměti.....	223
4.1.6 Souborové systémy.....	224
4.2 Internet.....	225
4.2.1 Dokumentace.....	225
4.2.2 Motivace.....	226
4.2.3 Koncepce.....	226
4.2.4 Identifikace síťových prostředků.....	226
4.2.4.1 URI.....	226
4.2.4.2 URL.....	227
4.2.4.3 URN.....	229
4.2.4.4 Shrnutí.....	230
4.2.5 WWW.....	231
4.2.6 Úspěch WWW.....	232
4.2.7 HTTP.....	232
4.2.7.1 Spojení.....	232
4.2.7.2 Transakce.....	233
4.3 Bezpečnost v prostředí Internetu.....	233
4.3.1 Šifrování a dešifrování.....	234
4.3.1.1 Šifrování symetrickým klíčem.....	234
4.3.1.2 Šifrování veřejným klíčem.....	235
4.3.1.3 Hash.....	236
4.3.2 Digitální podpis.....	237
4.3.3 Certifikát.....	238
4.3.4 Certifikát X.509.....	238
4.3.4.1 Význačné jméno.....	240
4.3.4.2 Vytvoření certifikátu certifikační autority.....	241
4.3.4.3 Ověřování certifikátu.....	245
4.3.5 Hierarchie certifikátů.....	247
4.3.5.1 Řetězec certifikátů.....	248
4.3.5.2 Ověření řetězce certifikátů.....	249
4.4 Způsoby zabezpečení síťové komunikace.....	249
4.4.1 SSL.....	250
4.4.1.1 Základní vlastnosti.....	250
4.4.1.2 Úvodní výměna informací.....	250
4.4.1.3 Volba šifrovacího algoritmu.....	251
4.4.1.4 Autentizace serveru.....	251
4.4.1.5 Autentizace klienta.....	252
4.4.2 Útok typu MITM.....	254
4.4.3 Instalace certifikátu.....	255

4.4.3.1 Konfigurace HTTPS serveru	255
4.4.3.2 Konfigurace DNS	257
4.4.3.3 Implementace SSL klienta	257
4.4.3.4 Uživatelsky definované rozhodnutí o důvěryhodnosti certifikátu	259
4.5 LDAP	260
4.5.1 Adresář	261
4.5.1.1 Rozdíly mezi adresáři a databázemi	261
4.5.1.2 Architektura aplikací využívajících adresáře	262
4.5.1.3 Distribuované adresáře	262
4.5.2 LDAP	263
4.5.3 Informační model adresáře	263
4.5.3.1 Schéma	265
4.5.3.2 Model pojmenovávání položek	265
4.5.4 Vyhledávání	266
4.5.5 Implementace	268
4.5.5.1 JNDI	268



<b>5 Elektronické publikování a digitální fotografie</b> .....	<b>275</b>
5.1 Elektronické publikování .....	275
5.1.1 Vymezení pojmu .....	275
5.1.2 Prostředky pro elektronické publikování .....	275
5.2 Dokument a jeho životní cyklus .....	276
5.2.1 Dokument a jeho struktura .....	276
5.2.1.1 Způsob tvorby elektronických dokumentů .....	277
5.2.2 Životní cyklus dokumentu .....	277
5.2.3 Výstupní formáty dokumentů .....	278
5.2.3.1 Formáty vhodné pro tisk a distribuci .....	278
5.2.3.2 Formáty pro elektronickou nápovědu .....	278
5.2.3.3 Webové stránky .....	279
5.2.3.4 Proprietární formáty .....	279
5.3 Přehled XML .....	279
5.3.1 Zápis XML dokumentu .....	279
5.3.2 XSL .....	282
5.4 Docbook .....	282
5.4.1 Principy DocBooku .....	283
5.4.2 XMLMind XML Editor .....	286
5.5 Technologie pro tvorbu WWW stránek .....	288
5.5.1 HTML .....	288
5.5.2 XHTML .....	290
5.5.3 CSS .....	290
5.5.4 Skriptovací jazyky .....	290
5.5.5 Macromedia Flash .....	291
5.6 XHTML .....	291
5.6.1 Typy XHTML dokumentů .....	291
5.6.2 Rozdíly XHTML oproti HTML .....	293
5.6.3 Validita dokumentu .....	294
5.6.4 Tvorba XHTML dokumentů .....	295
5.7 Zpracování a archivace digitálních fotografií .....	296
5.7.1 Principy úprav digitálních fotografií .....	297
5.7.2 Prohlížení a katalogizování fotografií .....	299
5.7.2.1 Základní prostředky – Windows XP .....	299
5.7.2.2 ACDSee .....	300
5.7.2.3 Zoner Photo Studio .....	301
5.7.2.4 IrfanView .....	302
5.8 Nástroje pro editaci fotografií .....	303
5.8.1 Adobe Photoshop .....	303
5.8.2 Zoner Callisto .....	304
5.8.3 GIMP .....	305
5.9 Úprava fotografií .....	306

5.9.1 Formáty podporované editorem GIMP .....	306
5.10 Prostředí GIMPu .....	308
5.10.1 Hlavní panel GIMPu .....	309
5.10.2 Panel nástrojů .....	309
5.10.3 Okno s obrázkem .....	312
5.11 Základní úpravy .....	312
5.11.1 Než začneme upravovat .....	312
5.11.2 Získání obrázku .....	313
5.11.3 Škálování obrázku .....	313
5.11.4 Oříznutí .....	314
5.11.5 Uložení obrázku .....	316
5.12 Další úpravy v GIMPu .....	317
5.12.1 Odstín a sytost .....	317
5.12.2 Jas, kontrast .....	319
5.12.3 Histogram .....	321
5.12.4 Úrovně (levels) .....	321
5.13 Tipy k další práci .....	324

<b>6 Softwarové inženýrství</b>	<b>329</b>
6.1 Základní pojmy	329
6.1.1 Definice softwarového inženýrství	329
6.1.2 Schéma procesu vývoje softwarového díla	329
6.2 Softwarový proces	330
6.2.1 Definice softwarového procesu	330
6.2.2 Základní typy softwarového procesu	331
6.2.3 Proces RUP, jeho cykly, fáze a iterace	332
6.2.4 Základní a podpůrné toky činností	336
6.2.5 Jazyk UML	337
6.3 Byznys modelování	337
6.3.1 Specifikace byznys procesů	338
6.3.2 Model entit a pracovníků procesu	342
6.4 Specifikace požadavků	343
6.4.1 Aktéři a funkční specifikace pomocí případů použití	343
6.4.2 Diagramy scénářů užití	343
6.4.3 Toky činnosti popisující scénáře užití	345
6.5 Analýza a návrh	346
6.5.1 Modely a jejich diagramy	347
6.5.2 Objekty a jejich třídy	347
6.5.3 Vztahy mezi třídami a objekty	352
6.5.4 Diagramy tříd jazyka UML	361
6.5.5 Specifikace dynamického chování	362
6.5.6 Strukturování softwarového systému	364
6.5.7 Návrh a jeho cíle	365
6.5.8 Architektura výsledného systému	366
6.5.9 Model nasazení	367
6.6 Implementace	368
6.6.1 Mapování elementů logického modelu na komponenty	369
6.6.2 Zdrojové, binární a spustitelné komponenty	370
6.6.3 Diagramy nasazení	376
6.7 Testování a nasazení softwarového produktu	377
6.7.1 Cíle procesu verifikace a validace	378
6.7.2 Modely testování	378
6.7.3 Nasazení softwarového systému	379

