

<b>Předmluva vydavatele</b>	<b>7</b>
<b>Předmluva</b>	<b>11</b>
<b>Obsah</b>	<b>15</b>
<b>1 Jemný úvod do DNS</b>	<b>25</b>
1.1 Historie DNS	25
1.2 K čemu slouží	27
<b>I Základní principy</b>	<b>31</b>
<b>2 Jak to funguje</b>	<b>33</b>
2.1 Doménový strom	33
2.2 DNS záznamy	37
2.3 Domény a servery	38
2.4 Resolver čili řešič	41
2.5 Život jednoho dotazu	43
2.6 Rekurzivní a nerekurzivní chování serverů	47
2.7 Domény, zóny a zónové soubory	48
2.8 Reverzní dotazy aneb hledá se jméno pro adresu	53
<b>3 Vnitřní život DNS</b>	<b>59</b>
3.1 Doménová jména	59
3.2 Formát DNS zpráv	61
3.3 Komunikace mezi klientem a serverem	67
3.3.1 Klient	68
3.3.2 Server	70
3.4 Zónové přenosy	72
3.5 Žolíkové záznamy	76
3.6 Vyrovnávací paměť	81
<b>4 DNS z pohledu klienta</b>	<b>85</b>
4.1 Konfigurace	86
4.1.1 Microsoft Windows 11	86
4.1.2 Microsoft Windows 10, 8 a 7	89
4.1.3 Linux a systémy odvozené z Unixu	93
4.1.4 macOS	96
4.2 Programy pro dotazování DNS	98
4.2.1 host	98
4.2.2 nslookup	102
4.2.3 dig	105
4.3 Resolver a relativní jména	110
4.4 DNS přímo z aplikace	112



<b>5 Transportní vrstva pro DNS</b>	<b>115</b>
5.1 UDP	115
5.2 TCP	117
5.3 Stavové DNS	119
5.4 Šifrované DNS	121
5.5 DNS po TLS (DoT)	123
5.6 DNS po DTLS (DoD)	124
5.7 DNS po HTTPS (DoH)	125
5.8 DNS po QUIC (DoQ)	128
<b>6 DNS v praxi</b>	<b>131</b>
6.1 Scénáře použití	131
6.1.1 Pouze klienti	131
6.1.2 Klienti a autoritativní server	133
6.1.3 Neveřejný autoritativní server	135
6.1.4 DNS hosting	136
6.1.5 Otevřené rekurzivní servery	137
6.2 Návrh nasazení DNS	139
6.3 Podpůrné programy	140
6.3.1 Programy doprovázející server	141
6.3.2 Zonemaster	143
6.3.3 dnswalk	145
6.3.4 Squish DNS Checker	147
6.3.5 MX Toolbox	149
6.3.6 DNSDiag	151
6.3.7 DNS Benchmark	153
6.3.8 Programy pro správu DNS dat	155
<b>7 Správa domén a vlastně i celého Internetu</b>	<b>157</b>
7.1 Jak to celé začalo	157
7.2 Éra ICANN	158
7.3 Rozšiřování domén nejvyšší úrovně	161
7.4 Správa kořenové zóny	164
7.5 Klíče od Internetu	165
7.6 Správa domén – registr, registrátor, držitel	168
7.7 Registrace domény	171
7.8 Vlastní registrace	174
7.9 Informace o doménách a držitelích	176
7.10 Historie domény cz a sdružení CZ.NIC	182



<b>II DNS pro starší a pokročilé</b>	<b>189</b>
<b>8 Principy DNSSEC</b>	<b>191</b>
8.1 Digitální podpisy	192
8.2 Autentizační řetězec	194
8.3 Když řetězec nenavazuje	198
8.4 Ověřená neexistence	199
8.5 Příklad	202
8.6 Chování serverů a klientů	208
8.7 DNSSEC a žolíkové záznamy	212
<b>9 DNSSEC prakticky</b>	<b>217</b>
9.1 Ověřování odpovědí	218
9.2 Klíče	222
9.3 Podpis vlastní zóny	235
9.4 Dokumentace	243
<b>10 Národní znaky v doménách, čili IDN</b>	<b>245</b>
10.1 Jak funguje IDN	246
10.1.1 Přípustné znaky a jmenovky	251
10.1.2 Punycode	252
10.1.3 IDNA2003 – Nameprep, ToASCII a ToUnicode	254
10.2 Problémy a otázky	256
10.2.1 Bezpečnost	256
10.2.2 Přístupnost	258
10.2.3 Politika a strategie	259
10.3 IDN ve světě a u nás	261
<b>11 Dynamické DNS</b>	<b>263</b>
11.1 Jak funguje	263
11.2 Chování serveru	267
11.3 Zase ta bezpečnost	269
11.4 Praktický příklad	271
<b>12 ENUM</b>	<b>279</b>
12.1 Jak funguje	280
12.2 Nasazení	284
12.3 Infrastrukturní ENUM	284
12.4 Situace v České republice	286
<b>13 Na pokraji DNS</b>	<b>287</b>
13.1 Skupinové DNS (mDNS)	287
13.2 Link-Local Multicast Name Resolution (LLMNR)	291
13.3 Výběrové adresování aneb anycast	294



13.4	DNS a rozkládání zátěže	296
13.5	Aktivní server aneb DNS push	299
13.6	Katalogové zóny	301
<b>14</b>	<b>DNS v cizích službách</b>	<b>305</b>
14.1	SPF – Sender Policy Framework	306
14.2	Sender ID	315
14.3	DKIM – DomainKeys Identified Mail	316
14.4	DNSBL a seznamy hodných, zlých a ošklivých	328
14.5	Automatická konfigurace poštovních klientů	330
14.6	DNS a objevování služeb (DNS-SD)	332
14.7	Certifikáty, klíče, PKI a další bezpečnostní harampádí	336
14.8	DNS a TLS čili DANE	339
14.9	Osobní certifikáty a klíče pro elektronickou poštu	343
<b>15</b>	<b>Bezpečnost protokolu DNS</b>	<b>345</b>
15.1	Bellovinův útok	345
15.2	Kaminského útok aneb otrávení vyrovnávací paměti	346
15.3	Fragmentační útoky	350
15.4	Útok náhodnými dotazy	352
15.5	Útok nekonečnou rekurzí	353
15.6	Zesilované útoky	354
15.7	Lhaní pod kontrolou aneb RPZ	359
15.8	Ochrana soukromí a minimalizace dotazů	363
<b>III</b>	<b>Typy záznamů</b>	<b>367</b>
<b>16</b>	<b>Obecně o zdrojových záznamech</b>	<b>369</b>
<b>17</b>	<b>Základní typy</b>	<b>371</b>
17.1	A – Address (1)	371
17.2	AAAA – IPv6 Address (28)	371
17.3	CNAME – Canonical Name (5)	371
17.4	MX – Mail Exchange (15)	373
17.5	NS – Name Server (2)	374
17.6	PTR – Pointer (12)	375
17.7	SOA – Start of Authority (6)	376
17.8	TXT – Text (16)	378
<b>18</b>	<b>Servisní typy</b>	<b>379</b>
18.1	AXFR – Full Zone Transfer (252)	379
18.2	CSYNC – Child-to-Parent Synchronization (62)	379
18.3	DHCID – DHCP Identifier (49)	381



18.4	DNAME – Delegation Name (39)	381
18.5	IXFR – Incremental Zone Transfer (251)	383
18.6	OPT – Option (41)	384

## **19 Typy pro DNSSEC a bezpečnostní mechanismy** **391**

19.1	CAA – Certificate Authority Authorization (257)	391
19.2	CDNSKEY – Child DNS Key (60)	393
19.3	CDS – Child Delegation Signer (59)	394
19.4	CERT – Certificate (37)	395
19.5	DNSKEY – DNS Key (48)	397
19.6	DS – Delegation Signer (43)	398
19.7	IPSECKEY – IPsec Key (45)	401
19.8	KEY (25)	403
19.9	NSEC – Next Secure (47)	404
19.10	NSEC3 – Next Secure version 3 (50)	405
19.11	NSEC3PARAM – NSSEC3 Parameters (51)	408
19.12	OPENPGPKEY (61)	408
19.13	RRSIG – RR Signature (46)	409
19.14	SIG – Signature (24)	412
19.15	SMIMEA (53)	412
19.16	SSHFP – SSH Key Fingerprint (44)	413
19.17	TKEY – Transaction Key (249)	415
19.18	TLSA (52)	417
19.19	TSIG – Transaction Signature (250)	419
19.20	ZONEMD – Zone Message Digest (63)	422

## **20 Aplikační a ostatní typy** **423**

20.1	AMTRELAY (260)	423
20.2	EUI48 (108)	424
20.3	EUI64 (109)	425
20.4	HIP – Host Identity Protocol (55)	425
20.5	L32 – Locator32 (105)	425
20.6	L64 – Locator64 (106)	426
20.7	LP – Locator Pointer (107)	426
20.8	NAPTR – Naming Authority Pointer (35)	427
20.9	NID – Node Identifier (104)	431
20.10	NULL (10)	431
20.11	SRV – Service (33)	432
20.12	URI – Uniform Resource Identifier (256)	433

## **21 Typy odmítnuté, zastaralé a nepoužívané** **435**

21.1	A6 – IPv6 Address (38)	435
21.2	AFSDB – AFS Data Base (18)	435
21.3	APL – Address Prefix List (42)	436



21.4 ATMA – ATM Address (34)	436
21.5 DLV – DNSSEC Lookaside Validation (32769)	436
21.6 EID – Endpoint Identifier (31)	436
21.7 GID (102)	437
21.8 GPOS – Geographical Position (27)	437
21.9 HINFO – Host Information (13)	437
21.10 ISDN (20)	437
21.11 KX – Key Exchanger (36)	437
21.12 LOC – Location (29)	437
21.13 MAILA – Mail Agent (254)	438
21.14 MAILB – Mailbox Related (253)	438
21.15 MB – Mailbox (7)	438
21.16 MD – Mail Destination (3)	438
21.17 MF – Mail Forwarder (4)	438
21.18 MG – Mail Group (8)	438
21.19 MINFO – Mail Information (14)	438
21.20 MR – Mail Rename (9)	439
21.21 NIMLOC – Nimrod Locator (32)	439
21.22 NINFO – Zone Information (56)	439
21.23 NSAP – NSAP Address (22)	439
21.24 NSAP-PTR – NSAP Pointer (23)	439
21.25 NXT – Next Domain (30)	439
21.26 PX – X.400 Mail Mapping (26)	439
21.27 RKEY – Resource Key (57)	440
21.28 RP – Responsible Person (17)	440
21.29 RT – Route Through (21)	440
21.30 SINK – Kitchen Sink (40)	440
21.31 SPF – Sender Policy Framework (99)	440
21.32 TA – DNSSEC Trust Authorities (32768)	441
21.33 UID (101)	441
21.34 UINFO (100)	441
21.35 UNSPEC (103)	441
21.36 WKS – Well Known Service (11)	441
21.37 X25 – X.25 Address (19)	441

## **IV DNS servery 443**

### **22 Obecně ke konfiguraci serveru 445**

22.1 Typ serveru a obsluhovaná komunita	445
22.2 Zónové soubory	446
22.2.1 localhost	446
22.2.2 Reverzní zóny pro localhost	447
22.2.3 Kořenové servery	447



22.3 Ošetření nesmyslných reverzních dotazů	451
<b>23 BIND</b>	<b>455</b>
23.1 Základní konfigurace	455
23.1.1 Autoritativní server	456
23.1.2 Rekurzivní server	464
23.1.3 Smíšený server	467
23.2 Doprovodné programy	469
23.2.1 Kontrola konfigurace a dat	469
23.2.2 rndc – pan řídící	470
23.3 Konfigurace pro náročné	472
23.3.1 Automatické podepisování DNSSEC	472
23.3.2 Pohledy	474
23.4 Bundy, dříve BIND 10	477
<b>24 NSD</b>	<b>479</b>
24.1 Základní konfigurace	479
24.2 Doprovodné programy	484
24.2.1 nsd-checkconf	484
24.2.2 nsd-control	485
24.3 Konfigurace pro náročné	486
24.3.1 DNSSEC	486
24.3.2 Dynamické zóny	487
24.3.3 Omezování frekvence dotazů	488
<b>25 Unbound</b>	<b>491</b>
25.1 Základní konfigurace	491
25.2 Doprovodné programy	495
25.2.1 unbound-checkconf	495
25.2.2 unbound-control	496
25.2.3 unbound-host	497
25.3 Konfigurace pro náročné	499
25.3.1 Řízení vyrovnávací paměti a optimalizace	499
25.3.2 Speciální zóny a předávání dotazů	500
<b>26 Knot DNS</b>	<b>505</b>
26.1 Základní konfigurace	505
26.2 Doprovodné programy	513
26.2.1 knotc	513
26.2.2 kdig a khost	515
26.3 Pokročilé nastavení	515
26.3.1 DNSSEC	515
26.3.2 Moduly	517
26.3.3 Dynamické aktualizace	520



<b>27 Knot Resolver</b>	<b>523</b>
27.1 Základní konfigurace	523
27.2 Spuštění a komunikace s programem	527
<b>28 PowerDNS</b>	<b>529</b>
28.1 Základní konfigurace	530
28.2 Doprovodné programy	536
28.2.1 WWW server	536
28.2.2 pdns_control	537
28.2.3 zone2sql	538
28.3 Konfigurace pro náročné	538
28.3.1 DNSSEC	539
28.3.2 Dynamické aktualizace	543
<b>29 PowerDNS Recursor</b>	<b>545</b>
29.1 Základní konfigurace	545
29.2 Doprovodné programy	547
29.2.1 rec_control	547
29.3 Konfigurace pro náročné	549
29.3.1 Speciální zóny	549
29.3.2 Skriptování	549
<b>30 OpenDNSSEC</b>	<b>551</b>
30.1 Koncepce programu	551
30.2 Instalace a konfigurace	554
30.3 Provoz	570
30.4 Bezpečnostní modul	573
<b>V Přílohy</b>	<b>575</b>
<b>A Přehled RFC</b>	<b>577</b>
A.1 Jádru protokolu	577
A.2 Transport	577
A.3 Speciální prvky a typy záznamů	577
A.4 DNSSEC	578
A.5 IDN	578
A.6 ENUM	578
A.7 IPv6	579
A.8 Různé	579
A.9 Související technologie	579
<b>Literatura</b>	<b>581</b>
<b>Rejstřík</b>	<b>585</b>