

Table des matières

Préface	1
1. Introduction	5
1.1 Usage des réseaux d'ordinateurs	7
1.1.1 Applications professionnelles	7
1.1.2 Applications domestiques	10
1.1.3 Utilisateurs nomades	15
1.1.4 Aspects sociaux	18
1.2 Caractéristiques physiques des réseaux	22
1.2.1 Réseaux personnels (PAN)	23
1.2.2 Réseaux locaux (LAN)	24
1.2.3 Réseaux métropolitains (MAN)	28
1.2.4 Réseaux étendus (WAN)	29
1.2.5 Interréseaux	33
1.3 Logiciels de réseaux	34
1.3.1 Hiérarchie de protocoles	34
1.3.2 Principes de conception des couches	39
1.3.3 Services avec connexion et sans connexion	41
1.3.4 Primitives de service	43
1.3.5 Relations des services aux protocoles	46
1.4 Modèles de référence	47
1.4.1 Le modèle de référence OSI	47
1.4.2 Le modèle de référence TCP/IP	51
1.4.3 Le modèle utilisé dans ce livre	54
1.4.4 Comparaison des modèles de référence OSI et TCP/IP	55
1.4.5 Critique du modèle et des protocoles OSI	57
1.4.6 Critique du modèle de référence TCP/IP	59
1.5 Exemples de réseaux	60
1.5.1 L'Internet	60
1.5.2 Réseaux de téléphonie mobile de troisième génération	71
1.5.3 LAN sans fil : 802.11	76
1.5.4 RFID et les réseaux de capteurs	80

1.6	Normalisation des réseaux	82
1.6.1	Le Who's Who des télécommunications	83
1.6.2	Le Who's Who de la normalisation internationale	85
1.6.3	Le Who's Who de la normalisation de l'Internet	87
1.7	Système métrique	89
1.8	Aperçu de la suite de cet ouvrage	90
1.9	Résumé	91
	Exercices	93
2.	La couche physique	97
2.1	Bases théoriques de la transmission de données	98
2.1.1	Analyse de Fourier	98
2.1.2	Signaux sur une bande passante étroite	99
2.1.3	Débit binaire maximal d'un canal de transmission	102
2.2	Supports de transmission guidés : la transmission filaire	103
2.2.1	Supports magnétiques	103
2.2.2	Paire torsadée	104
2.2.3	Câble coaxial	106
2.2.4	Courant porteur en ligne	107
2.2.5	Fibre optique	108
2.3	Supports de transmission non guidés : la transmission sans fil	114
2.3.1	Le spectre électromagnétique	115
2.3.2	Transmission d'ondes radio	118
2.3.3	Transmission de micro-ondes	120
2.3.4	Transmission d'ondes infrarouges	123
2.3.5	Transmission d'ondes lumineuses	124
2.4	Satellites de télécommunications	125
2.4.1	Satellites géostationnaires (GEO)	127
2.4.2	Satellites à orbite moyenne (MEO)	130
2.4.3	Satellites à orbite basse (LEO)	131
2.4.4	Satellites <i>versus</i> fibre optique	133
2.5	Modulation numérique et multiplexage	135
2.5.1	Transmission en bande de base	135
2.5.2	Transmission passe-bande	140
2.5.3	Multiplexage fréquentiel	143
2.5.4	Multiplexage temporel	145
2.5.5	Multiplexage par répartition en code	146

2.6	Le réseau téléphonique commuté	149
2.6.1	Structure du réseau téléphonique	150
2.6.2	Orientations marquantes du système téléphonique	153
2.6.3	Desserte locale : modems, ADSL et fibre	155
2.6.4	Artères interurbaines et multiplexage	164
2.6.5	Commutation	172
2.7	Systèmes de téléphonie mobile	177
2.7.1	Systèmes sans fil de première génération (1G) : voix analogique	179
2.7.2	Systèmes mobiles de deuxième génération (2G) : voix numérique	182
2.7.3	Systèmes mobiles de troisième génération (3G) : voix et données numériques	187
2.8	Le réseau de télévision câblée	192
2.8.1	Système avec antenne collective (CATV)	192
2.8.2	L'Internet par le câble	193
2.8.3	Allocation de fréquences	195
2.8.4	Modem-câble	196
2.8.5	ADSL <i>versus</i> le câble	198
2.9	Résumé	200
	Exercices	202
3.	La couche liaison de données	209
3.1	Fonctions de la couche liaison de données	209
3.1.1	Services fournis à la couche réseau	210
3.1.2	La notion de trame	212
3.1.3	Contrôle d'erreurs	216
3.1.4	Contrôle de flux	217
3.2	Détection et correction d'erreurs	218
3.2.1	Codes correcteurs d'erreurs	220
3.2.2	Codes détecteurs d'erreurs	226
3.3	Protocoles de liaison de données élémentaires	232
3.3.1	Un protocole simplex utopique	237
3.3.2	Un protocole simplex de type arrêt et attente pour un canal exempt de bruit	238
3.3.3	Un protocole simplex de type arrêt et attente pour un canal bruité	240

3.4	Protocoles avec fenêtre d'anticipation	244
3.4.1	Un protocole à fenêtre d'une largeur de 1 bit	247
3.4.2	Un protocole à fenêtre de largeur n	249
3.4.3	Protocole à rejet sélectif	256
3.5	Exemples de protocoles pour la couche liaison.	262
3.5.1	Paquets sur SONET.	263
3.5.2	ADSL (<i>Asymmetric Digital Subscriber Line</i>)	266
3.6	Résumé	269
	Exercices.	271
4.	La sous-couche MAC de contrôle d'accès au canal	277
4.1	Problème d'allocation d'un canal	278
4.1.1	Allocation statique d'un canal.	278
4.1.2	Hypothèses pour l'allocation dynamique d'un canal	280
4.2	Protocoles de gestion d'accès.	281
4.2.1	ALOHA.	281
4.2.2	Protocoles d'accès par écoute de porteuse (CSMA)	286
4.2.3	Protocoles sans collision.	290
4.2.4	Protocoles à contention limitée.	294
4.2.5	Protocoles de LAN sans fil.	298
4.3	Ethernet	301
4.3.1	Couche physique de l'Ethernet classique.	302
4.3.2	Protocole de sous-couche MAC de l'Ethernet classique	303
4.3.3	Performances d'Ethernet	307
4.3.4	Ethernet commuté.	309
4.3.5	Fast Ethernet	312
4.3.6	Gigabit Ethernet.	315
4.3.7	10 Gigabit Ethernet	319
4.3.8	Rétrospective d'Ethernet	320
4.4	LAN sans fil (WLAN et Wi-Fi).	321
4.4.1	Architecture et pile de protocoles de 802.11	322
4.4.2	Couche physique de 802.11	324
4.4.3	Protocole de la sous-couche MAC de 802.11.	326
4.4.4	Structure d'une trame de 802.11	332
4.4.5	Services associés aux LAN sans fil	334

4.5	Sans fil à large bande (WMAN et WLL)	336
4.5.1	Comparaison de 802.16 avec 802.11 et 3G	337
4.5.2	Architecture et pile de protocoles de 802.16	338
4.5.3	Couche physique de 802.16	339
4.5.4	Sous-couche MAC de 802.16	341
4.5.5	Structure d'une trame de 802.16	342
4.6	Bluetooth	343
4.6.1	Architecture de Bluetooth	344
4.6.2	Applications de Bluetooth	345
4.6.3	Pile de protocoles de Bluetooth	346
4.6.4	Couche radio Bluetooth	347
4.6.5	Couches de liaison Bluetooth	348
4.6.6	Structure d'une trame Bluetooth	349
4.7	RFID	351
4.7.1	Architecture EPC Gen2	352
4.7.2	Couche physique EPC Gen2	352
4.7.3	Couche d'identification d'étiquette EPC Gen2	354
4.7.4	Formats des messages d'identification d'étiquette	355
4.8	Commutation au niveau liaison de données	356
4.8.1	Utilisations des ponts	356
4.8.2	Ponts d'apprentissage	358
4.8.3	Arbre recouvrant	361
4.8.4	Répéteurs, hubs, ponts, commutateurs, routeurs et passerelles	364
4.8.5	LAN virtuels (VLAN)	366
4.9	Résumé	373
	Exercices	375
5.	La couche réseau	381
5.1	Problèmes de conception de la couche réseau	381
5.1.1	Commutation de paquets en mode différé (<i>store-and-forward</i>)	381
5.1.2	Services fournis à la couche transport	382
5.1.3	Implémentation d'un service sans connexion	383
5.1.4	Implémentation d'un service avec connexion	385
5.1.5	Réseau de datagrammes <i>versus</i> réseau de circuits virtuels	387
5.2	Algorithmes de routage	388
5.2.1	Principe d'optimalité	391

5.2.2	Algorithme du plus court chemin	392
5.2.3	Routage par inondation	394
5.2.4	Routage par vecteur de distance	396
5.2.5	Routage par informations d'état de lien	400
5.2.6	Routage hiérarchique	405
5.2.7	Routage broadcast	407
5.2.8	Routage multicast	409
5.2.9	Routage anycast	413
5.2.10	Routage pour les hôtes mobiles	414
5.2.11	Routage dans les réseaux ad hoc	416
5.3	Algorithmes de contrôle de congestion	420
5.3.1	Méthodes de contrôle de congestion	422
5.3.2	Routage basé sur le trafic	424
5.3.3	Contrôle d'admission	425
5.3.4	Étranglement du trafic	426
5.3.5	Délestage de charge	429
5.4	Qualité de service	432
5.4.1	Exigences des applications	433
5.4.2	Canalisation du trafic	435
5.4.3	Ordonnancement des paquets	439
5.4.4	Contrôle d'admission	443
5.4.5	Services intégrés	447
5.4.6	Services différenciés	450
5.5	Interconnexion de réseaux	453
5.5.1	Différences entre les réseaux	454
5.5.2	Équipements d'interconnexion	455
5.5.3	Technique du tunnel	458
5.5.4	Routage dans un interréseau	460
5.5.5	Fragmentation	461
5.6	Couche réseau dans l'Internet	465
5.6.1	Protocole IPv4	468
5.6.2	Adresses IP	471
5.6.3	IPv6	485
5.6.4	Protocoles de contrôle internet	495
5.6.5	Commutation par étiquettes et MPLS	501
5.6.6	Protocole OSPF	504

5.6.7	Protocole BGP	510
5.6.8	Diffusion multicast sur l'Internet	515
5.6.9	Protocole IP mobile	517
5.7	Résumé	520
	Exercices	522
6.	Couche transport	529
6.1	Service de transport	529
6.1.1	Services fournis aux couches supérieures	529
6.1.2	Primitives du service de transport	531
6.1.3	Sockets de Berkeley	535
6.1.4	Exemple de programmation de socket : un serveur de fichiers internet	537
6.2	Éléments de protocoles de transport	541
6.2.1	Adressage	543
6.2.2	Établissement d'une connexion	546
6.2.3	Libération d'une connexion	552
6.2.4	Contrôle de flux et mémorisation	556
6.2.5	Multiplexage	561
6.2.6	Reprise après incident	562
6.3	Contrôle de congestion	565
6.3.1	Allocation de bande passante souhaitable	565
6.3.2	Régulation du taux d'envoi	570
6.3.3	Particularités des réseaux sans fil	574
6.4	Protocole de transport internet : UDP	576
6.4.1	Introduction à UDP	576
6.4.2	RPC : appel de procédure à distance	578
6.4.3	Protocoles de transport en temps réel : RTP et RTCP	581
6.5	Protocole de transport internet : TCP	587
6.5.1	Introduction à TCP	587
6.5.2	Modèle de service TCP	588
6.5.3	Protocole TCP	591
6.5.4	L'en-tête du segment TCP	592
6.5.5	Établissement d'une connexion TCP	596
6.5.6	Libération de la connexion TCP	597
6.5.7	Gestion de la connexion TCP	598

6.5.8	Fenêtre de TCP	600
6.5.9	Gestion du temporisateur TCP	604
6.5.10	Contrôle de congestion TCP	607
6.5.11	L'avenir de TCP	618
6.6	Problèmes de performances	619
6.6.1	Problèmes de performances	620
6.6.2	Mesure des performances d'un réseau	621
6.6.3	Conception d'hôtes pour des réseaux à haut débit	624
6.6.4	Traitement rapide des segments	628
6.6.5	Compression d'en-tête	631
6.6.6	Protocoles des réseaux WAN à haut débit	633
6.7	Réseaux tolérants aux délais	637
6.7.1	Architecture DTN	639
6.7.2	Protocole de groupage ou <i>protocole bundle</i>	641
6.8	Résumé	644
	Exercices	646
7.	La couche application	651
7.1	DNS (<i>Domain Name System</i>)	651
7.1.1	Espace de noms du système DNS	652
7.1.2	Enregistrements de ressources de domaines	656
7.1.3	Serveurs de noms	660
7.2	Messagerie électronique	664
7.2.1	Architecture et services	665
7.2.2	Agent utilisateur	668
7.2.3	Formats de messages	672
7.2.4	Transfert de messages	679
7.2.5	Remise finale	686
7.3	Le Web (<i>World Wide Web</i>)	689
7.3.1	Présentation de l'architecture	690
7.3.2	Pages web statiques	706
7.3.3	Pages web dynamiques et applications web	716
7.3.4	HTTP – Le protocole de transfert hypertexte	728
7.3.5	Web sans fil	739
7.3.6	Recherche sur le Web	741

7.4	Streaming	744
7.4.1	Principe de l'audio numérique	746
7.4.2	Principes de la vidéo numérique	751
7.4.3	Streaming de données enregistrées	760
7.4.4	Streaming de données multimédias en direct	768
7.4.5	Conférences en temps réel	773
7.5	Distribution de contenus	783
7.5.1	Contenu et trafic internet	785
7.5.2	Fermes de serveurs et serveurs web mandataires	788
7.5.3	Réseaux de distribution de contenu	793
7.5.4	Réseaux P2P	798
7.5.5	Tables de hachage distribuées (DHT)	803
7.6	Résumé	808
	Exercices	811
8.	La sécurité des réseaux	817
8.1	Cryptographie	820
8.1.1	Introduction à la cryptographie	821
8.1.2	Chiffres de substitution	824
8.1.3	Chiffres de transposition	825
8.1.4	Masques jetables (<i>one-time pad</i>)	827
8.1.5	Les deux principes fondamentaux de la cryptographie	832
8.2	Algorithmes à clé symétrique	834
8.2.1	DES : le standard de chiffrement de données	835
8.2.2	AES (<i>Advanced Encryption Standard</i>)	839
8.2.3	Modes de chiffrement	842
8.2.4	Autres chiffrements	848
8.2.5	Cryptanalyse	848
8.3	Algorithmes à clé publique	849
8.3.1	RSA	850
8.3.2	Autres algorithmes à clé publique	852
8.4	Signatures numériques	853
8.4.1	Signatures à clé symétrique	853
8.4.2	Signatures à clé publique	854
8.4.3	Condensats de messages	856
8.4.4	Attaque de l'anniversaire	860

8.5	Gestion des clés publiques	863
8.5.1	Certificats	863
8.5.2	X.509	865
8.5.3	Infrastructures à clés publiques	866
8.6	Sécurité des communications	870
8.6.1	IPsec	870
8.6.2	Pare-feu	875
8.6.3	Réseaux privés virtuels	878
8.6.4	Sécurité des réseaux sans fil	880
8.7	Protocoles d'authentification	885
8.7.1	Authentification fondée sur une clé secrète partagée	886
8.7.2	Établissement d'une clé partagée : l'échange de clés de Diffie-Hellman	890
8.7.3	Authentification à l'aide d'un centre de distribution de clés ..	892
8.7.4	Authentification au moyen de Kerberos	896
8.7.5	Authentification par cryptographie à clé publique	898
8.8	Sécurité du courrier électronique	899
8.8.1	PGP (<i>Pretty Good Privacy</i>)	899
8.8.2	S/MIME	904
8.9	Sécurité du Web	904
8.9.1	Menaces	904
8.9.2	Sécurité du nommage	905
8.9.3	SSL (<i>Secure Sockets Layer</i>)	911
8.9.4	Sécurité des pages dynamiques	915
8.10	Problèmes sociaux	919
8.10.1	Vie privée	919
8.10.2	Liberté d'expression	922
8.10.3	Copyright	926
8.11	Résumé	929
	Exercices	931
	Bibliographie	939
	Index	941