



Ressourcesinformatiques

Réseaux informatiques

Notions fondamentales

(Protocoles, Architectures,
Réseaux sans fil, Virtualisation,
Sécurité, IPv6...)

7^e édition

José DORDOIGNE

Fichiers complémentaires
à télécharger



Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence ENI de l'ouvrage **RI7RES** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

Chapitre 1

Présentation des concepts réseau

1. Historique	19
1.1 Début de l'informatique réseau	19
1.1.1 L'informatique centralisée	19
1.1.2 Le premier réseau informatique à grande échelle	21
1.1.3 Le développement d'une norme de fait : TCP/IP	23
1.1.4 L'informatique répartie	23
1.2 Réseaux hétérogènes	24
1.3 Réseaux informatiques actuels	25
1.4 Rencontre avec les réseaux informatiques	27
2. Principaux éléments d'un réseau	32
2.1 Client/Serveur	32
2.1.1 Principes	32
2.1.2 Définitions	32
2.1.3 Le système d'exploitation réseau	37
2.2 Point de vue matériel	45
2.2.1 L'interconnexion	45
2.2.2 Les protocoles de communication	45
3. Technologie des réseaux	46
3.1 Définition d'un réseau informatique	46
3.2 Topologies de réseaux informatiques	46
3.2.1 Le réseau personnel	47
3.2.2 Le réseau local	47

2 Réseaux informatiques

Notions fondamentales

3.2.3	Le réseau métropolitain	47
3.2.4	Le réseau étendu	47
3.3	Partage des ressources	48
3.3.1	Les services de fichiers	49
3.3.2	Les services de gestion électronique de documents	53
3.3.3	Les services de base de données	54
3.3.4	Les services d'impression	54
3.3.5	Les services de messagerie et de travail collaboratif	56
3.3.6	Les services d'application	57
3.3.7	Les services de stockage	59
3.3.8	Les services de sauvegarde	77
3.3.9	Les protocoles de réplication entre baies	81
3.3.10	WAAS et compression de flux	83
3.4	Virtualisation	86
3.4.1	Introduction	86
3.4.2	Quelques notions de virtualisation	87
3.4.3	Solutions de virtualisation types	90
3.4.4	Synthèse des technologies de virtualisation	93
3.5	Cloud computing	96
4.	Plan de continuité d'activité	99
4.1	Disponibilité	99
4.1.1	La fiabilisation lors du stockage	99
4.1.2	La fiabilisation des échanges	102
4.2	Confidentialité	103
4.2.1	La sécurisation du système de fichiers	103
4.2.2	La sécurisation des échanges	105
4.3	Redondance des données	106
4.3.1	La tolérance de panne	106
4.3.2	Le miroir de disques	109
4.3.3	Le miroir de contrôleurs et de disques	109
4.3.4	Les agrégats par bandes avec parité	111
4.3.5	La neutralisation des secteurs défectueux	114

- 4.4 Solutions de redondance serveur 114
 - 4.4.1 La tolérance de panne 115
 - 4.4.2 La répartition de charge réseau 116
 - 4.4.3 La configuration des cartes réseaux en teaming 117
 - 4.4.4 La virtualisation comme solution à part entière 119
- 4.5 Stratégie de sauvegardes. 120
 - 4.5.1 La sauvegarde complète. 121
 - 4.5.2 La sauvegarde incrémentale 121
 - 4.5.3 La sauvegarde différentielle. 122
- 4.6 Continuité et reprise d'activité en cas de sinistre 123
 - 4.6.1 Les principes. 123
 - 4.6.2 Le plan de continuité d'activité (PCA) 123
 - 4.6.3 Le plan de reprise d'activité (PRA) 124

Chapitre 2
Normalisation des protocoles

- 1. Modèle OSI 127
 - 1.1 Principes 128
 - 1.2 Communication entre couches 129
 - 1.3 Encapsulation et modèle OSI. 131
 - 1.4 Protocoles 134
 - 1.5 Rôle des différentes couches 135
 - 1.5.1 La couche Physique 135
 - 1.5.2 La couche Liaison (ou Liaison de données) 135
 - 1.5.3 La couche Réseau 136
 - 1.5.4 La couche Transport 137
 - 1.5.5 La couche Session 137
 - 1.5.6 La couche Présentation 137
 - 1.5.7 La couche Application. 138
- 2. Approche pragmatique du modèle en couches 138
 - 2.1 Niveau 1 - couche Physique 139
 - 2.2 Niveau 2 - couche Liaison de données 139

4 Réseaux informatiques

Notions fondamentales

2.3	Niveau 3 - couche Réseau	143
2.3.1	Les principes	143
2.3.2	L'adressage logique	144
2.3.3	La sortie du réseau logique	146
2.3.4	La transmission du datagramme sur l'inter-réseau	147
2.3.5	L'aiguillage du datagramme sur le routeur	150
2.4	Niveau 4 - couche Transport	152
2.4.1	Le mode connecté TCP	152
2.4.2	Le mode non connecté UDP	154
2.5	Niveau 5 et supérieurs	154
3.	Normes et organismes	155
3.1	Types de normes	155
3.2	Quelques organismes de normalisation pour le réseau	155
3.2.1	American National Standards Institute (ANSI)	155
3.2.2	Union internationale des télécommunications (UIT)	157
3.2.3	Electronic Industries Alliance (EIA)	158
3.2.4	Institute of Electrical and Electronics Engineers (IEEE)	158
3.2.5	ISO	160
3.2.6	Internet Engineering Task Force (IETF)	160

Chapitre 3

Transmission des données couche Physique

1.	Rôle d'une interface réseau	161
1.1	Principes	161
1.2	Préparation des données	162
2.	Options et paramètres de configuration	162
2.1	Adresse physique	162
2.2	Interruption	165
2.3	Adresse d'entrée/sortie	166
2.4	Adresse de mémoire de base	166
2.5	Canal DMA (Direct Memory Access)	166

2.6	Bus	166
2.6.1	Le bus PCI (Peripheral Component Interconnect)	167
2.6.2	Le bus PC Card	169
2.6.3	Le bus USB	170
2.6.4	Le bus IEEE 1394	173
2.7	Connecteurs de câble réseau	175
2.7.1	Le connecteur RJ45	175
2.7.2	Le connecteur BNC	176
2.7.3	Les connecteurs fibre optique	176
2.8	Débits	179
2.9	Autres interfaces réseau	179
3.	Amorçage à partir du réseau	181
3.1	Principes	181
3.2	Protocoles	181
3.2.1	La liaison entre adresses physique et logique	181
3.2.2	Le protocole BOOTP	182
3.2.3	Le protocole DHCP	182
3.2.4	PXE	183
3.2.5	Wake-On-LAN : WOL	185
4.	Codage des données	189
4.1	Types de données et signaux	189
4.1.1	Le signal analogique	189
4.1.2	Le signal numérique	190
4.1.3	Les utilisations	190
4.2	Codage des données	191
4.2.1	Le codage des données numériques en signaux analogiques	191
4.2.2	Le codage des données numériques en signaux numériques	192
4.2.3	Les codages en ligne	193
4.2.4	Les codages complets	194

6 Réseaux informatiques

Notions fondamentales

4.3	Multiplexage de signaux	195
4.3.1	Le système bande de base	195
4.3.2	Le système large bande	196
4.3.3	Le multiplexage	196
5.	Conversion des signaux	198
5.1	Définitions	198
5.2	Modem	199
5.3	Codec	200
6.	Supports de transmission	201
6.1	Supports limités	201
6.1.1	La paire torsadée	202
6.1.2	Le câble coaxial	209
6.1.3	La fibre optique	211
6.1.4	Les critères de choix des différents médias	215
6.2	Supports non limités	217
6.2.1	L'infrarouge	217
6.2.2	Le laser	218
6.2.3	Les ondes radio terrestres	218
6.2.4	Les ondes radio par satellites	219

Chapitre 4

Éléments logiciels de communication

1.	Configuration de la carte réseau	221
1.1	Configuration matérielle	221
1.2	Configuration logicielle	222
1.3	Spécifications NDIS et ODI	224
2.	Installation et configuration du pilote de carte réseau	226
2.1	Principes	226
2.2	Utilisation d'un outil fourni par le constructeur	226

- 2.3 Utilisation du système d'exploitation 228
 - 2.3.1 Sous Windows 10 ou Windows Server 2016 229
 - 2.3.2 Sous Linux Red Hat 231
 - 2.3.3 Sous Mac OS X 235
 - 2.3.4 Sur un smartphone Android 239
 - 2.3.5 Tethering 245
 - 2.3.6 Sur un iPhone 255
- 3. Pile de protocoles 262
- 4. Détection d'un problème réseau 264
 - 4.1 Connectique physique réseau 264
 - 4.1.1 Le type de câble 264
 - 4.1.2 Le type de composants 265
 - 4.2 Configuration logicielle réseau 266

Chapitre 5
Architecture réseau et interconnexion

- 1. Topologies 267
 - 1.1 Principes 267
 - 1.2 Topologies standards 267
 - 1.2.1 Le bus 267
 - 1.2.2 L'étoile 268
 - 1.2.3 L'anneau 269
 - 1.2.4 L'arbre 270
 - 1.2.5 Les topologies dérivées 270
 - 1.2.6 Le cas des réseaux sans fil 272
- 2. Choix de la topologie réseau adaptée 273
- 3. Gestion de la communication 274
 - 3.1 Sens de communication 274
 - 3.1.1 Le mode simplex 274
 - 3.1.2 Le mode half-duplex 275
 - 3.1.3 Le mode full-duplex 275

8 Réseaux informatiques

Notions fondamentales

3.2	Types de transmission	275
3.3	Méthodes d'accès au support	276
3.3.1	La contention	276
3.3.2	L'interrogation (polling)	278
3.3.3	Le jeton passant	278
3.4	Techniques de commutation	279
3.4.1	La commutation de circuits	279
3.4.2	La commutation de messages	280
3.4.3	La commutation de paquets	280
4.	Interconnexion de réseaux	282
4.1	Principes	282
4.2	Composants d'interconnexion et modèle OSI	283
4.3	Description fonctionnelle des composants	284
4.3.1	Le répéteur	284
4.3.2	Le pont	285
4.3.3	Le commutateur	294
4.3.4	Le routeur	306
4.3.5	La passerelle	320
4.4	Choix des matériels de connexion appropriés	321
4.4.1	Le répéteur	321
4.4.2	Le pont	322
4.4.3	Le commutateur	322
4.4.4	Le routeur	323
4.4.5	La passerelle	323
4.5	Exemple de topologie réseau locale sécurisée	323

Chapitre 6
Couches basses des réseaux locaux

- 1. Couches basses et IEEE. 327
 - 1.1 Différenciation des couches. 327
 - 1.2 IEEE 802.1 328
 - 1.3 IEEE 802.2 329
 - 1.3.1 Les principes de Logical Link Control (LLC) 329
 - 1.3.2 Les types de service 330
- 2. Ethernet et IEEE 802.3 330
 - 2.1 Généralités 330
 - 2.2 Caractéristiques de couche Physique. 331
 - 2.2.1 Les spécificités d'Ethernet 331
 - 2.2.2 Les spécificités de Fast Ethernet 338
 - 2.2.3 Le gigabit Ethernet 340
 - 2.2.4 Le 10 gigabit Ethernet 341
 - 2.2.5 Le 40/100 gigabit Ethernet 342
 - 2.2.6 Récapitulatif. 344
 - 2.3 En-tête de trame Ethernet 345
 - 2.4 Les cartes hybrides Ethernet/SAN. 346
- 3. Token Ring et IEEE 802.5 348
 - 3.1 Configuration du réseau. 348
 - 3.2 Autoreconfiguration de l'anneau 352
- 4. Wi-Fi et IEEE 802.11 353
 - 4.1 Présentation 353
 - 4.2 Normes de couche Physique 354
 - 4.2.1 802.11b 355
 - 4.2.2 802.11a 356
 - 4.2.3 802.11g 356
 - 4.2.4 802.11n 356
 - 4.2.5 802.11ac 357
 - 4.2.6 802.11ad 361
 - 4.2.7 802.11ah - Wi-Fi HaLow 362

4.2.8	802.11ax - High Efficiency WLAN (HEW)	363
4.3	Matériels	364
4.3.1	La carte réseau	364
4.3.2	L'équipement d'infrastructure	365
4.3.3	Les périphériques Wi-Fi	366
4.4	Architecture	367
4.5	Sécurisation	368
4.5.1	Introduction	368
4.5.2	WEP	370
4.5.3	WPA	371
4.6	Usages	374
4.7	En-tête de trame Wi-Fi	374
5.	Bluetooth et IEEE 802.15	375
5.1	Historique	376
5.2	Standardisation	377
5.3	Réseau Bluetooth	380
5.4	Classes d'équipements	381
6.	Autres technologies	382
6.1	Autres standards de l'IEEE	382
6.1.1	802.16	383
6.1.2	802.17	383
6.1.3	802.18	384
6.1.4	802.19	384
6.1.5	802.21	384
6.1.6	802.22	384
6.1.7	802.24	385
6.2	Infrared Data Association (IrDA)	385
6.2.1	Le protocole IrDA DATA	386
6.2.2	Le protocole IrDA CONTROL	388
6.3	Courant porteur en ligne (CPL)	389
6.3.1	Les principes	389
6.3.2	Le fonctionnement	392

- 7. L'univers des objets connectés, IoT 394
 - 7.1 Introduction 394
 - 7.2 Évolution des objets connectés 396
 - 7.3 Accès aux objets connectés 398
 - 7.4 Problèmes soulevés par les objets connectés 399

Chapitre 7
Protocoles des réseaux MAN et WAN

- 1. Interconnexion du réseau local 401
 - 1.1 Usages du réseau téléphonique 401
 - 1.2 Réseau numérique à intégration de services (RNIS) 403
 - 1.2.1 Les principes 403
 - 1.2.2 Le rapport au modèle OSI 404
 - 1.2.3 Les types d'accès disponibles 405
 - 1.3 Ligne spécialisée (LS) 406
 - 1.3.1 Les principes 406
 - 1.3.2 Les débits 406
 - 1.4 Techniques xDSL 407
 - 1.4.1 Les principes 407
 - 1.4.2 Les différents services 407
 - 1.4.3 Les offres "quadruple play" 410
 - 1.5 Câble public 412
 - 1.6 Plan très haut débit en France (THD) 412
 - 1.7 WiMAX 415
 - 1.7.1 La boucle locale radio 415
 - 1.7.2 La solution WiMAX 415
 - 1.8 Réseaux cellulaires 417
 - 1.8.1 Les principes 417
 - 1.8.2 Les débuts 419
 - 1.8.3 L'évolution vers le transport de données 420
 - 1.8.4 Les nouvelles générations de téléphonie cellulaire. 421

12 Réseaux informatiques

Notions fondamentales

1.9	Fiber Distributed Data Interface (FDDI)	425
1.9.1	Les principes	425
1.9.2	La topologie	426
1.9.3	Le fonctionnement	427
1.10	Asynchronous Transfer Mode (ATM)	428
1.10.1	Les principes	428
1.10.2	Le relais de cellule	429
1.10.3	La régulation du trafic	429
1.10.4	Les types de services	430
1.10.5	La topologie et les débits	431
1.11	Synchronous Optical Network (SONET) et Synchronous Digital Hierarchy (SDH)	432
1.11.1	L'historique	432
1.11.2	Les caractéristiques de SDH	433
1.11.3	Les débits	433
1.12	X.25	434
1.13	Relais de trame	436
1.14	MPLS	437
1.14.1	Origine	437
1.14.2	Les principes	438
1.14.3	Le circuit virtuel et l'étiquetage	439
1.14.4	Le routage	439
2.	Accès distant et réseaux privés virtuels	440
2.1	Utilisation et évolution	440
2.2	Protocole d'accès distant	440
2.3	Réseau privé virtuel	441
2.3.1	L'établissement de la connexion	441
2.3.2	L'authentification	442
2.3.3	Le chiffrement	443
2.4	Les clients légers et l'accès distant	443

Chapitre 8**Protocoles des couches moyennes et hautes**

1. Principales familles de protocoles	445
1.1 IPX/SPX	445
1.1.1 L'historique	445
1.1.2 Les protocoles	446
1.2 NetBIOS	447
1.2.1 L'historique	447
1.2.2 Les principes	447
1.2.3 Les noms NetBIOS	449
1.3 TCP/IP	452
1.3.1 L'historique	452
1.3.2 La suite de protocoles	453
1.3.3 Le rapport au modèle OSI	454
1.3.4 L'adoption en entreprise	454
2. Protocole IP version 4	455
2.1 Principes	455
2.2 Adressage	455
2.2.1 L'adresse IPv4	455
2.2.2 Le masque	456
2.2.3 Les classes d'adresses	457
2.2.4 Les adresses privées	459
2.2.5 Les adresses APIPA	460
2.3 L'adressage sans classe	460
2.3.1 Les principes	460
2.3.2 La notation CIDR	461
2.3.3 Le rôle du masque en réseau	462
2.3.4 La décomposition en sous-réseaux	468
2.3.5 La factorisation des tables de routage	475
3. Protocole IP version 6	477
3.1 Introduction	477
3.2 Principes	478

14 Réseaux informatiques

Notions fondamentales

3.3	Structure d'une adresse IP	479
3.3.1	Catégories d'adresses	479
3.3.2	Portée d'une adresse	480
3.3.3	Adresse unicast	481
3.3.4	Formalisme	482
3.3.5	Identifiant EUI-64	484
3.3.6	Adresses réservées	486
3.3.7	Décomposition des plages par l'IETF	488
3.3.8	Découpage des catégories	491
3.3.9	Autoconfiguration des adresses IPv6	496
3.4	Tunnels	499
3.4.1	Introduction	499
3.4.2	Types de tunnels	500
3.5	Organismes d'attribution d'adresses	505
3.6	En-tête IPv6	507
4.	Autres protocoles de couche Internet	508
4.1	Internet Control Message Protocol (ICMP)	508
4.2	Internet Group Management Protocol (IGMP)	511
4.3	Address Resolution Protocol (ARP) et Reverse Address Resolution Protocol (RARP)	512
4.4	Internet Protocol Security (IPsec)	513
4.5	Liste des numéros de protocoles de couche Internet	514
5.	Voix sur IP (VoIP)	514
5.1	Principes	514
5.2	Quelques définitions importantes	515
5.3	Avantages	517
5.4	Fonctionnement	519
5.4.1	Le protocole H323	519
5.4.2	Les éléments terminaux	519
5.4.3	Les applications	520
6.	Protocoles de transport TCP et UDP	521
6.1	Transmission Control Protocol (TCP)	521
6.2	User Datagram Protocol (UDP)	522

- 7. Couche applicative TCP/IP 522
 - 7.1 Services de messagerie 522
 - 7.1.1 Simple Mail Transfer Protocol (SMTP) 522
 - 7.1.2 Post Office Protocol 3 (POP3)..... 524
 - 7.1.3 Internet Message Access Protocol (IMAP)..... 525
 - 7.2 Services de transfert de fichier..... 526
 - 7.2.1 HyperText Transfer Protocol (HTTP)..... 526
 - 7.2.2 File Transfer Protocol (FTP) et Trivial FTP (TFTP) ... 530
 - 7.2.3 Network File System (NFS) 534
 - 7.3 Services d'administration et de gestion réseau 536
 - 7.3.1 Domain Name System (DNS) 536
 - 7.3.2 Dynamic Host Configuration Protocol v.4 (DHCPv4) . 548
 - 7.3.3 Telnet 561
 - 7.3.4 Network Time Protocol (NTP)..... 562
 - 7.3.5 Simple Network Management Protocol (SNMP) 565

Chapitre 9

Principes de sécurisation d'un réseau

- 1. Compréhension du besoin en sécurité 573
 - 1.1 Garanties exigées 573
 - 1.2 Dangers encourus 574
 - 1.2.1 La circulation des données 574
 - 1.2.2 Les protocoles Réseau et Transport 575
 - 1.2.3 Les protocoles applicatifs standards..... 575
 - 1.2.4 Les protocoles de couches basses 576
 - 1.2.5 Le risque au niveau logiciel 576
- 2. Outils et types d'attaques 577
 - 2.1 Ingénierie sociale..... 577
 - 2.2 Écoute réseau 582
 - 2.3 Analyse des ports 583
 - 2.4 Codes malveillants 585
 - 2.5 Programmes furtifs..... 586

2.6	Ransomware	588
3.	Notions de sécurisation sur le réseau local	588
3.1	Services de la sécurité	588
3.1.1	Le contrôle d'accès au système	589
3.1.2	La gestion des habilitations	589
3.1.3	L'intégrité	590
3.1.4	La non-répudiation	590
3.2	Authentification	591
3.2.1	L'identification	591
3.2.2	L'authentification par mot de passe	595
3.2.3	L'authentification avec support physique	596
3.2.4	L'authentification par caractéristique humaine	596
3.3	Confidentialité	597
3.3.1	Le chiffrement à clés symétriques	598
3.3.2	Le chiffrement à clés asymétriques	599
3.4	Protection des données utilisateur	602
3.4.1	Protection de l'amorçage du disque	604
3.4.2	Chiffrement des disques locaux	608
3.4.3	Chiffrement des disques USB	611
4.	Sécurisation de l'interconnexion de réseaux	613
4.1	Routeur filtrant	613
4.2	Translateur d'adresse	614
4.3	Pare-feu	615
4.4	Proxy	616
4.5	Zone démilitarisée	617

Chapitre 10
Dépannage du réseau

- 1. Méthode d'approche 619
- 2. Exemples de diagnostic de couches basses 620
 - 2.1 Matériels 621
 - 2.1.1 Le testeur de câbles 621
 - 2.1.2 Le réflectomètre 622
 - 2.1.3 Le voltmètre 623
 - 2.2 Analyse de trames 623
 - 2.3 Autres problèmes avec Ethernet 624
 - 2.3.1 L'unicité d'adresse MAC 625
 - 2.3.2 La configuration physique de la carte réseau 625
 - 2.3.3 Les paramètres de communication 625
 - 2.4 IPX et Ethernet 626
 - 2.5 Autres problèmes avec Token Ring 626
 - 2.5.1 Le conflit de configuration 626
 - 2.5.2 La configuration de la carte Token Ring 627
 - 2.5.3 La connexion aux équipements 628
 - 2.6 Autres problèmes avec FDDI 628
- 3. Utilisation des outils TCP/IP adaptés 629
 - 3.1 Principes 629
 - 3.2 Exemples d'utilisation des outils 629
 - 3.2.1 arp 629
 - 3.2.2 ping 631
 - 3.2.3 tracert/traceroute 633
 - 3.2.4 ipconfig/ifconfig 633
 - 3.2.5 netstat 636
 - 3.2.6 nbtstat 639
 - 3.2.7 nslookup 641
- 4. Outils d'analyse des couches hautes 644
 - 4.1 Analyse de requêtes applicatives 644
 - 4.2 Analyse de requêtes web 645

Annexes

- 1. Conversion du décimal (base 10) vers le binaire (base 2).....649
 - 1.1 Vocabulaire utilisé649
 - 1.2 Conversion à partir de la base 10.....650
- 2. Conversion du binaire (base 2) vers le décimal (base 10).....651
- 3. Conversion de l'hexadécimal (base 16) vers le décimal (base 10) ..653
- 4. Conversion de l'hexadécimal (base 16) vers le binaire (base 2) ...654
- 5. Glossaire656

- Index677

Chapitre 3

Transmission des données couche Physique

1. Rôle d'une interface réseau

Dans un premier temps, nous allons examiner les paramètres qui permettent de configurer les périphériques d'un PC et plus particulièrement une carte réseau.

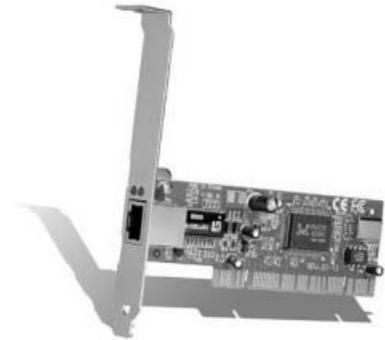
1.1 Principes

L'interface réseau fait office d'intermédiaire entre l'ordinateur et le support de transmission. Elle peut être un simple composant soudé à la carte mère ou bien une carte réseau (NIC - *Network Interface Card*) à part entière. Dans ce dernier cas, elle est installée dans un connecteur d'extension (slot). Son rôle est de préparer les données à transmettre avant de les envoyer et d'interpréter celles reçues. Pour cela, elle contient un émetteur-récepteur.

Le lien entre la carte et le système d'exploitation réseau est assuré par le pilote (driver) périphérique. Ce composant logiciel correspond à la couche Liaison de données du modèle OSI.

1.2 Préparation des données

La couche physique met en forme les données (bits) à transmettre sous forme de signaux. Les échanges entre l'ordinateur et la carte s'effectuent via le bus de la machine en parallèle. La carte réseau va donc sérialiser les informations avant de transmettre les signaux sur le support physique.



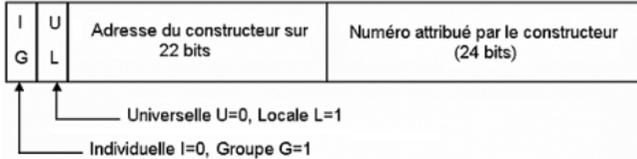
2. Options et paramètres de configuration

Tout point d'entrée/sortie sur un réseau doit être identifié afin que la trame soit reçue (acceptée) par le bon périphérique. Une carte réseau ou un port série, doivent avoir un numéro qui doit permettre de les repérer au plus bas niveau (du modèle OSI).

2.1 Adresse physique

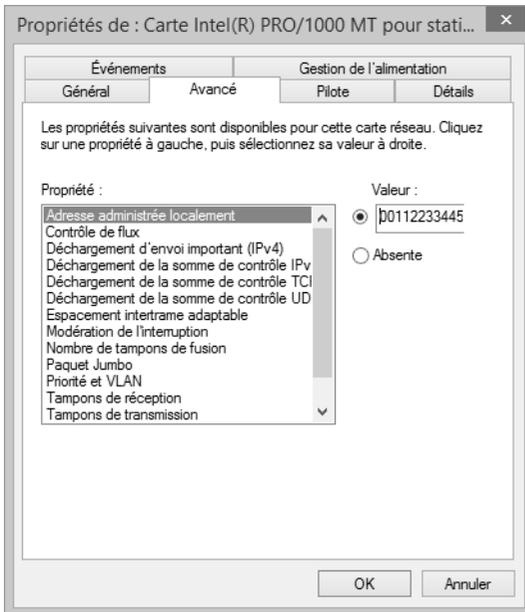
Sur un réseau local de type Ethernet (le plus courant, que nous aborderons plus tard), c'est une adresse physique sur six octets, qui permet d'identifier l'interface réseau. Les trois premiers octets de cette adresse sont attribués par l'IEEE pour identifier le constructeur du matériel (ex. 00AA00 pour le constructeur Intel et 00A024 pour 3Com). Les trois octets restants sont laissés à la disposition du constructeur, qui doit faire en sorte de vendre des cartes, de telle manière qu'aucune n'ait la même adresse physique, sur le même réseau de niveau 2.

Une adresse MAC va soit identifier une carte réseau unique ($I=0$), soit être associée à un ensemble de cartes ($G=1$). Cette adresse pourra être unique globalement ($U=0$) ou simplement unique sur un périmètre limité ($L=1$).



Remarque

Théoriquement, rien n'empêche le système d'exploitation réseau de travailler avec des adresses physiques différentes de celles du constructeur. Par exemple, sous Windows, en accédant aux Propriétés de la carte réseau, il est possible d'imposer une nouvelle adresse physique différente de celle proposée par défaut. Il suffit alors de valider, et la nouvelle adresse MAC devient effective immédiatement !



Affichage des propriétés avancées d'une carte réseau sous Windows

Remarque

La commande **ipconfig /all** sous Windows ou **ifconfig -a** sous UNIX/Linux permet de le vérifier.

Cette adresse est utilisée chaque fois qu'une station, ou plutôt sa carte réseau, a besoin d'émettre une trame vers une autre carte réseau. Il est néanmoins possible d'envoyer un paquet non pas à une, mais à plusieurs cartes en remplaçant l'adresse unique du destinataire par une adresse multiple (souvent une adresse de diffusion, soit `FFFFFFFFFFFF`, c'est-à-dire tous les bits des six octets mis à 1).

Ainsi, toute adresse référant plusieurs hôtes aura son bit de poids fort (le plus à gauche) à '1' (ex. `FFFFFF.FFFFFFF`), à '0' dans le cas contraire (ex. `00AA00.123456`).

Par exemple, lorsqu'une carte réseau effectue une requête *Address Resolution Protocol* (ARP), elle envoie une diffusion sur son réseau de niveau 2, c'est-à-dire que le destinataire physique de la trame émise est "Tout le monde", `FF-FF-FF-FF-FF-FF`, comme ci-dessous :

```

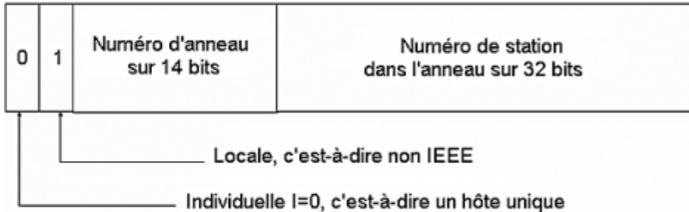
⊕Frame: Base frame properties
⇨ETHERNET: ETYPE = 0x0806 : Protocol = ARP: Address Resolution Protocol
  ⊕ETHERNET: Destination address : FFFFFFFFFF
  ⊕ETHERNET: Source address : 00A024B6132D
  ETHERNET: Frame Length : 60 (0x003C)
  ETHERNET: Ethernet Type : 0x0806 (ARP: Address Resolution Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 46 (0x002E)
⇨ARP_RARP: ARP: Request, Target IP: 172.17.0.3
  ARP_RARP: Hardware Type = Ethernet (10Mb)
  ARP_RARP: Protocol Type = 2048 (0x800)
  ARP_RARP: Hardware Address Length = 6 (0x6)
  ARP_RARP: Protocol Address Length = 4 (0x4)
  ARP_RARP: Opcode = Request
  ARP_RARP: Sender's Hardware Address = 00A024B6132D
  ARP_RARP: Sender's Protocol Address = 172.17.0.92
  ARP_RARP: Target's Hardware Address = 000000000000
  ARP_RARP: Target's Protocol Address = 172.17.0.3
  ARP_RARP: Frame Padding

```

Identification d'une adresse de diffusion (niv. 2)

Une adresse attribuée par l'IEEE aura son deuxième bit de poids fort à '0', tandis qu'une valeur '1' précisera que l'adresse correspond à une adresse non normalisée.

Par exemple, en Token Ring, l'adresse d'un hôte était constituée comme suit :



Adressage physique Token Ring

■ Remarque

Historiquement, il était possible de créer des groupes en Token Ring ($G=1$).

■ Remarque

La liste exhaustive des préfixes d'adresses MAC attribués aux constructeurs (OUI - Organizationally Unique Identifiers) peut être consultée à partir de l'URL suivante : <http://standards-oui.ieee.org/oui.txt>

2.2 Interruption

Tout périphérique du PC est relié au microprocesseur par une ligne dédiée, ou ligne d'interruption (IRQ - *Interrupt ReQuest*). Lorsque le périphérique a besoin du microprocesseur pour travailler, il lui envoie un signal par cette ligne (tension électrique qui passe à l'état bas). Historiquement, les premiers PCs comportaient 2 fois 8 lignes en cascades. Aujourd'hui, les systèmes d'exploitations intègrent 256 interruptions gérées de manière logicielle (Plug and Play). Certaines lignes sont attribuées par défaut et d'autres sont disponibles pour recevoir les périphériques supplémentaires. Le microprocesseur gère ces lignes par ordre de priorité : plus le numéro de l'interruption est faible, plus la priorité est élevée.

■ Remarque

Grâce à la technique du *Plug and Play*, qui permet la détection de la carte et l'affectation automatique de ses paramètres, il n'est plus vraiment utile aujourd'hui de connaître ces informations.

2.3 Adresse d'entrée/sortie

Un périphérique interrompt le microprocesseur chaque fois que des informations ont besoin d'être échangées. Ces informations sont reçues ou envoyées par une porte d'entrée/sortie localisée à une adresse particulière : l'adresse d'entrée/sortie. Cette adresse pointe sur une plage d'au plus 32 octets, qui va permettre de stocker des données, mais aussi des informations indiquant ce qu'il faut faire de ces données.

2.4 Adresse de mémoire de base

Il s'agit d'une adresse de mémoire volatile dont le rôle est de faire un tampon (buffer), lors de la réception ou l'émission de trame sur le réseau.

Cette adresse doit être un multiple de 16, elle est donc souvent écrite en hexadécimal sans le '0' final qui est sous-entendu.

2.5 Canal DMA (Direct Memory Access)

Dans la plupart des cas, les périphériques dépendent du microprocesseur pour transférer des informations de leur tampon vers la mémoire vive ou en sens inverse. Ainsi, il existe des périphériques qui disposent d'un canal particulier pour pouvoir échanger directement des informations avec la mémoire vive du PC, sans avoir recours au microprocesseur (dans un deuxième temps).

Certains périphériques, notamment des cartes réseau disposent d'un canal DMA, de 1 à 7.

2.6 Bus

Toutes les données échangées entre les périphériques et l'ordinateur passent par des bus de données. Pendant longtemps, cet échange était surtout effectué à travers des voies parallèles, et la vitesse de transmission dépendait beaucoup de sa largeur, par exemple 16, 32 ou 64 bits. Les nouvelles technologies de bus privilégient des solutions de transferts en série, dans lesquels les bits sont envoyés les uns après les autres.