

Les exemples à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence ENI de l'ouvrage **RIHS-10RES** 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 Débuts 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.	25
1.2 Réseaux hétérogènes.	27
1.3 Réseaux informatiques actuels	28
1.4 Rencontre avec les réseaux informatiques	29
2. Principaux éléments d'un réseau	36
2.1 Client/serveur	37
2.1.1 Principes	37
2.1.2 Définitions	37
2.1.3 Le système d'exploitation réseau	45
2.2 Point de vue matériel	59
2.2.1 L'interconnexion.	59
2.2.2 Les protocoles de communication	59
3. Technologie des réseaux.	59
3.1 Définition d'un réseau informatique	59
3.2 Topologies de réseaux informatiques	60
3.2.1 Le réseau personnel.	60
3.2.2 Le réseau local	60

2 Réseaux informatiques

Notions fondamentales

3.2.3	Le réseau métropolitain	61
3.2.4	Le réseau étendu	61
3.3	Partage des ressources.	61
3.3.1	Les services de fichiers	62
3.3.2	Les services de gestion électronique de documents	66
3.3.3	Les services de base de données	67
3.3.4	Les services d'impression	70
3.3.5	Les services de messagerie et de travail collaboratif	71
3.3.6	Les services d'application	73
3.3.7	Les services de stockage	74
3.3.8	Les services de sauvegarde	94
3.3.9	Les protocoles de réplication entre baies.	98
3.3.10	WAAS et compression de flux	100
3.4	Virtualisation	103
3.4.1	Introduction	103
3.4.2	Quelques notions de virtualisation	103
3.4.3	Solutions de virtualisation types	107
3.4.4	Synthèse des technologies de virtualisation	110
3.4.5	Desktop as a Service	113
3.5	Cloud computing	118
4.	Plan de continuité d'activité.	121
4.1	Disponibilité	121
4.1.1	La fiabilisation lors du stockage.	121
4.1.2	La fiabilisation des échanges	124
4.2	Confidentialité	125
4.2.1	La sécurisation du système de fichiers	125
4.2.2	La sécurisation des échanges	127
4.3	Redondance des données	128
4.3.1	La tolérance de pannes	128
4.3.2	Le miroir de disques	133
4.3.3	Le miroir de contrôleurs et de disques.	135
4.3.4	Les agrégats par bandes avec parité	136
4.3.5	La neutralisation des secteurs défectueux.	139

- 4.4 Solutions de redondance serveur 139
 - 4.4.1 La tolérance de pannes 140
 - 4.4.2 La répartition de charge réseau 143
 - 4.4.3 La configuration des cartes réseau en teaming 144
 - 4.4.4 La virtualisation comme solution à part entière. 146
- 4.5 Stratégie de sauvegardes. 147
 - 4.5.1 La sauvegarde complète 148
 - 4.5.2 La sauvegarde incrémentale 148
 - 4.5.3 La sauvegarde différentielle 148
 - 4.5.4 Sanctuarisation des sauvegardes 149
 - 4.5.5 Sauvegardes immuables 150
- 4.6 Continuité et reprise d'activité en cas de sinistre 150
 - 4.6.1 Les principes 150
 - 4.6.2 Le plan de continuité d'activité (PCA) 151
 - 4.6.3 Le plan de reprise d'activité (PRA). 152

Chapitre 2
Normalisation des protocoles

- 1. Modèle OSI 153
 - 1.1 Principes 154
 - 1.2 Communication entre couches 155
 - 1.3 Encapsulation et modèle OSI. 157
 - 1.4 Protocoles 163
 - 1.5 Rôle des différentes couches 164
 - 1.5.1 La couche Physique. 164
 - 1.5.2 La couche Liaison (ou Liaison de données) 164
 - 1.5.3 La couche Réseau 165
 - 1.5.4 La couche Transport. 166
 - 1.5.5 La couche Session 166
 - 1.5.6 La couche Présentation. 167
 - 1.5.7 La couche Application 167

4 Réseaux informatiques

Notions fondamentales

2.	Approche pragmatique du modèle en couches	168
2.1	Niveau 1 - couche Physique	168
2.2	Niveau 2 - couche Liaison de données	169
2.3	Niveau 3 - couche Réseau	172
2.3.1	Les principes	172
2.3.2	L'adressage logique	172
2.3.3	La sortie du réseau logique	174
2.3.4	La transmission du datagramme sur l'interréseau	176
2.3.5	L'aiguillage du datagramme sur le routeur	179
2.4	Niveau 4 - couche Transport	181
2.4.1	Le mode connecté TCP	181
2.4.2	Le mode non connecté UDP	183
2.5	Niveau 5 et supérieurs	183
3.	Normes et organismes	184
3.1	Types de normes	184
3.2	Quelques organismes de normalisation pour le réseau	184
3.2.1	American National Standards Institute (ANSI)	184
3.2.2	Union internationale des télécommunications (UIT)	186
3.2.3	Electronic Component Industry Association (ecia)	187
3.2.4	Institute of Electrical and Electronics Engineers (IEEE)	188
3.2.5	ISO	190
3.2.6	Internet Engineering Task Force (IETF)	190

Chapitre 3

Transmission des données couche physique

1.	Rôle d'une interface réseau	191
1.1	Principes	191
1.2	Préparation des données	192
2.	Options et paramètres de configuration	193
2.1	Adresse physique	193
2.2	Interruption	197
2.3	Adresse d'entrée/sortie	198

2.4	Adresse de mémoire de base	198
2.5	Canal DMA (Direct Memory Access)	198
2.6	Bus	198
2.6.1	Le bus PCI (Peripheral Component Interconnect)	200
2.6.2	Le bus USB	203
2.7	Connecteurs de câble réseau	207
2.7.1	Le connecteur RJ45	207
2.7.2	Le connecteur BNC	208
2.7.3	Les connecteurs fibre optique	209
2.7.4	Les connecteurs hybrides	211
2.8	Débits	212
2.9	Autres interfaces réseau	212
3.	Amorçage à partir du réseau	213
3.1	Principes	213
3.2	Protocoles	214
3.2.1	La liaison entre adresses physique et logique	214
3.2.2	Le protocole BOOTP	215
3.2.3	Le protocole DHCP	215
3.2.4	PXE	216
3.2.5	Wake-On-LAN : WOL	218
4.	Codage des données	222
4.1	Types de données et signaux	222
4.1.1	Le signal analogique	222
4.1.2	Le signal numérique	223
4.1.3	Les utilisations	224
4.2	Codage des données	224
4.2.1	Le codage des données numériques en signaux analogiques	224
4.2.2	Le codage des données numériques en signaux numériques	226
4.2.3	Les codages en ligne	226
4.2.4	Les codages complets	229

6 Réseaux informatiques

Notions fondamentales

4.3	Multiplexage de signaux	229
4.3.1	Le système bande de base	229
4.3.2	Le système large bande	230
4.3.3	Le multiplexage	230
5.	Conversion des signaux	232
5.1	Définitions	232
5.2	Modem	233
5.3	Codec	234
6.	Supports de transmission	235
6.1	Supports limités	235
6.1.1	La paire torsadée	236
6.1.2	Le câble coaxial	243
6.1.3	La fibre optique	246
6.1.4	Les critères de choix des différents médias	250
6.1.5	La Boucle Locale Optique Mutualisée	251
6.1.6	Les câbles sous-marins intercontinentaux	254
6.2	Supports non limités	255
6.2.1	L'infrarouge	256
6.2.2	Le laser	256
6.2.3	Les ondes radio terrestres	256
6.2.4	Les ondes radio par satellites	258
6.2.5	L'orbite terrestre basse	259
6.2.6	Les ondes radio suivant les fréquences	262

Chapitre 4

Éléments logiciels de communication

1.	Configuration de la carte réseau	267
1.1	Configuration matérielle	268
1.2	Configuration logicielle	268
1.3	Spécifications NDIS et ODI	271

2.	Installation et configuration du pilote de carte réseau	273
2.1	Principes	273
2.2	Utilisation d'un outil fourni par le constructeur	274
2.3	Utilisation du système d'exploitation	275
2.3.1	Sous Windows	276
2.3.2	Sous Linux Red Hat	278
2.3.3	Sous macOS	283
2.3.4	Sur un smartphone Android	286
2.3.5	Tethering.	296
2.3.6	Sur un iPhone	306
3.	Pile de protocoles	312
4.	Détection d'un problème réseau	314
4.1	Connectique physique réseau	314
4.1.1	Le type de câble.	314
4.1.2	Le type de composants.	315
4.2	Configuration logicielle réseau	316

Chapitre 5

Architecture réseau et interconnexion

1.	Topologies.	319
1.1	Principes	319
1.2	Topologies standards	319
1.2.1	Le bus.	319
1.2.2	L'étoile	320
1.2.3	L'anneau	321
1.2.4	L'arbre	322
1.2.5	Les topologies dérivées.	322
1.2.6	Le cas des réseaux sans fil.	324
2.	Choix de la topologie réseau adaptée	325

8 Réseaux informatiques

Notions fondamentales

3.	Gestion de la communication	326
3.1	Sens de communication	326
3.1.1	Le mode simplex	326
3.1.2	Le mode half-duplex	327
3.1.3	Le mode full-duplex	327
3.2	Types de transmission	327
3.3	Méthodes d'accès au support	328
3.3.1	La contention	328
3.3.2	L'interrogation (polling)	330
3.3.3	Le jeton passant	330
3.4	Techniques de commutation	331
3.4.1	La commutation de circuits	331
3.4.2	La commutation de messages	332
3.4.3	La commutation de paquets	333
4.	Interconnexion de réseaux	334
4.1	Principes	334
4.2	Composants d'interconnexion et modèle OSI	335
4.3	Description fonctionnelle des composants	336
4.3.1	Le répéteur	336
4.3.2	Le pont	338
4.3.3	Le commutateur	350
4.3.4	Le routeur	366
4.3.5	La passerelle	388
4.4	Choix des matériels de connexion appropriés	388
4.4.1	Le répéteur	389
4.4.2	Le pont	389
4.4.3	Le commutateur	389
4.4.4	Le routeur	390
4.4.5	La passerelle	390
4.5	Exemple de topologie réseau locale sécurisée	390

Chapitre 6**Couches basses des réseaux locaux**

1. Couches basses et IEEE	393
1.1 Différenciation des couches	393
1.2 IEEE 802.1	394
1.3 IEEE 802.2	395
1.3.1 Les principes de Logical Link Control (LLC)	395
1.3.2 Les types de service	396
2. Ethernet et IEEE 802.3	396
2.1 Généralités	396
2.2 Caractéristiques de couche physique	397
2.2.1 Les spécificités d'Ethernet	397
2.2.2 Les spécificités de Fast Ethernet	404
2.2.3 Le gigabit Ethernet	406
2.2.4 Le 10 gigabit Ethernet	407
2.2.5 Le 40/100 gigabit Ethernet	408
2.2.6 Récapitulatif	410
2.3 En-tête de trame Ethernet	411
2.4 Les cartes hybrides Ethernet/SAN	412
3. Token Ring et IEEE 802.5	414
3.1 Configuration du réseau	414
3.2 Autoreconfiguration de l'anneau	418
4. Wi-Fi et IEEE 802.11	419
4.1 Présentation	419
4.2 Normes de couche physique	420
4.2.1 802.11b	421
4.2.2 802.11a	422
4.2.3 802.11g	422
4.2.4 802.11n	422
4.2.5 802.11ac	423
4.2.6 802.11ad	425
4.2.7 802.11ah - Wi-Fi HaLow	427

4.2.8	802.11ax - High Efficiency WLAN (HEW)	428
4.2.9	802.11be - Extremely High Throughput (EHT)	429
4.2.10	Normes et logos Wi-Fi	430
4.3	Matériels	432
4.3.1	La carte réseau	432
4.3.2	L'équipement d'infrastructure	432
4.3.3	Les périphériques Wi-Fi	434
4.4	Architecture	434
4.5	Sécurisation	435
4.5.1	Introduction	435
4.5.2	WEP	438
4.5.3	WPA/WPA 2	439
4.5.4	WPA 3	441
4.6	Usages	444
4.7	En-tête de trame Wi-Fi	445
5.	Bluetooth et IEEE 802.15	446
5.1	Historique	447
5.2	Standardisation	447
5.3	Réseau Bluetooth	451
5.4	Classes d'équipements	452
6.	Autres technologies	453
6.1	Autres standards de l'IEEE	453
6.1.1	802.16	454
6.1.2	802.17	454
6.1.3	802.18	455
6.1.4	802.19	455
6.1.5	802.21	455
6.1.6	802.22	455
6.1.7	802.24	456
6.2	Infrared Data Association (IrDA)	456
6.2.1	Le protocole IrDA DATA	457
6.2.2	Le protocole IrDA CONTROL	459

- 6.3 Courant porteur en ligne (CPL)..... 460
 - 6.3.1 Les principes 460
 - 6.3.2 Le fonctionnement 463
- 7. L'univers des objets connectés, IoT 465
 - 7.1 Introduction 465
 - 7.2 Évolution des objets connectés 467
 - 7.3 Accès aux objets connectés 469
 - 7.4 Problèmes soulevés par les objets connectés..... 470

Chapitre 7
Protocoles des réseaux MAN et WAN

- 1. Interconnexion du réseau local 473
 - 1.1 Usages du réseau téléphonique 473
 - 1.2 Réseau numérique à intégration de services (RNIS) 475
 - 1.2.1 Les principes 475
 - 1.2.2 Le rapport au modèle OSI 476
 - 1.2.3 Les types d'accès disponibles 477
 - 1.3 Ligne spécialisée (LS) 478
 - 1.3.1 Les principes 478
 - 1.3.2 Les débits..... 478
 - 1.4 Techniques xDSL 479
 - 1.4.1 Les principes 479
 - 1.4.2 Les différents services..... 480
 - 1.4.3 Les offres « quadruple play »..... 482
 - 1.5 Câble public 484
 - 1.6 Plan très haut débit en France (THD)..... 484
 - 1.7 WiMAX..... 487
 - 1.7.1 La boucle locale radio 487
 - 1.7.2 La solution WiMAX..... 487
 - 1.8 Réseaux cellulaires 489
 - 1.8.1 Les principes 489
 - 1.8.2 Les débuts 491

12 Réseaux informatiques

Notions fondamentales

1.8.3	L'évolution vers le transport de données	492
1.8.4	La troisième génération (3G) de téléphonie cellulaire . .	494
1.8.5	La quatrième génération (4G)	495
1.8.6	La cinquième génération (5G)	497
1.9	Fiber Distributed Data Interface (FDDI)	506
1.9.1	Les principes	506
1.9.2	La topologie	506
1.9.3	Le fonctionnement	507
1.10	Asynchronous Transfer Mode (ATM)	509
1.10.1	Les principes	509
1.10.2	Le relais de cellule	509
1.10.3	La régulation du trafic	510
1.10.4	Les types de services	511
1.10.5	La topologie et les débits	511
1.11	Synchronous Optical Network (SONET) et Synchronous Digital Hierarchy (SDH)	512
1.11.1	L'historique	512
1.11.2	Les caractéristiques de SDH	513
1.11.3	Les débits	513
1.12	X.25	514
1.13	Relais de trame	516
1.14	MPLS	517
1.14.1	Origine	517
1.14.2	Les principes	518
1.14.3	Le circuit virtuel et l'étiquetage	519
1.14.4	Le routage	519
2.	Accès distant et réseaux privés virtuels	520
2.1	Utilisation et évolution	520
2.2	Protocole d'accès distant	521
2.3	Réseau privé virtuel	521
2.3.1	L'établissement de la connexion	521
2.3.2	L'authentification	522
2.3.3	Le chiffrement	523

Chapitre 8
Protocoles des couches moyennes et hautes

- 1. Principales familles de protocoles 525
 - 1.1 IPX/SPX..... 525
 - 1.1.1 L'historique 525
 - 1.1.2 Les protocoles 526
 - 1.2 NetBIOS 527
 - 1.2.1 L'historique 527
 - 1.2.2 Les principes 528
 - 1.2.3 Les noms NetBIOS 529
 - 1.3 TCP/IP..... 533
 - 1.3.1 L'historique 533
 - 1.3.2 La suite de protocoles 534
 - 1.3.3 Le rapport au modèle OSI 535
 - 1.3.4 L'adoption en entreprise..... 535
- 2. Protocole IP version 4 536
 - 2.1 Principes 536
 - 2.2 Adressage..... 536
 - 2.2.1 L'adresse IPv4 536
 - 2.2.2 Le masque 537
 - 2.2.3 Les classes d'adresses..... 538
 - 2.2.4 Les adresses privées..... 542
 - 2.2.5 Les adresses APIPA 542
 - 2.3 L'adressage sans classe 543
 - 2.3.1 Les principes 543
 - 2.3.2 La notation CIDR..... 544
 - 2.3.3 Le rôle du masque en réseau 546
 - 2.3.4 La décomposition en sous-réseaux 552
 - 2.3.5 La factorisation des tables de routage 559
- 3. Protocole IP version 6 561
 - 3.1 Introduction 561
 - 3.2 Principes 562

14 Réseaux informatiques

Notions fondamentales

3.3	Structure d'une adresse IP	563
3.3.1	Catégories d'adresses	563
3.3.2	Portée d'une adresse	564
3.3.3	Adresse unicast	565
3.3.4	Formalisme	566
3.3.5	Identifiant EUI-64	568
3.3.6	Adresses réservées	570
3.3.7	Décomposition des plages par l'IETF	572
3.3.8	Découpage des catégories	575
3.3.9	Autoconfiguration des adresses IPv6	580
3.4	Tunnels	583
3.4.1	Introduction	583
3.4.2	Types de tunnels	584
3.5	Organismes d'attribution d'adresses	589
3.6	En-tête IPv6	591
4.	Autres protocoles de couche internet	592
4.1	Internet Control Message Protocol (ICMP)	592
4.2	Internet Group Management Protocol (IGMP)	595
4.3	Address Resolution Protocol (ARP) et Reverse Address Resolution Protocol (RARP)	596
4.4	Internet Protocol Security (IPsec)	597
4.5	Liste des numéros de protocoles de couche internet	598
5.	Voix sur IP (VoIP)	599
5.1	Principes	599
5.2	Quelques définitions importantes	599
5.3	Avantages	601
5.4	Fonctionnement	603
5.4.1	Le protocole H323	603
5.4.2	Les éléments terminaux	603
5.4.3	Les applications	604
6.	Protocoles de transport TCP et UDP	605
6.1	Transmission Control Protocol (TCP)	605
6.2	User Datagram Protocol (UDP)	606

- 7. Couche applicative TCP/IP 606
 - 7.1 Services de messagerie 606
 - 7.1.1 Simple Mail Transfer Protocol (SMTP) 606
 - 7.1.2 Post Office Protocol 3 (POP3) 608
 - 7.1.3 Internet Message Access Protocol (IMAP) 609
 - 7.2 Services de transfert de fichiers 610
 - 7.2.1 HyperText Transfer Protocol (HTTP) 610
 - 7.2.2 File Transfer Protocol (FTP) et Trivial FTP (TFTP) 613
 - 7.2.3 Network File System (NFS)..... 617
 - 7.3 Services d'administration et de gestion réseau 620
 - 7.3.1 Domain Name System (DNS) 620
 - 7.3.2 Dynamic Host Configuration Protocol v.4 (DHCPv4) . 631
 - 7.3.3 Telnet 645
 - 7.3.4 Network Time Protocol (NTP) 646
 - 7.3.5 Simple Network Management Protocol (SNMP). 649
 - 7.4 Services d'authentification..... 658
 - 7.4.1 Méthodes d'authentification 658
 - 7.4.2 NTLM 659
 - 7.4.3 Kerberos..... 662
 - 7.4.4 SAML 2.0..... 669
 - 7.4.5 OpenID Connect 670

Chapitre 9
Principes de sécurisation d'un réseau

- 1. Compréhension du besoin en sécurité 671
 - 1.1 Garanties exigées 671
 - 1.2 Dangers encourus 672
 - 1.2.1 La circulation des données 672
 - 1.2.2 Les protocoles Réseau et Transport..... 673
 - 1.2.3 Les protocoles applicatifs standards 673
 - 1.2.4 Les protocoles de couches basses 674
 - 1.2.5 Le risque au niveau logiciel 674

16 Réseaux informatiques

Notions fondamentales

2. Outils et types d'attaques	675
2.1 Ingénierie sociale	675
2.2 Écoute réseau	684
2.3 Analyse des ports	685
2.4 Codes malveillants	687
2.5 Programmes furtifs	688
2.6 Ransomware	689
3. Notions de sécurisation sur le réseau local	690
3.1 Services de la sécurité	690
3.1.1 Le contrôle d'accès au système	690
3.1.2 La gestion des habilitations	691
3.1.3 L'intégrité	691
3.1.4 La non-répudiation	692
3.2 Authentification	692
3.2.1 L'identification	693
3.2.2 L'authentification par mot de passe	697
3.2.3 L'authentification avec support physique	698
3.2.4 L'authentification par caractéristique humaine	699
3.3 Confidentialité	700
3.3.1 Le chiffrement à clés symétriques	701
3.3.2 Le chiffrement à clés asymétriques	702
3.4 Protection des données utilisateur	705
3.4.1 Protection de l'amorçage du disque	707
3.4.2 Chiffrement des disques locaux	711
3.4.3 Chiffrement des disques USB	713
3.5 Outils d'investigation liés à la sécurité	715
3.5.1 Vérification d'URL	715
3.5.2 Vérification de pièce jointe	718
3.5.3 Obtention d'informations complémentaires	720
4. Sécurisation de l'interconnexion de réseaux	726
4.1 Routeur filtrant	727
4.2 Translateur d'adresse	727
4.3 Pare-feu	728

4.4 Proxy 729
 4.5 Zone démilitarisée 730

Chapitre 10
Dépannage du réseau

1. Méthode d'approche 733
 2. Exemples de diagnostic de couches basses 734
 2.1 Matériels 735
 2.1.1 Le testeur de câbles 735
 2.1.2 Le réflectomètre 736
 2.1.3 Le multimètre numérique 737
 2.2 Analyse de trames 737
 2.3 Autres problèmes avec Ethernet 739
 2.3.1 L'unicité de l'adresse MAC 739
 2.3.2 La configuration physique de la carte réseau 739
 2.3.3 Les paramètres de communication 739
 2.4 IPX et Ethernet 740
 2.5 Autres problèmes liés à la fibre 740
 3. Utilisation des outils TCP/IP adaptés 741
 3.1 Principes 741
 3.2 Exemples d'utilisation des outils 741
 3.2.1 arp 741
 3.2.2 Neighbor Discovery Table 744
 3.2.3 ping 744
 3.2.4 tracert/traceroute 746
 3.2.5 ipconfig/ip address 748
 3.2.6 netstat 751
 3.2.7 Identification d'une adresse IP 753
 3.2.8 Géolocalisation d'une adresse IP 754
 3.2.9 nbtstat 754
 3.2.10 nslookup 756

18 Réseaux informatiques

Notions fondamentales

4. Outils d'analyse des couches hautes	759
4.1 La boîte à outils sysinternals	759
4.2 Analyse de requêtes applicatives	766
4.3 Analyse de requêtes web	767

Annexes

1. Conversion du décimal (base 10) vers le binaire (base 2)	771
1.1 Vocabulaire utilisé	771
1.2 Conversion à partir de la base 10	772
2. Conversion du binaire (base 2) vers le décimal (base 10)	774
3. Conversion de l'hexadécimal (base 16) vers le décimal (base 10)	775
4. Conversion de l'hexadécimal (base 16) vers le binaire (base 2)	777
5. Glossaire	778

Index	801
-----------------	-----

Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EI3RESAS** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

1. Introduction	15
2. Public concerné et démarche	17
3. Contenu	18
4. Organisation	22
5. Remerciements	23

Chapitre 1

Évolution des métiers autour des réseaux

1. Évolution de l'informatique et des réseaux	25
1.1 Les premiers ordinateurs	25
1.2 Réseaux à commutation de circuits	26
1.3 Réseaux à commutation de paquets	27
1.4 L'émergence des réseaux LAN et du protocole TCP/IP	29
1.5 L'évolution vers les réseaux ATM	30
1.6 L'émergence de la virtualisation de serveurs	31
1.7 Développement de l'Internet et du WAN	32
1.8 Le cloud computing	33
2. Le métier d'administrateur réseau	34
2.1 Tâches et missions de l'administrateur réseau	34
2.2 Extension et évolution du métier	35

2 _____ Les réseaux informatiques

Guide pratique pour l'administration, la sécurité et la supervision

2.3	De nouveaux domaines à maîtriser	36
2.3.1	Mouvance DevOps	36
2.3.2	Le contexte de la virtualisation	37
2.3.3	Certifications et outils d'autoformation	38
2.3.4	Un métier purement technique ?	43

Chapitre 2

Conception d'un réseau local

1.	Ethernet et les liaisons physiques	45
1.1	Historique	45
1.2	Principaux standards Ethernet et évolutions	46
1.3	Du courant fort sur Ethernet : le PoE	51
1.3.1	Principes de la norme	51
1.3.2	Performances et utilisation en pratique	53
1.4	Connexions fibrées sur un réseau local	55
2.	Segmentation d'un réseau	59
2.1	Pourquoi segmenter un réseau ?	59
2.1.1	Segmentation géographique	59
2.1.2	Segmentation fonctionnelle et sécuritaire	61
2.1.3	Segmentation pour raisons de performances	64
2.2	Segmentation réseau par la mise en place de VLANs	69
2.2.1	Principe des VLANs	69
2.2.2	Types de VLANs	70
2.2.3	Norme 802.1Q	71
2.2.4	Mise en place de liaisons interswitch et VLAN tagging	72
2.2.5	Gestion du tagging par les équipements réseau	74
2.3	Conception avancée de réseau à partir de VLANs	83
2.3.1	La norme QinQ ou 802.3ad : VLANs dans un VLAN	83
2.3.2	Extension des VLANs avec VXLAN	87
2.3.3	Private VLAN	90

Chapitre 3
Architectures opérateur et WAN

- 1. Le cadre légal des opérateurs en France 95
 - 1.1 Définition 95
 - 1.2 Les différents types d'opérateurs 96
 - 1.2.1 Les FAI : fournisseurs d'accès à Internet 96
 - 1.2.2 Opérateurs d'infrastructures 97
 - 1.2.3 Opérateurs de réseaux d'initiative publique (RIP) 97
 - 1.2.4 Opérateurs de téléphonie 99
 - 1.3 Les obligations légales. 100
- 2. Organisation technique des FAI 102
 - 2.1 Registres Internet régionaux (RIR) 102
 - 2.2 Blocs IP et numéro d'AS (ASN) 103
 - 2.3 Relations d'acheminement de trafic entre opérateurs :
Peering et Transit 105
 - 2.3.1 Relations de Transit IP 105
 - 2.3.2 Relations de Peering 108
 - 2.4 Hiérarchie entre opérateurs : les trois niveaux Tiers 113
- 3. Gestion de la boucle locale et raccordement physique au FAI. 115
 - 3.1 Vue d'ensemble de l'acheminement du trafic
de l'utilisateur final vers Internet 115
 - 3.2 Boucle locale optique 116
 - 3.3 Réseau de collecte et backbone 121
 - 3.3.1 Liaison PMZ - NRO 121
 - 3.3.2 La liaison NRO - point de présence opérateur (PoP) . . . 126
 - 3.4 Le choix d'une offre d'accès WAN pour une entreprise 127
 - 3.4.1 Critère de choix de l'accès WAN 127
 - 3.4.2 Accès fibre entreprise : FTTO 130
 - 3.4.3 Accès fibre réservés aux professionnels 131
 - 3.4.4 Conclusion : MultiWAN 133

4 _____ Les réseaux informatiques

Guide pratique pour l'administration, la sécurité et la supervision

Chapitre 4

Gestion des actifs et haute disponibilité

1. Gestion des commutateurs et routeurs	137
1.1 Outils et interfaces d'administration	137
1.1.1 Interfaces CLI	137
1.1.2 Interfaces web	142
1.1.3 Management via une application lourde	147
1.1.4 Management de l'équipement via API Rest pour l'automatisation	149
1.1.5 Les outils de développement dans la gestion des configurations : interrogation d'une API	153
1.1.6 Les outils de développement dans la gestion des configurations : gestion des versions avec Git	154
1.2 Gestion des configurations des éléments actifs	156
1.2.1 Mémoires d'un équipement et synchronisation	156
1.2.2 Synchronisation de la configuration	157
1.2.3 Sauvegarde et restauration de configuration	160
1.3 Gestion des systèmes d'exploitation des éléments actifs	162
1.3.1 Inventaire	162
1.3.2 Homogénéité du matériel	165
1.3.3 Mise à jour des équipements réseau	168
2. Haute disponibilité	171
2.1 Introduction	171
2.2 Redondance des liens physiques et agrégation	172
2.2.1 Principe du spanning-tree	172
2.2.2 Protocoles d'agrégation d'interfaces	174
2.3 Stacking de commutateurs	179
2.3.1 Stacking traditionnel	179
2.3.2 Capacité de commutation d'un commutateur	181
2.3.3 Particularités d'implémentation de stack	183
2.3.4 Stacking virtuel et MLAG	185

- 2.4 Redondance et clustering de niveau 3 195
 - 2.4.1 Principe du clustering sur des routeurs 195
 - 2.4.2 Le protocole VRRP et son fonctionnement 196
 - 2.4.3 Solutions propriétaires 201
 - 2.4.4 Redondance de liens opérateurs. 202

Chapitre 5

Principes de sécurité sur un réseau local

- 1. Sécurité au niveau des commutateurs. 211
 - 1.1 Les faiblesses du protocole ARP. 211
 - 1.2 Mécanisme de sécurité de port ou port-security 216
 - 1.3 Sécurité autour des mécanismes d'adressage IP 217
 - 1.3.1 Adressage statique ou dynamique via DHCP. 217
 - 1.3.2 DHCP Snooping 219
 - 1.4 Politiques d'accès au réseau 222
 - 1.4.1 Principe du NAC : Network Access Control 222
 - 1.4.2 Authentification 802.1x sur port de commutateur 223
 - 1.5 Saut de VLANs : hopping 226
- 2. Les firewalls. 229
 - 2.1 Caractéristiques d'un firewall 229
 - 2.1.1 Fonction et positionnement dans un réseau. 229
 - 2.1.2 Analyse jusqu'à la couche transport 232
 - 2.1.3 Analyse jusqu'à la couche applicative 235
 - 2.2 Les solutions du marché et comment faire son choix 238
 - 2.2.1 Solutions commerciales NGFW
(Next Generation Firewall) 238
 - 2.2.2 Solutions libres 240
 - 2.2.3 Intelligence Artificielle et firewall 242
 - 2.2.4 Critères de choix et métriques 244
 - 2.2.5 Firewall matériel ou virtuel ? 247

6 ————— Les réseaux informatiques

Guide pratique pour l'administration, la sécurité et la supervision

2.3	Tester son firewall	249
2.3.1	Utiliser des scanners de vulnérabilités pour tester l'analyse applicative	249
2.3.2	Tester l'état d'un port ou simuler un port ouvert sur une machine	250
2.3.3	Déterminer les ports ouverts en sortie d'un firewall	253
3.	Les attaques de déni de service	255
3.1	Principe de l'attaque	255
3.2	Dénis de service distribués	257
3.3	Moyens de protection	259

Chapitre 6

Gestion des accès distants aux ressources

1.	Connexion à distance sécurisée : VPN nomade	261
1.1	Principe	261
1.2	Solutions nomades libres	265
1.3	Solutions commerciales gratuites pour un usage limité	269
2.	Connexion site à site : VPN IPSec	271
2.1	Le principe	271
2.2	Les phases et la négociation d'un tunnel VPN IPSec	272
2.3	Les problématiques de NAT	275
2.4	Problématiques d'adressage IP	276
2.5	Guide pour une configuration IPSec site à site rapide et simple	278
3.	Autres types de VPN et ZTNA	279
3.1	VPN opérateurs : MPLS, VXLAN et EVPN	279
3.2	L'approche Zero Trust Network Acces ZTNA : le « reverse VPN par service »	281

Chapitre 7
Cyberattaques sur le réseau

- 1. Contexte et étapes d'une attaque 285
- 2. Récolte active d'informations sur le réseau..... 287
 - 2.1 Préambule 287
 - 2.2 Énumération de machines d'un réseau 287
 - 2.3 Énumération de services : scan de ports 290
 - 2.4 Énumération de services et de version 292
- 3. Récolte passive d'informations 296
 - 3.1 Informations par rapport à un nom de domaine 296
 - 3.2 Open Source Intelligence (OSINT) 299
 - 3.2.1 Principes 299
 - 3.2.2 Les Google Dorks 300
 - 3.2.3 Reconnaissance de services via des outils en ligne 301
 - 3.3 Ingénierie sociale (social engineering) 302
- 4. Phase d'exploitation 305
 - 4.1 Vulnérabilités et exploits 305
 - 4.1.1 Types de vulnérabilités..... 305
 - 4.1.2 Concept d'exploit 308
 - 4.2 La charge utile ou payload 308
 - 4.3 Actions post-intrusion 310
 - 4.3.1 Persistance, élévation des privilèges et latéralisation ... 310
 - 4.3.2 Anonymisation et SIEM 311
- 5. Cas d'étude : intrusion sur un réseau d'entreprise via l'exploitation d'une vulnérabilité sur une passerelle VPN SSL 314
 - 5.1 Préambule 314
 - 5.2 Contexte 314
 - 5.3 Reconnaissance de la cible 315
 - 5.4 Récupération d'un exploit et intrusion 316
 - 5.5 Utilisation directe du framework Metasploit..... 319
 - 5.6 Épilogue..... 321

8 ————— Les réseaux informatiques

Guide pratique pour l'administration, la sécurité et la supervision

Chapitre 8

Approche globale de la supervision avec SNMP

1. Définition de la supervision	323
1.1 Contexte de la DSI	323
1.2 Comment détecter un problème technique ?	324
1.3 Comment traiter un problème technique ?	325
1.4 Améliorer la disponibilité effective	326
2. Approche ISO	327
2.1 Cahier des charges initial	327
2.2 Gestion des incidents	328
2.3 Gestion des configurations	329
2.4 Gestion des performances	333
2.4.1 Mesure de la performance	333
2.4.2 Les politiques de qualité de service	334
2.5 Gestion de la sécurité	336
2.6 Gestion de la comptabilité	336
3. Entreprendre un projet de supervision	338
3.1 Erreurs à éviter	338
3.2 Que superviser au niveau réseau ?	340
3.2.1 Disponibilité des actifs	340
3.2.2 Variables à contrôler selon le type d'équipement réseau	344
4. Supervision réseau via le protocole SNMP	346
4.1 Principes du protocole SNMP	346
4.1.1 Caractéristiques du protocole SNMP	346
4.1.2 Modélisation d'un élément actif : la MIB	347
4.1.3 Première approche sur la structure de la MIB par un cas d'étude	349
4.2 Les MIB publiques et privées	353
4.2.1 Principe général de la MIB I et la MIB II	353
4.2.2 Organisation de la MIB I	356
4.2.3 Organisation de la MIB II	362

4.2.4	MIB privées et intégration dans le manager	364
4.3	Configurer SNMP	365
4.3.1	Les communautés et les droits	365
4.3.2	Les types de messages	369
4.3.3	Requêtes sur la MIB selon la communauté et les droits sur l'OID	373
4.3.4	Étapes de configuration minimale SNMP	375

Chapitre 9

Autres protocoles de supervision réseau

1.	Gestion des journaux avec Syslog	377
1.1	Enjeux de la journalisation des événements	377
1.1.1	Fonctions initiales des logs	377
1.1.2	Enjeux juridiques	378
1.1.3	Besoin d'une gestion centralisée	380
1.2	Principes du protocole Syslog	381
1.2.1	Fonctionnement global	381
1.2.2	Classification des logs générés	383
1.2.3	Format de la trame	386
1.3	Configuration de Syslog	388
1.4	Solutions de collecte et d'analyse de logs	392
1.4.1	Critères de choix du collecteur	392
1.4.2	Les collecteurs basés sur de l'open source ou gratuits	394
1.4.3	Autres collecteurs	399
2.	Les protocoles de supervision de flux réseau	405
2.1	Introduction à NetFlow	405
2.1.1	Origines du protocole	405
2.1.2	Cas d'utilisation	406
2.1.3	Caractéristiques et contenu d'un flux NetFlow	407
2.1.4	Fonctionnement et architectures	410
2.2	Configuration sur un actif réseau	411

10 _____ Les réseaux informatiques

Guide pratique pour l'administration, la sécurité et la supervision

2.3	Les collecteurs NetFlow et les applications d'analyse	415
2.3.1	Le marché	415
2.3.2	Les collecteurs basés sur de l'open source ou gratuits . .	415
2.3.3	Les solutions payantes et propriétaires	419
2.4	Le protocole sFlow	423
2.4.1	Principes de sFlow	423
2.4.2	NetFlow vs sFlow	424
2.5	Les sondes RMON	426
2.5.1	Principes de RMON	426
2.5.2	Fonctionnalités apportées par RMON	428
2.5.3	Exploration des MIB RMON 1 et 2	429
2.5.4	Configuration de RMON	434

Chapitre 10

Métriologie et mesure de performances

1.	Métriologie et métriques réseau	437
1.1	Définition de la métriologie	437
1.2	Les métriques réseau	439
1.3	Méthodologie de tests de performances	441
2.	Mesure de débit et optimisation	443
2.1	Débit brut et débit applicatif	443
2.2	Outils Iperf/Jperf	445
2.3	Ajuster les paramètres réseau pour augmenter le débit	449
2.4	Débits au-delà du gigabit et jumbo frames	452
2.5	Importance des performances dans un réseau SAN	458
2.6	Communication directe entre mémoire et carte réseau : le RDMA	462
2.7	Dimensionnement du débit applicatif	465
2.7.1	Caractéristiques des réseaux IP en matière de débit	465
2.7.2	Mesure de débit sur le serveur ou le poste utilisateur	466
2.7.3	Captures de trames et mesures via le SPAN	468

3.	Mesurer les temps de réponse	470
3.1	Mesure de la latence et de la gigue	470
3.1.1	Ping	470
3.1.2	Traceroute	472
3.1.3	Calculer la gigue	473
3.2	Perte de paquets et disponibilité	474
3.2.1	Évaluation de la perte de paquet	474
3.2.2	Taux de disponibilité d'un service	475
3.2.3	Disponibilité d'un service en « nombre de neuf »	476
3.2.4	Analyse des services joignables	477
3.3	Temps de réponse applicatif	479
3.3.1	Notion d'Expérience Utilisateur (UX)	479
3.3.2	Scripts de surveillance	479
3.3.3	Monitoring des utilisateurs en temps réel (RUM)	481
3.4	Temps de réponse d'une application web	483
3.4.1	Introduction	483
3.4.2	Responsabilités techniques des performances d'une application web hébergée	483
3.4.3	Temps de réponse et montée en charge	487
3.4.4	Métriques spécifiques pour caractériser une application web	488
3.5	Performances d'un réseau de téléphonie IP	492
3.5.1	Gestion de la téléphonie par l'équipe réseau	492
3.5.2	Exigences des réseaux temps réel par rapport aux réseaux de données	493
3.5.3	Bande passante pour la téléphonie IP et codecs	495
3.5.4	Adaptation du réseau pour transmettre les flux VoIP	497
4.	Les outils de supervision spécialisés en métrologie	498
4.1	Stocker les mesures	498
4.1.1	Problématique de stockage des données de métrologie	498
4.1.2	Outils répandus de stockage des données de métrologie	499

12 _____ Les réseaux informatiques

Guide pratique pour l'administration, la sécurité et la supervision

4.2	Afficher les données mesurées	500
4.2.1	Représentation des données.	500
4.2.2	Outils répandus et conçus pour l'affichage de données métrologiques	501
4.3	Collecter les mesures	503
4.3.1	Moyens de collecte	503
4.3.2	Outils libres de collecte multiprotocoles.	504
4.4	Solutions complètes libres	505
4.4.1	Les fonctions à couvrir	505
4.4.2	InfluxDB/Telegraf/Graphana	505
4.4.3	ELK avec agents Beat	506
4.4.4	Cacti	507
4.4.5	LibreNMS	508
4.4.6	Graphite	509

Chapitre 11

Virtualisation du réseau et SDN

1.	Virtualisation du réseau	511
1.1	Virtualisation et cloud computing	511
1.1.1	Historique et principe de la virtualisation	511
1.1.2	Services de cloud computing proposés au sein des datacenters.	513
1.2	Cloud computing et réseaux des datacenters.	516
1.2.1	Architecture réseau traditionnelle.	516
1.2.2	Modifications de l'architecture réseau des datacenters .	517
1.2.3	Ajout d'une couche virtuelle au sein du réseau.	522
1.3	Virtualisation des fonctions réseau : NFV	523
1.3.1	Technologies de virtualisation réseau	523
1.3.2	Problématiques des appliances matérielles	524
1.3.3	Avantages apportés par la NFV.	524
1.3.4	Solutions proposées par éditeurs et équipementiers . . .	526
1.3.5	Performances des appliances réseau virtuelles	527

1.4	Gestion des actifs réseau d'un datacenter	528
2.	Approche du SDN (Software Defined Network)	529
2.1	Architecture de commutation et routage	529
2.1.1	La commutation de paquets	529
2.1.2	Plans de données, de contrôle et de gestion	529
2.2	Caractéristiques du SDN	533
2.2.1	Définition du SDN	533
2.2.2	Technologies pionnières et analogies	535
2.2.3	Le standard OpenFlow	537
2.2.4	Le contrôleur SDN	540
2.2.5	Implémentations du SDN	541
2.3	Solutions du marché.	542
2.3.1	Solutions libres	542
2.3.2	Solutions propriétaires	543
2.4	Le SD-WAN (Software-Defined WAN)	546
2.4.1	Les nouvelles attentes du WAN.	546
2.4.2	Principes du SD-WAN	547
2.4.3	Les acteurs du marché et les évolutions vers le SASE. . .	550
	Glossaire	553
	Index	569