

### Avant-propos

|                                       |           |
|---------------------------------------|-----------|
| <b>1. Introduction</b>                | <b>11</b> |
| <b>2. Public concerné et démarche</b> | <b>13</b> |
| <b>3. Contenu</b>                     | <b>13</b> |
| <b>4. Organisation</b>                | <b>16</b> |
| <b>5. Remerciements</b>               | <b>16</b> |

### Évolution des métiers autour des réseaux

|  |           |
|--|-----------|
| <b>1. Évolution de l'informatique et des réseaux</b>   | <b>19</b> |
| 1.1 Les premiers ordinateurs                           | 19        |
| 1.2 Réseaux à commutation de circuits                  | 20        |
| 1.3 Réseaux à commutation de paquets                   | 21        |
| 1.4 L'émergence des réseaux LAN et du protocole TCP/IP | 23        |
| 1.5 L'évolution vers les réseaux ATM                   | 24        |
| 1.6 L'émergence de la virtualisation de serveurs       | 25        |
| 1.7 Développement de l'Internet et du WAN              | 26        |
| 1.8 Le cloud computing                                 |           |

27

## 2. Le métier d'administrateur réseau

28

2.1 Tâches et missions de l'administrateur réseau

28

2.2 Extension et évolution du métier

28

2.3 De nouveaux domaines à maîtriser

29

2.3.1 Mouvance DevOps

29

2.3.2 Le contexte de la virtualisation

30

2.3.3 Certifications et outils d'autoformation

31

2.3.4 Un métier purement technique ?

35

## Conception d'un réseau local

### 1. Ethernet et les liaisons physiques

37

1.1 Historique

37

1.2 Principaux standards Ethernet et évolutions

38

1.3 Du courant fort sur Ethernet : le PoE

41

1.3.1 Principes de la norme

41

1.3.2 Performances et utilisation en pratique

42

### 2. Segmentation d'un réseau

44

2.1 Pourquoi segmenter un réseau ?

44

|       |   |    |
|-------|---|----|
| 2.1.1 | Segmentation géographique                             | 44 |
| 2.1.2 | Segmentation fonctionnelle et sécuritaire             | 45 |
| 2.1.3 | Segmentation pour raisons de performances             | 49 |
| 2.2   | Segmentation réseau par la mise en place de VLANs     | 54 |
| 2.2.1 | Principe des VLANs                                    | 54 |
| 2.2.2 | Types de VLANs  | 54 |
| 2.2.3 | Norme 802.1Q  | 56 |
| 2.2.4 | Mise en place de liaisons interswitch et VLAN tagging | 57 |
| 2.2.5 | Gestion du tagging par les équipements réseau         | 59 |
| 2.3   | Conception avancée de réseau à partir de VLANs        | 66 |
| 2.3.1 | La norme QinQ ou 802.3ad : VLANs dans un VLAN         | 66 |
| 2.3.2 | Extension des VLANs avec VXLAN                        | 70 |
| 2.3.3 | Private VLAN  | 73 |

## Gestion des actifs et haute disponibilité

### 1. Gestion des commutateurs et routeurs

|       |                                       |    |
|-------|---------------------------------------|----|
| 1.1   | Outils et interfaces d'administration | 79 |
| 1.1.1 | Interfaces CLI                        | 79 |
| 1.1.2 | Interfaces web                        | 84 |
| 1.1.3 | Autres possibilités de management     | 86 |

|   |            |
|---|------------|
| 1.2 Gestion des configurations des éléments actifs          | 89         |
| 1.2.1 Mémoires d'un équipement et synchronisation           | 89         |
| 1.2.2 Synchronisation de la configuration                   | 89         |
| 1.2.3 Sauvegarde et restauration de configuration           | 92         |
| 1.3 Gestion des systèmes d'exploitation des éléments actifs | 94         |
| 1.3.1 Inventaire  | 94         |
| 1.3.2 Homogénéité du matériel                               | 96         |
| 1.3.3 Mise à jour des équipements réseau                    | 99         |
| <b>2. Haute disponibilité</b>                               | <b>103</b> |
| 2.1 Introduction  | 103        |
| 2.2 Redondance des liens physiques et agrégation            | 103        |
| 2.2.1 Principe du spanning-tree                             | 103        |
| 2.2.2 Protocoles d'agrégation d'interfaces                  | 106        |
| 2.3 Stacking de commutateurs                                | 111        |
| 2.3.1 Stacking traditionnel                                 | 111        |
| 2.3.2 Capacité de commutation d'un commutateur              | 113        |
| 2.3.3 Particularités d'implémentation de stack              | 115        |
| 2.3.4 Vers un stack virtuel                                 | 117        |
| 2.4 Redondance et clustering de niveau 3                    | 118        |
| 2.4.1 Principe du clustering sur des routeurs               | 118        |

|   |     |
|---|-----|
| 2.4.2 Le protocole VRRP et son fonctionnement | 119 |
| 2.4.3 Solutions propriétaires                 | 124 |
| 2.4.4 Redondance de liens opérateurs          | 125 |

## Principes de sécurité sur un réseau local

|   |            |
|---|------------|
| <b>1. Sécurité au niveau des commutateurs</b>         | <b>133</b> |
| 1.1 Les faiblesses du protocole ARP                   | 133        |
| 1.2 Mécanisme de sécurité de port ou port-security    | 138        |
| 1.3 Sécurité autour des mécanismes d'adressage IP     | 140        |
| 1.3.1 Adressage statique ou dynamique via DHCP        | 140        |
| 1.3.2 DHCP Snooping                                   | 141        |
| 1.4 Politiques d'accès au réseau                      | 144        |
| 1.4.1 Principe du NAC : Network Access Control        | 144        |
| 1.4.2 Authentification 802.1x sur port de commutateur | 145        |
| 1.5 Saut de VLANs : hopping                           | 147        |
| <b>2. Les firewalls</b>                               | <b>151</b> |
| 2.1 Caractéristiques d'un firewall                    | 151        |
| 2.1.1 Fonction et positionnement dans un réseau       | 151        |
| 2.1.2 Analyse jusqu'à la couche transport             | 154        |
| 2.1.3 Analyse jusqu'à la couche applicative           |            |

|  |            |
|--|------------|
| 2.2 Les solutions du marché et comment faire son choix       | 157        |
| 2.2.1 Solutions commerciales NGFW (Next Generation Firewall) | 158        |
| 2.2.2 Solutions libres                                       | 158        |
| 2.2.3 Critères de choix et métriques                         | 161        |
| 2.2.4 Firewall matériel ou virtuel ?                         | 162        |
| 2.3 Tester son firewall                                      | 165        |
| <b>3. Les attaques de déni de service</b>                    | <b>167</b> |
| 3.1 Principe de l'attaque                                    | 169        |
| 3.2 Dénis de services distribués                             | 172        |
| 3.3 Moyens de protection                                     | 173        |
| <b>4. Gestion des accès distants</b>                         | <b>174</b> |
| 4.1 Connexion à distance sécurisée : VPN nomade              | 174        |
| 4.1.1 Principe   | 174        |
| 4.1.2 Solutions nomades libres                               | 179        |
| 4.2 Connexion site à site : VPN IPSEC                        | 182        |
| 4.2.1 Le principe  | 182        |
| 4.2.2 Les phases et la négociation d'un tunnel VPN IPSEC     | 183        |
| 4.2.3 Les problématiques de NAT                              | 185        |
| 4.2.4 Problématiques d'adressage IP                          | 187        |

|   |     |
|---|-----|
| 4.2.5 Guide pour une configuration IPSEC site à site rapide et simple | 188 |
| 4.3 Autres types de VPN   | 189 |

## Approche globale de la supervision avec SNMP

|   |            |
|---|------------|
| <b>1. Définition de la supervision</b>          | <b>191</b> |
| 1.1 Contexte de la DSI                          | 191        |
| 1.2 Comment détecter un problème technique ?    | 192        |
| 1.3 Comment traiter un problème technique ?     | 193        |
| 1.4 Améliorer la disponibilité effective        | 194        |
| <b>2. Approche ISO</b>                          | <b>195</b> |
| 2.1 Cahier des charges initial                  | 195        |
| 2.2 Gestion des incidents                       | 196        |
| 2.3 Gestion des configurations                  | 197        |
| 2.4 Gestion des performances                    | 199        |
| 2.4.1 Mesure de la performance                  | 199        |
| 2.4.2 Les politiques de qualité de service      | 200        |
| 2.5 Gestion de la sécurité                      | 202        |
| 2.6 Gestion de la comptabilité                  | 203        |
| <b>3. Entreprendre un projet de supervision</b> | <b>204</b> |

|   |            |
|---|------------|
| 3.1 Erreurs à éviter  | 204        |
| 3.2 Que superviser au niveau réseau ?                                 | 206        |
| 3.2.1 Disponibilité des actifs  | 206        |
| 3.2.2 Variables à contrôler selon le type d'équipement réseau         | 208        |
| <b>4. Supervision réseau via le protocole SNMP</b>                    | <b>210</b> |
| 4.1 Principes du protocole SNMP                                       | 210        |
| 4.1.1 Caractéristiques du protocole SNMP                              | 210        |
| 4.1.2 Modélisation d'un élément actif : la MIB                        | 211        |
| 4.1.3 Première approche sur la structure de la MIB par un cas d'étude | 213        |
| 4.2 Les MIB publiques et privées                                      | 217        |
| 4.2.1 Principe général de la MIB I et la MIB II                       | 217        |
| 4.2.2 Organisation de la MIB I  | 220        |
| 4.2.3 Organisation de la MIB II                                       | 226        |
| 4.2.4 MIB privées et intégration dans le manager                      | 228        |
| 4.3 Configurer SNMP   | 229        |
| 4.3.1 Les communautés et les droits                                   | 229        |
| 4.3.2 Les types de messages   | 231        |
| 4.3.3 Requêtes sur la MIB selon la communauté et les droits sur l'OID | 235        |
| 4.3.4 Étapes de configuration minimale SNMP                           | 237        |



### Autres protocoles de supervision réseau

|  |            |
|--|------------|
| <b>1. Gestion des journaux avec Syslog</b>                   | <b>239</b> |
| 1.1 Enjeux de la journalisation des événements               | 239        |
| 1.1.1 Fonctions initiales des logs                           | 239        |
| 1.1.2 Enjeux juridiques                                      | 240        |
| 1.1.3 Besoin d'une gestion centralisée                       | 242        |
| 1.2 Principes du protocole Syslog                            | 243        |
| 1.2.1 Fonctionnement global                                  | 243        |
| 1.2.2 Classification des logs générés                        | 245        |
| 1.2.3 Format de la trame                                     | 248        |
| 1.3 Configuration de Syslog                                  | 250        |
| 1.4 Solutions de collecte et d'analyse de logs               | 254        |
| 1.4.1 Critères de choix du collecteur                        | 254        |
| 1.4.2 Les collecteurs basés sur de l'open source ou gratuits | 256        |
| 1.4.3 Autres collecteurs                                     | 261        |
| <b>2. Les protocoles de supervision de flux réseau</b>       | <b>264</b> |
| 2.1 Introduction à NetFlow                                   | 264        |
| 2.1.1 Origines du protocole                                  | 264        |
| 2.1.2 Cas d'utilisation                                      | 265        |

|       |  |     |
|-------|--|-----|
| 2.1.3 | Caractéristiques et contenu d'un flux NetFlow          | 266 |
| 2.1.4 | Fonctionnement et architectures                        | 268 |
| 2.2   | Configuration sur un actif réseau                      | 270 |
| 2.3   | Les collecteurs NetFlow et les applications d'analyse  | 273 |
| 2.3.1 | Le marché  | 273 |
| 2.3.2 | Les collecteurs basés sur de l'open source ou gratuits | 274 |
| 2.3.3 | Les solutions payantes                                 | 277 |
| 2.4   | Le protocole sFlow                                     | 281 |
| 2.4.1 | Principes de sFlow                                     | 281 |
| 2.4.2 | NetFlow vs sFlow                                       | 282 |
| 2.5   | Les sondes RMON  | 285 |
| 2.5.1 | Principes de RMON                                      | 285 |
| 2.5.2 | Fonctionnalités apportées par RMON                     | 287 |
| 2.5.3 | Exploration des MIB RMON 1 et 2                        | 288 |
| 2.5.4 | Configuration de RMON                                  | 293 |

## Métrologie et mesure de performances

|  |            |
|--|------------|
| <b>1. Métrologie et métriques réseau</b> | <b>295</b> |
| 1.1 Définition de la métrologie          | 295        |
| 1.2 Les métriques réseau                 | 297        |

|   |            |
|---|------------|
| 1.3 Méthodologie de tests de performances                         | 299        |
| <b>2. Mesure de débit et optimisation</b>                         | <b>301</b> |
| 2.1 Débit brut et débit applicatif                                | 301        |
| 2.2 Outils Iperf/Jperf  | 303        |
| 2.3 Ajuster les paramètres réseau pour augmenter le débit         | 306        |
| 2.4 Mesurer des débits au-delà du gigabit                         | 309        |
| 2.5 Importance des performances dans un réseau SAN                | 313        |
| 2.6 Communication directe entre mémoire et carte réseau : le RDMA | 317        |
| 2.7 Dimensionnement du débit applicatif                           | 320        |
| 2.7.1 Caractéristiques des réseaux IP en matière de débit         | 320        |
| 2.7.2 Mesure de débit sur le serveur ou le poste utilisateur      | 321        |
| 2.7.3 Captures de trames et mesures via le SPAN                   | 323        |
| <b>3. Mesurer les temps de réponse</b>                            | <b>325</b> |
| 3.1 Mesure de la latence et de la gigue                           | 325        |
| 3.1.1 Ping  | 325        |
| 3.1.2 Traceroute  | 327        |
| 3.1.3 Calculer la gigue   | 328        |
| 3.2 Perte de paquets et disponibilité                             | 329        |
| 3.2.1 Évaluation de la perte de paquet                            | 329        |
| 3.2.2 Taux de disponibilité d'un service                          | 329        |

|  |            |
|--|------------|
| 3.2.3 Disponibilité d'un service en « nombre de neuf »                           | 329        |
| 3.2.4 Analyse des services joignables  | 331        |
| 3.3 Temps de réponse applicatif  | 332        |
| 3.3.1 Notion d'Expérience Utilisateur (UX)                                       | 334        |
| 3.3.2 Scripts de surveillance  | 334        |
| 3.3.3 Monitoring des utilisateurs en temps réel (RUM)                            | 336        |
| 3.4 Temps de réponse d'une application web                                       | 338        |
| 3.4.1 Introduction   | 338        |
| 3.4.2 Responsabilités techniques des performances d'une application web hébergée | 338        |
| 3.4.3 Temps de réponse et montée en charge                                       | 342        |
| 3.4.4 Métriques spécifiques pour caractériser une application web                | 343        |
| 3.5 Performances d'un réseau de téléphonie IP                                    | 347        |
| 3.5.1 Gestion de la téléphonie par l'équipe réseau                               | 347        |
| 3.5.2 Exigences des réseaux temps réel par rapport aux réseaux de données        | 348        |
| 3.5.3 Bande passante pour la téléphonie IP et codecs                             | 350        |
| 3.5.4 Adaptation du réseau pour transmettre les flux VOIP                        | 352        |
| <b>4. Les outils de supervision spécialisés en métrologie</b>                    | <b>353</b> |
| 4.1 Stocker les mesures  | 353        |
| 4.1.1 Problématique de stockage des données de métrologie                        | 353        |
| 4.1.2 Outils répandus de stockage des données de métrologie                      |            |

|   |     |
|---|-----|
| 4.2 Afficher les données mesurées   | 354 |
| 4.2.1 Représentation des données  | 355 |
| 4.2.2 Outils répandus et conçus pour l'affichage de données métrologiques | 355 |
| 4.3 Collecter les mesures   | 356 |
| 4.3.1 Moyens de collecte  | 358 |
| 4.3.2 Outils libres de collecte multiprotocoles                           | 358 |
| 4.4 Solutions complètes libres  | 359 |
| 4.4.1 Les fonctions à couvrir   | 360 |
| 4.4.2 InfluxDB/Telegraf/Graphana  | 360 |
| 4.4.3 ELK avec agents Beat  | 361 |
| 4.4.4 Cacti   | 361 |
| 4.4.5 LibreNMS  | 362 |
| 4.4.6 Graphite  | 364 |
|   | 364 |

## Une nouvelle approche du réseau : SDN et NFV

### 1. Virtualisation du réseau

|  |     |
|--|-----|
| 1.1 Virtualisation et cloud computing                              | 367 |
| 1.1.1 Historique et principe de la virtualisation                  | 367 |
| 1.1.2 Services de cloud computing proposés au sein des datacenters | 367 |
| 1.2 Cloud computing et réseaux des datacenters                     | 369 |

|  |            |
|--|------------|
| 1.2.1 Architecture réseau traditionnelle                     | 372        |
| 1.2.2 Modifications de l'architecture réseau des datacenters | 372        |
| 1.2.3 Ajout d'une couche virtuelle au sein du réseau         | 373        |
| 1.3 Virtualisation des fonctions réseau : NFV                | 375        |
| 1.3.1 Technologies de virtualisation réseau                  | 375        |
| 1.3.2 Problématiques des appliances matérielles              | 375        |
| 1.3.3 Avantages apportés par la NFV                          | 376        |
| 1.3.4 Solutions proposées par éditeurs et équipementiers     | 376        |
| 1.3.5 Performances des appliances réseau virtuelles          | 378        |
| 1.4 Gestion des actifs réseau d'un datacenter                | 379        |
| <b>2. Approche du SDN (Software Defined Network)</b>         | <b>380</b> |
| 2.1 Architecture de commutation et routage                   | 380        |
| 2.1.1 La commutation de paquets                              | 380        |
| 2.1.2 Plans de données, de contrôle et de gestion            | 380        |
| 2.2 Caractéristiques du SDN                                  | 383        |
| 2.2.1 Définition du SDN                                      | 383        |
| 2.2.2 Technologies pionnières et analogies                   | 385        |
| 2.2.3 Le standard OpenFlow                                   | 387        |
| 2.2.4 Le contrôleur SDN                                      | 390        |
| 2.2.5 Implémentations du SDN                                 | 390        |

# Les réseaux informatiques

Guide pratique pour l'administration et la supervision

|                                      |            |
|--------------------------------------|------------|
| 2.3 Solutions du marché              | 391        |
| 2.3.1 Solutions libres               | 392        |
| 2.3.2 Solutions propriétaires        | 392        |
| 2.4 Le SD-WAN (Software-Defined WAN) | 394        |
| 2.4.1 Les nouvelles attentes du WAN  | 395        |
| 2.4.2 Principes du SD-WAN            | 395        |
| 2.4.3 Les acteurs du marché          | 396        |
|                                      | 399        |
| <b>Glossaire</b>                     | <b>401</b> |
| <b>Index</b>                         | <b>411</b> |