

Administration et sécurisation des infrastructures réseaux

3.1. Introduction à l'infrastructure réseau

L'infrastructure réseau constitue l'ossature de tout système d'information : c'est **le lien entre les équipements, les utilisateurs, les services hébergés localement et dans le cloud**. Un réseau bien administré garantit la **connectivité, la sécurité, la performance** et la **résilience** des services informatiques.

L'administrateur d'infrastructures sécurisées doit maîtriser **l'ensemble des composants physiques et logiques** du réseau, en tenant compte des **besoins métiers, des contraintes de sécurité et de la réglementation**.

3.2. Architecture d'un réseau d'entreprise

Composants de base :

- **Commutateurs (switches)** : niveau 2 et 3, cœur du réseau local
- **Routeurs** : interconnexion des réseaux, accès Internet
- **Points d'accès sans fil (Wi-Fi)** : mobilité des utilisateurs
- **Pare-feux** : segmentation et filtrage du trafic
- **Passerelles VPN** : connexions sécurisées à distance
- **Baies de brassage, câblage structuré** : organisation physique

Modèles d'architecture :

- **Modèle OSI (7 couches) et TCP/IP** : bases protocolaires
 - **Topologie hiérarchique** : accès – distribution – cœur
 - **Segmentation réseau** : VLAN, DMZ, zones de confiance
-

3.3. Sécurisation de l'infrastructure réseau

La **sécurité réseau** repose sur plusieurs piliers essentiels :

? Filtrage et contrôle d'accès

- ACL (Access Control Lists)
- VLAN privés
- Filtrage MAC / 802.1X / NAC
- Authentification forte (MFA)

? Cloisonnement logique

- VLAN : séparation par fonction ou par niveau de sensibilité
- Routage inter-VLAN contrôlé par pare-feu ou ACL

? Surveillance du trafic

- Analyse des flux via NetFlow, sFlow
- Logs réseau centralisés (Syslog)
- Inspection des paquets (deep packet inspection)

? Solutions spécialisées

- IDS/IPS (Snort, Suricata, Cisco Firepower)
 - Bastions d'administration
 - Reverse proxy, WAF, load balancer
-

3.4. Administration des réseaux locaux (LAN) et étendus (WAN)

Réseau local (LAN) :

- Configuration des commutateurs (Cisco, HP, Mikrotik...)
- Déploiement VLAN : voix, data, invité, sécurité
- Gestion de l'alimentation PoE, des boucles (Spanning Tree Protocol)

Réseau étendu (WAN) :

- Routage : statique vs dynamique (OSPF, BGP)
 - Interconnexion multisites : MPLS, SD-WAN, VPN IPsec
 - Redondance et haute disponibilité (HSRP, VRRP, BFD)
-

3.5. Administration des connexions distantes et nomades

Accès nomade :

- VPN SSL / IPsec
- Client VPN intégré (Windows, OpenVPN, FortiClient)
- MFA avec OTP ou token matériel

Mobilité et BYOD :

- Portail captif (Eduroam, Cisco ISE, Aruba)
- Contrôle de conformité (NAC) avant accès réseau

- Segmentation spécifique pour périphériques personnels
-

3.6. Surveillance et évaluation des performances réseau

L'AIS doit surveiller et évaluer la **qualité de service réseau (QoS)** :

Indicateur	Objectif
Bande passante	Saturation des liens
Latence	Réactivité des applications
Jitter	Stabilité du flux (visioconférence, VoIP)
Perte de paquets	Fiabilité des transmissions

Outils associés :

- Ping, Traceroute, iperf
 - SNMP (Simple Network Management Protocol)
 - NMS (Zabbix, PRTG, SolarWinds)
 - Sondes d'analyse passive (Wireshark, tcpdump)
-

3.7. Plan d'adressage IP et gestion des services réseau

Adressage IP :

- IPv4/IPv6
- Répartition logique par VLAN
- DHCP centralisé
- Plan d'adressage documenté et versionné

Services associés :

- **DNS** : résolution interne/externe, serveurs maîtres/esclaves
 - **DHCP** : baux réservés, failover
 - **NTP** : horodatage synchronisé
 - **Syslog** : centralisation des événements
-

3.8. Documentation et procédures réseau

Un réseau professionnel nécessite une **documentation complète et normalisée** :

- Cartographie réseau (LAN, WAN, VLAN, Wi-Fi)
- Plans d'adressage IP
- Procédures d'ajout/suppression d'équipements

- Procédures de diagnostic, de reconfiguration, de redémarrage
 - Documents de sécurité (pare-feu, règles NAT, accès distants)
 - Historique des changements (gestion de configuration)
-

3.9. Conformité réglementaire et recommandations ANSSI

Les AIS doivent se référer aux **règles françaises et européennes** :

- **ANSSI** : guides techniques pour les équipements réseau, VPN, Firewalls
- **CNIL / RGPD** : protection des données en transit, sécurisation des accès
- **Respect des SLA fournisseurs** : niveau de disponibilité, support, sécurité

Recommandations ANSSI :

- Journalisation obligatoire sur équipements critiques
 - Accès distant via bastion sécurisé
 - Tests réguliers des plans de reprise réseau
 - Cloisonnement des flux d'administration
 - Revue annuelle des configurations
-

3.10. Activités pratiques et évaluation

Mises en situation :

- Création d'un VLAN segmenté
- Configuration d'un VPN IPsec
- Diagnostic d'un problème réseau avec Wireshark
- Intégration de règles sur un pare-feu UTM
- Simulation de coupure réseau et bascule

Évaluations proposées :

- **QCM** : architecture réseau, sécurité, modèles OSI/TCP-IP
 - **Projet** : documentation + sécurisation d'un réseau d'entreprise fictif
 - **Oral** : présentation d'une architecture réseau sécurisée
-

✓ Cette section permet aux apprenants du Greta d'acquérir une maîtrise complète de l'administration des réseaux, avec un ancrage fort dans les réalités techniques, les normes françaises (ANSSI), les outils industriels et les pratiques de sécurité.