FICHE DE RÉVISION — RÉSEAUX AVANCÉS

1. NAT — Network Address Translation

Les adresses privées (192.168.x.x, 10.x.x.x, 172.16.x.x) ne sont pas routables sur Internet. Le NAT, activé sur le routeur, traduit les IP privées en IP publique pour permettre la communication vers l'extérieur.

Concept	Explication
Adresses privées	10.0.0.0/8 · 172.16.0.0/12 · 192.168.0.0/16 → non routables sur Internet
Rôle du NAT	Traduit les IP privées en IP publique. Le routeur maintient une table de correspondance pour renvoyer les réponses à la bonne machine.
Route statique	Destination précise configurée manuellement. Ex : 8.8.8.0/255.255.255.0 via 10.50.0.1
Default Gateway (routeur)	La GW d'un routeur = adresse d'un autre routeur. Ce qu'un routeur ne connaît pas, il l'envoie à son routeur parent. Évite les routes statiques à rallonge.

En maquette : ne jamais utiliser l'adresse de la gateway de salle (10.50.0.1) pour les configs NAT. Utiliser 10.50.X.254.

Commande de vérification du routage : tracert 8.8.8.8 — permet de voir chaque saut entre ta machine et la destination.

2. TCP vs UDP — couche 4 OSI

IP = adresse de l'immeuble. Port = numéro d'appartement. Notation : IP:Port (ex : 192.168.10.1:53). 65 536 ports au total (0–65535). Ports 0–1023 = réservés aux services standards.

	TCP	UDP
Mode	Orienté connexion (SYN → SYN-ACK → ACK)	Sans connexion — paquets envoyés directement
Garanties	Livraison garantie · Ordre respecté · Retransmission si perte	Aucune garantie de livraison ni d'ordre
Vitesse	Plus lent, en-têtes lourds	Très rapide, léger — idéal temps réel
Usages	HTTP/HTTPS · SSH · FTP · SMTP · IMAP · transferts de zone DNS	DNS (requêtes) · DHCP · VoIP · Streaming · Jeux en ligne

Ports essentiels

Lignes surlignées = priorité absolue à connaître.

Port	Proto	Service	Priorité
20/21	TCP	FTP	
22	TCP	SSH	★
23	TCP	Telnet	
25	TCP	SMTP	
53	TCP + UDP	DNS — UDP pour requêtes courantes, TCP pour transferts de zone et réponses >512 octets	★
67/68	UDP	DHCP	★

80	TCP	HTTP	★
110	TCP	POP3	
143	TCP	IMAP	
443	TCP	HTTPS	★
3306	TCP	MySQL	
5432	TCP	PostgreSQL	
8080	TCP	HTTP alternatif	

> *Le port 53 utilise UDP pour les requêtes DNS courantes (rapide, léger) et TCP pour les transferts de zone (zone transfer) et les réponses dépassant 512 octets.*

3. DNS avancé — résolution complète

Ordre exact des 6 étapes de résolution DNS. Les étapes 1 et 2 se font côté client. À partir de l'étape 3, c'est le serveur DNS qui prend le relai.

Étape	Mécanisme	Description
1	**Cache DNS local**	La machine vérifie ce qu'elle a déjà résolu récemment. Commande : ipconfig /displaydns
2	**Fichier hosts**	C:\Windows\System32\drivers\etc\hosts — résolution statique locale, prioritaire sur le DNS.
3	**Zone de recherche directe**	Le serveur DNS vérifie ses propres enregistrements (A, CNAME…). Si la réponse est là, il répond directement.
4	**Redirecteurs conditionnels**	Règle pour un domaine précis → envoie vers un DNS spécifique configuré manuellement. Ex : corp.lan → DNS 10.0.0.1
5	**Redirecteurs généraux**	Tout ce qui est inconnu sans règle précise → transmet à un DNS externe. Ex : 8.8.8.8 (Google) ou 1.1.1.1 (Cloudflare)
6	**Root DNS (racine)**	Dernier recours. 13 serveurs racine mondiaux (Anycast). Ne connaissent pas l'adresse finale mais orientent selon le TLD (.com, .fr…). Root hints stockés en dur dans le serveur DNS.

> *Étapes 1–2 : côté client. Étapes 3–6 : côté serveur DNS. Le point final dans un FQDN (ex : www.psg.fr.) représente la racine DNS (étape 6) — les navigateurs le masquent.*

Anycast — une IP, des centaines de machines

Problème : si chacun des 13 serveurs racine existait en un seul exemplaire physique, une panne datacenter rendrait une partie d'Internet inaccessible.

Unicast (normal) — 1 adresse IP = 1 machine précise.

Anycast — 1 adresse IP = des centaines de machines réparties dans le monde. Le paquet est routé vers la plus proche au sens réseau, sans que l'émetteur le sache. Analogie : le 15 (SAMU) — le plus proche décroche.

4. Zones DNS — principale, secondaire, transfert

Zone principale vs zone secondaire

Zone principale	Zone secondaire
Lecture / écriture. Source de vérité. Stockée sur DNS #1.	Copie en lecture seule. Doit être strictement identique à la principale. Stockée sur DNS #2. Transfert via TCP/53.

Sécurisation du transfert de zone

Règle de base : d'abord valider que ça fonctionne (niveau 1), ensuite sécuriser.

Niv.	Règle	Description	Sécurité
1	Vers n'importe quel serveur	Aucune restriction. Tout le monde peut recevoir une copie de la zone.	**DANGEREUX**
2	Vers les serveurs NS déclarés	Seuls les serveurs déjà enregistrés comme NS dans la zone peuvent recevoir le transfert.	**Recommandé**
3	Liste IP manuelle	L'admin définit lui-même les IP autorisées, indépendamment des enregistrements NS.	**Maximum**

> *Niveau 1 en production = un attaquant peut récupérer l'intégralité de ta zone DNS (énumération complète de tous tes enregistrements). Toujours verrouiller après validation.*

Bascule DNS secondaire → principal

Si le DNS principal tombe définitivement : sur DNS #2, propriétés de la zone secondaire → cliquer sur "Modifier" pour changer le type de zone → passer en zone principale.

> *La bascule est possible uniquement parce que la zone secondaire était strictement identique à la principale. C'est tout l'intérêt de la synchronisation rigoureuse.*

5. Enregistrements DNS — A vs CNAME

Type	Pointe vers	Usage / remarque
A (Hôte)	Une adresse IP	Serveur, machine physique. Entrée de base.
CNAME (Alias)	Un autre nom DNS (pas une IP)	Si l'IP change, on ne modifie que le A — tous les CNAME suivent automatiquement. Indispensable avec plusieurs services sur la même machine.

> *Un CNAME ne peut pas pointer directement vers une IP — uniquement vers un autre nom DNS. Si l'IP change, on ne modifie que l'enregistrement A : tous les CNAME suivent automatiquement.*

Exemple concret :

- A : serveur01.padom.local → 192.168.1.10
- CNAME : web.padom.local → serveur01.padom.local
- CNAME : ftp.padom.local → serveur01.padom.local
- Si l'IP change → on modifie uniquement le A. Les deux CNAME suivent sans toucher à rien.