

FICHE DE RÉVISION — BASES DU RÉSEAU

1. Modèle OSI — 7 couches

En formation : 3 couches suffisent. Couche 1 = physique, couche 2/3 = protocole (TCP/IP), couche 7 = applicative. Chaque couche dépend de celle du dessous.

Couche	Nom OSI	Rôle en formation
7	Application	Logiciels réseau — HTTP, DNS, FTP, SMTP...
6	Présentation	Encodage, chiffrement, compression
5	Session	Gestion des sessions de communication
4	Transport	TCP / UDP — ports, segmentation, contrôle de flux
3	Réseau	Adresses IP, routage — on travaille ici en formation
2	Liaison	MAC adresses, switch, protocole Ethernet
1	Physique	Câbles, cartes réseau, signaux électriques / optiques

2. Couche physique — câbles, switch, topologie

Câbles et connectique

Technologie	Caractéristique	Remarque
Câble Ethernet (cuivre)	Cat5e minimum	1 Gb standard entreprise. Perte de signal à distance (impédance). Norme actuelle : Cat6E (meilleur blindage alu).
Fibre optique	Distance illimitée (théorique)	Avantage : distance. Inconvénient : fragilité et coût. À utiliser quand on dépasse la limite cuivre.
Connecteur RJ45	Pas de catégorie	Les prises murales ont une catégorie, pas le connecteur RJ45 lui-même.
Laser / Hertzien	Liaisons sans fil	Laser = miroirs pour interconnexion. Hertzien = super WiFi, débit limité, à la marge.

Diagnostic réseau : Ordinateur → Prise murale → Baie de brassage → Switch. Toujours un câble neuf dans sa trousse. LED éteinte sur la carte réseau = câble défaillant ou non branché (MAIS attention au Spanning Tree qui peut prendre 30 sec).

Switch vs Hub

Équipement	Fonctionnement	Statut
Switch	Multiprise réseau intelligente. Mémorise les MAC par port. N'envoie que sur le bon port. Économise la bande passante.	Standard actuel
Hub	Multiprise sans intelligence. Broadcast sur tous les ports, connectés ou non.	OBSOLÈTE

- MAC Adresse = identifiant unique gravé sur la carte réseau
- Attaque MAC flooding : surcharge de la mémoire du switch → bascule en mode HUB (plus de filtre)

- Spanning Tree : mécanisme anti-boucle — le switch vérifie qu'il n'est pas lui-même au bout du câble. Délai jusqu'à 30 sec avant que la LED s'allume.
- Topologie en étoile = standard (tout passe par un switch central = cœur de réseau avec redondance d'alimentation)
- VLAN : isolation logique de ports d'un switch — coupe la communication entre groupes de machines

Types de communication — Unicast / Broadcast / Multicast

Type	Définition	Exemple
Unicast	1 machine → 1 machine précise	ping 192.168.1.10
Broadcast général	1 machine → TOUTES les machines du réseau	IP : 255.255.255.255 / MAC : ffff.ffff.ffff
Broadcast partiel	1 machine → tous les hôtes du même numéro de réseau	Dernière adresse du sous-réseau (ex : 192.168.29.255)
Multicast	1 machine → un groupe précis d'abonnés	Plage 224.0.0.0–239.255.255.255. Ex : IPTV (chaque chaîne = 1 flux multicast)

Le switch ne sait pas lire les IP. Il fonctionne avec les MAC adresses. Pour un broadcast général, la MAC destination est ffff.ffff.ffff → le switch balance sur tous les ports.

3. Adressage IP — binaire, ET logique, calculs

Tableau de conversion binaire ↔ décimal

2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
128	64	32	16	8	4	2	1

Méthode décimal→binaire : est-ce que le nombre ≥ 128 ? Si oui mettre 1 et soustraire, sinon 0. Recommencer avec 64, 32, 16, 8, 4, 2, 1.

20 = 00010100 | 137 = 10001001 | 255 = 11111111 | 192 = 11000000

ET logique (&) — calcul du numéro de réseau

A	B	A & B	= Résultat
0	0	0 & 0	0
0	1	0 & 1	0
1	0	1 & 0	0
1	1	1 & 1	1

IP & Masque = Numéro de réseau. Si masque = 255 sur un octet → résultat = cet octet de l'IP. Si masque = 0 → résultat = 0. Si valeur exotique → passer en binaire.

192.168.29.1 & 255.255.255.0 = 192.168.29.0 ← numéro de réseau

192.168.150.22 & 255.255.240.0 → passer l'octet 150 & 240 en binaire

Les 2 règles TCP/IP fondamentales

RÈGLE 1 : Pour que 2 machines communiquent, elles doivent avoir le MÊME numéro de réseau.

RÈGLE 2 : Pour que 2 machines communiquent, elles doivent avoir des adresses IP DIFFÉRENTES.

Adresses réservées dans chaque sous-réseau

- 1ère adresse = numéro de réseau → INTERDITE (identifie le réseau)
- Dernière adresse = broadcast partiel → INTERDITE (communication vers tous les hôtes du réseau)
- Nombre d'adresses utilisables = $2^n - 2$ (n = nombre de bits à 0 dans le masque en binaire)

Masques courants

Masque	CIDR	IP possibles	Utilisables (-2)
255.0.0.0	/8	16 777 216	16 777 214
255.255.0.0	/16	65 536	65 534
255.255.255.0	/24	256	254 — le plus courant
255.255.254.0	/23	512	510 — 2×/24 fusionnés
255.255.252.0	/22	1 024	1 022 — 4×/24 fusionnés
255.255.255.128	/25	128	126 — 2^7-2
255.255.255.192	/26	64	62 — 2^6-2
255.255.255.240	/28	16	14 — 2^4-2

Valeurs exotiques d'un octet de masque : 128 · 192 · 224 · 240 · 248 · 252 · 254. Toujours des 1 contigus. Jamais un 0 avant un 1.

CIDR — Classless Inter-Domain Routing

/X = nombre de bits à 1 dans le masque. Rend les classes A/B/C obsolètes.

192.168.1.2 / 255.255.255.0 → 192.168.1.2/24

Exercices corrigés

IP / Masque	Résultats	Méthode
192.168.29.1 255.255.255.0 (/24)	NR : 192.168.29.0 1ère : 192.168.29.1 Dern : 192.168.29.254 BP : 192.168.29.255	ET logique simple. $256-2 = 254$ utilisables.
192.168.150.22 255.255.240.0 (/20)	NR : 192.168.144.0 1ère : 192.168.144.1 Dern : 192.168.159.254 BP : 192.168.159.255	Passer en binaire : 150=10010110, 240=11110000. ET→10010000=144 (3e octet). Broadcast : mettre tous les bits machine à 1 → 159.255. $2^{12}-2 = 4094$.
192.168.192.168 255.255.255.240 (/28)	NR : 192.168.192.160 1ère : 192.168.192.161 Dern : 192.168.192.174 BP : 192.168.192.175	168=10101000, 240=11110000. ET→10100000=160. Broadcast: 10101111=175. $2^4-2 = 14$ utilisables.

4. Adresses IP privées et spéciales — PAR CŒUR

Réseau	CIDR	Classe	Remarque
10.0.0.0	/8	A	16,7 millions d'adresses
172.16.0.0	/12	B	1 million d'adresses
192.168.0.0	/16	C	65 536 adresses — la plus courante en entreprise
169.254.0.0 (APIPA)	/16	—	Auto-attribuée si pas de DHCP. Visible en ipconfig = problème DHCP. Conflit : 1/65 536.
127.0.0.1 (loopback)	—	—	Test TCP/IP interne. ping 127.0.0.1 = pile TCP/IP installée. Ne sort jamais sur le réseau.

5. DHCP — Dynamic Host Configuration Protocol

Serveur qui attribue automatiquement les paramètres IP aux clients (IP, masque, GW, DNS).

Méthode DORA

Lettre	Message	Qui → Qui / Contenu
D	DHCP DISCOVER	Client → Broadcast : "J'ai besoin d'une IP !"
O	DHCP OFFER	Serveur → Broadcast : "Voici une IP dispo : 192.168.x.x"
R	DHCP REQUEST	Client → Broadcast : "Je prends celle-là !"
A	DHCP ACK	Serveur → Client : "OK c'est à toi ! + masque, GW, DNS"

Règles importantes

- Un serveur DHCP NE PEUT PAS être client DHCP → IP fixe obligatoire
- Éviter 2 serveurs DHCP sur le même réseau (premier arrivé premier servi en broadcast)
- Le DHCP enregistre la MAC adresse du client avec l'IP attribuée (bail/lease)
- Renouvellement du bail : à 1/2, 8/10e, puis à expiration
- Durées de bail : 8 jours en entreprise | 24h en hôtel | 30 min en gare/restaurant
- Réservation DHCP : pour toujours donner la même IP à une machine → lier sa MAC adresse

Relais DHCP (Agent de relais)

LES ROUTEURS NE LAISSENT PAS PASSER LES BROADCASTS.

Conséquence : si un routeur sépare les clients DHCP du serveur DHCP, les DISCOVER ne passent pas.
Solution : activer l'Agent de relais DHCP sur le routeur. Il intercepte les broadcasts DHCP et les transmet en unicast au serveur DHCP. Nécessite de créer une étendue par sous-réseau sur le serveur.

6. Routage statique — Static Route

Règle du petit train — PAR CŒUR

Quand une machine veut joindre une autre machine qui n'est pas dans son numéro de réseau, elle envoie le paquet à sa **PASSERELLE PAR DÉFAUT (Default Gateway)**.

La GW d'une machine est obligatoirement dans son propre numéro de réseau.

La GW d'un routeur = l'adresse IP d'un autre routeur (ce qu'il ne connaît pas, il l'envoie à son routeur parent).

Structure d'une route statique

Champ	Valeur	Explication
Network	Numéro de réseau destination	L'adresse réseau qu'on veut atteindre
Mask	Masque du réseau destination	Le masque associé à ce réseau de destination
Next Hop / GW	IP du routeur intermédiaire	L'adresse IP du routeur par lequel passer pour atteindre la destination

On écrit **TOUJOURS** en premier le numéro de réseau de destination, puis le masque, puis le Next Hop.

Pour éviter les routes statiques à rallonge : configurer une **Default Gateway** sur chaque routeur.

7. DNS — Domain Name Server

Annuaire qui convertit les noms de domaine (FQDN) en adresses IP = Résolution de noms.

- FQDN = URL = nom de domaine = nom de domaine pleinement qualifié = nom DNS → TOUT PAREIL
- Ex : www.psg.fr → www = nom d'hôte | psg.fr = nom de domaine = zone de recherche directe
- Noms DNS : lettres, chiffres, tirets (-) et underscores (_). Max 255 caractères.
- Port 53 UDP pour les requêtes courantes | Port 53 TCP pour les transferts de zone et réponses > 512 octets

Résolution DNS complète — 6 étapes (côté client : 1-2 | côté serveur DNS : 3-6)

Étape	Mécanisme	Description
1	Cache DNS local	La machine consulte ce qu'elle a déjà résolu. ipconfig /displaydns
2	Fichier hosts	C:\Windows\System32\drivers\etc\hosts — résolution statique prioritaire
3	Zone de recherche directe	Le serveur DNS vérifie ses propres enregistrements (A, CNAME...)
4	Redirecteurs conditionnels	Règle pour un domaine précis → DNS spécifique configuré manuellement
5	Redirecteurs généraux	Tout inconnu sans règle précise → DNS externe (8.8.8.8, 1.1.1.1...)
6	Root DNS	13 serveurs racine (Anycast). Orientent selon le TLD (.com, .fr...).

Configuration DNS dans DHCP

Le serveur DNS peut être configuré dans les étendues DHCP (vert = s'applique à l'étendue) ou dans les options de serveur (jaune = s'applique à tout le serveur).

8. WINS — Windows Internet Name Service

Service de résolution de noms NetBIOS (héritage Windows). API NetBIOS (Windows) vs Socket (UNIX/Linux).

	DNS (Socket)	WINS (NetBIOS)
API utilisée	Socket	NetBIOS
Longueur nom max	255 caractères	15 caractères
Serveur	Serveur DNS	Serveur WINS
Statut	Standard actuel	Héritage — voué à disparaître mais maintenu pour compatibilité applicative

Ordre résolution NetBIOS (max 15 caractères)

- 1 — Cache NetBIOS
- 2 — Serveur WINS
- 3 — Broadcast (bloqué par les routeurs)
- 4 — Fichier LMHOSTS (sur le disque dur local)

9. IPv6

IPv4 = 32 bits = 4 milliards d'adresses → limite atteinte. IPv6 = 128 bits = 4 trilliards. Plus besoin de masques ni d'optimisation VLSM.

Caractéristique	Valeur / explication
Longueur	128 bits (vs 32 bits pour IPv4). 4 trilliards d'adresses.
Format	8 blocs de 4 caractères hexadécimaux : fa23:125a:1234:2ff5:55ff:12ff:25da:0001
Hexadécimal	0-9 puis a=10, b=11, c=12, d=13, e=14, f=15
Découpage	64 bits gauche = ID Réseau 64 bits droite = ID Machine. Pas de masque de sous-réseau.
Abréviation "::"	Remplace les blocs de zéros consécutifs — une seule fois par adresse.
APIPA IPv6	Commence par Fe80:: (équivalent de 169.254.x.x en IPv4)
Broadcast	N'existe PAS en IPv6 — remplacé par le Multicast. (Note : ffff:fff:... = adresse multicast all-nodes, pas un broadcast)
Règles TCP/IP	Identiques à IPv4 : routeur, DHCP, DNS, routes statiques fonctionnent de la même façon.

10. VLSM — Variable Length Subnet Mask

Objectif : trouver le masque adapté aux besoins réels. NE PAS GASPILLER D'ADRESSES IP.

Tableau des subdivisions à partir d'un /24

CIDR	Masque	IP totales	Utilisables	Sous-réseaux (/24 de base)
------	--------	------------	-------------	----------------------------

/24	255.255.255.0	256	254	1 bloc entier
/25	255.255.255.128	128	126	2 moitiés de /24
/26	255.255.255.192	64	62	4 quarts de /24
/27	255.255.255.224	32	30	8 blocs dans /24
/28	255.255.255.240	16	14	16 blocs dans /24
/30	255.255.255.252	4	2	Liens point-à-point entre routeurs

Méthode du tableau et méthode du camembert

Méthode du tableau (subdivisions /24)	Méthode du camembert (même logique, visuelle)
192.168.29.0/24 → 256 adresses <pre> ├─ /25 → 128 adresses (0-127) │ └─ /26 → 64 adresses (0-63) │ └─ /27 → 32 adresses │ └─ /27 → 32 adresses │ └─ /26 → 64 adresses (64-127) └─ /25 → 128 adresses (128-255) </pre> Règle : +1 bit = ÷2 -1 bit = ×2 Formule : $2^n - 2$ (n = bits à 0 du masque)	Le /24 = le camembert entier (256 parts) Chaque découpe = moitié du bloc précédent. Attribuer les plus grands blocs EN PREMIER. Objectif : ne pas gaspiller d'adresses IP.

Toujours attribuer les plus grands blocs en premier, puis subdiviser pour les besoins plus petits. +1 bit = ÷2 adresses. -1 bit = ×2 adresses (×256 si on recule d'un octet entier).

11. Commandes réseau — référence

Commande	Usage
ipconfig	IP, masque, passerelle de la machine
ipconfig /all	Idem + MAC adresse, bail DHCP, serveur DHCP/DNS
ipconfig /release	Libère le bail DHCP
ipconfig /renew	Renouvelle le bail DHCP (redemande une IP au serveur)
ipconfig /displaydns	Affiche le cache DNS local
ipconfig /flushdns	Vide le cache DNS local
ping 127.0.0.1	Test interne TCP/IP. Confirme que la pile est installée. Ne sort pas sur le réseau.
ping [IP]	Test de joignabilité. Bloqué par le pare-feu Windows par défaut.
tracert [IP]	Affiche tous les sauts (routeurs) entre ta machine et la destination
nslookup	Teste la résolution DNS d'un nom de domaine
ncpa.cpl	Configuration des cartes réseau (Win+R)
wf.msc	Console du pare-feu Windows (Win+R)
sysdm.cpl	Propriétés système — renommer l'ordinateur (Win+R)

ON NE DÉSACTIVE JAMAIS LE PARE-FEU EN PRODUCTION. En formation uniquement pour autoriser les pings entre machines.

Après toute modification du serveur DHCP (pool, étendue, options) : faire **ipconfig /release** puis **ipconfig /renew** sur les postes clients.