APPRENDRE LE RÉSEAU : DU DÉBUTANT AU CCNA

acquérir toutes les compétences réseau attendues par le référentiel TSSR (RNCP — CCP « Exploiter un réseau IP » et « Maintenir et sécuriser les interconnexions ») tout en couvrant l'intégralité du blueprint Cisco CCNA 200-301 1.

20 min de lecture · 6 août 2026 · Vincent

SOMMAIRE

OUTILS LINUX · INTERMÉDIAIRE

APPRENDRE LE RÉSEAU : DU DÉBUTANT AU CCNA

acquérir toutes les compétences réseau attendues par le référentiel TSSR (RNCP — CCP « Exploiter un réseau IP » et « Maintenir et sécuriser les interconnexions ») tout en couvrant l'intégralité du blueprint Cisco CCNA 200-301 1.

20 min · 6 août 2026

Parcours complet dans le cadre de la formation TSSR (Titre Professionnel niveau 5)

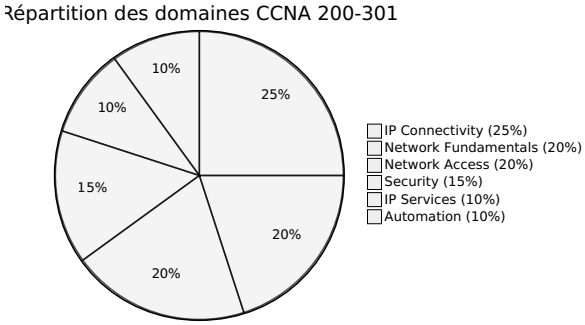
> **Objectif** : acquérir toutes les compétences réseau attendues par le référentiel TSSR (RNCP — CCP « Exploiter un réseau IP » et « Maintenir et sécuriser les interconnexions ») tout en couvrant l'intégralité du blueprint **Cisco CCNA 200-301** 1. Contexte : TSSR et CCNA

1.1 LE TITRE PROFESSIONNEL TSSR

Le **Technicien Supérieur Systèmes et Réseaux** (titre professionnel de niveau 5, équivalent Bac+2) exploite, maintient et sécurise l'infrastructure informatique des organisations. Le titre est structuré en **blocs de compétences (CCP)** dont plusieurs concernent directement le réseau :

1.2 LE CCNA 200-301 V1.1

Le CCNA est la certification Cisco de référence pour valider un niveau « associate » en réseau. L'examen dure **120 minutes** et couvre **6 domaines pondérés** :

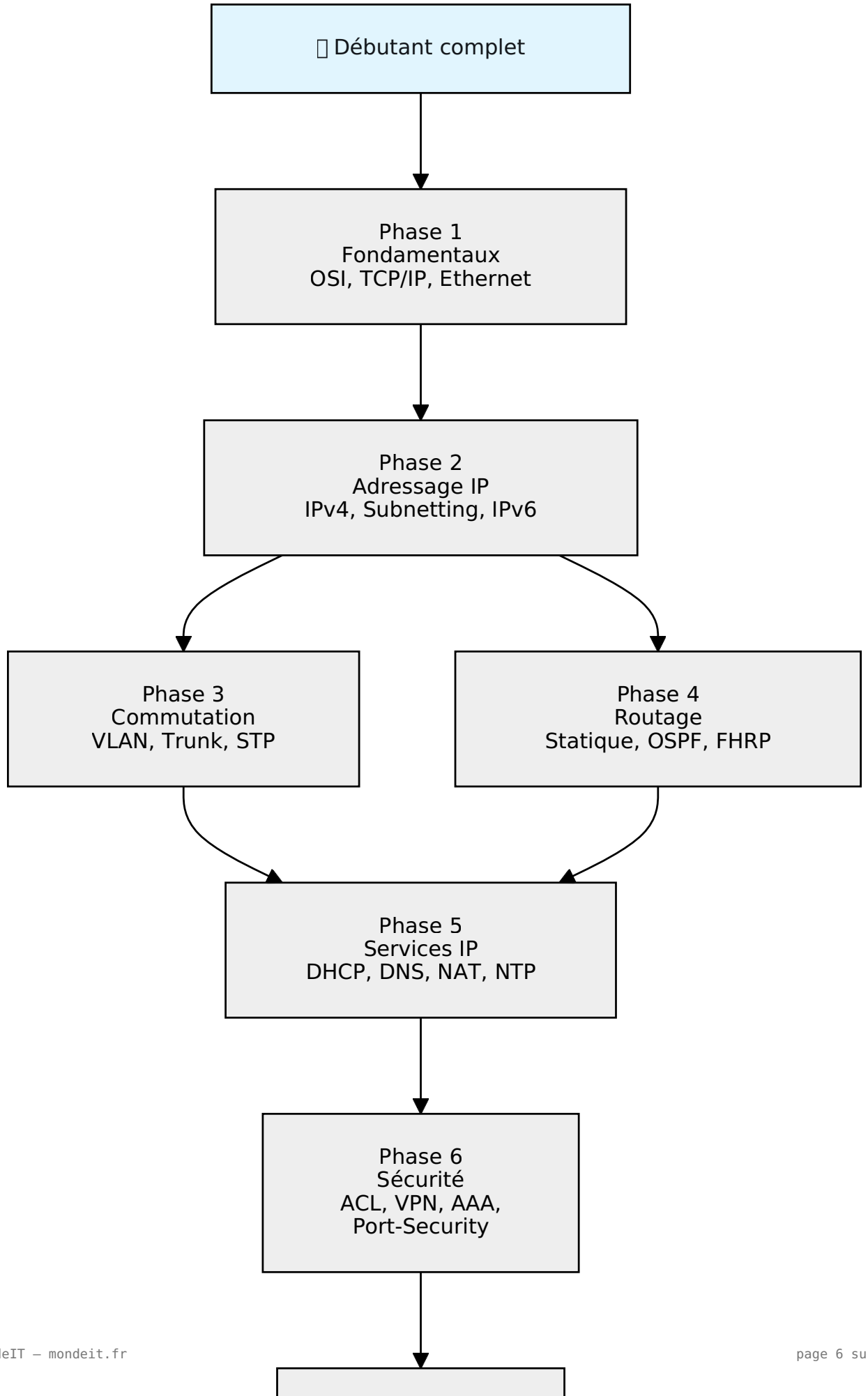


> **i INFORMATION**
>
> **Synergie TSSR / CCNA** : le CCNA couvre et dépasse les attendus réseau du TSSR. Préparer le CCNA pendant la formation TSSR, c'est sécuriser l'examen du titre **et** obtenir une certification reconnue mondialement.

---

2. ROADMAP GÉNÉRALE

Règle d'or : chaque notion étudiée doit être **immédiatement pratiquée en lab** (Packet Tracer, GNS3 ou matériel réel). Au CCNA comme à l'examen TSSR, on vous demande de configurer, vérifier et dépanner, pas de réciter.


Débutant complet
Phase 1
Fondamentaux
OSI, TCP/IP, Ethernet
Phase 2
Adressage IP
IPv4, Subnetting, IPv6
Phase 3
Commutation
VLAN, Trunk, STP
Phase 4
Routage
Statique, OSPF, FHRP
Phase 5
Services IP
DHCP, DNS, NAT, NTP
Phase 6
Sécurité
ACL, VPN, AAA,
Port-Security

3. PHASE 1 — FONDAMENTAUX DES RÉSEAUX

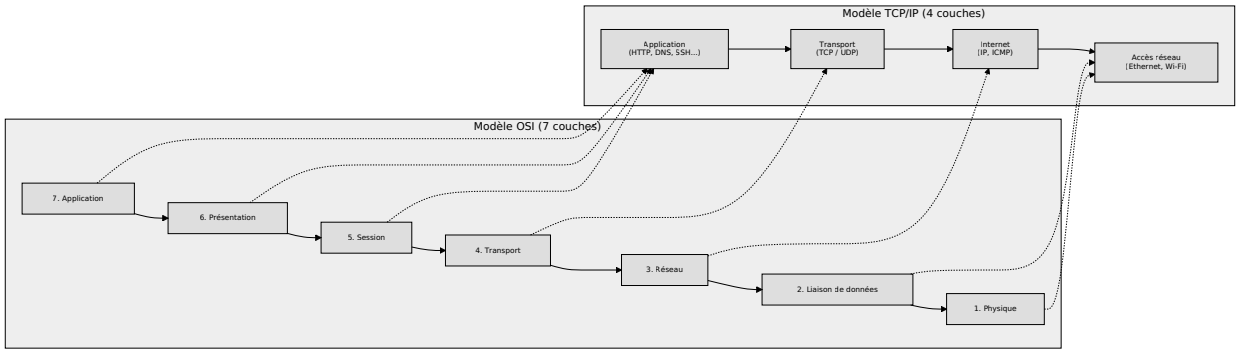
3.1 QU'EST-CE QU'UN RÉSEAU ?

Un réseau relie des équipements (hôtes) pour partager des ressources. On distingue :

- **LAN** (Local Area Network) : réseau local d'entreprise ou domestique.
- **WAN** (Wide Area Network) : interconnexion de sites distants (Internet, MPLS, VPN).
- **WLAN** : LAN sans fil (Wi-Fi).
- **SAN** : réseau de stockage.

3.2 LES ÉQUIPEMENTS

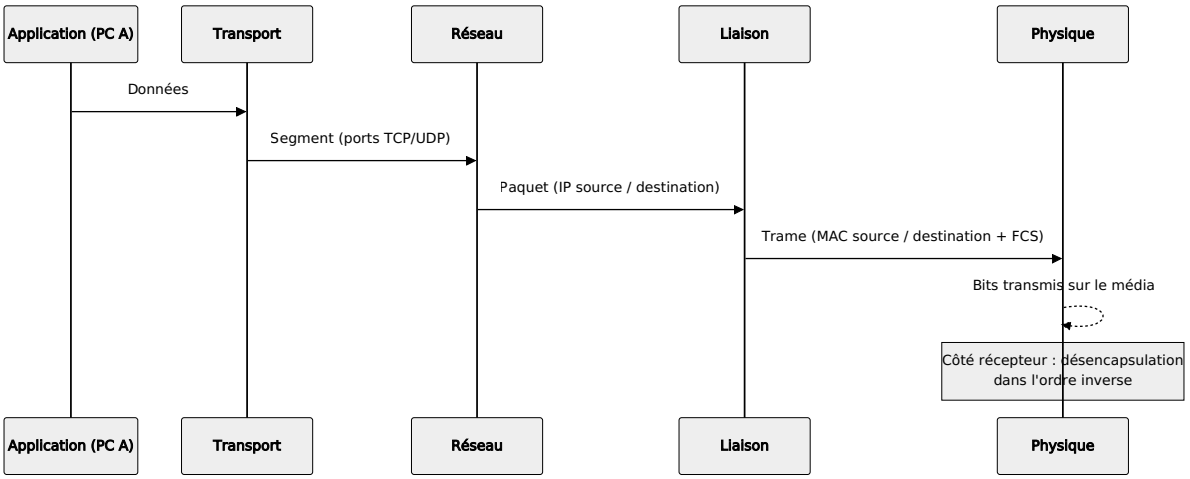
3.3 LE MODÈLE OSI ET LE MODÈLE TCP/IP



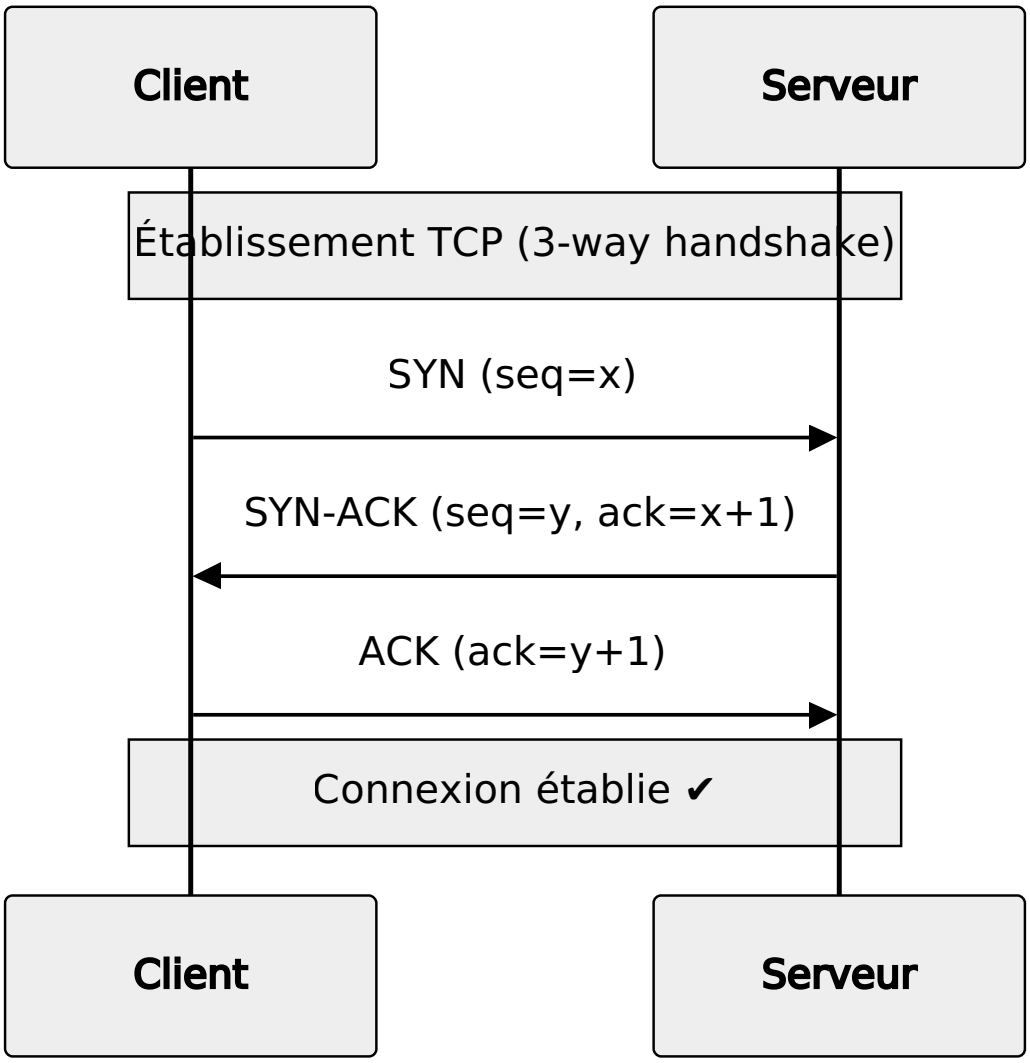
Moyen mnémotechnique (7→1) : « **P**our **L**e **R**éseau, **T**out **S**e **P**asse **A**utomatiquement ».

3.4 L'ENCAPSULATION

Chaque couche ajoute son en-tête : les **données** deviennent un **segment** (L4), puis un **paquet** (L3), puis une **trame** (L2), enfin des **bits** (L1).


Application (PC A)
Transport
Réseau
Liaison
Physique
Données
Segment (ports TCP/UDP)
Paquet (IP source / destination)
Trame (MAC source / destination + FCS)
Bits transmis sur le média
Côté récepteur : désencapsulation dans l'ordre inverse
Application (PC A)
Transport
Réseau
Liaison
Physique

3.5 TCP VS UDP


Client
Serveur
Établissement TCP (3-way handshake)
SYN (seq=x)
SYN-ACK (seq=y, ack=x+1)
ACK (ack=y+1)
Connexion établie ✔
Client
Serveur

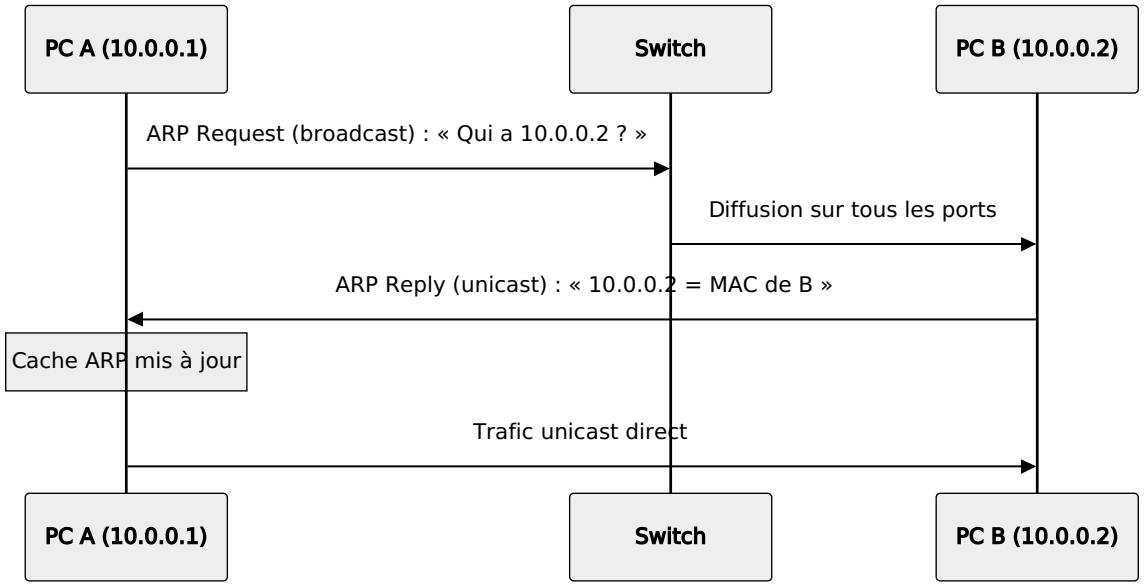
3.6 PORTS À CONNAÎTRE PAR CŒUR

3.7 CÂBLAGE ET COUCHE PHYSIQUE

- **Cuivre à paires torsadées** : Cat5e (1 Gb/s), Cat6/6a (10 Gb/s), connecteur RJ45. Câbles droits et croisés (Auto-MDIX rend le croisé rarement nécessaire).
- **Fibre optique** : monomode (longues distances) / multimode (datacenter, courtes distances). Connecteurs LC, SC ; modules SFP/SFP+.
- **PoE** (802.3af/at/bt) : alimentation des AP, caméras et téléphones IP via le câble Ethernet.
- Problèmes L1 courants : collisions, erreurs CRC, duplex mismatch, runts/giants.

3.8 LA TRAME ETHERNET ET L'ADRESSE MAC

- Adresse **MAC** : 48 bits, notée `AA:BB:CC:DD:EE:FF` (24 bits OUI constructeur + 24 bits carte).
- Le switch construit sa **table MAC** en lisant les adresses sources, puis commute les trames vers le bon port (flood si adresse inconnue, broadcast `FF:FF:FF:FF:FF:FF`).
- **ARP** fait le lien entre IP et MAC sur le réseau local.



Checkpoint Phase 1 — Vous savez : citer les 7 couches OSI, expliquer l'encapsulation, différencier TCP/UDP, lire une table MAC, reconnaître les ports usuels, choisir le bon câble.

Quiz illisible. Ligne 2 : une explication sans question.

```
> Il commute des trames en lisant les adresses MAC.

1. [ ] Couche 1 (Physique)
1. [x] Couche 2 (Liaison de données)
    > Exact : le switch lit les adresses MAC contenues dans les trames.
1. [ ] Couche 3 (Réseau)
1. [ ] Couche 4 (Transport)

> On part des données et on descend les couches.

1. Données
2. Segment
3. Paquet
4. Trame
5. Bits


> Pensez au 3-way handshake.

- [x] Il est orienté connexion
- [x] Il garantit l'ordre et la retransmission des segments
- [ ] Il est plus rapide qu'UDP car sans contrôle
- [ ] Il est utilisé par le streaming vidéo en temps réel de préférence à UDP
- [x] HTTP et SSH s'appuient sur lui

1. [ ] DNS
1. [ ] DHCP
1. [x] ARP
    > ARP Request en broadcast, ARP Reply en unicast.
1. [ ] ICMP


> Les services qui privilégient la rapidité sur la fiabilité.

- [x] DNS (port 53)
- [x] DHCP (ports 67/68)
- [ ] SSH (port 22)
- [x] NTP (port 123)
- [ ] HTTPS (port 443)


1. [ ] 80
1. [x] 443
1. [ ] 22
1. [ ] 3389
```

---

4. PHASE 2 — ADRESSAGE IP ET SUBNETTING

> ⚠ Le subnetting est LA compétence pivot : sans elle, impossible de comprendre le routage (25 % du CCNA) ni de réussir les mises en situation TSSR.

4.1 IPV4 : STRUCTURE

- Adresse sur **32 bits**, notée en décimal pointé : `192.168.1.10`.

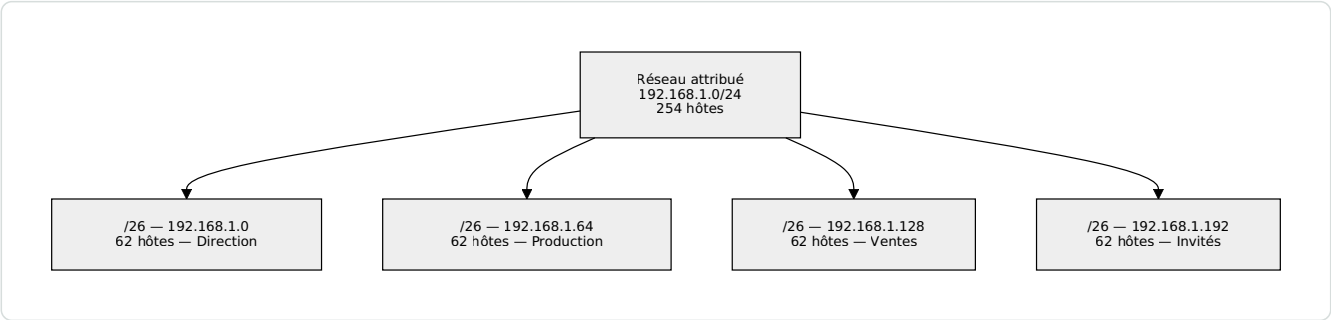
- Toujours associée à un **masque** : `255.255.255.0` ou notation CIDR `/24`.
- Partie **réseau** + partie **hôte**. Adresse de réseau (bits hôte à 0) et de broadcast (bits hôte à 1) inutilisables pour un hôte.

4.2 ADRESSES PRIVÉES (RFC 1918) ET SPÉCIALES

4.3 MÉTHODE DE SUBNETTING RAPIDE

1. **Nombre magique** = 256 − dernier octet du masque.
2. Les sous-réseaux se suivent de « nombre magique » en « nombre magique ».
3. Hôtes utilisables = 2^(bits hôte) − 2.

Exemple : `192.168.1.0/26` → masque `255.255.255.192` → nombre magique = 64 → sous-réseaux : `.0`, `.64`, `.128`, `.192` → 62 hôtes chacun.



4.4 VLSM (MASQUES DE LONGUEUR VARIABLE)

Découper en attribuant à chaque besoin la taille juste nécessaire, en commençant par le **plus grand** besoin :

4.5 IPV6

- Adresse sur **128 bits**, 8 groupes hexadécimaux : `2001:0db8:0000:0000:0000:0000:0000:0001` → abrégée `2001:db8::1`.
- Types : **Global Unicast** (`2000::/3`), **Link-Local** (`fe80::/10`, obligatoire sur chaque interface), **Unique Local** (`fc00::/7`), **Multicast** (`ff00::/8`). Pas de broadcast !
- Attribution : statique, **SLAAC** (autoconfiguration via RA), DHCPv6.
- Préfixe standard d'un LAN : `/64`.

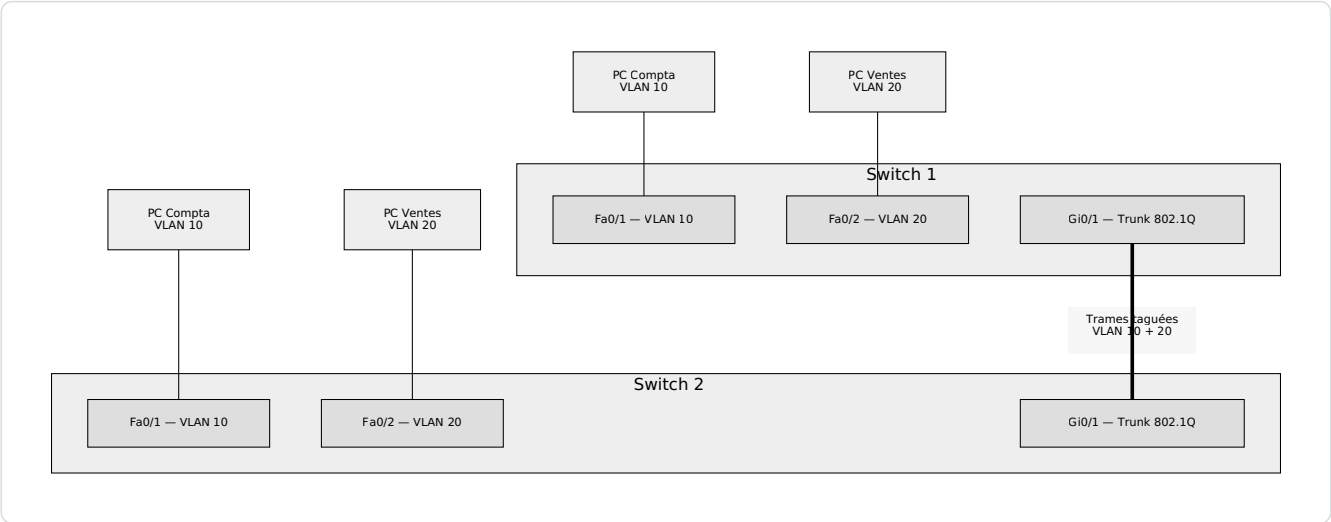
Checkpoint Phase 2 — Vous savez : subnetter en moins d'une minute, faire un plan d'adressage VLSM, abréger une adresse IPv6, expliquer SLAAC.

---

5. PHASE 3 — COMMUTATION (SWITCHING)

5.1 VLAN : SEGMENTER LE LAN

Un **VLAN** est un domaine de broadcast logique : on isole les services (Direction, Prod, VoIP, Invités) sur la même infrastructure physique.



Configuration type :

```
Switch(config)# vlan 10
Switch(config-vlan)# name COMPTA
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# interface gi0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99
```

> ⚠ **Piège classique** : un native VLAN mismatch entre deux extrémités d'un trunk fait atterrir le trafic non tagué dans le mauvais VLAN.

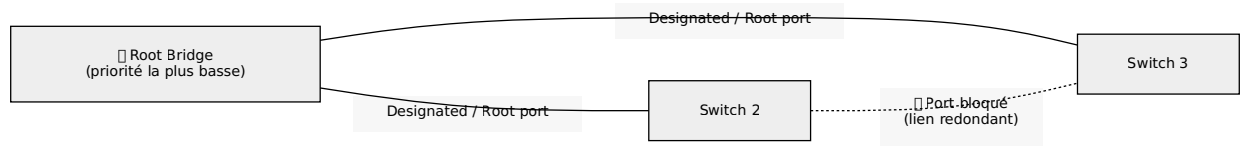
5.2 ROUTAGE INTER-VLAN

Trois méthodes : routeur avec une interface par VLAN (obsolète), **Router-on-a-Stick** (sous-interfaces 802.1Q), **SVI sur switch L3** (méthode moderne).

```
R1(config)# interface gi0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
```

5.3 SPANNING TREE PROTOCOL (STP)

STP (802.1D) et **Rapid PVST+** (802.1w, défaut Cisco) empêchent les boucles de commutation en bloquant les liens redondants.



- Élection du **Root Bridge** : priorité (défaut 32768) + adresse MAC la plus basse.
- Rôles de ports : Root Port, Designated Port, port bloqué (Alternate).
- Protections : **PortFast** (ports d'accès) + **BPDU Guard** (désactive le port si un switch pirate est branché).

5.4 ETHERCHANNEL

Agrégation de 2 à 8 liens physiques en un lien logique (bande passante cumulée + redondance sans blocage STP). Protocoles de négociation : **LACP** (standard, `mode active`) ou PAgP (Cisco, `mode desirable`).

5.5 PROTOCOLES DE DÉCOUVERTE

- **CDP** (Cisco) et **LLDP** (standard) : `show cdp neighbors` révèle la topologie réelle — réflexe indispensable en dépannage TSSR.

Checkpoint Phase 3 — Vous savez : créer VLAN + trunk, configurer un routage inter-VLAN, identifier le Root Bridge, sécuriser avec PortFast/BPDU Guard, monter un EtherChannel LACP.

---

6. PHASE 4 — ROUTAGE (IP CONNECTIVITY)

> **25 % de l'examen CCNA** : le domaine le plus lourd. Maîtrise obligatoire.

6.1 LIRE UNE TABLE DE ROUTAGE

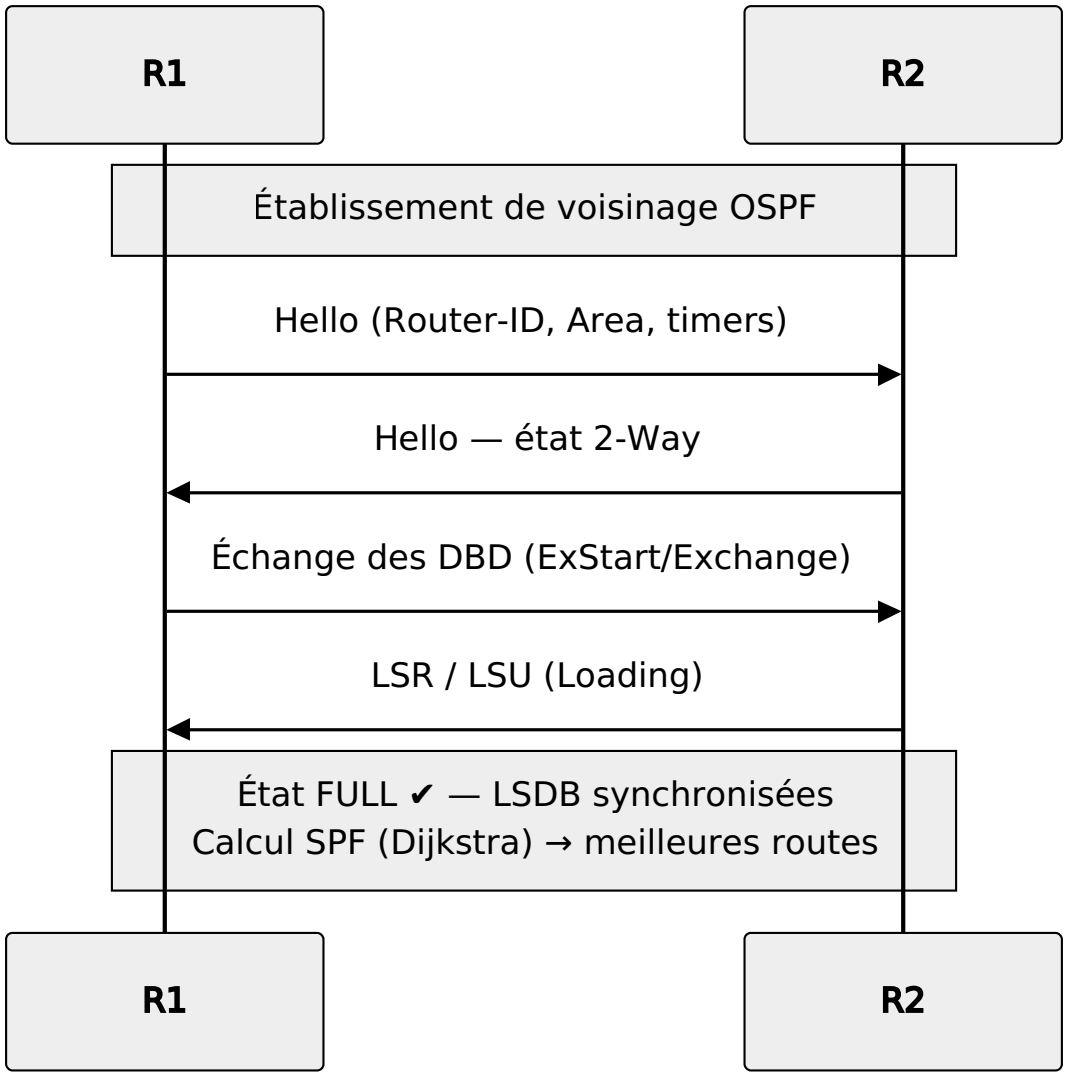
```
R1# show ip route
S*   0.0.0.0/0 [1/0] via 203.0.113.1        ← route par défaut statique
O    10.2.0.0/24 [110/2] via 10.12.0.2      ← apprise via OSPF
C    10.1.0.0/24 is directly connected      ← réseau connecté
L    10.1.0.1/32 is directly connected      ← adresse locale
```

Le routeur choisit dans l'ordre : 1. **Le préfixe le plus long** (longest prefix match) ; 2. La **distance administrative** la plus basse (Connecté 0 < Statique 1 < OSPF 110 < …) ; 3. La **métrique** la plus basse.

6.2 ROUTAGE STATIQUE

```
R1(config)# ip route 10.2.0.0 255.255.255.0 10.12.0.2        ← route statique
R1(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.1             ← route par défaut
R1(config)# ip route 10.2.0.0 255.255.255.0 10.13.0.3 90     ← route flottante (AD 90, secours)
R1(config)# ipv6 route 2001:db8:2::/64 2001:db8:12::2        ← statique IPv6
```

6.3 OSPF (SINGLE-AREA, OSPFV2)



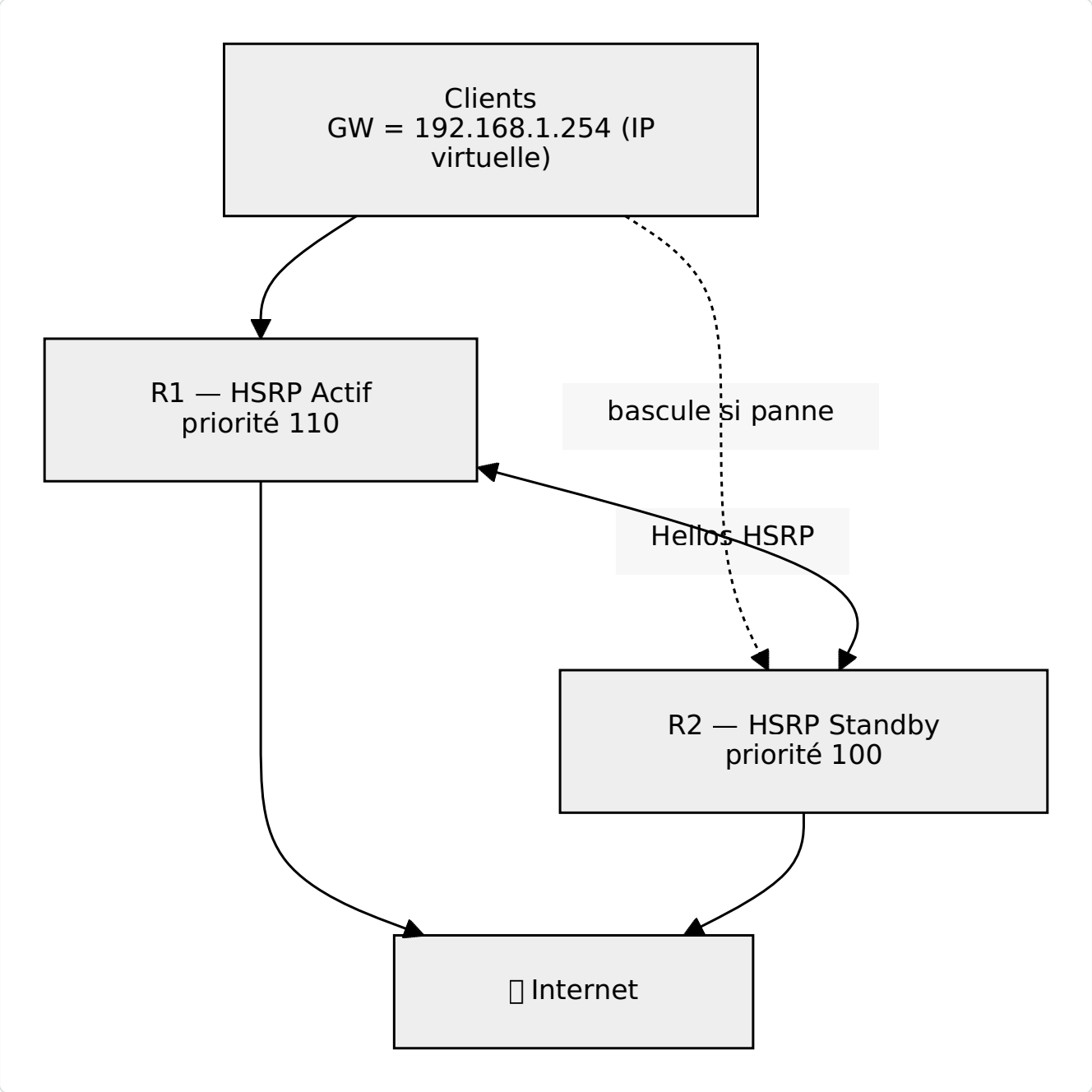

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.0.0 0.0.0.255 area 0
R1(config-router)# passive-interface gi0/1
```

Points clés : conditions de voisinage (même subnet, area, timers Hello/Dead 10/40), élection **DR/BDR** sur les segments multi-accès (priorité puis Router-ID), coût = 100 Mb/s ÷ bande passante (ajuster `auto-cost reference-bandwidth`).

Vérification : `show ip ospf neighbor`, `show ip protocols`, `show ip route ospf`.

6.4 REDONDANCE DE PASSERELLE (FHRP)

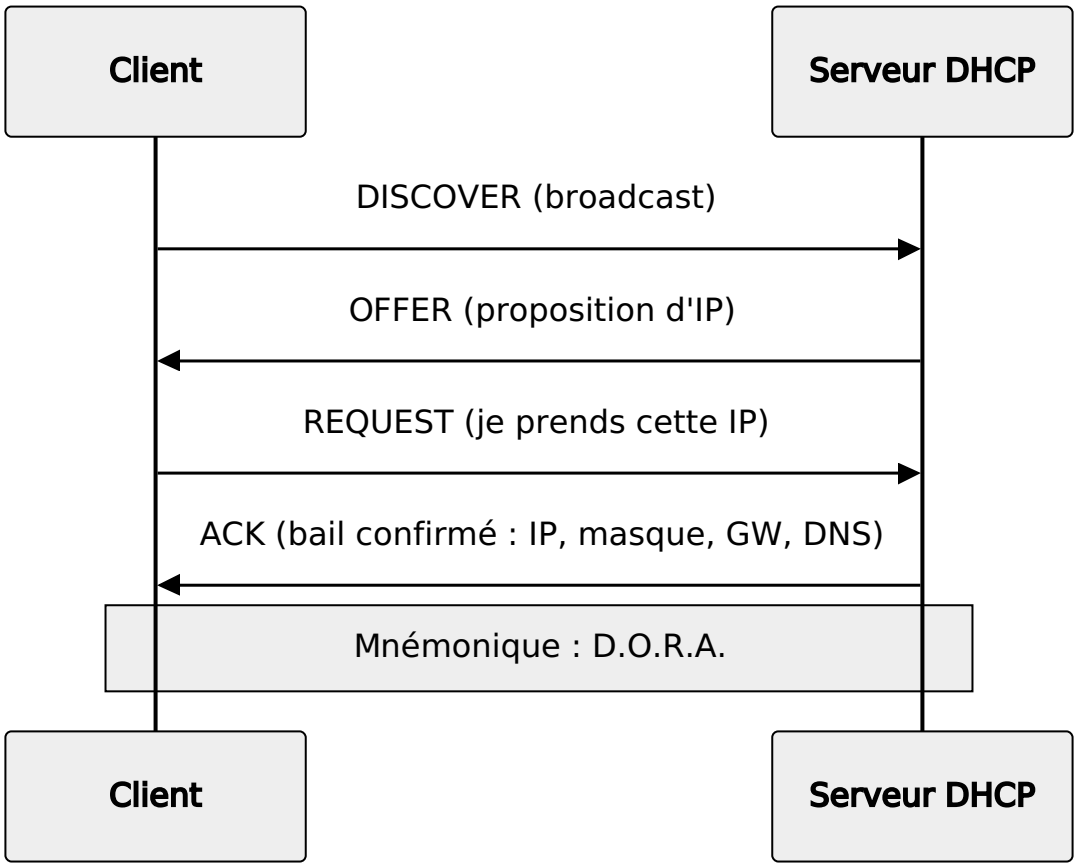
HSRP : deux routeurs partagent une IP virtuelle qui sert de passerelle aux clients ; si l'actif tombe, le standby prend le relais.



Checkpoint Phase 4 — Vous savez : lire et interpréter `show ip route`, poser des statiques et une route flottante, monter un OSPF single-area et dépanner un voisinage bloqué, expliquer HSRP.

7. PHASE 5 — SERVICES IP

7.1 DHCP

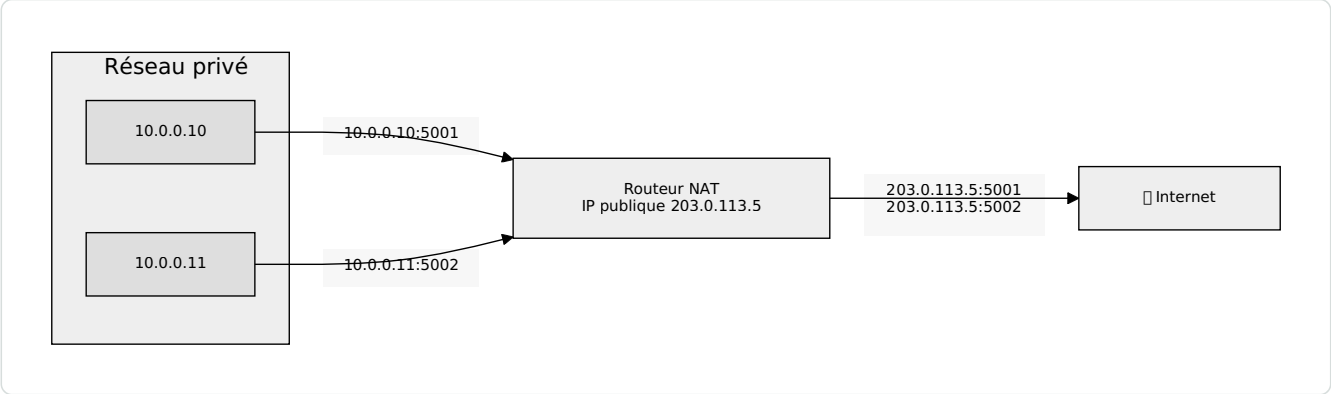


- Sur un routeur Cisco : `ip dhcp pool LAN`, `network`, `default-router`, `dns-server`, `ip dhcp excluded-address`.
- **DHCP Relay** : `ip helper-address <IP-serveur>` sur l'interface du VLAN client quand le serveur est distant — incontournable en entreprise multi-VLAN.

7.2 DNS

Résolution nom → IP. Savoir configurer un client (`ip name-server`) et diagnostiquer avec `nsloo-kup` / `dig`. Types d'enregistrements : A, AAAA, CNAME, MX, PTR.

7.3 NAT / PAT



PAT (NAT overload) — configuration type :

```
R1(config)# access-list 1 permit 10.0.0.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface gi0/0 overload
R1(config)# interface gi0/1
R1(config-if)# ip nat inside
R1(config)# interface gi0/0
R1(config-if)# ip nat outside
```

Vérification : `show ip nat translations`, `show ip nat statistics`.

7.4 NTP, SYSLOG, SNMP

- **NTP** (port 123) : horloge synchronisée = logs exploitables et certificats valides. `ntp server 192.168.1.1` ; notion de stratum.
- **Syslog** (port 514) : niveaux 0 (emergency) → 7 (debug). Mnémonique : « Every Awesome Cisco Engineer Will Need Ice-cream Daily ». `logging host`, `logging trap warnings`.
- **SNMP** (161/162) : supervision (versions 2c avec communautés, v3 sécurisée). En TSSR : intégration avec Zabbix, Centreon ou PRTG.

7.5 QOS (NOTIONS)

Classification et marquage (DSCP), files d'attente, priorité voix (EF). Objectif CCNA : comprendre les concepts (delay, jitter, loss) plus que configurer.

Checkpoint Phase 5 — Vous savez : monter un serveur DHCP avec relay, configurer un PAT complet, expliquer NTP/Syslog/SNMP et les intégrer dans une supervision.

---

8. PHASE 6 — SÉCURITÉ

8.1 CONCEPTS FONDAMENTAUX

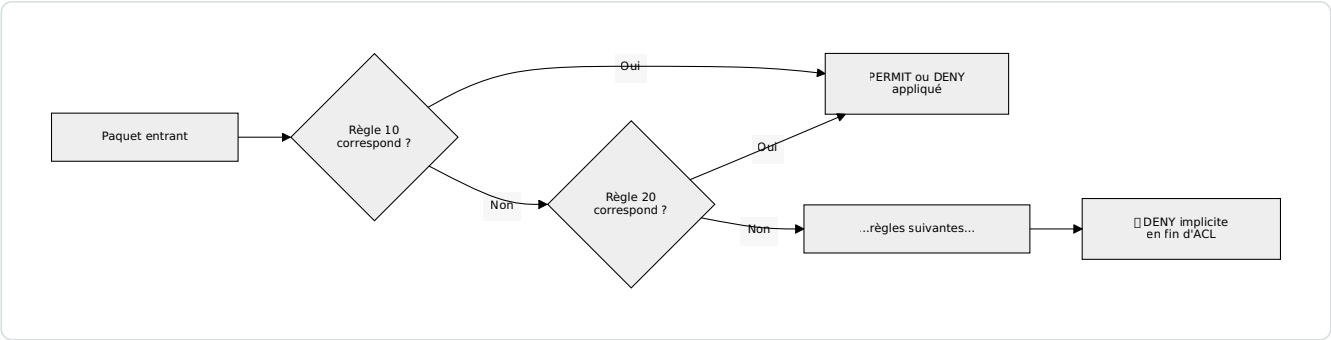
- **CIA** : Confidentialité, Intégrité, Disponibilité.

- Menaces courantes : phishing, malware, DoS/DDoS, man-in-the-middle, spoofing, attaques par mot de passe.
- **AAA** : Authentication, Authorization, Accounting (serveurs RADIUS/TACACS+).
- Défense en profondeur : chaque couche (physique, L2, L3, applicative, humaine) porte ses contrôles.

8.2 SÉCURISER L'ACCÈS AUX ÉQUIPEMENTS

```
R1(config)# enable secret P@ssw0rdFort
R1(config)# username admin secret P@ssw0rdFort
R1(config)# ip domain-name entreprise.local
R1(config)# crypto key generate rsa modulus 2048
R1(config)# line vty 0 4
R1(config-line)# transport input ssh          ← SSH uniquement, jamais Telnet
R1(config-line)# login local
R1(config)# banner motd # Accès réservé - poursuites en cas d'intrusion #
```

8.3 ACL (ACCESS CONTROL LISTS)



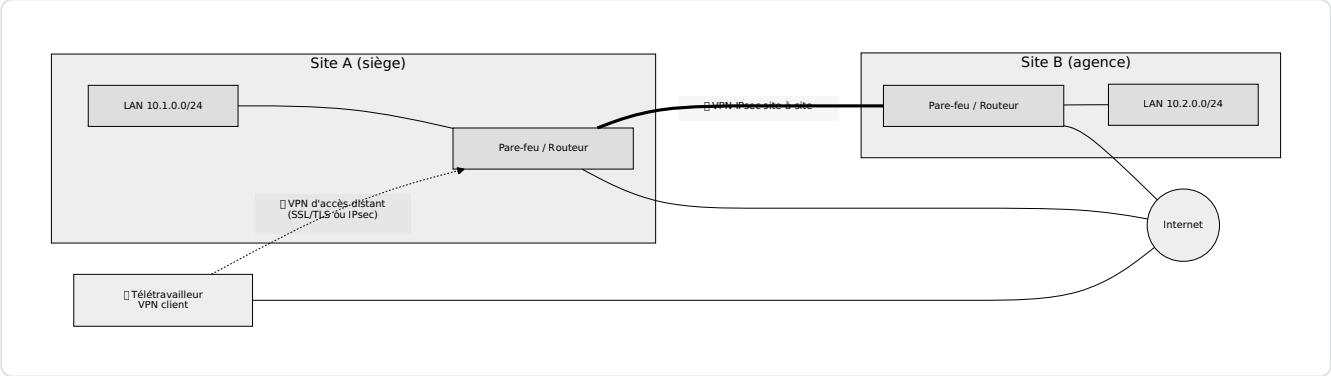
- **Standard** (1–99) : filtre sur l'IP source uniquement → placer **près de la destination**.
- **Étendue** (100–199) : source + destination + protocole + port → placer **près de la source**.

```
R1(config)# ip access-list extended BLOQUE-TELNET
R1(config-ext-nacl)# deny tcp 10.0.0.0 0.0.0.255 any eq 23
R1(config-ext-nacl)# permit ip any any
R1(config)# interface gi0/1
R1(config-if)# ip access-group BLOQUE-TELNET in
```

8.4 SÉCURITÉ DE COUCHE 2

```
SW(config-if)# switchport port-security
SW(config-if)# switchport port-security maximum 2
SW(config-if)# switchport port-security mac-address sticky
SW(config-if)# switchport port-security violation shutdown
```

8.5 VPN ET INTERCONNEXION SÉCURISÉE (CŒUR TSSR)



- **Site-à-site (IPsec)** : chiffre le trafic entre deux réseaux via Internet.
- **Accès distant** : client VPN (SSL/TLS type OpenVPN/AnyConnect, ou WireGuard côté TSSR).
- Concepts crypto : chiffrement symétrique/asymétrique, hachage, PKI/certificats.

8.6 PARE-FEU ET ZONES

Politique par défaut deny all, ouverture au besoin ; notion de **DMZ** pour les services exposés (web, mail). En formation TSSR : mise en pratique fréquente avec **pfSense/OPNsense** ou Stormshield.

Checkpoint Phase 6 — Vous savez : durcir un équipement (SSH, secrets), écrire et placer une ACL, activer port-security/DHCP snooping, expliquer et schématiser un VPN site-à-site, structurer un pare-feu avec DMZ.

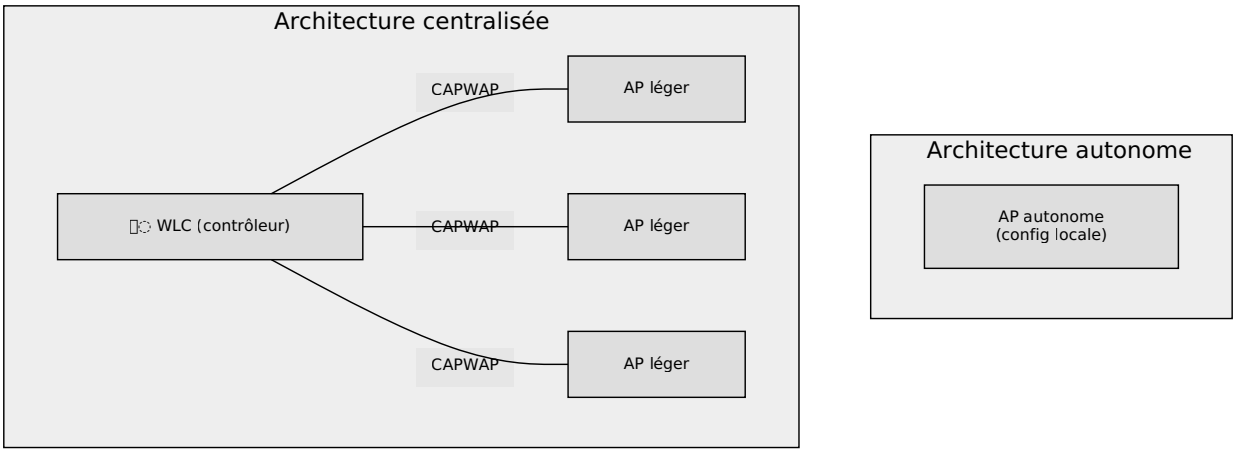
---

9. PHASE 7 — RÉSEAUX SANS FIL (WLAN)

9.1 NOTIONS RADIO

- Bandes **2,4 GHz** (portée, 3 canaux non recouvrants : 1, 6, 11), **5 GHz** et **6 GHz** (débit, plus de canaux).
- Normes : 802.11n (Wi-Fi 4), ac (Wi-Fi 5), **ax (Wi-Fi 6/6E)**, be (Wi-Fi 7).
- Vocabulaire : SSID, BSSID, canal, roaming, cellule.

9.2 ARCHITECTURES



Le **WLC** centralise SSID, sécurité, canaux et puissance ; les AP légers le rejoignent via le tunnel **CAPWAP**.

9.3 SÉCURITÉ WI-FI

Checkpoint Phase 7 — Vous savez : choisir canaux et bandes, expliquer AP autonome vs WLC/CAPWAP, configurer un SSID WPA2/WPA3, décrire le 802.1X.

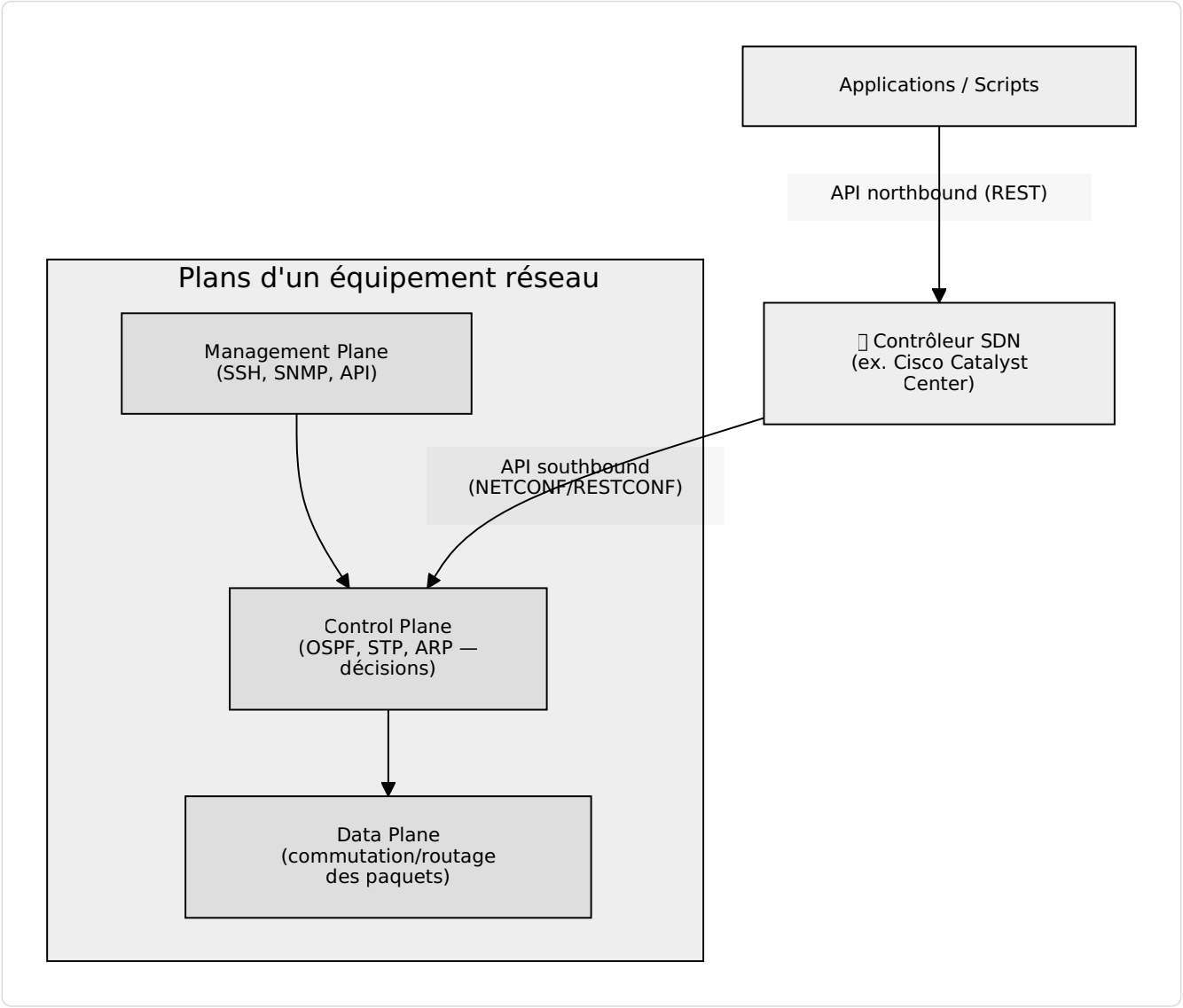
---

10. PHASE 8 — AUTOMATISATION ET PROGRAMMABILITÉ

10.1 POURQUOI AUTOMATISER ?

Configurer 200 switchs à la main = lent et source d'erreurs. L'automatisation apporte cohérence, rapidité et traçabilité — et pèse 10 % du CCNA v1.1 (qui ajoute désormais l'IA générative et le cloud management).

10.2 CONCEPTS SDN



- **Underlay / Overlay / Fabric**, comparaison réseau traditionnel vs controller-based.
- Cisco **Catalyst Center (ex-DNA Center)** vs gestion traditionnelle.

10.3 REST, JSON ET OUTILS

- **API REST** : verbes HTTP (GET/POST/PUT/DELETE), codes de retour (200, 201, 401, 404), authentification.
- **JSON** : savoir lire et repérer objets `{}`, tableaux `[]`, paires clé/valeur.

```JSON
{
  "hostname": "SW-ETAGE1",
  "vlans": [
    { "id": 10, "name": "COMPTA" },
    { "id": 20, "name": "VENTES" }
  ]
}
```

- Outils de gestion de configuration : **Ansible** (agentless, YAML), Terraform ; comparaison avec Puppet/Chef.
- Côté TSSR : scripting **PowerShell** et **Bash/Python** pour l'exploitation quotidienne.
- Nouveautés v1.1 : rôle de l'**IA générative** et du **machine learning** dans l'exploitation réseau (analyse prédictive, assistants de configuration).

Checkpoint Phase 8 — Vous savez : distinguer les 3 plans, expliquer le SDN et les API northbound/southbound, lire du JSON, décrire un playbook Ansible.

---

11. LABS ET PRATIQUE

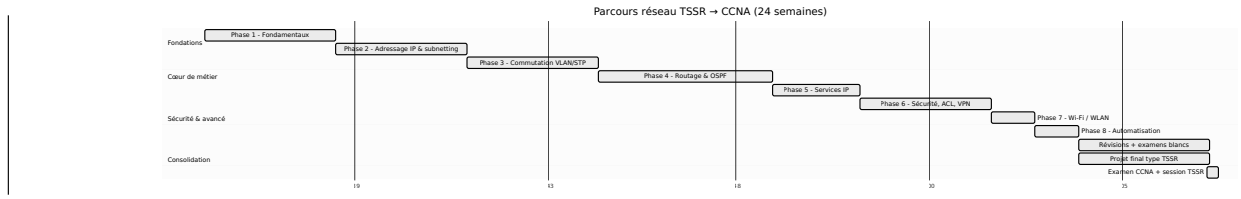
11.1 OUTILS

11.2 LABS INCONTOURNABLES (PROGRESSION)

1. LAN simple : 2 PC + switch, ping, ARP, Wireshark.
2. Plan d'adressage VLSM sur 4 sites + documentation.
3. VLAN + trunk sur 2 switchs + routage inter-VLAN (router-on-a-stick puis SVI).
4. STP : forcer le Root Bridge, observer un port bloqué, PortFast + BPDU Guard.
5. Routage statique 3 routeurs + route par défaut + route flottante.
6. OSPF single-area multi-routeurs + passive-interface + dépannage de voisinage.
7. DHCP centralisé avec relay + DNS + NTP + Syslog vers un serveur.
8. PAT vers Internet + ACL de filtrage.
9. Port-security + DHCP snooping + durcissement SSH.
10. VPN site-à-site entre deux pfSense + télétravailleur en accès distant.
11. WLC + 2 AP + SSID WPA2-Enterprise (simulation Packet Tracer).
12. Mini-projet final type examen TSSR : infrastructure complète 2 sites (AD, DHCP, DNS, VLAN, routage, pare-feu, sauvegarde, supervision) + dossier documentaire.

---

12. PLANNING DE FORMATION SUR 24 SEMAINES



Rythme conseillé : 60 % pratique / 40 % théorie, 10–15 min de drills de subnetting quotidiens, un examen blanc par semaine sur les 3 dernières semaines.

13. AIDE-MÉMOIRE : COMMANDES IOS ESSENTIELLES

```
! ---------- Navigation & sauvegarde ----------
enable                          ! mode privilégié
configure terminal              ! mode configuration
copy running-config startup-config
show running-config

! ---------- Diagnostic (le réflexe TSSR) ----------
ping / traceroute <ip>
show ip interface brief         ! état des interfaces en un coup d'œil
show interfaces status          ! (switch) vitesse, duplex, VLAN
show mac address-table
show vlan brief
show interfaces trunk
show spanning-tree
show ip route
show ip ospf neighbor
show ip nat translations
show ip dhcp binding
show cdp neighbors detail
show access-lists
show port-security interface fa0/1
show logging
show version | include uptime
```

Méthode de dépannage (attendue au TSSR comme au CCNA) : procéder par couches — L1 (câble, LED, `show interfaces`) → L2 (VLAN, trunk, MAC) → L3 (IP, masque, passerelle, route) → L4+ (ACL, NAT, service). Documenter chaque intervention (ticket).

14. PRÉPARATION AUX EXAMENS

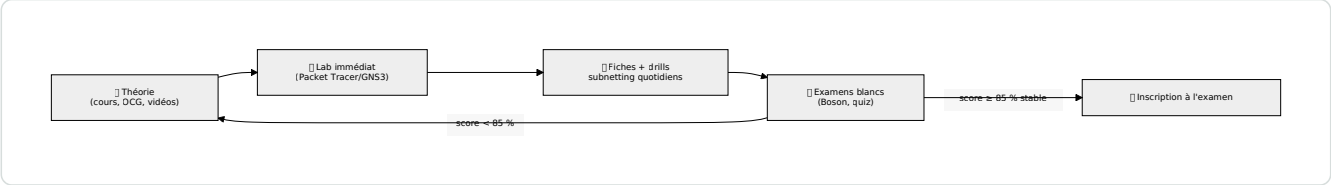
14.1 EXAMEN DU TITRE TSSR

- **Mise en situation professionnelle** pratique (installation/dépannage d'une infrastructure) ;
- **Questionnaire professionnel** ;
- **Dossier professionnel (DP)** retraçant vos réalisations ;
- **Entretiens technique et final** avec un jury de professionnels ;
- Les **ECF** (évaluations en cours de formation) alimentent le livret présenté au jury.

Conseils : soignez la **documentation** (schémas, plans d'adressage, procédures), entraînez-vous à **verbaliser** vos choix techniques, gardez des traces de tous vos labs pour le DP.

14.2 EXAMEN CCNA 200-301

- 120 minutes, environ 100–120 questions (QCM, drag-and-drop, **labs de simulation**) ; **pas de retour en arrière** possible sur une question.
- Les simulations portent surtout sur : VLAN/trunk, routage statique, OSPF, ACL — d'où l'importance du CLI.
- Stratégie : viser large sur IP Connectivity (25 %), lire les sorties `show` avec méthode, gérer son temps (~1 min/question).



15. RESSOURCES

OFFICIELLES

- **Blueprint Cisco CCNA 200-301 v1.1** (exam topics PDF sur cisco.com) — votre checklist ultime.
- **Cisco Networking Academy** (NetAcad) : cours CCNA 1-2-3 souvent intégrés aux formations TSSR.
- **REAC / RC du titre TSSR** (francecompetences.fr) : le référentiel officiel des compétences évaluées.

COURS ET VIDÉOS

- Jeremy's IT Lab (YouTube, gratuit, labs Packet Tracer inclus) — référence CCNA.
- CCNA 200-301 Official Cert Guide (Wendell Odom, vol. 1 & 2).

- OpenClassrooms / cours francophones réseaux pour les bases.

PRATIQUE ET ENTRAÎNEMENT

- **Packet Tracer** + labs de ce document ; GNS3/EVE-NG pour aller plus loin.
- **Boson ExSim** : examens blancs les plus fidèles.
- **subnettingpractice.com** / applis de drills : 10 min par jour.
- **Wireshark** : analysez chaque protocole étudié (ARP, DHCP, TCP handshake, OSPF Hello…).

COMMUNAUTÉS

- r/ccna, forums learningnetwork.cisco.com, Discords francophones sysadmin/réseau.

> **Le mot de la fin** : la différence entre réussir et échouer ne se joue pas sur la quantité de cours lus, mais sur les **heures de lab** et la **régularité**. Un concept par jour, un lab par concept, une doc par lab — et dans 6 mois, le titre TSSR et le CCNA sont à vous. Bon courage !