Mémo CISCO

I. Modes et rappels rapides

- `enable` → passer en mode *privileged EXEC* (`#`).
- `configure terminal` (ou `conf t`) → passer en *global configuration* (`(config)#`).
- Dans *interface config* : `interface <type><num>` (ex. `interface vlan 10`, `interface GigabitEthernet0/0`).
- `end` ou `exit` → remonter d'un niveau de configuration.
- `?` pour l'aide contextuelle.

II. Création de VLANs

- `vlan <id>` → crée/entre dans la configuration du VLAN.
- `name <nom>` → nommer le VLAN.
- Exemple :

```
conf t
 vlan 10
  name RH
 exit
```

III. Ports en mode access (affecter un port à un VLAN)

- `interface range Fa0/1 - 6` → sélectionner une plage d'interfaces.
- `switchport mode access` → mettre en mode access.
- `switchport access vlan <id>` → affecter le VLAN.
- `spanning-tree portfast` → activer PortFast sur ports terminaux.

```
interface range Fa0/1 - 6
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 exit
```

IV. Trunk entre switches

- `interface <port>` (ex. `Gi0/1`) puis :
    - `switchport trunk encapsulation dot1q` (si nécessaire)

- `switchport mode trunk`
- `switchport trunk allowed vlan 10,20,30,40,50` → limiter les VLANs autorisés
- `switchport nonegotiate` → désactiver DTP (sécurité)
- `switchport trunk native vlan <id>` → optionnel, définir native VLAN

```
interface Gi0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50
 switchport nonegotiate
```

V. SVI (Interface VLAN) — adresse IP / passerelle

- `interface vlan <id>` puis :
  - `ip address <IP> <mask>`
  - `no shutdown`

```
interface vlan 10
 ip address 192.168.8.1 255.255.255.0
 no shutdown
```

- Activer le routage L3 sur un switch L3 : `ip routing` (global).

VI. Router-on-a-stick (sous-interfaces sur routeur)

- Créer sous-interfaces et tagger DOT1Q :

```
interface Gig0/0.10
 encapsulation dot1Q 10
 ip address 192.168.8.1 255.255.255.0
```

VII. DHCP relay / ip helper-address

- `interface vlan <id>`
  - `ip helper-address <IP_serveur_DHCP>` → relaie les broadcasts (DHCP/BOOTP et autres UDP par défaut)

```
interface vlan 10
 ip helper-address 192.168.50.10
```

- Pour limiter les ports relayés (global) :
  - `no ip forward-protocol udp 137` (ex. pour NetBIOS) etc.

VIII. ACLs (Extended) — création et application

- Créer : `ip access-list extended <NAME>` ou `access-list <num> ...` (ancienne syntaxe).

- Exemple (bloquer RH ↔ Comptabilité puis autoriser le reste) :

```
ip access-list extended BLOCK_RH_COMPTA
 deny ip 192.168.8.0 0.0.0.255 192.168.9.0 0.0.0.255
 deny ip 192.168.9.0 0.0.0.255 192.168.8.0 0.0.0.255
 permit ip any any
```

- Appliquer sur un SVI (in/out) :

```
interface vlan 10
 ip access-group BLOCK_RH_COMPTA in
```

- Règle d'or : **l'ordre compte** — `deny` avant `permit`. ACL finale implicite : `deny ip any any` (avec numérotation classique) — faites attention.

IX. Sauvegarde / persistances

- `copy running-config startup-config` ou `write memory` → sauvegarder la config.

X. Vérifications / show utiles

- `show vlan brief` — VLANs et ports.
- `show interfaces trunk` — ports trunk et VLANs autorisés.
- `show ip interface brief` — SVI et état IP.
- `show running-config` — config courante.
- `show access-lists` — affichage ACL et compteurs.
- `show ip route` — table de routage (après `ip routing`).
- `show ip dhcp snooping` / `show ip dhcp snooping binding` — état DHCP snooping.
- `show mac address-table` — table MAC du switch.
- `show ip interface vlan <id>` — détails SVI.
- `show logging` / `show buffers` — débogage basique.

XI. Debug (avec précaution)

- `debug ip dhcp server` ou `debug ip packet` → utile en TP mais **à éviter en production** (CPU impact). Toujours utiliser `undebug all` pour désactiver.