CISCO-BASIC

- Les commande de base des élément réseau

Les commande de base des élément réseau

Documentation Réseau Cisco — Routeur C921-4P / Switch L3 Catalyst 1300 / Switch L2 SF500-24

Table des matières

Les configuration faite pour le projet GSB sont ici :

>

> https://sioaubusson.fr/books/cisco

1. Commandes de base et navigation IOS

Ces commandes fonctionnent sur le Routeur C921-4P, le Switch L3 Catalyst 1300 et le Switch L2 SF500-24.

Modes de navigation

```
>                       # Mode utilisateur (lecture seule)
enable                  # Passer en mode privilégié (#)
configure terminal      # Passer en mode configuration globale (config)
exit                    # Revenir au niveau précédent
end                     # Revenir directement au mode privilégié (#)
```

Commandes de vérification essentielles

```
show running-config                 # Affiche la configuration active en mémoire vive
show startup-config                 # Affiche la configuration sauvegardée (qui sera chargée
au boot)
show ip interface brief             # Affiche un résumé de toutes les interfaces et leurs IP
show ip route                       # Affiche la table de routage
show vlan                           # Affiche les VLANs configurés et les ports associés
show interfaces                     # Affiche l'état détaillé de toutes les interfaces
show version                        # Affiche la version IOS et les infos matérielles
```

Sauvegarde de la configuration courante

```
write memory            # Sauvegarde la config active dans la mémoire de démarrage (NVRAM)
copy running-config startup-config   # Équivalent à write memory (plus explicite)
```

> **Important :** Sans cette commande, toute configuration sera perdue au redémarrage de l'équipement.

---

2. Configuration initiale — Mode de base

Nommage de l'équipement

```
conf t
hostname NomDeLEquipement
```

Cette commande définit le nom affiché dans le prompt (ex : `NomDeLEquipement#`). Elle est utile pour identifier rapidement sur quel équipement on travaille en cas de connexion à plusieurs équipements simultanément.

Mot de passe du mode privilégié (enable)

```
conf t
enable secret MonMotDePasse
```

La commande `enable secret` est préférable à `enable password` car elle stocke le mot de passe de façon chiffrée dans la configuration.

Chiffrement global des mots de passe en clair

```
conf t
service password-encryption
```

Cette commande chiffre tous les mots de passe qui seraient autrement stockés en clair dans la configuration (mot de passe de console, de lignes VTY, etc.).

Désactivation des messages intempestifs en cours de saisie

```
conf t
no ip domain-lookup
line console 0
  logging synchronous
```

`no ip domain-lookup` empêche le routeur d'essayer de résoudre en DNS une commande mal tapée (ce qui peut bloquer la saisie pendant plusieurs secondes). `logging synchronous` évite que les messages de log viennent interrompre une saisie en cours.

---

3. Configuration des interfaces

Routeur C921-4P — Port WAN (vers réseau lycée / Internet) en DHCP

```
conf t
interface GigabitEthernet4
  ip address dhcp
  no shutdown
```

`ip address dhcp` demande automatiquement une adresse IP au serveur DHCP du réseau auquel le port est connecté. `no shutdown` active l'interface (par défaut, les interfaces sont désactivées).

Routeur C921-4P — Port LAN (vers le Switch L3) avec IP fixe

```
conf t
interface GigabitEthernet5
  ip address 192.168.80.2 255.255.255.252
  no shutdown
```

On attribue ici une adresse IP fixe sur le lien entre le routeur et le Switch L3. Le masque `/30` (`255.255.255.252`) est adapté à un lien point à point entre deux équipements.

Vérification des interfaces

```
show ip interface brief
```

Exemple de sortie attendue :

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet4	10.123.33.205	YES	DHCP	up	up
GigabitEthernet5	192.168.80.2	YES	manual	up	up

---

4. Configuration SSH sur le Routeur C921-4P

SSH permet d'administrer le routeur à distance de façon sécurisée (contrairement à Telnet qui transmet tout en clair). Toutes ces commandes se font en mode `configure terminal`.

Étape 1 — Définir un nom de domaine (obligatoire pour SSH)

```
conf t
ip domain-name gsb.local
```

Un nom de domaine est nécessaire pour que le routeur puisse générer les clés cryptographiques RSA. Remplacer `gsb.local` par le nom de domaine souhaité.

Étape 2 — Générer la clé RSA

```
crypto key generate rsa
```

Le routeur demande ensuite la taille de la clé :

```
How many bits in the modulus [512]: 2048
```

Saisir **2048** minimum. Une clé de 2048 bits offre un niveau de sécurité acceptable pour une infrastructure locale. Une clé de 4096 bits peut être utilisée pour plus de sécurité (au prix d'une génération plus longue).

Étape 3 — Activer SSH version 2

```
ip ssh version 2
```

SSH v2 est plus sécurisé que SSH v1. Cette commande force l'utilisation de la version 2 exclusivement.

Étape 4 — Paramètres de sécurité SSH

```
ip ssh logging events
ip ssh time-out 60
ip ssh authentication-retries 3
```

- `ip ssh logging events` : journalise toutes les tentatives de connexion SSH dans les logs du routeur.
- `ip ssh time-out 60` : déconnecte un client qui ne s'est pas encore authentifié après 60 secondes.
- `ip ssh authentication-retries 3` : après 3 tentatives d'authentification échouées, la connexion SSH est fermée.

Étape 5 — Créer un utilisateur local

```
service password-encryption
username cisco password 0 caribou23000
```

- `service password-encryption` chiffre le mot de passe dans la configuration.
- `username cisco password 0 caribou23000` crée un utilisateur `cisco` avec le mot de passe `caribou23000`. Le `0` signifie que le mot de passe est fourni en clair (il sera chiffré par `service password-encryption`).

Étape 6 — Configurer les lignes VTY (connexions distantes)

```
line vty 0 3
  transport input ssh
  login local
```

- `line vty 0 3` : configure 4 sessions distantes simultanées (de 0 à 3).
- `transport input ssh` : autorise uniquement SSH comme protocole de connexion à distance (Telnet est refusé).
- `login local` : demande une authentification avec les comptes locaux définis sur l'équipement (ici, l'utilisateur `cisco`).

Vérification SSH

```
show ip ssh
show ssh
```

`show ip ssh` affiche la version et les paramètres SSH configurés. `show ssh` affiche les sessions SSH actuellement actives.

---

5. Connexion SSH depuis Linux (Fedora 43)

Certains algorithmes de cryptographie anciens utilisés par les routeurs Cisco sont désactivés par défaut sur les distributions Linux récentes. Il faut donc les réactiver manuellement côté client.

Modifier le fichier de configuration SSH client

Éditer le fichier `/etc/ssh/ssh_config` en ajoutant à la fin (utiliser **4 espaces** pour l'indentation, pas des tabulations) :

```
Host 192.168.80.2
    KexAlgorithms +diffie-hellman-group1-sha1,diffie-hellman-group14-sha1
    HostKeyAlgorithms +ssh-rsa
    PubkeyAcceptedKeyTypes +ssh-rsa
    Ciphers +aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
```

Remplacer `192.168.80.2` par l'adresse IP réelle de votre équipement, ou utiliser `*` pour appliquer à tous les hôtes (moins recommandé en production).

Se connecter en SSH

```
ssh cisco@192.168.80.2
```

Remplacer `cisco` par le nom d'utilisateur configuré sur le routeur et `192.168.80.2` par l'adresse IP de l'interface du routeur.

---

6. Interface Admin et Console — Switch L3 Catalyst 1300

Interface d'administration IP (accès distant)

L'interface d'administration permet d'accéder au Switch L3 via le réseau (SSH, navigateur web). Elle se configure sur un port physique dédié.

```
conf t
interface GigabitEthernet[X]
  ip address 192.168.1.1 255.255.255.252
  no shutdown
```

Remplacer `[X]` par le numéro du port physique sur lequel on branche le câble d'administration. Le masque `/30` est recommandé pour une interface d'administration point à point.

Interface Console (accès physique direct)

La connexion console est utilisée lorsqu'on n'a pas accès réseau à l'équipement (configuration initiale, récupération après erreur, etc.).

Matériel nécessaire :

- Câble Ethernet branché sur le port **Console** de l'équipement
- Ce câble est redirigé vers une prise Ethernet de la baie (ex : prise verte B-11)
- Un adaptateur **USB vers VGA** + **VGA vers Ethernet** branché sur un port USB de la machine
- L'autre extrémité de l'adaptateur sur la prise Ethernet correspondante de la baie

Logiciel : Ouvrir **PuTTY** et configurer :

- Connection type : **Serial**
- Serial line : `COM[X]` (voir le Gestionnaire de périphériques Windows pour identifier le bon port COM)
- Speed : **9600** (valeur standard pour console Cisco)

---

7. Configuration des VLANs — Switch L3 Catalyst 1300

Création des VLANs

```
conf t
vlan 2,3,4,5,6,7,8,9,10,11,12,13,14,99
```

Cette commande crée tous les VLANs d'un coup. Les VLANs seront ensuite nommés et configurés individuellement.

Attribution des adresses IP aux interfaces VLAN

Chaque interface VLAN représente la passerelle par défaut des machines de ce VLAN.

```
conf t
interface vlan 2
  ip address 192.168.10.1 255.255.255.0
  no shutdown

interface vlan 3
  ip address 192.168.20.1 255.255.255.0
  no shutdown

interface vlan 4
  ip address 192.168.30.1 255.255.255.0
  no shutdown

interface vlan 5
  ip address 192.168.40.1 255.255.255.0
  no shutdown

interface vlan 6
  ip address 192.168.50.1 255.255.255.0
  no shutdown

interface vlan 7
  ip address 192.168.60.1 255.255.255.0
```

```
  no shutdown

interface vlan 8
  ip address 192.168.70.1 255.255.255.0
  no shutdown

interface vlan 9
  ip address 192.168.80.1 255.255.255.252
  no shutdown

interface vlan 99
  ip address 192.168.99.1 255.255.255.0
  no shutdown
```

Le VLAN 9 (`Sortie`) est en `/30` car il s'agit d'un lien point à point vers le routeur. Le VLAN 99 est un VLAN vide utilisé comme "poubelle" pour les ports non utilisés.

Vérification des interfaces VLAN

```
show ip interface brief
```

Toutes les interfaces VLAN configurées doivent apparaître avec le statut `up/up` si un port actif leur est rattaché, ou `up/down` si aucun port actif n'est encore dans ce VLAN.

---

8. Configuration des ports — Switch L3 Catalyst 1300

Port vers le Routeur (mode access VLAN 9 — Sortie)

```
conf t
interface GigabitEthernet1
  switchport mode access
  switchport access vlan 9
```

Ce port est en mode **access** car il relie le Switch L3 au routeur sur un seul VLAN (le VLAN 9, réseau de sortie).

Port vers le Proxmox (mode trunk)

```
conf t
interface GigabitEthernet2
  switchport mode trunk
  switchport trunk allowed vlan add 2,10,11,12,13,14
```

Le mode **trunk** permet de faire transiter plusieurs VLANs sur un même lien physique. On n'autorise que les VLANs nécessaires pour Proxmox.

Port vers le Switch L2 (mode trunk)

```
conf t
interface GigabitEthernet3
  switchport mode trunk
  switchport trunk allowed vlan add 3,4,5,6,7,8
```

Le Switch L2 ne transporte que les VLANs utilisateurs, on n'autorise donc que les VLANs correspondants.

Port non utilisé (VLAN vide pour sécurité)

```
conf t
interface GigabitEthernet[X]
  switchport mode access
  switchport access vlan 99
  shutdown
```

Les ports non utilisés doivent être placés dans le VLAN 99 (vide) **et** désactivés avec `shutdown` pour éviter tout accès non autorisé.

Retirer un VLAN d'un port trunk

```
conf t
interface GigabitEthernet[X]
  switchport trunk allowed vlan remove 99
```

Vérification des VLANs et des ports

```
show vlan
show interfaces trunk
```

`show vlan` affiche quels ports appartiennent à quel VLAN. `show interfaces trunk` affiche les ports en mode trunk et les VLANs autorisés.

---

9. Routage statique — Switch L3 et Routeur

Route par défaut sur le Switch L3 (vers le Routeur)

```
conf t
ip route 0.0.0.0 0.0.0.0 192.168.80.2
```

Cette route par défaut envoie tout le trafic inconnu vers le routeur (`192.168.80.2`). C'est la passerelle de sortie du Switch L3 vers Internet.

Routes spécifiques par VLAN sur le Switch L3

Ces routes indiquent au Switch L3 comment atteindre les réseaux qui ne lui sont pas directement connectés (ex : VLANs gérés par OPNsense/Proxmox).

```
conf t
ip route 192.168.10.0 255.255.255.0 192.168.80.2
ip route 192.168.20.0 255.255.255.0 192.168.80.2
ip route 192.168.30.0 255.255.255.0 192.168.80.2
ip route 192.168.40.0 255.255.255.0 192.168.80.2
ip route 192.168.50.0 255.255.255.0 192.168.80.2
ip route 192.168.60.0 255.255.255.0 192.168.80.2
ip route 192.168.70.0 255.255.255.0 192.168.80.2
ip route 192.168.90.0 255.255.255.0 192.168.80.2
ip route 192.168.100.0 255.255.255.0 192.168.80.2
ip route 192.168.110.0 255.255.255.0 192.168.80.2
```

```
ip route 192.168.120.0 255.255.255.0 192.168.80.2
ip route 192.168.130.0 255.255.255.0 192.168.80.2
```

Route par défaut sur le Routeur (vers le réseau lycée)

```
conf t
ip route 0.0.0.0 0.0.0.0 10.123.33.245
```

Cette route sur le routeur pointe vers la passerelle du réseau lycée (obtenue lors de la configuration DHCP du port WAN).

Vérification du routage

```
show ip route
```

La table de routage affiche :

- `C` = réseau directement connecté
- `S` = route statique configurée manuellement
- `S*` = route statique par défaut

---

10. Configuration NAT — Routeur C921-4P

Le NAT (Network Address Translation) permet aux machines du réseau local (adresses privées) d'accéder à Internet en masquant leurs adresses derrière l'IP publique du routeur.

Étape 1 — Définir les interfaces inside et outside

```
conf t
interface GigabitEthernet5
  ip nat inside

interface GigabitEthernet4
```

```
 ip nat outside
```

- **inside** : interface côté réseau local (LAN, vers le Switch L3)
- **outside** : interface côté réseau externe (WAN, vers Internet/lycée)

Étape 2 — Créer les ACLs (listes de contrôle d'accès) pour chaque VLAN

Les ACLs définissent quels réseaux sont autorisés à utiliser la NAT.

```
conf t
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 permit 192.168.20.0 0.0.0.255
access-list 2 permit 192.168.30.0 0.0.0.255
access-list 2 permit 192.168.40.0 0.0.0.255
access-list 2 permit 192.168.50.0 0.0.0.255
access-list 2 permit 192.168.60.0 0.0.0.255
access-list 2 permit 192.168.70.0 0.0.0.255
access-list 2 permit 192.168.80.0 0.0.0.3
access-list 2 permit 192.168.90.0 0.0.0.15
access-list 2 permit 192.168.100.0 0.0.0.15
access-list 2 permit 192.168.110.0 0.0.0.7
access-list 2 permit 192.168.120.0 0.0.0.3
access-list 2 permit 192.168.130.0 0.0.0.255
```

> **Note sur les masques génériques (wildcard) :** Le masque générique est l'inverse du masque de sous-réseau. Exemples :
>
> - `/24` → `255.255.255.0` → wildcard `0.0.0.255`
> - `/30` → `255.255.255.252` → wildcard `0.0.0.3`
> - `/28` → `255.255.255.240` → wildcard `0.0.0.15`
> - `/29` → `255.255.255.248` → wildcard `0.0.0.7`

Étape 3 — Activer la NAT avec overload (PAT)

```
conf t
ip nat inside source list 2 interface GigabitEthernet4 overload
```

- `list 2` : utilise l'ACL numéro 2 définie précédemment
- `interface GigabitEthernet4` : traduit les adresses sources vers l'IP du port WAN
- `overload` : active le PAT (Port Address Translation), permettant à plusieurs machines de partager la même IP publique en utilisant des ports différents

Vérification de la NAT

```
show ip nat translations
show ip nat statistics
```

`show ip nat translations` affiche les traductions NAT actives (les connexions en cours). `show ip nat statistics` affiche les compteurs de paquets traduits et les erreurs éventuelles.

---

11. Redirection de port (NAT statique) — Routeur C921-4P

La redirection de port (NAT statique) permet de rendre accessible depuis l'extérieur un service interne (serveur web, Proxmox, etc.) en redirigeant un port de l'IP publique vers une IP interne.

Afficher les redirections de port existantes

```
show ip nat translations
```

```
show running-config | include ip nat inside source
```

La première commande affiche les traductions actives en temps réel. La seconde filtre la configuration pour n'afficher que les règles NAT configurées.

Créer une redirection de port

```
conf t
ip nat inside source static tcp 192.168.120.2 80 10.123.33.205 80
```

Cette commande redirige les connexions arrivant sur `10.123.33.205:80` (IP publique, port 80) vers `192.168.120.2:80` (Proxmox, port 80 en interne).

Syntaxe générale :

```
ip nat inside source static tcp [IP_INTERNE] [PORT_INTERNE] [IP_EXTERNE] [PORT_EXTERNE]
```

Autres exemples :

```
ip nat inside source static tcp 192.168.120.2 8006 10.123.33.205 8006
ip nat inside source static tcp 192.168.90.1 443 10.123.33.205 443
```

Supprimer une redirection de port

```
conf t
no ip nat inside source static tcp 192.168.120.2 80 10.123.33.205 80
```

Ajouter `no` devant la commande d'origine pour la supprimer. Sur les routeurs Cisco IOS, il n'est pas possible de désactiver temporairement une règle NAT statique : la seule solution est de la supprimer puis de la recréer.

> **Remarque :** Cette limitation n'existe pas sur les équipements Cisco ASA/Firepower qui disposent d'une interface graphique avec une option Enable/Disable par règle.

Sauvegarder après modification

```
write memory
```

Ne pas oublier de sauvegarder après chaque modification de configuration NAT.

---

12. Sauvegarde et restauration de configuration sur clé USB

La sauvegarde sur clé USB permet de conserver une copie de la configuration hors de l'équipement et de la restaurer rapidement en cas de panne, réinitialisation ou remplacement de matériel.

Prérequis — Préparation de la clé USB

Outil recommandé : AOMEI Partition Assistant

La clé USB doit être formatée avec les caractéristiques suivantes :

Paramètre	Valeur
Système de fichiers	**FAT16**
Taille de la partition	**Inférieure à 2 Go**
Clé recommandée	PNY

> **Important :** Le routeur Cisco C921-4P ne reconnaît pas les partitions FAT32 ou NTFS pour l'accès USB. La partition doit impérativement être en FAT16 et faire moins de 2 Go.

Routeur C921-4P — Sauvegarde de la configuration

Brancher la clé USB sur le port USB du routeur, puis en mode privilégié (`#`) :

```
copy startup-config usbflash0:config_routeur_backup.cfg
```

- `startup-config` : la configuration sauvegardée en NVRAM (celle qui sera chargée au prochain démarrage)
- `usbflash0:` : désigne le premier port USB du routeur
- `config_routeur_backup.cfg` : nom du fichier sur la clé (choisir un nom explicite)

Routeur C921-4P — Restauration de la configuration

```
copy usbflash0:config_routeur_backup.cfg startup-config
reload
```

La commande `copy` charge le fichier de la clé vers la NVRAM. La commande `reload` redémarre le routeur pour appliquer la configuration restaurée.

> **Attention :** Un `reload` redémarre l'équipement. Toutes les connexions actives seront interrompues pendant le redémarrage (~2 minutes).

Switch L3 Catalyst 1300 — Sauvegarde

```
copy startup-config usbflash0:config_switchL3_backup.cfg
```

Switch L3 Catalyst 1300 — Restauration

```
copy usbflash0:config_switchL3_backup.cfg startup-config
reload
```

Switch L2 SF500-24 — Sauvegarde

```
copy startup-config usbflash0:config_switchL2_backup.cfg
```

Switch L2 SF500-24 — Restauration

```
copy usbflash0:config_switchL2_backup.cfg startup-config
reload
```

Vérifier le contenu de la clé USB

```
dir usbflash0:
```

Cette commande liste tous les fichiers présents sur la clé USB insérée dans l'équipement.

Bonnes pratiques de sauvegarde

- Nommer les fichiers avec la date : `config_routeur_2025-01-15.cfg`
- Sauvegarder **avant** toute modification importante
- Sauvegarder **après** toute configuration validée et testée (`write memory` puis `copy startup-config usbflash0:...`)
- Conserver plusieurs versions horodatées sur la clé

Documentation rédigée pour le réseau GSB — Équipements : Cisco C921-4P / Catalyst 1300 / SF500-24