Labs en Réseaux Informatiques avec Cisco Packet Tracer & GNS3

Formation Pratique - Niveau L2, L3 et Master

August 7, 2025

Introduction

Présentation du livre Ce livre a pour objectif de vous guider à travers la réalisation de labs en réseaux informatiques en utilisant Cisco Packet Tracer et GNS3. Vous apprendrez à configurer et à gérer différents aspects des réseaux informatiques de manière pratique et interactive, avec une progression adaptée aux niveaux L2, L3 et Master.

Public cible

Ce livre est destiné aux étudiants de 2ème, 3ème année et plus, aux professionnels de l'informatique et à toute personne intéressée par les réseaux informatiques pratiques.

Importance des labs en réseaux informatiques Les labs sont essentiels pour comprendre les concepts théoriques et pour acquérir des compétences pratiques en réseaux informatiques.

Prérequis Pour suivre ce livre, vous devez avoir des connaissances de base en réseaux informatiques et avoir installé Cisco Packet Tracer et/ou GNS3.

Chapter 1

Fondamentaux des Réseaux Informatiques

1.1 Origine des Réseaux Informatiques

1.2 Historique des Réseaux Informatiques

Les réseaux informatiques ont évolué depuis les premiers jours de l'informatique. Les premiers réseaux étaient des connexions point à point entre ordinateurs.

1.3 Évolution des Réseaux

Les réseaux ont évolué pour inclure des technologies comme Ethernet, Wi-Fi, et les réseaux mobiles.

1.4 Transmission des Informations

1.5 Notion de Transmission de Données

La transmission de données est le processus de transfert de données d'un point à un autre.

1.6 Types de Transmission

Il existe différents types de transmission de données, y compris la transmission série et parallèle.

Chapter 2

IANA et Répartition des Adresses IP

2.1 Introduction à l'IANA

L'IANA (Internet Assigned Numbers Authority) a été créée par Jon Postel, l'un des pionniers de l'Internet, dans les années 1970. Initialement, elle était gérée par l'Université de Californie du Sud (USC) sous contrat avec le gouvernement américain. En 1998, la gestion de l'IANA a été transférée à l'ICANN, marquant une étape importante dans la privatisation de la gestion de l'Internet.

L'IANA est une organisation clé dans le domaine des réseaux informatiques et de l'Internet. Elle est responsable de la coordination mondiale des attributions uniques les adresses IP, les noms de domaine, et les numéros de port.

2.2 Répartition des Adresses IP

Les adresses IP sont réparties entre différents RIR (Regional Internet Registries).

2.3 RIR (Regional Internet Registries)

Introduction aux RIR Registres Internet Régionaux (RIR) : Il existe cinq RIR dans le monde, chacun couvrant une région géographique spécifique : AFRINIC : Afrique APNIC : Asie-Pacifique ARIN : Amérique du Nord LACNIC : Amérique latine et Caraïbes RIPE NCC : Europe, Moyen-Orient et Asie centrale

Rôle des RIR Les RIR sont des organisations qui gèrent les adresses IP au niveau régional. Leur rôle est d'attribuer des adresses aux fournisseurs d'accès à internet.

2.4 FAI (Fournisseurs d'Accès Internet)

Introduction aux FAI Les ISP reçoivent des blocs d'adresses IP des RIR et les distribuent à leurs clients, qui peuvent être des entreprises, des institutions éducatives, des particuliers, etc.

Rôle des FAI Les organisations et les utilisateurs finaux reçoivent des adresses IP de leurs ISP. Ces adresses peuvent être publiques (accessibles directement depuis l'Internet) ou privées (utilisées à l'intérieur d'un réseau local).

Chapter 3

Équipements Réseaux

3.1 Cartes Réseaux

Une carte réseau, également appelé carte d'interface réseau (NIC pour Network Interface Card en anglais), est un composant matériel qui permet à un ordinateur de se connecter à un réseau informatique.

3.1.1 Différentes Cartes Réseaux

3.1.2 Fonctionnement des Cartes Réseaux

Les cartes réseaux permettent la communication entre les ordinateurs et les réseaux.

Fonctionnement Carte Réseau Description détaillée du fonctionnement d'une carte réseau.

Types Cartes Réseaux Sur les marchés actuels, il existe essentiellement deux catégories de cartes réseaux.

Cartes Internes Ethernet : Utilisée pour les connexions filaires via des câbles Ethernet. Wi-Fi : Permet les connexions sans fil via des ondes radio. Fibre Optique : Utilisée pour les connexions à très haute vitesse via des câbles en fibre optique.

Cartes Réseau Externes La carte réseau externe vient pallier en cas de défaillance de la carte réseau interne installée sur le hardware même. Ils se connectent via des slots d'extension comme le PCI ou le PCIe.

Débit d'une Carte Réseau Les cartes réseau sont classées par leur débit, c'est-à-dire la vitesse à laquelle elles peuvent transmettre des données. Par exemple, une carte Ethernet peut être de 10/100 Mbps, 1 Gbps, ou même 10 Gbps.

3.2 Équipements de Connexion

3.2.1 Les Différents Types de Câbles Ethernet

3.2.2 Câbles en Cuivre

Description des câbles Ethernet en cuivre.

3.2.3 Câbles en Fibre Optique

Description des câbles Ethernet en fibre optique.

3.2.4 Les Différentes Catégories de Câbles Ethernet

Catégories et Vitesses pour les Câbles en Cuivre

1. **Câble Cat 5**
    - **Description** : Catégorie 5 (Cat 5) est un type de câble Ethernet capable de supporter des vitesses de transmission de données jusqu'à 100 Mbps (Fast Ethernet).
    - **Longueur Maximale** : 100 mètres (328 pieds).
2. **Câble Cat 5e**
    - **Description** : Catégorie 5e (Cat 5e) est une version améliorée de Cat 5, capable de supporter des vitesses de transmission de données jusqu'à 1 Gbps (Gigabit Ethernet).
    - **Longueur Maximale** : 100 mètres (328 pieds).
3. **Câble Cat 6**
    - **Description** : Catégorie 6 (Cat 6) est un type de câble Ethernet capable de supporter des vitesses de transmission de données jusqu'à 10 Gbps sur des distances plus courtes (jusqu'à 55 mètres) et 1 Gbps sur des distances plus longues.
    - **Longueur Maximale** : 100 mètres (328 pieds) pour 1 Gbps, 55 mètres (180 pieds) pour 10 Gbps.
4. **Câble Cat 6a**
    - **Description** : Catégorie 6a (Cat 6a) est une version améliorée de Cat 6, capable de supporter des vitesses de transmission de données jusqu'à 10 Gbps sur des distances plus longues.
    - **Longueur Maximale** : 100 mètres (328 pieds) pour 10 Gbps.
5. **Câble Cat 7**
    - **Description** : Catégorie 7 (Cat 7) est un type de câble Ethernet capable de supporter des vitesses de transmission de données jusqu'à 10 Gbps et offre une meilleure protection contre les interférences électromagnétiques (EMI).
    - **Longueur Maximale** : 100 mètres (328 pieds).
6. **Câble Cat 8**
    - **Description** : Catégorie 8 (Cat 8) est le type de câble Ethernet le plus récent, capable de supporter des vitesses de transmission de données jusqu'à 40 Gbps sur des distances plus courtes.
    - **Longueur Maximale** : 30 mètres (98 pieds) pour 40 Gbps.

3.2.5 Catégories et Vitesses pour les Câbles en Fibre Optique

1. **Fibre Multimode**
    - **Description** : La fibre multimode utilise plusieurs modes de lumière pour transmettre des données, ce qui permet des distances plus courtes mais avec une capacité de transmission de données élevée.

- **Longueur Maximale** :
  - **OM1** : 275 mètres pour 1 Gbps, 33 mètres pour 10 Gbps.
  - **OM2** : 550 mètres pour 1 Gbps, 82 mètres pour 10 Gbps.
  - **OM3** : 550 mètres pour 10 Gbps, 100 mètres pour 40/100 Gbps.
  - **OM4** : 400 mètres pour 10 Gbps, 150 mètres pour 40/100 Gbps.

2. **Fibre Monomode**

   - **Description** : La fibre monomode utilise un seul mode de lumière pour transmettre des données, ce qui permet des distances beaucoup plus longues avec une capacité de transmission de données élevée.
   - **Longueur Maximale** :
     - **OS1** : Jusqu'à 40 kilomètres pour 10 Gbps, 10 kilomètres pour 40/100 Gbps.
     - **OS2** : Jusqu'à 40 kilomètres pour 10 Gbps, 10 kilomètres pour 40/100 Gbps.

3.3 Équipements d'Interconnexion

Les Constructeurs

En réseaux informatiques, les composantes matérielles essentielles sont fabriquées par plusieurs constructeurs. Néanmoins, certains en sont les leaders. Il s'agit entre autres de :

1. **Cisco Systems**

   - **Description** : Cisco est l'un des leaders mondiaux dans le domaine des réseaux.
   - **Produits Notables** : Cisco ISR, Cisco ASR, Cisco CRS.

2. **Juniper Networks**

   - **Description** : Juniper est un autre grand acteur dans le domaine des réseaux.
   - **Produits Notables** : Juniper MX Series, Juniper PTX Series.

3. **Huawei, Arista Networks, Nokia, HPE, D-Link, TP-Link, Netgear, MikroTik, Ubiquiti Networks, Fortinet, Zyxel, Extreme Networks, Palo Alto Networks**

3.3.1 Hubs

Description des hubs et leurs caractéristiques (équipements obsolètes mais importants historiquement).

3.3.2 Switches

Description des switches et leurs caractéristiques.

3.3.3 Types de Switches

- **Switches non managés** : Configuration automatique, plug-and-play
- **Switches managés** : Configuration avancée, VLANs, sécurité
- **Switches L3** : Capacités de routage inter-VLAN

3.3.4 Routeurs

Description des routeurs et leurs caractéristiques.

Fonctionnement des Routeurs

Les routeurs sont des dispositifs essentiels dans les réseaux informatiques, permettant la communication entre différents réseaux. Ils dirigent le trafic réseau en utilisant des tables de routage et des algorithmes de routage pour déterminer le meilleur chemin pour les paquets de données.

Types de Mémoire dans les Routeurs

RAM (Random Access Memory)

- **Fonction** : Stockage temporaire des données et instructions
- **Caractéristiques** : Volatile, données perdues à l'extinction
- **Utilisation** : Tables de routage, buffers de paquets, informations de session

Flash Memory

- **Fonction** : Stockage du firmware (IOS Cisco)
- **Caractéristiques** : Non volatile
- **Utilisation** : Système d'exploitation, mises à jour

NVRAM (Non-Volatile Random Access Memory)

- **Fonction** : Stockage de la configuration de démarrage
- **Caractéristiques** : Non volatile
- **Utilisation** : Configuration startup-config

ROM (Read-Only Memory)

- **Fonction** : Firmware de base et instructions de démarrage
- **Caractéristiques** : Non volatile, non modifiable
- **Utilisation** : Programme de bootstrap

3.3.5 Les différentes types de Routeurs

Routeurs dommestiques

Routeurs dommestiques

Routeurs d entreprises

Routeurs de Coeur Réseau

Liste des Routeurs Cisco en fonction de la vitesse des ports

Chapter 4

Outils de Simulation

4.1 Cisco Packet Tracer vs GNS3

Caractéristique	Cisco Packet Tracer	GNS3
Type de logiciel	Propriétaire	Open-source
Support des dispositifs	Cisco uniquement	Multi-fabricants
Interface utilisateur	Graphique	Graphique
Utilisation principale	Éducation et formation	Éducation, formation, et développement
Complexité des simulations	Moyenne	Élevée
Support des protocoles	Limité	Étendu
Niveau recommandé	L2-L3	L3-Master

Table 4.1: Comparaison entre Cisco Packet Tracer et GNS3

4.1.1 Prise en main de Cisco Packet Tracer

4.1.2 Installation et configuration initiale

Téléchargement et installation de Packet Tracer.

4.1.3 Présentation complète de l'interface Cisco Packet Tracer

Description détaillée de l'interface utilisateur et des fonctionnalités.

4.1.4 Création de votre premier projet

Création d'un nouveau projet et ajout de dispositifs réseau.

4.2 Prise en main de GNS3

4.2.1 Installation et configuration GNS3

Guide d'installation pour les labs avancés.

4.2.2 Import d'images IOS

Procédure pour importer les images Cisco IOS dans GNS3.

Chapter 5

Commandes de configuration de Base

5.1 Commandes de configuration switches

5.1.1 Configuration d'identité

```
hostname [nom]                          # Définir le nom du switch
banner motd [message]                   # Message du jour
```

5.1.2 Configuration des mots de passe

```
enable password [motdepasse]            # Mot de passe mode privilégié (non chiffré)
enable secret [motdepasse]              # Mot de passe mode privilégié (chiffré)
line console 0                          # Configuration de la console
password [motdepasse]                   # Mot de passe console
login                                   # Activer l'authentification
line vty 0 15                           # Configuration Telnet/SSH
password [motdepasse]                   # Mot de passe pour accès distant
login                                   # Activer l'authentification
service password-encryption             # Chiffrer tous les mots de passe
```

5.1.3 Configuration des interfaces

```
interface [type][numero]                # Entrer dans la configuration d'interface
description [description]               # Description de l'interface
shutdown                                # Désactiver l'interface
no shutdown                             # Activer l'interface
```

5.1.4 Commandes de vérification

```
show version                            # Informations système
show interfaces                         # État des interfaces
show mac address-table                  # Table d'adresses MAC
show vlan                               # Informations VLAN
```

5.1.5 Configuration des VLANs

```
vlan [numero]                                # Créer un VLAN
name [nom]                                   # Assigner un nom à un VLAN
interface range [type] [numero1] - [numero2] # Sélectionner une plage d'interfaces
switchport mode access                       # Configurer une interface en mode accès
switchport access vlan [numero]              # Assigner un VLAN à une interface
switchport mode trunk                        # Configurer une interface en mode trunk
switchport trunk allowed vlan [liste]        # Spécifier les VLANs autorisés
switchport trunk native vlan [numero]        # Définir le VLAN natif
```

5.1.6 Configuration des Ports

```
speed [vitesse]                              # Définir la vitesse d'un port
duplex [mode]                                # Définir le mode duplex (full, half, auto)
spanning-tree portfast                       # Activer le mode PortFast
spanning-tree bpduguard enable               # Activer la protection BPDU Guard
```

5.1.7 Sécurité des Ports

```
switchport port-security                     # Activer la sécurité des ports
switchport port-security maximum [nombre]  # Nombre max d'adresses MAC
switchport port-security mac-address [adresse] # Assigner une MAC spécifique
switchport port-security violation [action] # Action en cas de violation
switchport port-security mac-address sticky # Apprentissage automatique des MAC
```

5.1.8 Configuration des ACL (Access Control Lists)

```
access-list [numero] permit [source] [destination] # Créer une règle ACL
ip access-group [numero] in                  # Appliquer une ACL en entrée
ip access-group [numero] out                 # Appliquer une ACL en sortie
```

5.1.9 Configuration EtherChannel/LACP

```
interface port-channel [numero]              # Créer un canal de liaison
channel-group [numero] mode active           # Mode LACP actif
channel-group [numero] mode passive          # Mode LACP passif
channel-group [numero] mode on               # Mode statique
```

5.1.10 Configuration Spanning Tree

```
spanning-tree mode [pvst/rapid-pvst/mst]  # Mode STP
spanning-tree vlan [numero] root primary   # Définir comme root bridge
spanning-tree vlan [numero] priority [valeur] # Définir la priorité
spanning-tree portfast default               # PortFast par défaut
spanning-tree bpduguard default              # BPDU Guard par défaut
```

5.1.11 Configuration VTP

```
vtp mode [server/client/transparent]        # Mode VTP
vtp domain [nom]                            # Domaine VTP
vtp password [mot de passe]                 # Mot de passe VTP
vtp version [1/2/3]                         # Version VTP
```

5.1.12 Commandes de Vérification Switch

```
show running-config                         # Configuration en cours
show vlan brief                             # Résumé des VLANs
show interfaces status                      # État des interfaces
show spanning-tree                          # Informations STP
show etherchannel summary                   # Résumé EtherChannel
show port-security                          # Sécurité des ports
show mac address-table                      # Table des adresses MAC
show vtp status                             # État VTP
```

5.2 Commandes de configuration routeurs

5.2.1 Configuration de Base

```
enable                                      # Mode privilégié
configure terminal                          # Configuration globale
hostname [nom]                              # Nom du routeur
interface [type] [numero]                   # Configuration d'interface
ip address [IP] [masque]                    # Adresse IP d'interface
no shutdown                                 # Activation d'interface
```

5.2.2 Routage Statique

```
ip route [reseau] [masque] [next-hop]       # Route statique
ip route 0.0.0.0 0.0.0.0 [next-hop]         # Route par défaut
```

5.2.3 Routage Dynamique

OSPF

```
router ospf [process-id]                    # Configuration OSPF
network [reseau] [wildcard] area [area]     # Réseau OSPF
router-id [ID]                              # Router ID OSPF
```

EIGRP

```
router eigrp [AS]                           # Configuration EIGRP
network [reseau]                            # Réseau EIGRP
no auto-summary                             # Désactive la summarisation automatique
```

RIP

```
router rip                                    # Configuration RIP
version 2                                     # RIP version 2
network [reseau]                              # Réseau RIP
no auto-summary                               # Désactive la summarisation
```

5.2.4 NAT Configuration

```
ip nat inside                                 # Interface interne NAT
ip nat outside                                # Interface externe NAT
ip nat inside source list [ACL] pool [pool] overload # NAT dynamique avec PAT
ip nat pool [nom] [IP-debut] [IP-fin] netmask [masque] # Pool NAT
```

5.2.5 DHCP Configuration

```
ip dhcp excluded-address [debut] [fin]      # Adresses exclues
ip dhcp pool [nom]                          # Pool DHCP
network [reseau] [masque]                   # Réseau du pool
default-router [IP]                         # Passerelle par défaut
dns-server [IP]                             # Serveur DNS
```

5.2.6 Commandes de Vérification Routeur

```
show ip interface brief                     # Résumé des interfaces
show ip route                               # Table de routage
show ip protocols                           # Protocoles de routage
show ip nat translations                    # Traductions NAT
show ip dhcp binding                        # Attributions DHCP
show ip ospf neighbor                       # Voisins OSPF
show ip eigrp neighbors                     # Voisins EIGRP
```

Chapter 6

Labs Pratiques Niveau L2-L3

6.1 Labs de Base (Niveau L2)

6.1.1 Lab 1: Configuration de base d'un réseau local (LAN)

Objectif : Connecter deux ordinateurs via un switch.

Matériel virtuel :

- 2 PC
- 1 Switch 2960
- Câbles Ethernet droits

Étapes :

1. Lancer Cisco Packet Tracer
2. Ajouter les dispositifs dans l'espace de travail
3. Connecter les PC au switch avec des câbles droits
4. Configurer les adresses IP des PC (192.168.1.10/24 et 192.168.1.20/24)
5. Tester la connectivité avec ping

Hôtes/PC	Adresses IP	Ports Switch
PC1	192.168.1.10/24	FastEthernet0/1
PC2	192.168.1.20/24	FastEthernet0/2

Table 6.1: Configuration des hôtes pour le Lab 1

Configuration CLI des PC et du Switch

Configuration de PC1

```
PC1>ipconfig 192.168.1.10 255.255.255.0 192.168.1.1  # Configurer l'adresse IP et la
    passerelle
```

Configuration de PC2

```
PC2>ipconfig 192.168.1.20 255.255.255.0 192.168.1.1  # Configurer l'adresse IP et la
    passerelle
```

Configuration du Switch 2960

```
Switch>enable                                # Passer en mode privilégié
Switch#configure terminal                    # Entrer en mode de configuration globale
Switch(config)#hostname Switch1              # Définir le nom du switch
Switch1(config)#interface FastEthernet0/1    # Configurer le port pour PC1
Switch1(config-if)#switchport mode access    # Définir le mode accès
Switch1(config-if)#no shutdown               # Activer le port
Switch1(config-if)#exit                      # Sortir du mode interface
Switch1(config)#interface FastEthernet0/2    # Configurer le port pour PC2
Switch1(config-if)#switchport mode access    # Définir le mode accès
Switch1(config-if)#no shutdown               # Activer le port
Switch1(config-if)#end                       # Retourner au mode privilégié
Switch1#                                     # Prompt final
```

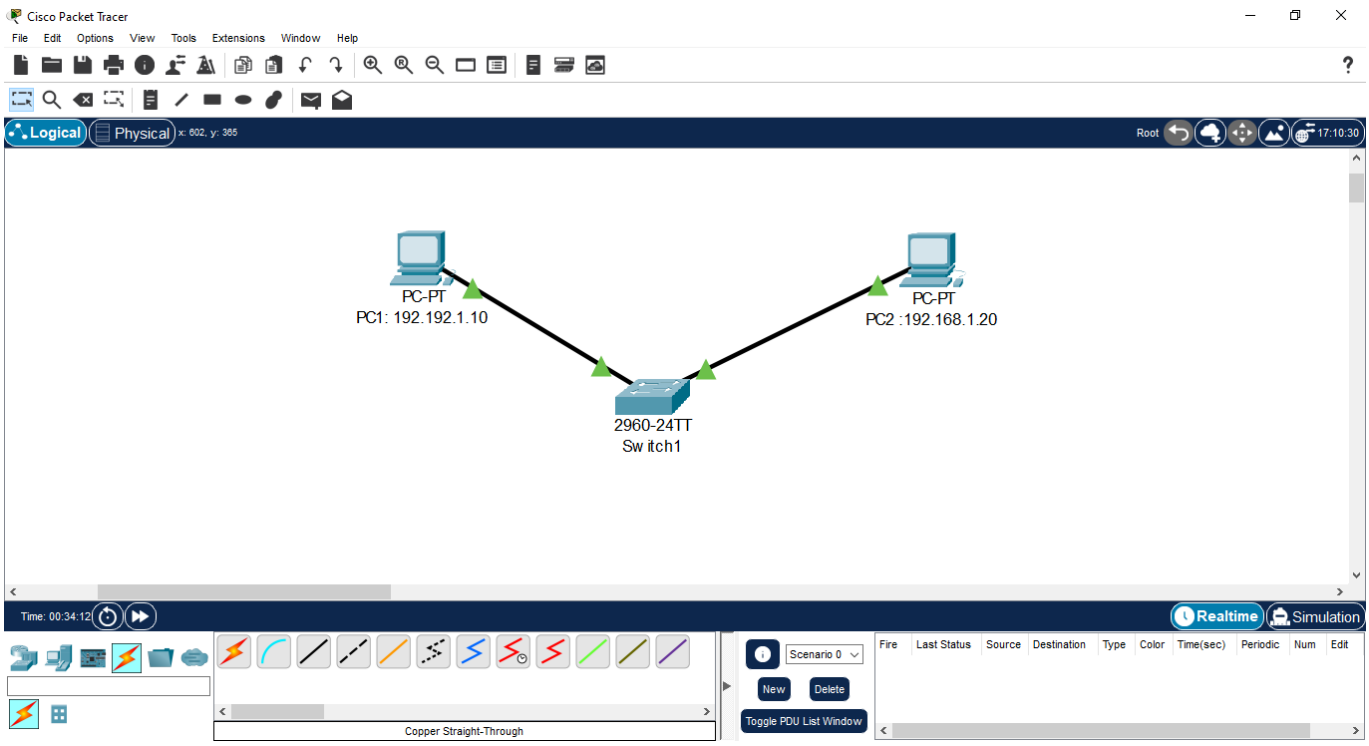

Figure 6.1: Lab 1:LAN1

Liens utils Recommandés

1. vidéo:
2. Livre p-10:
3. Livre P-13:

6.1.2 Lab 2: Configuration de base d'un switch

Objectif : Configurer les paramètres de base d'un switch.
Configuration :

1. Accéder au switch via console
2. Configurer le hostname
3. Configurer les mots de passe (enable, console, vty)
4. Configurer une adresse IP de gestion
5. Sauvegarder la configuration

6.1.3 Lab 3: Configuration des VLANs

Objectif : Segmenter un réseau avec des VLANs.
Scenario :

- VLAN 10 : Département IT (192.168.10.0/24)
- VLAN 20 : Département RH (192.168.20.0/24)

Configuration :

1. Créer les VLANs sur le switch
2. Assigner les ports aux VLANs appropriés
3. Configurer un port trunk entre switches
4. Tester l'isolation des VLANs

6.1.4 Lab 4: Configuration d'un routeur de base

Objectif : Configurer les paramètres de base d'un routeur.
Configuration :

1. Accéder au routeur via console
2. Configurer le hostname et les mots de passe
3. Configurer les interfaces avec des adresses IP
4. Configurer une route statique
5. Tester la connectivité inter-réseaux

6.1.5 Lab 5: Routage inter-VLAN

Objectif : Permettre la communication entre VLANs via un routeur.
Matériel :

- 1 Routeur (Router-on-a-stick ou routeur L3)
- 1 Switch managé
- 4 PC (2 par VLAN)

Configuration :

1. Configurer les VLANs sur le switch
2. Configurer le trunking vers le routeur
3. Configurer les sous-interfaces sur le routeur
4. Tester la communication inter-VLAN

6.2 Labs Intermédiaires (Niveau L2-L3)

6.2.1 Lab 6: Configuration Spanning Tree Protocol (STP)

Objectif : Comprendre et configurer STP pour éviter les boucles.
Scenario : Réseau avec redondance physique

- 3 Switches interconnectés en triangle
- Observer la convergence STP
- Forcer un switch comme root bridge
- Simuler une panne de lien

Configuration STP avancée :

1. **spanning-tree mode rapid-pvst** : Activer RSTP
2. **spanning-tree vlan 1 root primary** : Root bridge principal
3. **spanning-tree vlan 1 root secondary** : Root bridge secondaire
4. **spanning-tree portfast default** : PortFast sur tous les ports d'accès
5. **spanning-tree bpduguard default** : Protection BPDU Guard

6.2.2 Lab 7: Configuration EtherChannel/LACP

Objectif : Agréger plusieurs liens physiques pour augmenter la bande passante.
Scenario :

- 2 Switches connectés par 2 liens FastEthernet
- Configurer LACP pour créer un lien logique de 200 Mbps
- Tester la répartition de charge

- Simuler la panne d'un lien

Configuration :

1. Sélectionner les interfaces à agréger
2. **channel-group 1 mode active** : LACP actif
3. **interface port-channel 1** : Configuration du canal
4. **switchport mode trunk** : Mode trunk sur le port-channel
5. Vérifier avec **show etherchannel summary**

6.2.3 Lab 8: Sécurité des ports (Port Security)

Objectif : Sécuriser les ports d'accès contre les accès non autorisés.
Configuration avancée :

1. **switchport port-security** : Activer la sécurité
2. **switchport port-security maximum 2** : Maximum 2 MAC par port
3. **switchport port-security mac-address sticky** : Apprentissage automatique
4. **switchport port-security violation restrict** : Action en cas de violation
5. **switchport port-security aging time 10** : Vieillissement des MAC

Tests :

- Connecter plus d'équipements que autorisé
- Observer les violations et les actions prises
- Vérifier les logs avec **show port-security**

6.2.4 Lab 9: DHCP Snooping et sécurité

Objectif : Protéger contre les serveurs DHCP malveillants.
Configuration :

1. **ip dhcp snooping** : Activer DHCP Snooping globalement
2. **ip dhcp snooping vlan 10,20** : Activer sur les VLANs spécifiques
3. **ip dhcp snooping trust** : Interface de confiance (vers serveur DHCP légitime)
4. **ip dhcp snooping information option** : Option 82
5. **ip dhcp snooping database flash:dhcp.txt** : Base de données persistante

6.2.5 Lab 10: Serveurs réseau (DHCP, DNS, TFTP, FTP, Web)

Objectif : Configurer et tester les services réseau essentiels.
Serveur DHCP sur routeur :

1. **ip dhcp excluded-address 192.168.1.1 192.168.1.10** : Exclure les adresses
2. **ip dhcp pool LAN** : Créer le pool
3. **network 192.168.1.0 255.255.255.0** : Réseau du pool
4. **default-router 192.168.1.1** : Passerelle
5. **dns-server 8.8.8.8** : Serveur DNS
6. **lease 7** : Durée du bail (7 jours)

Tests :

- Configurer les PC en DHCP automatique
- Vérifier l'attribution d'adresses avec **show ip dhcp binding**
- Tester les services DNS, TFTP, FTP, Web depuis les PC

6.3 Labs Avancés (Niveau L3)

6.3.1 Lab 11: Routage dynamique RIP

Objectif : Configurer RIP v2 pour l'échange automatique de routes.
Topologie : 3 routeurs interconnectés avec différents réseaux LAN.
Configuration RIP v2 :

1. **router rip** : Activer RIP
2. **version 2** : Utiliser RIP version 2
3. **network 192.168.1.0** : Annoncer les réseaux
4. **no auto-summary** : Désactiver la summarisation automatique
5. **passive-interface [interface]** : Interface passive (ne pas envoyer de mises à jour)

Vérifications :

- **show ip route rip** : Routes apprises via RIP
- **show ip protocols** : Configuration des protocoles
- **debug ip rip** : Déboguer RIP (attention en production !)

6.3.2 Lab 12: Routage dynamique OSPF

Objectif : Configurer OSPF pour des réseaux plus complexes.
Configuration OSPF avancée :

1. **router ospf 1** : Processus OSPF
2. **router-id 1.1.1.1** : ID unique du routeur
3. **network 192.168.1.0 0.0.0.255 area 0** : Réseau dans l'aire 0
4. **area 0 authentication message-digest** : Authentification MD5
5. **ip ospf message-digest-key 1 md5 cisco** : Clé d'authentification sur l'interface
6. **ip ospf cost 100** : Modifier le coût d'une interface

Concepts OSPF à explorer :

- Aires OSPF (Area 0 = backbone)
- DR/BDR (Designated Router/Backup)
- LSA (Link State Advertisement)
- Convergence rapide vs RIP

6.3.3 Lab 13: Routage dynamique EIGRP

Objectif : Configurer EIGRP, protocole propriétaire Cisco.
Configuration EIGRP :

1. **router eigrp 100** : Système autonome EIGRP
2. **network 192.168.1.0 0.0.0.255** : Réseau avec wildcard mask
3. **no auto-summary** : Désactiver la summarisation
4. **eigrp router-id 1.1.1.1** : ID du routeur
5. **bandwidth 1544** : Modifier la bande passante sur l'interface
6. **ip hello-interval eigrp 100 5** : Intervalle Hello
7. **ip hold-time eigrp 100 15** : Temps de maintien

Fonctionnalités EIGRP :

- Métrique composite (bande passante, délai, charge, fiabilité)
- Convergence rapide avec DUAL algorithm
- Support du VLSM et CIDR
- Répartition de charge inégale

6.3.4 Lab 14: NAT/PAT Configuration avancée

Objectif : Maîtriser les différents types de NAT.

NAT Statique :

1. **ip nat inside source static 192.168.1.10 203.0.113.10** : Mappage 1:1

NAT Dynamique :

1. **ip nat pool PUBLIC 203.0.113.10 203.0.113.20 netmask 255.255.255.0** : Pool d'adresses
2. **access-list 1 permit 192.168.1.0 0.0.0.255** : ACL pour les adresses internes
3. **ip nat inside source list 1 pool PUBLIC** : Mappage dynamique

PAT (Port Address Translation) :

1. **ip nat inside source list 1 pool PUBLIC overload** : PAT avec pool
2. **ip nat inside source list 1 interface fastethernet0/0 overload** : PAT avec interface

6.3.5 Lab 15: ACL (Access Control Lists) avancées

Objectif : Contrôler le trafic réseau avec des règles de filtrage.

ACL Standard (1-99) :

1. **access-list 10 deny 192.168.1.10** : Bloquer une adresse spécifique
2. **access-list 10 permit 192.168.1.0 0.0.0.255** : Autoriser un réseau
3. **ip access-group 10 in** : Appliquer en entrée d'interface

ACL Étendues (100-199) :

1. **access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 80** : Bloquer HTTP
2. **access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 443** : Autoriser HTTPS
3. **access-list 100 deny icmp any any** : Bloquer ping
4. **access-list 100 permit ip any any** : Autoriser le reste

ACL Nommées :

1. **ip access-list extended BLOCK_P2P** : Créer ACL nommée
2. **deny tcp any any eq 6881** : Bloquer BitTorrent
3. **permit ip any any** : Autoriser le reste

6.3.6 Lab 16: Redondance avec HSRP (Hot Standby Router Protocol)

Objectif : Assurer la haute disponibilité des passerelles.
Configuration HSRP :

1. **interface fastethernet0/0** : Interface LAN
2. **ip address 192.168.1.2 255.255.255.0** : IP réelle du routeur
3. **standby 1 ip 192.168.1.1** : IP virtuelle HSRP (passerelle des clients)
4. **standby 1 priority 110** : Priorité (plus élevée = préféré)
5. **standby 1 preempt** : Reprendre le rôle actif si possible
6. **standby 1 authentication md5 key-string cisco** : Authentification

Tests :

- Configurer les PC avec l'IP virtuelle comme passerelle
- Arrêter le routeur actif et observer le basculement
- Vérifier avec **show standby brief**

6.4 Labs Sans Fil (Wi-Fi)

6.4.1 Lab 17: Configuration Wi-Fi basique

Objectif : Configurer un point d'accès Wi-Fi sécurisé.
Configuration Point d'Accès :

1. Configurer le SSID et la sécurité WPA2
2. Définir les canaux radio (éviter les interférences)
3. Configurer les VLANs pour segmenter le trafic Wi-Fi
4. Tester la connectivité des clients sans fil

6.4.2 Lab 18: Wi-Fi entreprise avec VLANs

Objectif : Segmenter les réseaux Wi-Fi par département.
Scenario :

- SSID "CORP_IT" $\rightarrow$ VLAN 10
- SSID "CORP_GUEST" $\rightarrow$ VLAN 99 (isolé)
- Configuration des clés WPA2 différentes
- Tests d'isolation entre réseaux

6.5 Labs Avancés Niveau Master (GNS3 Recommandé)

6.5.1 Perspectives pour les étudiants de 5ème année

Note : Ces labs nécessitent GNS3 avec des images IOS réelles ou des émulateurs avancés. Ils préparent aux certifications professionnelles CCNA/CCNP.

6.5.2 Lab 19: BGP (Border Gateway Protocol) - Niveau Master

Objectif : Configurer le routage entre systèmes autonomes.
Prérequis : Compréhension avancée du routage, GNS3 avec IOS réel.
Configuration BGP basique :

1. **router bgp 65001** : Système autonome local
2. **neighbor 203.0.113.2 remote-as 65002** : Voisin BGP externe
3. **network 192.168.1.0 mask 255.255.255.0** : Annoncer un réseau
4. **bgp router-id 1.1.1.1** : ID du routeur BGP

6.5.3 Lab 20: MPLS et VRF - Niveau Master

Objectif : Segmentation avancée avec MPLS VPN.
Note : Très avancé, nécessite des connaissances approfondies des FAI.

6.5.4 Lab 21: IPv6 Routing - Niveau Master

Objectif : Migration et coexistence IPv4/IPv6.
Configuration IPv6 :

1. **ipv6 unicast-routing** : Activer le routage IPv6
2. **interface fastethernet0/0**
3. **ipv6 address 2001:db8:1::1/64** : Adresse IPv6
4. **ipv6 enable** : Activer IPv6 sur l'interface

6.5.5 Lab 22: Firewall ASA - Niveau Master

Objectif : Configuration d'un firewall Cisco ASA.
Prérequis : Image ASA dans GNS3, concepts de sécurité avancés.

Lab 23: QoS (Quality of Service) - Niveau Master

Objectif : Prioriser le trafic réseau.
Configuration QoS basique :

1. Classification du trafic (voice, data, video)
2. Mise en queue et scheduling
3. Limitation de bande passante
4. Tests avec générateurs de trafic

6.5.6 Lab 24: Network Automation - Niveau Master

Objectif : Introduction à l'automatisation réseau.
Technologies :

- Python pour la gestion réseau
- NETCONF/RESTCONF APIs
- Ansible pour l'automatisation
- Git pour la gestion de configurations

6.6 Labs de Dépannage et Méthodologie

6.6.1 Lab 25: Méthodologie de dépannage réseau

Objectif : Développer une approche systématique pour résoudre les pannes.
Méthodologie OSI :

1. **Couche 1 (Physique)** : Vérifier les câbles, LEDs, alimentation
2. **Couche 2 (Liaison)** : MAC addresses, STP, VLANs
3. **Couche 3 (Réseau)** : Routage, ARP, ping
4. **Couche 4+ (Transport et plus)** : Ports, services, applications

Outils de diagnostic :

1. **ping** : Test basique de connectivité
2. **traceroute** : Tracer le chemin des paquets
3. **show arp** : Table ARP
4. **show mac address-table** : Table des adresses MAC
5. **show cdp neighbors** : Découverte des voisins
6. **show interfaces** : État détaillé des interfaces
7. **debug** : Débogage en temps réel (avec précaution)

6.6.2 Lab 26: Scénarios de pannes courantes

Objectif : Diagnostiquer et résoudre des pannes typiques.
Scénarios pratiques :

1. **Panne de connectivité totale** : Problème physique ou de configuration IP
2. **Connectivité partielle** : Problèmes de routage ou ACL
3. **Performance dégradée** : Duplex mismatch, congestion, STP non optimisé
4. **Problèmes VLAN** : Mauvaise assignation, trunk mal configuré
5. **Problèmes DHCP** : Serveur inaccessible, pool épuisé
6. **Problèmes de sécurité** : Port security, ACL trop restrictives

Chapter 7

Implémentation Physique

7.1 Labs avec VMware

Environnement Virtuel

Ce chapitre explique comment implémenter les labs dans des environnements virtuels avec VMware.

Installation de VMware Guide d'installation de VMware Workstation ou VMware Player pour créer des réseaux virtuels complexes.

Création de Machines Virtuelles

- VMs Linux pour serveurs (DHCP, DNS, Web)
- VMs Windows pour clients
- Intégration avec Packet Tracer et GNS3

Configuration Réseau dans VMware

- Réseaux NAT, Bridge, Host-Only
- VLANs virtuels
- Simulation de WANs avec latence

7.2 Environnement Physique

7.2.1 Matériel Requis pour un Lab Physique

Configuration minimale :

- 2-3 Switches Cisco 2960 ou similaires
- 1-2 Routeurs Cisco 1841/2811 ou ISR 4000
- Câbles Ethernet (droits, croisés, console)
- Ordinateurs portables avec adaptateurs série/USB

Configuration avancée :

- Points d'accès Wi-Fi
- Serveurs physiques (Linux/Windows Server)
- Équipements de mesure (analyseurs de protocole)
- Onduleurs et racks 19"

Guide d'achat des équipements

Équipements d'occasion recommandés :

- Cisco 2960 Series (switches) : 200-400€
- Cisco 1841/2811 (routeurs) : 150-300€
- Câbles console : 20-30€
- Licences logicielles éducatives

Alternatives open-source :

- Routeurs/switches Linux (OpenWrt, pfSense)
- Raspberry Pi comme routeurs
- Switch managés TP-Link/Netgear pour débuter

7.3 Certification et Perspectives Professionnelles

7.3.1 Préparation aux Certifications

CCNA (Cisco Certified Network Associate)

Domaines couverts par ce livre :

- Network Fundamentals (20%)
- Network Access (20%)
- IP Connectivity (25%)
- IP Services (10%)
- Security Fundamentals (15%)
- Automation and Programmability (10%)

Labs spécifiques CCNA

Les labs 1-18 de ce livre couvrent environ 80% des compétences pratiques requises pour le CCNA.

Certifications avancées (Niveau Master)

- **CCNP Enterprise** : Labs 19-24 constituent une introduction
- **CCNP Security** : Focus sur ASA, VPN, sécurité avancée
- **CCIE** : Niveau expert, nécessite des années d'expérience

7.3.2 Évolution Technologique

Tendances actuelles

- **SDN (Software Defined Networking)** : Programmabilité des réseaux
- **Cloud Networking** : AWS, Azure, Google Cloud
- **DevOps et NetOps** : Automatisation et Infrastructure as Code
- **IoT et Edge Computing** : Nouveaux défis de connectivité
- **5G et Wi-Fi 6** : Technologies sans fil de nouvelle génération

Compétences futures

- Python et APIs pour l'automatisation
- Containerisation (Docker, Kubernetes)
- Cloud providers et services réseau
- Sécurité zero-trust
- Analytics et Machine Learning appliqués aux réseaux

Chapter 8

Annexes

8.1 Tableau récapitulatif des labs par niveau

Lab	Niveau	Outil	Compétences
Lab 1-5	L2	Packet Tracer	Bases réseau, VLANs
Lab 6-10	L2-L3	Packet Tracer	STP, Sécurité, Services
Lab 11-18	L3	Packet Tracer	Routage, Wi-Fi, HSRP
Lab 19-24	Master	GNS3	BGP, MPLS, IPv6, QoS
Lab 25-26	Tous	Les deux	Dépannage, Méthodologie

Table 8.1: Répartition des labs par niveau et outil

8.2 Correspondance avec les certifications

Certification	Labs recommandés	Niveau requis
CCNA	Labs 1-18 + dépannage	L3 + expérience
CCNP Enterprise	Labs 11-24	Master + 2 ans exp.
CCNP Security	Labs sécurité + ASA	Master + spécialisation

Table 8.2: Correspondance labs-certifications

Conclusion

8.3 Résumé des compétences acquises

À l'issue de ce livre pratique, vous maîtriserez :

- Les fondamentaux des réseaux Ethernet et IP
- La configuration des switches (VLANs, STP, sécurité)
- Le routage statique et dynamique (RIP, OSPF, EIGRP)
- Les services réseau (DHCP, NAT, ACL)
- La redondance et la haute disponibilité (HSRP, EtherChannel)

- Les réseaux sans fil (Wi-Fi, sécurité)
- Le dépannage méthodique des pannes réseau
- Les bases pour les certifications Cisco CCNA/CCNP

8.4 Perspectives et formation continue

Le domaine des réseaux informatiques évolue rapidement. Il est essentiel de :

- Pratiquer régulièrement avec de nouveaux scénarios
- Suivre les évolutions technologiques (SDN, cloud, IoT)
- Obtenir des certifications reconnues
- Participer à des communautés techniques
- Expérimenter avec des équipements réels

Conseil final : La théorie est importante, mais seule la pratique intensive vous donnera la confiance et l'expertise nécessaires pour devenir un expert en réseaux. Continuez à expérimenter !

8.5 Glossaire

ACL : Access Control List - Liste de contrôle d'accès pour filtrer le trafic
BGP : Border Gateway Protocol - Protocole de routage entre systèmes autonomes
DHCP : Dynamic Host Configuration Protocol - Attribution automatique