Réseaux dans Packet Tracer
Méthode Générale de Configuration

Grégoire Roumache

Décembre 2020

Partie I
Méthode et Préparation

1 Méthode

1. **Préparation**:
   (a) calculer le nombre d'ip nécessaire par sous-réseau
   (b) calculer les netmasks, les ip des sous-réseaux, et les ip de tous les appareils
   (c) calculer les wildcards, et les synthèses de routes
2. **Couche physique**:
   (a) placer toutes les machines, ajouter des cartes réseaux si nécessaire
   (b) câbler les machines
3. **Configuration de base**:
   (a) initialiser les machines
   (b) donner un hostname, etc.
4. **Couche liaison de données**:
   (a) configurer cdp
   (b) configurer la sécurité des ports switchs
   (c) configurer les vlans
5. **Configuration réseau de base**:
   (a) configurer les interfaces
   (b) créer les routes statiques/par défaut
6. **Configuration réseau avancée**:
   (a) activer le routage des switchs L3
   (b) activer le routage rip
   (c) activer le routage ripng
   (d) activer le routage ospf
   (e) créer les acl et les activer sur les interfaces
7. **Couche application**:

(a) configurer le dhcp serveur/relai
(b) enregistrer une config sur un serveur ftp/tftp
(c) configurer ssh, telnet
(d) configurer la sécurité des machines (longueur min de mot de passe, durée de session, etc.)

8. **Récupération**: récupérer la config/le mot de passe.
9. **Déboguer**.

2 Calcul des VLSM

- **Explication VLSM**: si on ajoute 1 à la dernière adresse du sous-réseau, on obtient la première adresse du sous-réseau suivant. Exemple:

première adresse S.R.4	`172.121.0000 1111.0000 0000`
dernière adresse S.R.4	`172.121.0000 1111.1111 1111`
première adresse S.R.5	`172.121.0001 0000.0000 0000`

- Pour chaque sous-réseau:
  1. Calculer le nombre de bits nécessaire pour le sous-réseau.
  2. Calculer le netmask correspondant.
  3. Calculer la première adresse à l'aide de la dernière adresse du sous-réseau précédent.
  4. Calculer la dernière adresse du sous-réseau.
- Exemple: Voici un réseau à découper en 4 sous-réseaux:

`193.115.111.0  255.255.255.0`

SR0 = 32 | SR1 = 16 | SR2 = 128 | SR3 = 64 IP

1. Pour diviser un réseau en sous-réseaux de tailles différentes, il faut aller du plus grand au plus petit (dans l'ordre: sous-réseaux 2, 3, 0, 1).
2. Il faut $\log_2 128 = 7$ bits pour encoder le **sous-réseau 2**.
3. **Sous-réseau 2**:

masque	`255.255.255.1000 0000`
première adr.	`193.115.111.0000 0000`
dernière adr.	`193.115.111.0111 1111`

4. Il faut $\log_2 64 = 6$ bits pour encoder le **sous-réseau 3**.
5. **Sous-réseau 3**:

masque	`255.255.255.1100 0000`
première adr.	`193.115.111.1000 0000`
dernière adr.	`193.115.111.1011 1111`

6. Il faut $\log_2 32 = 5$ bits pour encoder le **sous-réseau 0**.
7. **Sous-réseau 0**:

masque	`255.255.255.1110 0000`
première adr.	`193.115.111.1100 0000`
dernière adr.	`193.115.111.1101 1111`

8. Il faut $\log_2 16 = 4$ bits pour encoder le **sous-réseau 1**.
9. **Sous-réseau 1**:

masque	255.255.255.1111 0000
première adr.	193.115.111.1110 0000
dernière adr.	193.115.111.1110 1111

3 Calcul des synthèses de routes

- **Explication synthèse de routes**: calcul de l'adresse pour créer une route vers plusieurs réseaux (≈ route par défaut) ne passant que par un routeur.
- Calcul d'une route de synthèse:
  1. Lister les réseaux en binaire.
  2. Compter le nombre de bits similaires à gauche pour déterminer le masque.
  3. Calculer l'adresse réseau.
- Exemple: Voici 4 réseaux, calculer la route de synthèse:

172.20.0.0 | 172.21.0.0 | 172.22.0.0 | 172.23.0.0

1. Liste des réseaux en binaire:

172.0001 0100.0.0
172.0001 0101.0.0
172.0001 0110.0.0
172.0001 0111.0.0

2. Nombre de bits similaires à gauche: 14 $\implies$ masque = 255.252.0.0.
3. Adresse réseau = 172.20.0.0.

4 Calcul des wildcards

- Exemple (1): calculer la wildcard pour les réseaux suivants:

192.168.0.0/24 | 192.168.1.0/24 | 192.168.2.0/24 | 192.168.3.0/24

réseau 1	192	168	0000 0000	0
réseau 2	192	168	0000 0001	0
réseau 3	192	168	0000 0010	0
netmask	255	255	1111 1111	0
wildcard	0	0	0000 0011	255

- Exemple (2): calculer les adresses min & max que l'ACL suivante bloque:

```
access-list  <num_liste>  deny    <ip>     <wildcard>
access-list       23      deny  35.8.2.3   3.7.15.31
```

réseau	0010 0011	0000 1000	0000 0010	0000 0011
wildcard	0000 0011	0000 0111	0000 1111	0001 1111
ip min	0010 0000	0000 1000	0000 0000	0000 0000
ip max	0010 0011	0000 1111	0000 1111	0001 1111

– ip min: 32.8.0.0

- ip max: 35.15.15.31

Partie II
Couche Physique

5 Packet Tracer

5.1 Matériel

- routeur = cisco 1941
- switch = cisco 2960

5.2 Configurer un PC

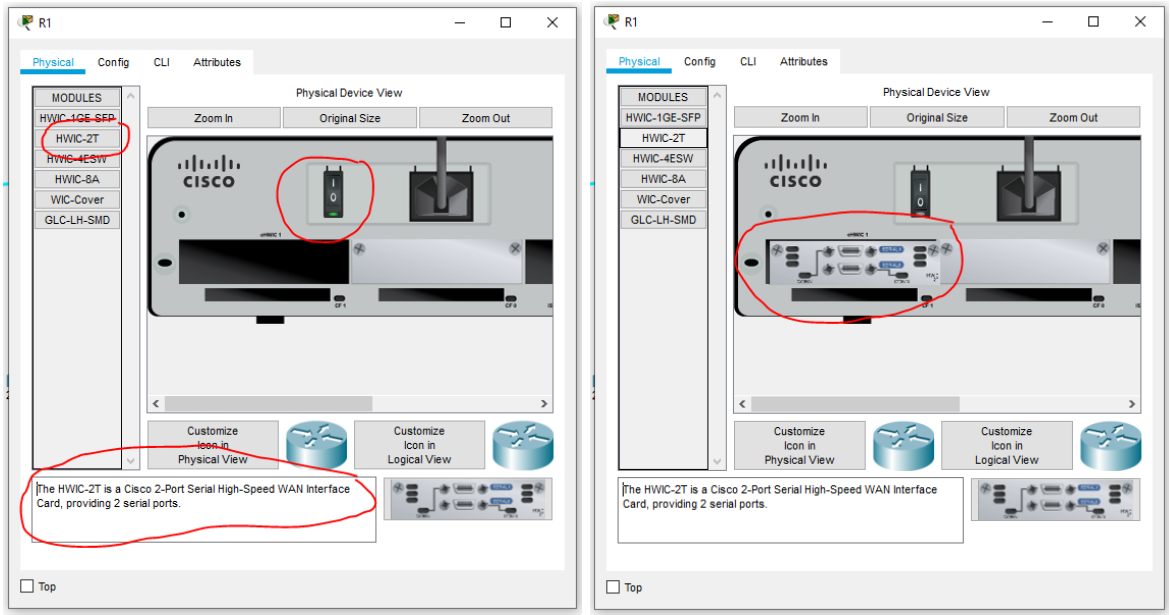
1. Cliquer sur le PC, puis cliquer sur l'onglet *Desktop* en haut de la fenêtre.
2. Cliquer sur *IP Configuration* qui est la première option en haut à gauche.

5.3 Désactiver le pare-feu d'un PC

1. Cliquer sur le PC, puis cliquer sur l'onglet *Desktop* en haut de la fenêtre.
2. Cliquer sur *Firewall* qui est en bas à droite.
3. Cliquer sur *Off* en haut à droite pour le désactiver.

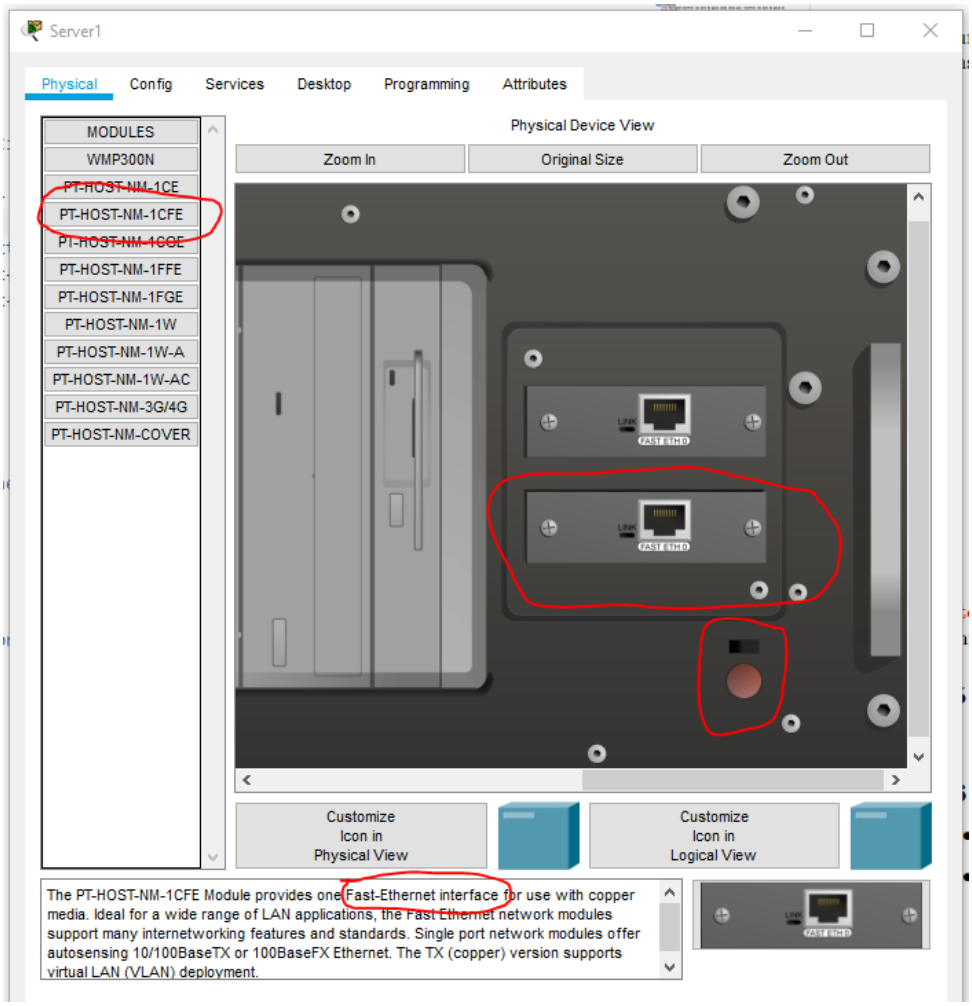
5.4 Ajouter une carte réseau au routeur pour les connexions série

Pour que les routeurs puissent communiquer entre eux, il faut ajouter des cartes réseau qui servent aux connexions séries:



Attention. Si on met la carte réseau à gauche, on aura `s0/1/0` et `s0/1/1`. Pour avoir les interfaces exactement comme dans l'énoncé, il faut placer la carte réseau à *droite*.

5.5 Ajouter une carte réseau à un serveur



Avant d'ajouter la nouvelle interface fastethernet, il faut appuyer sur le bouton rouge pour couper le courant.

5.6 Ports PC à utiliser

- Pour configurer les appareils cisco, il faut utiliser le câble console (cyan) en le connectant au port `RS232`.
- Pour se connecter au switch, on utilise le port `FastEthernet0` et le câble Copper Straight-Through (noir).

Partie III
Configuration de Base

6 Configuration de base

6.1 Initialisation (à faire à chaque configuration)

- `enable`
- `configure terminal`
- `no ip domain-lookup`
- `hostname <nom>`

- `banner motd %<messages>%`

6.2 Configurer la console en mode synchrone

- `line console 0`
- `logging synchronous`
- `exit`

6.3 Enregistrer la configuration

2 possibilités:

- `copy running-config startup-config`
- `write`

Partie IV
Couche liaison de données

7 Tester la couche 2 avec CDP

- `cdp run`
- `show cdp`
- `show cdp neighbors`
- `show cdp neighbors detail`

8 Configuration VLAN

8.1 Étapes configuration VLAN sur un switch

1. Désactiver DTP (dynamic transfer protocol) et mettre les interfaces en mode access:
   - `interface range f0/1-24`
   - `switchport mode access`
   - `switchport nonegotiate`
2. Créer les vlans:
   - `vlan <num>`
   - `name <nom>`
3. Configurer les interfaces en fonction des vlans:
   - `interface <interface>`
   - `switchport access vlan <num>`
4. Configurer des interfaces en trunk:
   - `interface <interface>`
   - `switchport mode trunk`

8.2 Étapes configuration VLAN sur un routeur

Attention ! Ne pas créer les vlans sur le routeur !

1. Activer l'interface:
   - `interface <interface>`
   - `no shutdown`
2. Configurer les sous-interfaces:
   - `interface <interface>.<num_vlan>`
   - `encapsulation dot1q <num_vlan>`
   - `ip address <réseau> <masque>`

8.3 Changer le vlan natif

- `switchport trunk native vlan <vlan_id>`

Explications: https://community.cisco.com/t5/switching/changing-the-native-vlan-command/td-p/1394020

8.4 Supprimer un vlan

- `no vlan <num_vlan>` (dans le mode de création de vlans)
- `no interface vlan <num_vlan>` (dans le mode de configuration)

Remarque: il faut faire les 2.

8.5 Supprimer une sous-interface vlan

- `no interface <interface>.<num_vlan>`

8.6 Vérifier la configuration des vlans

- `show vlan`
- `show vlan brief`
- `show interface trunk`
- `show interface switchport`

9 Sécurité des ports switchs

9.1 Désactiver les ports non-utilisés

- `interface range f0/<début>-<fin>`
- `shutdown`

9.2 Configuration port-security

Pour activer port-security sur un port, il faut utiliser la 1ère commande, elle ne fonctionne que si le port est en mode access (pas trunk).

- `switchport port-security`
- `switchport port-security maximum <nb>`
- `switchport port-security mac-address [sticky]`

Configuration port-security:

configuration	commande
statique	`switchport port-security mac-address <mac_address>`
dynamique	`switchport port-security mac-address sticky`
les 2	`switchport port-security mac-address sticky <mac_address>`

9.3 Configuration mode de violation

- `switchport port-security violation protect | restrict | shutdown`

Mode de violation:

	bloque le traffic	message syslog	++ compteur de violation	port shutdown
protect	**oui**	**non**	**non**	**non**
restrict	**oui**	**oui**	**oui**	**non**
shutdown	**oui**	**oui**	**oui**	**oui**

9.4 Vérifier la configuration de sécurité des ports switchs

- `show interfaces switchport`
- `show port-security`
- `show port-security address`
- `show port-security interface <interface>`

Partie V
Configuration réseau de base

10 Configuration réseau de base

10.1 Configurer une interface réseau

Pour un **switch**, on utilise l'interface `vlan1` (ou le vlan de management).

- `interface <interface>`
- `ip address <ip> <netmask>`
- `ipv6 address <ip>/<netmask> [eui-64]`
- `clock rate <clock_rate>`

- `no shutdown`
- `description <description_interface>`
- `exit`

Réinitialiser une interface:

- `default interface <interface>`

10.2 Ajouter une default gateway

- `ip default-gateway <gateway>`

Attention ! Pour l'ipv6, il faut créer une route statique par défaut.

10.3 Adresses IPv6

```
R-Bastogne#show ipv6 interface brief
GigabitEthernet0/0          [up/up]
    unassigned
GigabitEthernet0/0.30       [up/up]
  1 FE80::20A:41FF:FE26:2B01
  2 2000:FA1:10:1E::FFFF
GigabitEthernet0/1          [administratively down/down]
    unassigned
Serial0/0/0                 [up/up]
  1 FE80::20A:41FF:FE26:2B01
  2 2000:FA1:99:63::2
Serial0/0/1                 [administratively down/down]
    unassigned
Vlan1                       [administratively down/down]
    unassigned
```

(1)	`FE80::/10`	link-local	auto-configurée/obligatoire/réseau local
(2)	`2000::/3`	global unicast	adresse publique

- `ipv6 address <ip> link-local`
- `ipv6 address <ip>/<netmask>`
- `ipv6 address <réseau>/<netmask> eui-64`

10.4 Tester la connexion réseau

On peut utiliser ces commandes avec l'ipv4 et l'ipv6.

- Commun à tous les appareils:
  - `ping <ip>`
- Uniquement sur les appareils cisco:
  - `traceroute <ip>`
- Uniquement sur les pc:
  - `tracert <ip>`

11 Routes statiques

11.1 Configurer une route statique

- Route **récursive**:
  - `ip route <ip_réseau_à_atteindre> <netmask> <ip_routeur>`
  - `ipv6 route <réseau>/<netmask> <ip_routeur>`
- Route **récursive par défaut**:
  - `ip route 0.0.0.0 0.0.0.0 <ip_routeur>`
  - `ipv6 route ::/0 <ip_routeur>`
- Route **directement connectée**:
  - `ip route <ip_réseau_à_atteindre> <netmask> <interface_routeur>`
  - `ipv6 route <réseau>/<netmask> <interface_routeur>`
- Route **directement connectée par défaut**:
  - `ip route 0.0.0.0 0.0.0.0 <interface_routeur>`
  - `ipv6 route ::/0 <interface_routeur>`

11.2 Ajouter une route de backup

- `ip route <réseau> <netmask> <interface/ip_routeur> <distance_admin>`

type de route	distance
interface connectée	0
route statique	1
rip	120
inconnu	255

Plus la distance administrative est *faible*, plus la route est privilégiée.

11.3 Tester le routage (examiner l'état du réseau)

Sur les routeurs:

- `show ip interface brief`
- `show ip protocols`
- `show ip route [summary]`
- `debug ip protocol` (annuler avec: `no debug ip protocol`)

IPv6:

- `show ipv6 rip`
- `show ipv6 route [summary]`
- `show ipv6 protocols`
- `show ipv6 interface brief`

Partie VI
Configuration réseau avancée

12 Activer le routage sur un switch L3

- `ip routing`

13 Configuration RIP

13.1 Étapes de configuration RIP

1. Initialisation:
   - `router rip`
   - `version 2`
   - `no auto-summary`
2. Ajouter des routes connectées, et empêcher l'envoi d'informations de routage sur certaines interfaces:
   - `network <ip_réseau_connecté>`
   - `passive-interface <interface>`
3. Propager les routes:
   - `redistribute connected`
   - `redistribute static`
   - `default information-originate`

13.2 Vérifier le bon fonctionnement du RIP

- `debug ip rip`
- `show ip rip neighbors`
- `show ip rip database`

14 Configuration RIPng (RIP IPv6)

14.1 Étapes de configuration RIPng (RIP IPv6)

1. Initialisation:
   - `ipv6 unicast-routing`
2. Activation sur certaines interfaces:
   - `interface <interface>`
   - `ipv6 rip <name> enable`
3. Propagation des routes:
   - `ipv6 router rip <name>`
   - `redistribute static`
   - `redistribute connected`
   - `ipv6 rip <name> default-information originate`

Remarque: le paramètre `<name>` qui revient dans toutes les commandes est le nom du process et doit être le même sur tous les routeurs/interfaces.

14.2 Vérifier le bon fonctionnement du RIPng

- `debug ipv6 rip`
- `show ip protocols`
- `show ipv6 rip`
- `show ipv6 route`
- `show ipv6 route rip`
- `show ipv6 rip [name][database]`

15 Configuration OSPF

15.1 Étapes de configuration OSPF

1. Initialisation:
   - `router ospf <process-id>`
   - `router-id <router-id>`
   - `auto-cost reference-bandwidth <bandwidth>`
2. Ajouter des routes connectées, et empêcher l'envoi d'informations de routage sur certaines interfaces:
   - `network <réseau> <wildcard> area <zone-id>`
   - `passive-interface <interface>`
3. Propagation des routes:
   - `redistribute connected`
   - `redistribute static`
   - `default-information originate`

Choisir la bande passante (bandwidth):

- gigabit ethernet: `auto-cost reference-bandwidth 1000`
- 10 gigabit ethernet: `auto-cost reference-bandwidth 10000`
- revenir au défaut: `auto-cost reference-bandwidth 100`

15.2 Modifier la priorité OSPF

- `ip ospf priority <priorité>`

Remarques:

- DR = designated router
- BDR = backup designated router
- Priorité par défaut = 1
- Priorité max = 255, élection automatique à DR
- Priorité min = 0, impossible d'être élu en DR
- À priorité égale, c'est le routeur qui a le `<router-id>` le plus élevé qui est élu.

15.3 Vérifier le bon fonctionnement du OSPF

- `show ip protocols`
- `show ip ospf neighbor`
- `show ip ospf`
- `show ip ospf interface`

16 Configuration des ACL (= access control list)

16.1 Ajouter des ACL (= access control list) pour restreindre le routage

Commande pour créer une ACL (= access control list):

- `access-list <num_liste> {deny | permit} <ip> <wildcard>`
- `access-list <num_liste> {deny | permit} any`
- `access-list <num_liste> {deny | permit} host <ip>`

- `num_list` $\in [1, 99] \implies$ acl standard, contrôle l'ip source
- `num_list` $\in [100, 199] \implies$ acl étendue, contrôle l'ip source/destination, ou le port, ou le service

Sur une interface vlan ou ethernet (ou sur une interface physique directement pour un routeur):

- `ip access-group <num_access_list> {in | out}`

- `in` = inbound packets = paquets entrants
- `out` = outbound packets = paquets sortants

Remarque: pour un switch, il faut ajouter l'acl sur un vlan puis ajouter l'interface fastethernet au vlan.

16.2 Configurer une ACL nommée

Configurer l'acl et ses règles:

- `ip access-list {standard | extended} {<num_liste> | <nom_liste>}`
- `[<num_règle>] {deny | permit} <ip> <wildcard>`
- `[<num_règle>] {deny | permit} any`
- `[<num_règle>] {deny | permit} host <ip>`

Supprimer l'acl ou des règles:

- `no <num_règle>`
- `no {deny | permit} ...`
- `no ip access-list {standard | extended} {<num_liste> | <nom_liste>}`

Pour ajouter l'acl à l'interface:

- `ip access-group {<num_liste> | <nom_liste>} {in | out}`

16.3 Étapes de configuration une ACL IPv6

1. Créer l'acl nommée:
   - `ipv6 access-list <nom_acl>`
2. Créer des règles:
   - `{permit | deny} ipv6 <source> <destination>`
   - avec la source/destination = `{any | host <ip> | <ip>/<netmask>}`
3. Ajouter les acl sur les interfaces:
   - `ipv6 traffic-list <nom_acl> {in | out}`

16.4 Règles ACL IPv6 pour bloquer les requêtes HTTP/HTTPS

- `deny tcp <source> <destination> eq <port>`
- `deny tcp <source> <destination> eq www`
- `deny tcp <source> <destination> eq 443`

16.5 Supprimer/modifier une ACL (= access control list)

Supprimer une ACL:

- `no access-list <num_acl>`

Supprimer une partie de l'ACL:

- `ip access-list {standard | extended} <num_acl>`
- `no <num_règle>`

16.6 Vérifier la liste des ACL

- `show access-list`

Partie VII
Couche application

17 Sécurité des machines

17.1 Mots de passe

- Encrypter/chiffrer les mots de passe (même chose que: "chiffrer les mots de passe en texte clair"):
  - `service password-encryption`
- Exiger une longueur minimale de mot de passe:
  - `security passwords min-length 10`
- Attribuer un mot de passe chiffré EXEC privilégié:
  - `enable secret <mdp>`
- Attribuer un mot de passe à la console et activer la connexion:
  - `line console 0`

  - `password <mdp>`
  - `login`

- Attribuer un mot de passe VTY et activer la connexion (**routeur**):
  - `line vty 0 4`
  - `password <mdp>`
  - `login local`
- Attribuer un mot de passe VTY et activer la connexion (**switch**):
  - `line vty 0 15`
  - `password <mdp>`
  - `login local`

17.2 Déconnexion après 5 min d'inactivité

- `line console 0`
- `exec-timeout 5 0`
- `line vty 0 4`
- `exec-timeout 5 0`
- `exit`

17.3 Bloquer l'identification pendant 30 s après 2 échecs en 2 min

- `login block-for 30 attempts 2 within 120`

18 SSH/Telnet

18.1 Activer la connexion telnet

- `line vty 0 15`
- `transport input telnet`
- `password <password>`
- `login`

18.2 Activer la connexion ssh

1. Ajouter un nom de domaine, et créer un utilisateur pour la connexion ssh:
   - `ip domain-name <greg.com>`
   - `username <usename> privilege 1 secret <mdp>`
2. Configurer l'entrée des lignes VTY pour autoriser les connexions SSH:
   - `line vty 0 4`
3. Autoriser uniquement ssh (refuse telnet):
   - `transport input ssh`
4. La connexion doit se faire sur un compte local:
   - `login local`

- `exit`

5. Générer une clé rsa:
   - `crypto key generate rsa [general-keys modulus <nb_bits>]`

19 FTP/TFTP

19.1 Copier la configuration vers un serveur FTP

- `ip ftp username <username>`
- `ip ftp password <password>`
- `copy running-config ftp:` (autre configuration possible: `startup-config`)

19.2 Récupérer la configuration sur un serveur FTP

- `ip ftp username <username>`
- `ip ftp password <password>`
- `copy ftp: running-config`

19.3 Copier/Récupérer la configuration vers/sur un serveur TFTP

- `copy running-config tftp:`
- `copy tftp: running-config`

19.4 Vérifier la configuration

- `show running-config`

20 Configuration DHCP

20.1 Configuration d'un relai dhcp

Attention ! Il faut absolument que le serveur et les machines soient connectées à des interfaces fastethernet.

- `service dhcp`
- `ip helper-address <ip_serveur_dhcp>` (sur une interface, pas obligatoire)

Remarques:

- ça peut prendre du temps pour que la configuration d'une machine se termine (`alt+d` avance de 30 sec)
- la machine cliente doit absolument être dans le bon vlan
- le relai dhcp est nécessaire quand le serveur dhcp n'est pas dans le même vlan que les machines

20.2 Configuration d'un service dhcp

- `service dhcp`
- `ip dhcp pool <nom_pool>`
- `network <réseau> <masque>`
- `dns-server <adresse>`
- `default-router <adresse>`
- `ip dhcp excluded-address <1ère_ip> [<fin_range_ip>]`

Remarques:

- on peut créer un pool par vlan en donnant le nom du vlan au pool (ex: nom vlan = nom pool = *vlan10*)
- si on veut créer un pool global, il suffit de ne pas lui donner un nom de vlan (ex: nom pool = *globalpool*)
- il faut *absolument* configurer une ip sur les interfaces du routeurs (+ les vlans) avant que le dhcp fonctionne
- pas besoin d'exclure l'adresse ip du serveur dhcp, le service dhcp le fait automatiquement

Attention ! Les adresses àpd 224.0.0.0 sont *réservées* et ne doivent pas être utilisées. C'est possible de créer un pool avec ces adresses mais pas de les utiliser pour configurer une interface $\implies$ dhcp impossible.

20.3 Vérifier la configuration dhcp

- `show ip dhcp pool`
- `show ip dhcp pool <nom_pool>`
- `show ip dhcp binding`
- `show ip dhcp conflict`
- `show ip dhcp relay information trusted-sources`

Partie VIII
Récupération

21 Récupération de config/mot de passe

21.1 Récupération de config/mots de passe sur un routeur (avec rommon)

1. Rallumer la machine ou utiliser: `reload`.
2. Pendant la décompression de l'image de l'IOS (avec plein de ###):
   - Au labo: `ctrl+break`
   - Sur Packet Tracer: `ctrl+c` (sinon, essayer: `ctrl+maj+f6+c`)
3. `confreg 0x2142`
4. `reset`
5. `enable`
6. `copy startup-config running-config`
7. Redéfinir les mots de passe.

8. `write memory`, ou: `copy running-config startup-config`

Remarques:

- registre = 2142 $\Longrightarrow$ démarrer sans la *startup-config*
- registre = 2102 $\Longrightarrow$ démarrer avec la *startup-config*
- registre = 2100 $\Longrightarrow$ démarrer en mode rommon

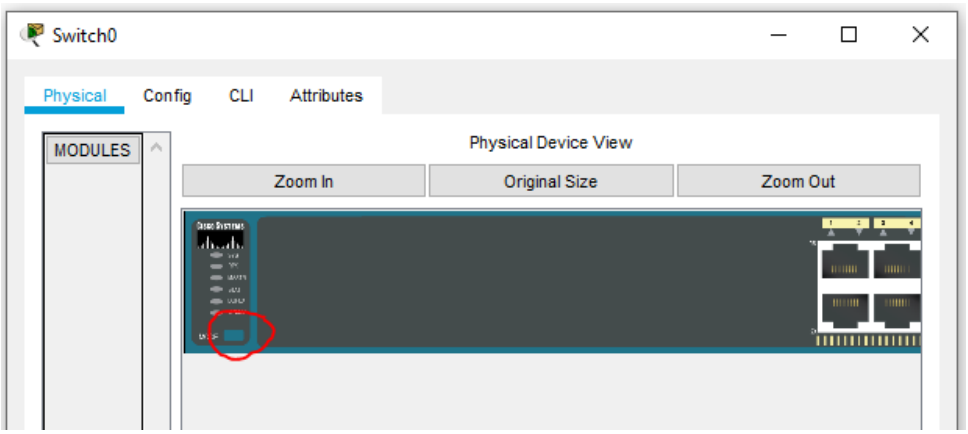
21.2 Récupération de config/mots de passe sur un routeur (PAS rommon)

Uniquement si on est déjà connecté:

- `enable`
- `configure terminal`
- `config-register 2142`
- `do reload`
- `enable`
- `copy startup-config running-config`
- Redéfinir les mots de passe.
- `write memory`, ou: `copy running-config startup-config`

21.3 Récupération de config/mots de passe sur un switch (recovery mode)

1. Se connecter au port console avec un débit de: 9600.
2. Rallumer la machine ou utiliser: `reload`.
3. Appuyer sur le bouton *mode* pendant 3 secondes.

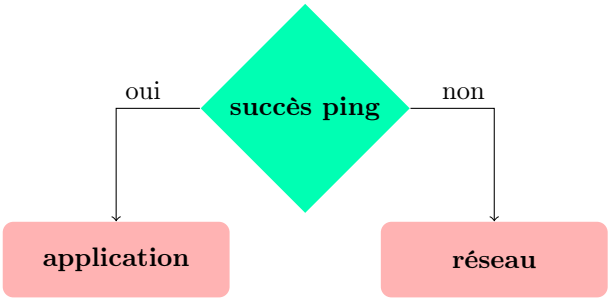


4. `flash_init`
5. `load_helper` (pas sur Packet Tracer)
6. `dir flash:`
7. `rename flash:config.text flash:<name>`
8. `reset`

9. `enable`
10. `copy flash running-config` (on demande de rentrer le nom du fichier après)
11. Changer les mots de passe, puis enregistrer la nouvelle configuration.

Partie IX
Déboguer la config réseau

22 Déterminer l'origine du problème – Approche intermédiaire



En cas de problème à la fin de la manip:

1. Entrer en mode simulation dans Packet Tracer, et essayer de ping entre les machines (**couche 3**).
2. Si le ping fonctionne, c'est que le problème vient de la couche application (dhcp, ftp, ssh, etc.).

   > Exemple – problème dhcp:
   >
   > (a) filtrer les paquets en fonction du protocole dhcp
   > (b) vérifier si le paquet a un problème au niveau du serveur ou du relai

3. Si le ping ne fonctionne pas, on vérifie la couche réseau:
   (a) vérifier la config ip des machines entre lesquelles le ping ne passe pas
   (b) vérifier la table de routage (routes statiques & protocole rip)
   (c) vérifier les acl
4. Si ça ne fonctionne toujours pas (ou si ça bloque sur un switch), on passe à la couche liaison de données:
   (a) vérifier que les vlans sont bien configurés
   (b) vérifier que la sécurité des ports switchs est configurée correctement
   (c) vérifier que la machine trouve bien ses voisins avec le protocole cdp
5. A priori, on n'a pas besoin de descendre à la couche physique mais si besoin...
   (a) vérifier que les machines sont allumées
   (b) vérifier que les bonnes interfaces sont allumées
   (c) vérifier que les câbles sont branchés aux bonnes interfaces

23 Déboguer la configuration réseau en labo – Approche bottom-up

1. **Couche physique** – Vérifier que le cablâge est correct:
   (a) regarder si les câbles sont dans les bons ports du routeur (g0/0 ou g0/1)
   (b) regarder si les câbles sont branchés dans les bons ports sur les panneaux de brassage
   (c) regarder si la couleur des câbles est la bonne (console = bleu, communication = vert)
   (d) regarder si le câble est bien branché sur le PC
   (e) regarder si le routeur est bien allumé
   (f) regarder si une led s'allume sur le routeur quand on branche le câble, **sinon**, changer le câble
2. **Couche liaison de données** – Vérifier la configuration des cartes réseaux:
   (a) dans la barre de recherche du pc, taper `ncpa.cpl`
   (b) pour identifier la carte réseau à configurer : débrancher le câble connecté au routeur
   (c) rebrancher le câble et configurer la carte réseau où il y a eu le changement
3. **Couche réseau** – Vérifier la configuration IP:
   (a) utiliser: `ipconfig`, sur les PC, et: `show ip interface brief`, sur les routeurs
   (b) utiliser: `show cdp neighbors detail`, pour afficher les ip des machines voisines
   (c) utiliser: `ping`, `traceroute [-h <max_nb_hop>]`, `tracert [-h <max_nb_hop>]`
   (d) afficher les routes sur les routeurs, reconfigurer le rip, ou ajouter des routes statiques
4. **Couche application**:
   (a) désactiver les pare-feux des pc/serveurs
   (b) vérifier que le service est bien activé
   (c) vérifier que les machines clientes sont bien configurées (pc en dhcp, ip du dns qui correspond)
   (d) reconfigurer le dns, dhcp, ftp, etc.

Partie X
Annexes

24 Problèmes de Packet Tracer

- Impossible d'utiliser: `login block-for 30 attempts 2 within 120`, sur un switch dans Packet Tracer.
- Impossible d'ajouter des adresses IP secondaires dans Packet Tracer.
- Impossible d'utiliser la commande: `load_helper`, dans Packet Tracer.
- Impossible de créer des sous-interfaces sur les interfaces fastethernet dans Packet Tracer.

25 Modes de la console cisco

routeur>	exécution utilisateur
routeur#	exécution privilégiée
routeur(config)#	configuration (privilégiée)
routeur(config-if)#	configuration d'interface
routeur(config-router)#	configuration du protocole de routage
routeur(config-rtr)#	configuration du protocole de routage ipv6
routeur(config-line)#	configuration d'une ligne de terminal
routeur(config-std-nacl)#	configuration d'une acl standard nommée
routeur(config-ext-nacl)#	configuration d'une acl étendue nommée
routeur(vlan)#	création des vlans
routeur(dhcp-config)#	configuration du service dhcp
rommon 1>	mode rommon (= rom monitor)
switch:	mode rommon (= rom monitor)
switch(config-vlan)#	configuration de vlan

26 Aides dans le terminal

- `?` = montre les commandes qui peuvent être utilisé dans le mode actuel
- `<début_commande>?` = montre les commandes qui commencent par *début_commande*
- `<commande> ?` = montre les arguments/options que prend la commande
- `<commande>` (sans arguments) = propose des arguments par défaut qui peuvent être modifiés

Remarques:

- pour certaines commandes (ex: `copy`), il n'y a pas d'argument par défaut (par contre: `copy ?`, fonctionne)
- *mais*: `copy flash ftp`, fonctionne, tout comme: `copy flash running-config`
- `copy flash flash`, ne fonctionne pas

27 Pense-bête VLSM

masque en /	masque	wildcard	nombre d'ip
/1	128.0.0.0	127.255.255.255	2 147 483 648
/2	192.0.0.0	63.255.255.255	1 073 741 824
/3	224.0.0.0	31.255.255.255	536 870 912
/4	240.0.0.0	15.255.255.255	268 435 456
/5	248.0.0.0	7.255.255.255	134 217 728
/6	252.0.0.0	3.255.255.255	67 108 864
/7	254.0.0.0	1.255.255.255	33 554 432
/8	255.0.0.0	0.255.255.255	16 777 216
/9	255.128.0.0	0.127.255.255	8 388 608
/10	255.192.0.0	0.63.255.255	4 194 304
/11	255.224.0.0	0.31.255.255	2 097 152
/12	255.240.0.0	0.15.255.255	1 048 576
/13	255.248.0.0	0.7.255.255	524 288
/14	255.252.0.0	0.3.255.255	262 144
/15	255.254.0.0	0.1.255.255	131 072
/16	255.255.0.0	0.0.255.255	65 536
/17	255.255.128.0	0.0.127.255	32 768
/18	255.255.192.0	0.0.63.255	16 384
/19	255.255.224.0	0.0.31.255	8 192
/20	255.255.240.0	0.0.15.255	4 096
/21	255.255.248.0	0.0.7.255	2 048
/22	255.255.252.0	0.0.3.255	1 024
/23	255.255.254.0	0.0.1.255	512
/24	255.255.255.0	0.0.0.255	256
/25	255.255.255.128	0.0.0.127	128
/26	255.255.255.192	0.0.0.63	64
/27	255.255.255.224	0.0.0.31	32
/28	255.255.255.240	0.0.0.15	16
/29	255.255.255.248	0.0.0.7	8
/30	255.255.255.252	0.0.0.3	4
/31	255.255.255.254	0.0.0.1	2
/32	255.255.255.255	0.0.0.0	1

Table des matières