

Nouvelle page



Mémento Cisco/Windows/Pfsense

Table des matières

[1 - Principales commandes de configuration du commutateur Cisco 2](#)

[a - commandes de RAZ de la configuration et de changement de nom 2](#)

[b - commandes de configuration des VLAN 2](#)

[c - commandes de configuration VTP \(VLAN Trunking Protocol\) 3](#)

[d - commandes de configuration STP \(Spanning Tree Protocol\) 3](#)

[e - affectation d'une adresse IP à un commutateur 3](#)

[f - commandes de configuration de la fonction routeur d'un commutateur multi-niveaux 4](#)

[g - configuration SNMP pour la supervision d'un commutateur 4](#)

[h - configuration Etherchannel 4](#)

[i - configuration IP d'un switch 5](#)

[j - sauvegarde de la configuration du switch sur un serveur TFTP \(puis restauration\) 5](#)

[k - commandes de configuration de l'accès à distance à un switch via Telnet 5](#)

[l - commandes de configuration de l'accès à distance à un switch via SSH 6](#)

[2 - Principales commandes de configuration du routeur Cisco 7](#)

[a - commandes de RAZ de la configuration et de changement de nom 7](#)

[b - commandes de configuration d'une interface 7](#)

[c - configuration SNMP pour la supervision d'un routeur 7](#)

[d - commandes de configuration de routes 8](#)

[e - commandes de configuration du routage "Router-on-a-stick" 8](#)

[f - configuration des protocoles de routage dynamique OSPF et RIP 9](#)

[g - commandes de configuration de l'accès à distance à un routeur via Telnet 10](#)

[h - commandes de configuration de l'accès à distance à un routeur via SSH 10](#)

[i - commandes de configuration de la fonction NAT dynamique 11](#)

[j - commandes de configuration de la fonction NAT statique 11](#)

[k - commandes de configuration de la fonction NAT statique - redirection de port 11](#)

[l - commandes de configuration du serveur DHCP du routeur 11](#)

[m - commandes de configuration de relais DHCP 12](#)

[n - commandes de configuration d'une ACL 12](#)

[o - commandes de configuration VPN IPsec 13](#)

[p - sauvegarde de la configuration du routeur sur un serveur TFTP \(puis restauration\) 14](#)

[q - configuration HSRP 15](#)

[r - procédure pour que le routeur démarre bien avec la configuration que l'on a enregistrée \(si besoin\) 16](#)

[s - procédure pour réinitialiser le mot de passe du routeur \(si besoin\) 16](#)

[3 - Principales commandes de configuration de la borne wifi Air-Lap1142n-e-k9 17](#)

[a - configuration de l'interface virtuelle BVI du point d'accès 17](#)

[b - Création des SSID sur le point d'accès et mappage d'un SSID à chaque VLAN 17](#)

[c - Configuration d'une sous-interface Ethernet et d'une sous-interface radio pour chaque VLAN sur le point d'accès 18](#)

[d - Configuration de l'interface radio du point d'accès et mappage des SSID à cette interface radio 18](#)

[4 - Principales commandes de configuration du routeur Windows 19](#)

[a - configuration de la fonction de routage 19](#)

[b - commandes de configuration de routes 19](#)

[c - configuration d'une règle de filtrage 19](#)

[d - configuration du relais DHCP 19](#)

[5 - Principales commandes de configuration du routeur- parefeu Pfsense 20](#)

[a - présentation du Pfsense 20](#)

[b - configuration de routes 20](#)

[c - configuration d'une règle de filtrage 22](#)

[d -configuration de la redirection de port 23](#)

[e -configuration du serveur DHCP du routeur 23](#)

[f - commandes de configuration de relais DHCP 23](#)

1 - Principales commandes de configuration du commutateur Cisco

a - commandes de RAZ de la configuration et de changement de nom

Switch#**write erase** ou **erase nvram** :

Switch#**delete vlan.dat**

Switch#**reload**

System configuration has changed. Save ? **no**

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Would you like to terminate autoinstall? [yes]:**yes**

Switch(config)#**hostname SwitchGSB** dans la suite, le message d'invite devient alors
SwitchGSB(config)#

b - commandes de configuration des VLAN

Pour créer un VLAN (et lui attribuer un numéro) :

Switch(config)#**vlan 10**

Pour spécifier un nom à un VLAN :

Switch(config-vlan)#**name Faculte**

Pour lister les VLAN :

Switch#**show vlan**

Pour affecter un VLAN (exemple : le numéro 10) à une interface :

Switch(config)#**int fa0/1** (ou **interface fastEthernet0/1**)

Switch(config-if)#**switchport mode access**

Switch(config-if)#**switchport access vlan 10**

Pour configurer une agrégation trunk 802.1Q :

Switch(config)#**int Gi1/1** (ou **interface GigabitEthernet1/1**)

(définir le mode d'encapsulation dot1q - uniquement pour le commutateur multi-niveaux)

Switch(config-if)#**switchport trunk encapsulation dot1q**

Historiquement, les commutateurs Cisco prenaient en charge 2 méthodes d'encapsulation : ISL et dot1q.

Switch(config-if)#**switchport mode trunk**

Pour affecter un port agrégé à un VLAN natif (pour les paquets non-taggués) :

Switch(config-if)#**switchport trunk native vlan 99**

Pour afficher la configuration des interfaces (avec détails) :

Switch#**show interface**

Pour filtrer les VLAN sur un port trunk (agrégé 802.1Q) :

- Pour autorise seulement les VLANs 2,3 et 10 à passer par le port :

Switch(config)#**int Gi1/1** (ou **interface GigabitEthernet1/1**)

Switch(config-if)#**switchport trunk allowed vlan add 2, 3, 10**

Pour interdire le VLAN 3 de passer par le port :

Switch(config-if)#**switchport trunk allowed vlan remove 3**

c – commandes de configuration VTP (VLAN Trunking Protocol)

Pour configurer une interface d'interconnexion en lien trunk :

Switch(config)#**int fa0/1**

Switch(config-if)#**switchport mode trunk**

Pour configurer un commutateur en tant que serveur VTP :

Switch(config)#**vtp domain lenvers**

Switch(config)#**vtp password lenvers**

Switch(config)#**vtp version 2**

Switch(config)#**vtp mode server**

Pour configurer un commutateur en tant que client VTP :

```
Switch(config)#vtp domain lenvers
```

```
Switch(config)#vtp password lenvers
```

```
Switch(config)#vtp version 2
```

```
Switch(config)#vtp mode client
```

Pour vérifier la configuration VTP :

```
Switch#show vtp status
```

d – commandes de configuration STP (Spanning Tree Protocol)

Pour activer STP (automatiquement exécuté) :

```
Switch(config)#spanning-tree mode pvst
```

Pour afficher les informations concernant STP :

```
Switch#show spanning-tree (ou sh st)
```

Pour configurer une interface en "Portfast" (passage directe de l'état blocking à l'état forwarding uniquement pour les segments qui ne connectent pas de switches) :

```
Switch(config-if)#spanning-tree portfast
```

e – affectation d'une adresse IP à un commutateur

Pour attribuer une adresse IP à un commutateur dans un VLAN donné (exemple : vlan 30) :

```
Switch(config)#int vlan 30
```

```
Switch(config-if)#ip address 192.168.30.1 255.255.255.0
```

f – commandes de configuration de la fonction routeur d'un commutateur multi-niveaux

Pour activer la fonction routage du commutateur multi-niveaux :

```
Switch(config)#ip routing
```

Pour configurer une interface virtuelle SVI (Switch Virtual Interface : interface logique configurée pour un VLAN spécifique, et utilisée comme passerelle pour les hôtes de ce VLAN) :

```
Switch(config)#int vlan20
```

Pour définir l'adresse IP et le masque de sous-réseau de l'interface virtuelle :

```
Switch(config-if)#ip address 172.16.20.10 255.255.255.0
```

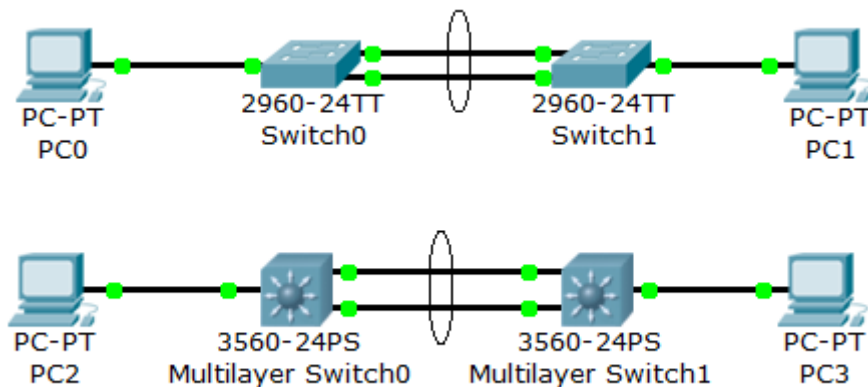
g – configuration SNMP pour la supervision d'un commutateur

Pour configurer et démarrer l'agent SNMP sur un commutateur, il est nécessaire de créer les deux noms de communauté suivants avec leurs droits respectifs : *public* (pour la lecture seule : Read Only), et *private* (pour la lecture - écriture : Read Write) :

```
Switch(config)#snmp-server community public RO
```

```
Switch(config)#snmp-server community private RW
```

h – configuration Etherchannel



Il s'agit de créer une agrégation de liens (regroupement de plusieurs ports physiques pour créer un port logique (PortChannelx, x étant le numéro du port logique)) à partir de deux liens Gi1/1-Gi1/1 et Gi1/2-Gi1/2.

Pour chaque interface à inclure dans un lien agrégé (les deux interfaces à inclure dans le lien peuvent être configurées séparément ou ensemble), spécifier le numéro du groupe (1 à 6) et le mode (protocole de dialogue : *On* si pas de protocole à utiliser, *Active/Passive* pour LACP, *Desirable* pour PAgP, ...), puis configurer le port en mode trunk :

```
Switch(config)#int gi1/1-2
```

```
Switch(config-if)#channel-group 1 mode on
```

```
Switch(config-if)#switchport mode trunk
```

Une interface Port-channel 1 (p1) est ainsi créée. Pour configurer ce port-channel en mode trunk (si pas fait automatique) :

```
Switch(config)#int p1
```

Switch(config-if)#**switchport mode trunk**

Pour vérifier la configuration Etherchannel :

Switch#**show etherchannel**

i – configuration IP d'un switch

On affecte une configuration IP à un switch pour l'administrer à distance, ou pour sauvegarder sa configuration sur un serveur TFTP, ou pour le superviser ; l'adresse IP est en général attribuée à l'interface virtuelle vlan1 (VLAN par défaut).

Switch(config)#**int vlan1**

Switch(config-if)#**ip address 192.168.30.10 255.255.255.0**

Switch(config-if)#**no shutdown**

Switch(config-if)#**exit**

Switch(config)#**ip default-gateway 192.168.30.2**

j – sauvegarde de la configuration du switch sur un serveur TFTP (puis restauration)

Switch#**copy run tftp:** (sauvegarde) Switch#**copy tftp: run** (restauration)

Adresse IP du serveur TFTP : **192.168.10.1**

Nom du fichier : **configSwitch**

Switch#**copy vlan.dat tftp:** (sauvegarde) Switch#**copy tftp: vlan.dat** (restauration)

Adresse IP du serveur TFTP : **192.168.10.1**

Nom du fichier : **vlan.dat**

Attention : si un routeur comportant une ACL doit être traversé pour atteindre le serveur TFTP, il faut rajouter à cette ACL une règle de filtrage autorisant le trafic UDP vers ce serveur : **access-list 101 permit udp any host 192.168.10.1**

k – commandes de configuration de l'accès à distance à un switch via Telnet

Il faut d'abord attribuer une ou plusieurs adresses IP au switch, en utilisant les interfaces virtuelles (par défaut, le VLAN 1).

Switch(config)#**int vlan10**


```
Switch(config-if)#ip address 192.168.10.200 255.255.255.0
```

```
Switch(config-if)#no shutdown
```

Les connexions telnet se font via les lignes VTY (Virtual Teletype). Leur nombre varie selon les modèles.

Pour configurer le mot de passe à entrer et le protocole autorisé pour la connexion à distance :

```
Switch(config)#line vty 0 15 (ou selon le nombre de lignes : line vty 0 4 )
```

```
Switch(config-line)#password cisco
```

```
Switch(config-line)#login
```

```
Switch(config-line)#transport input telnet
```

```
Switch(config-line)#exit
```

Pour configurer le mot de passe à entrer pour accéder au mode privilégié (enable) (obligatoire) :

```
Switch(config)#enable password cisco
```

Pour activer le cryptage des mots de passe (optionnel) :

```
Switch(config)# service password-encryption
```

I – commandes de configuration de l'accès à distance à un switch via SSH

Il faut d'abord attribuer une ou plusieurs adresses IP au switch, en utilisant les interfaces virtuelles (par défaut, le VLAN 1).

```
Switch(config)#int vlan10
```

```
Switch(config-if)#ip address 192.168.10.200 255.255.255.0
```

Il faut ensuite configurer un nom d'hôte et un nom de domaine :

```
Switch(config)#hostname SwitchGSB dans la suite, le message d'invite devient alors  
SwitchGSB(config)#
```

```
Switch(config)#ip domain-name mondomaine.local
```

Les connexions SSH sont possibles avec un switch ou un routeur Cisco seulement si son IOS supporte ssh : la mention *k9* doit figurer dans le nom de l'IOS lorsqu'on exécute la commande *show version*

Pour activer le serveur SSH sur le switch et pour générer une paire de clés RSA (clé publique + clé privée) :

Switch(config)#**crypto key generate rsa** (puis saisir la longueur conseillée pour les clés : 1024 octets)

ou Switch(config)#**crypto key generate rsa general-keys modulus 1024**

Pour activer SSH :

Switch(config)#**ip ssh version 2**

Pour ajouter un compte administrateur :

Switch(config)#**username admin secret cisco**

Pour désactiver Telnet et n'autoriser que le protocole ssh pour accéder au switch :

Switch(config)#**line vty 0 15** (ou selon le nombre de lignes : **line vty 0 4**)

Switch(config-line)#**login local**

Switch(config-line)#**transport input ssh**

Pour configurer le mot de passe à entrer pour accéder au mode privilégié (enable) (obligatoire) :

Switch(config)#**enable password cisco**

Pour activer le cryptage des mots de passe (optionnel) :

Switch(config)# **service password-encryption**

Pour établir une connexion SSH au switch ainsi configuré, depuis un PC sous Linux (sous Windows utiliser Putty) :

PC> ssh -l *admin* 192.168.10.200

Password: *cisco*

Switch>**enable**

Password: *cisco*

Pour sortir de la session SSH : switch>**exit**

2 – Principales commandes de configuration du routeur Cisco

a – commandes de RAZ de la configuration et de changement de nom

Router#**write erase** ou **erase nvram** :

Router#**reload**

System configuration has changed. Save ? **no**

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Would you like to terminate autoinstall? [yes]:**yes**

Router(config)#**hostname RouteurGSB** dans la suite, le message d'invite devient alors
RouteurGSB(config)#

b – commandes de configuration d'une interface

Pour configurer une interface (FastEthernet, Serial, ...) :

Router(config)#**int Se2/0** (ou **interface Serial2/0**)

Pour définir l'adresse IP et le masque de sous-réseau de l'interface :

Router(config-if)#**ip address 194.168.50.1 255.255.255.0**

Pour définir la fréquence d'horloge (uniquement pour les interfaces Série) :

Router(config-if)#**clock rate 64000**

Pour activer l'interface (mettre à On) :

Router(config-if)#**no shutdown**

c – configuration SNMP pour la supervision d'un routeur

Pour configurer et démarrer l'agent SNMP sur un routeur, il est nécessaire de créer les deux noms de communauté suivants avec leurs droits respectifs : *public* (pour la lecture seule : Read Only), et *private* (pour la lecture - écriture : Read Write) :

Router(config)#**snmp-server community public RO**

Router(config)#**snmp-server community private RW**

d – commandes de configuration de routes

Pour configurer une route statique :

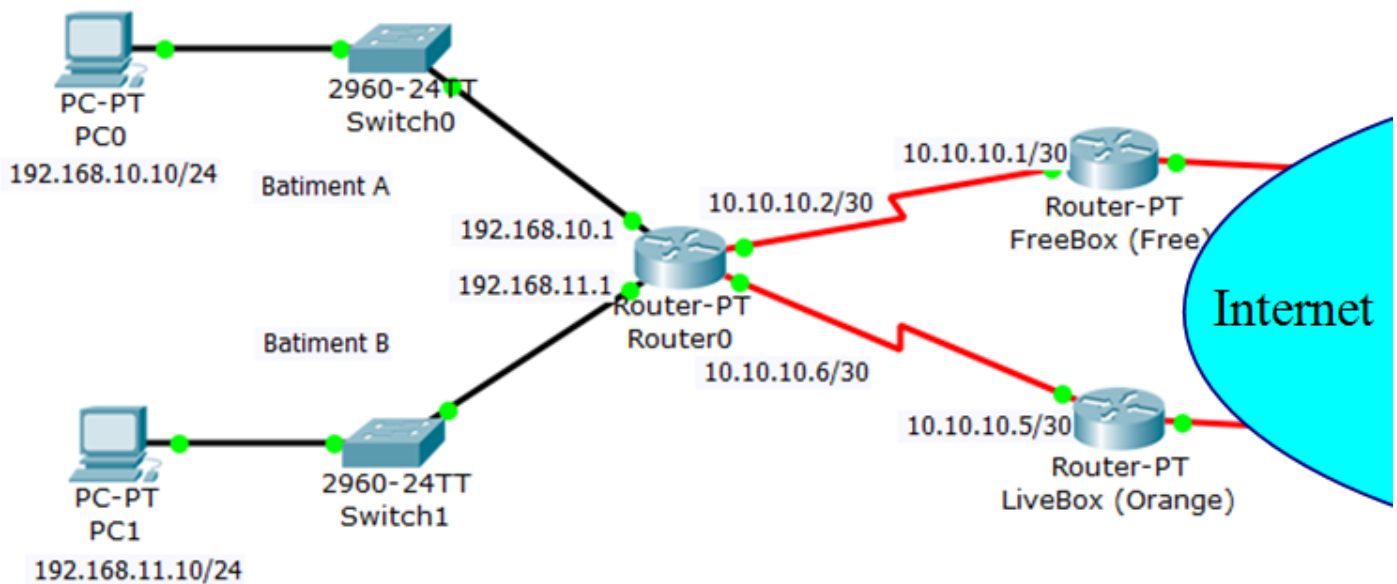
Router(config)#**ip route 196.168.2.0 255.255.255.0 192.168.50.2**

Pour supprimer une route statique :

```
Router(config)#no ip route 196.168.2.0 255.255.255.0 192.168.50.2
```

Pour afficher la table de routage :

```
Router#show ip route
```



Cas des routes statiques flottantes :

Les routes statiques flottantes sont des routes statiques utilisées pour fournir un chemin de secours à une route statique ou une route dynamique principale lorsque celle-ci n'est pas disponible.

Pour cela, la route statique flottante est configurée avec une distance administrative plus élevée que la route principale. La distance administrative indique la fiabilité d'une route. Si plusieurs chemins vers la destination existent, le routeur choisira le chemin présentant la plus courte distance administrative.

La distance administrative d'une route connectée est 0. La distance administrative d'une route statique est 1.

La distance administrative d'une route obtenue par un protocole de routage dépend du protocole utilisé.

```
Router0(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

```
Router0(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5 8
```

e - commandes de configuration du routage "Router-on-a-stick"

Pour configurer la sous-interface 2 d'une interface :

```
Router(config)#int fa0/0.2
```

Pour affecter la sous-interface au VLAN 20:

```
Router(config-subif)#encapsulation dot1q 20
```

Pour définir l'adresse IP et le masque de sous-réseau de la sous-interface :

```
Router(config-subif)#ip address 172.17.20.1 255.255.255.0
```

Origine de la route	Distance administrative
Connecté	0
Statique	1
Résumé du routage EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

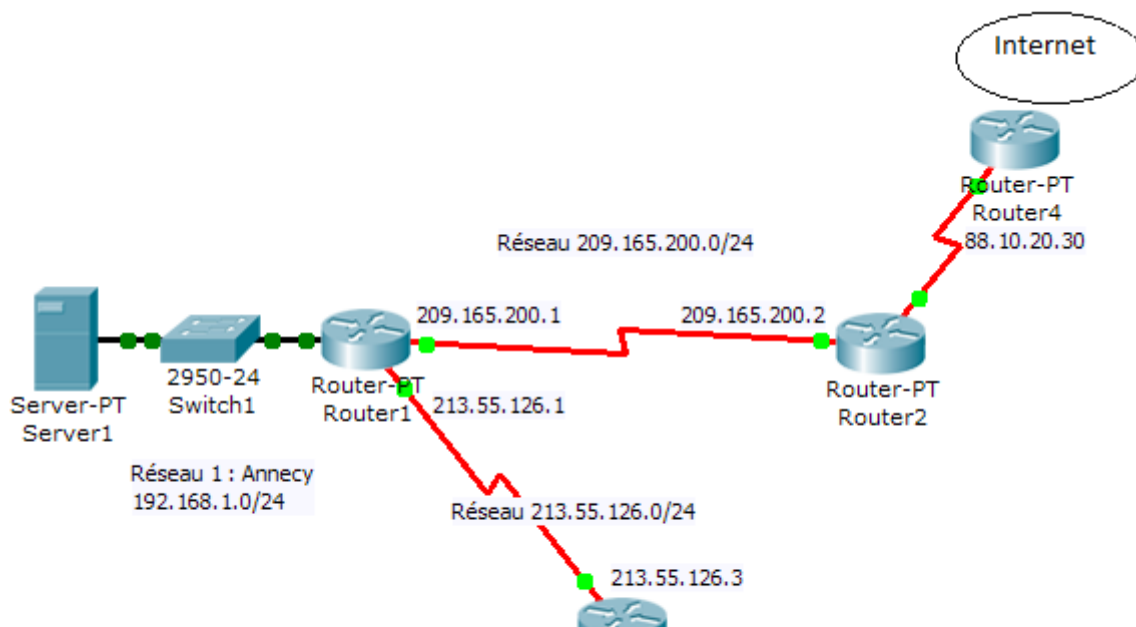
Les protocoles

de routage dynamique permettent à des routeurs de s'échanger des informations entre eux afin que chacun puisse construire sa table de routage de manière dynamique et automatique. Lorsqu'une route est en panne, le protocole recalcule automatiquement un autre chemin.

La distance Administrative est une valeur qui représente la fiabilité d'un protocole. Elle dépend du protocole de routage. Exemple : si un routeur apprend par deux protocoles RIP et OSPF une route menant à une même destination, il choisit la route OSPF car elle a la distance administrative la plus basse.

Configurer un routeur avec un protocole de routage dynamique consiste à annoncer les réseaux directement connectés à ce routeur pour lesquels on souhaite que le routage dynamique soit opérationnel.

RIP calcule le meilleur chemin en s'appuyant sur le nombre de routeurs à traverser (coût RIP = nombre de sauts).



Type d'interface	$10^8/\text{bits/s} = \text{Coût}$
Fast Ethernet et plus rapide	$10^8/100\,000\,000 \text{ bits/s} = 1$
Ethernet	$10^8/10\,000\,000 \text{ bits/s} = 10$
E1	$10^8/2\,048\,000 \text{ bits/s} = 48$
T1	$10^8/1\,544\,000 \text{ bits/s} = 64$
128 Kbits/s	$10^8/128\,000 \text{ bits/s} = 781$
64 Kbits/s	$10^8/64\,000 \text{ bits/s} = 1\,562$
56 Kbits/s	$10^8/56\,000 \text{ bits/s} = 1\,785$

OSPF calcul le meilleur chemin en

s'appuyant sur la vitesse (débit) (coût OSPF = $100\,000\,000 / \text{bande passante du lien en bits/s}$).

Pour configurer le protocole de routage dynamique **OSPF** :

```
Router1(config)#router ospf 1
```

```
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

```
Router1(config-router)#network 209.165.200.0 0.0.0.255 area 0
```

```
Router1(config-router)#network 213.55.126.0 0.0.0.255 area 0
```

Pour configurer le protocole de routage dynamique **RIP** (bien toujours penser à désactiver le résumé des réseaux à annoncer par classe, et rapporter ainsi tous les sous-réseaux avec des informations de masque de sous-réseau (RIPv2)) :

```
Router1(config)#router rip
```

Router1(config-router)#**version 2**

Router1(config-router)#**network 213.55.126.0**

Router1(config-router)#**network 192.168.1.0**

Router1(config-router)#**network 209.165.200.0**

Router1(config-router)#**no auto-summary**

Pour définir une route par défaut (dans OSPF ou RIP), et la propager aux autres routeurs (commande à rentrer seulement sur le routeur à l'origine de la route par défaut (celui disposant du lien vers Internet)) :

Router2(config)#**ip route 0.0.0.0 0.0.0.0 88.10.20.30**

Router2(config)#**router ospf 1 (ou router rip)**

Router2(config-router)#**default-information originate**

g – commandes de configuration de l'accès à distance à un routeur via Telnet

Les connexions telnet se font via les lignes VTY (Virtual Teletype). Leur nombre varie selon les modèles.

Pour configurer le mot de passe à entrer et le protocole autorisé pour la connexion à distance :

Router(config)#**line vty 0 15** (ou selon le nombre de lignes : **line vty 0 4**)

Router(config-line)#**password cisco**

Router(config-line)#**login**

Router(config-line)#**transport input telnet**

Router(config-line)#**exit**

Pour configurer le mot de passe à entrer pour accéder au mode privilégié (enable) (obligatoire) :

Router(config)#**enable password cisco**

Pour activer le cryptage des mots de passe (optionnel) :

Router(config)# **service password-encryption**

h – commandes de configuration de l'accès à distance à un routeur via SSH

Il faut configurer un nom d'hôte et un nom de domaine :

Router(config)#**hostname RouterGSB** dans la suite, le message d'invite devient alors
RouterGSB(config)#

Router(config)#**ip domain-name mondomaine.local**

Les connexions SSH sont possibles avec un switch ou un routeur Cisco seulement si son IOS supporte ssh : la mention *k9* doit figurer dans le nom de l'IOS lorsqu'on exécute la commande *show version*

Pour activer le serveur SSH sur le routeur et pour générer une paire de clés RSA (clé publique + clé privée) :

Router(config)#**crypto key generate rsa** (puis saisir la longueur conseillée pour les clés : 1024 octets)

ou Router(config)#**crypto key generate rsa general-keys modulus 1024**

Pour activer SSH :

Router(config)#**ip ssh version 2**

Pour ajouter un compte administrateur :

Router(config)#**username admin secret cisco**

Pour désactiver Telnet et n'autoriser que le protocole ssh pour accéder au routeur :

Router(config)#**line vty 0 15** (ou selon le nombre de lignes : **line vty 0 4**)

Router(config-line)#**login local**

Router(config-line)#**transport input ssh**

Pour configurer le mot de passe à entrer pour accéder au mode privilégié (enable) (obligatoire) :

Router(config)#**enable password cisco**

Pour activer le cryptage des mots de passe (optionnel) :

Router(config)# **service password-encryption**

Pour établir une connexion SSH au routeur ainsi configuré, depuis un PC sous Linux (sous Windows utiliser Putty) :

PC> *ssh -l admin 192.168.30.1*

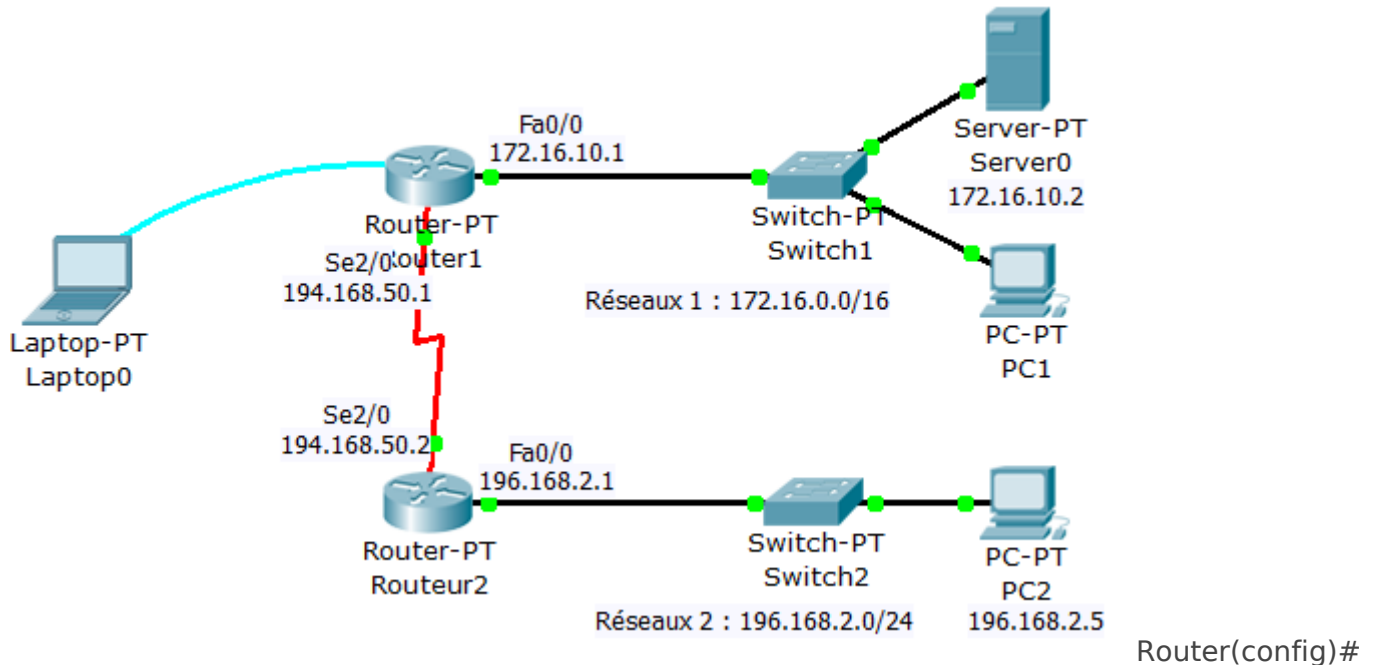
Password: *cisco*

Router>**enable**

Password: *cisco*

Pour sortir de la session SSH : Router>**exit**

i - commandes de configuration de la fonction NAT dynamique



access-list 1 permit 172.16.0.0 0.0.255.255 ou **access-list 1 permit any**

Pour activer NAT sur l'interface interne (LAN) :

Router(config)#**int fa0/0**

Router(config-if)#**ip nat inside**

Pour activer NAT sur l'interface externe (WAN) :

Router(config)#**int Se2/0**

Internet

Router(config-if)#**ip nat outside**

Pour traduire l'ensemble des adresses internes du réseau défini par la liste d'accès, en une seule adresse externe, celle attribuée à l'interface WAN (reliée à Internet ou au FAI) (overload signifie qu'on active le PAT) :

Router(config)#**ip nat inside source list 1 interface se2/0 overload**

j – commandes de configuration de la fonction NAT statique

Pour mapper l'adresse interne 172.16.10.2 à l'adresse externe 194.168.50.3 :

```
Router(config)#ip nat inside source static 172.16.10.2 194.168.50.3
```

k – commandes de configuration de la fonction NAT statique - redirection de port

Pour rediriger le trafic HTTP (tous les paquets TCP reçus sur le port 80 du routeur) vers le serveur Web (sur le port 80) :

```
Router(config)#ip nat inside source static tcp 172.16.10.2 80 194.168.50.1 80
```

l – commandes de configuration du serveur DHCP du routeur

Pour définir un pool d'adresses et lui attribuer un nom :

```
Router(config)#ip dhcp pool poolClient
```

Pour spécifier l'adresse-réseau et le masque correspondant au pool d'adresses :

```
Router(dhcp-config)#network 172.16.0.0 255.255.0.0
```

Pour exclure, si besoin, une plage d'adresse du pool d'adresses et éviter ainsi que le DHCP attribue ces adresses :

```
Router(dhcp-config)#ip dhcp excluded-address 172.16.0.1 172.16.0.3
```

Pour spécifier l'adresse IP d'un serveur DNS disponible pour un client DHCP :

```
Router(dhcp-config)#dns-server 172.16.10.2
```

Pour définir l'adresse IP de la passerelle par défaut pour les clients DHCP :

```
Router(dhcp-config)#default-router 172.16.10.1
```

Pour définir une réservation d'adresse (mappage adresse IP - adresse MAC) :

```
Router(dhcp-config)#ip dhcp pool p host 172.16.0.50 hardware-address02c7.f800.0422  
ieee802 client-name n
```

Pour définir la durée de réservation d'une adresse cliente (par défaut : 1 jour) :

```
Router(dhcp-config)#lease infinite
```

m – commandes de configuration de relais DHCP

Pour que le routeur laisse passer les requêtes/demandes DHCP sur une interface, il faut sélectionner cette interface et entrer l'adresse du serveur DHCP dans la commande *ip helper-address* (exemple : laisser passer sur l'interface Fa0/1 d'adresse 192.168.10.100, les requêtes/demandes DHCP vers le serveur DHCP 172.18.2.1) :

```
Router(config)#int fa0/1
```

```
Router(config)# ip helper-address 172.18.2.1
```

n – commandes de configuration d'une ACL

Pour créer une nouvelle règle dans l'ACL de numéro 100 (toujours en fin de liste) :

```
Router(config)#access-list 100 deny tcp any host 192.168.10.4 eq 80
```

Pour appliquer la liste 100 en entrée de l'interface Fa0/0 de Router0 :

```
Router(config)#int fa0/0
```

```
Router(config-if)ip access-group 100 in
```

Construction d'une règle d'une ACL étendue

access-list *number* **deny|permit** *protocole* *IPSource* *MasqueGSource* *opérateur*
applicationSource
IPDesti *MasqueGDesti* *opérateur* *applicationDesti*

number : nombre identifiant la liste entre 100-199 ou 2000-2699

deny|permit : refuser|autoriser le paquet

protocole : nom d'un protocole IP de couche 3 ou 4 à refuser ou à accepter : **icmp**, **tcp**, **udp**, **ospf**, **ipinip**, ...,

ip (tout protocole Internet (inclus **icmp**, **tcp**, et **udp**))

IPSource : adresse IP source que l'on refuse ou autorise à émettre

MasqueGSource : masque générique correspondant à l'adresse IP source

opérateur : opérateur : **eq** (=), **gt** (>), **lt** (<), **ne** (<>)

applicationSource : numéro de port source ou acronyme identifiant l'application source par son protocole de la

couche 7 (**21** ou **ftp**, ...)

IPDesti : adresse IP destination que l'on refuse ou autorise à recevoir

MasqueGDesti : masque générique correspondant à l'adresse IP destination

applicationDesti : numéro de port destination ou acronyme identifiant l'application destination par son protocole

de la couche 7 (**21** ou **ftp**, ...)

→ *opérateur* suivi de *application* sont facultatifs et ne peuvent être spécifiés que si *protocole* est **tcp** ou **udp** (interdit pour tout autre protocole)

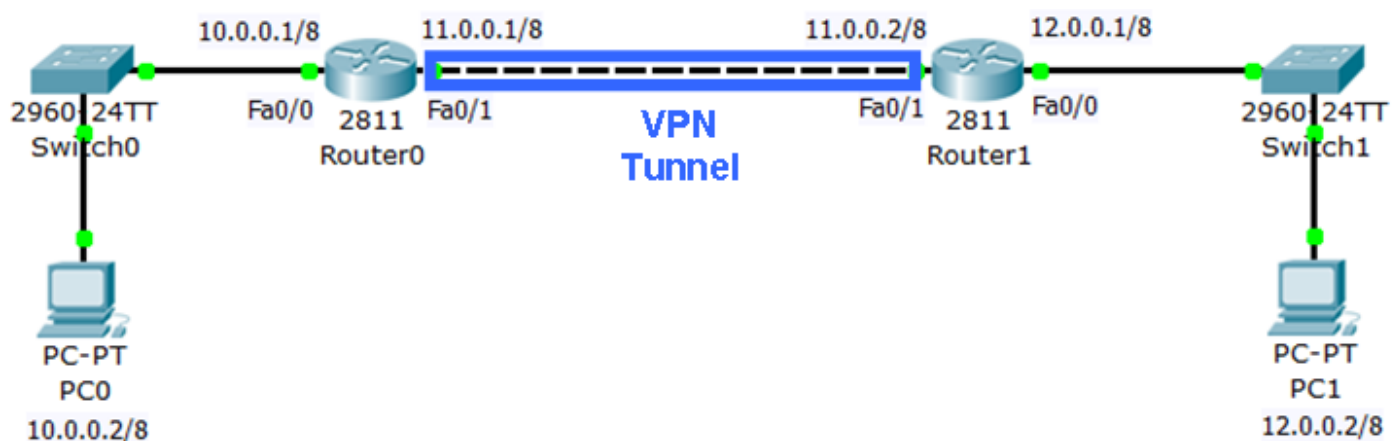
→ peuvent être ajoutés à la fin de l'instruction, de manière optionnelle :

echo-reply si protocole est **icmp** (autoriser seulement les réponses ICMP),

established si protocole est **tcp** (autoriser seulement les réponses aux demandes établies depuis le réseau interne).

Exemple : `access-list 122 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.89 eq 80`

o -commandes de configuration VPN IPsec



Phase 1 : spécification des algorithmes de chiffrement, et de hashage, du type de clé utilisée pour s'authentifier, du groupe Diffie-Helman, et création de la clé "mère" utilisée pour l'authentification (et à partir de laquelle seront générées les clés de chiffrement).

Sur Router0 :

Pour activer le module d'authentification et d'échange de clés ISAKMP (Internet Security Association and Key Management Protocol), dérivé de IPsec IKE :

Router(config)#**crypto isakmp enable**

Pour créer une nouvelle politique de sécurité ISAKMP (de numéro 1) :

Router(config)#**crypto isakmp policy 1**

Pour spécifier l'algorithme de cryptage (chiffrement) utilisé (AES, DES, 3DES) :

Router(config-isakmp)#**encryption aes**

Pour spécifier l'algorithme de hashage utilisé (MD5, SHA) (SHA par défaut) :

Router(config-isakmp)#**hash sha**

Pour définir une méthode d'authentification par clé partagée :

Router(config-isakmp)#**authentication pre-share**

Pour définir un groupe Diffie-Helman (group 1, 2, ou 5) :

Router(config-isakmp)#**group 2**

Pour définir la clé pré-partagée utilisée pour l'authentification, (ici : « 0 ») à entrer manuellement dans chaque routeur, ainsi que l'adresse IP du routeur distant avec lequel on veut communiquer (sous PKT, entrer 0.0.0.0 au lieu du masque) :

Router(config)#**crypto isakmp key 0 address 11.0.0.2 0.0.0.0**

Phase 2 : Etablissement des Associations de Sécurité (SA) : spécification du transform-set (ensemble d'algorithmes de chiffrement et d'authentification déterminant la manière dont le trafic doit être transformé par IPsec pour être protégé), du trafic à protéger, de la crypto-map (informations nécessaires à l'établissement d'une association de sécurité (SA) s'appliquant à une interface de routeur).

Pour définir un ensemble de transformations IPsec, de nom « montransform », il faut choisir l'un des deux protocoles de sécurité AH ou ESP pour l'authentification (MD5 ou SHA pour l'IPsec AH ou ESP) (ici, authentification SHA avec ESP), et pour le chiffrement (AES, DES ou 3DES pour l'IPsec ESP) (ici, chiffrement AES avec ESP) :

Router(config)#**crypto ipsec transform-set montransform esp-aes esp-sha-hmac**

Pour identifier le trafic qui utilisera le tunnel VPN (en créant une règle d'ACL de numéro 100) :

Router(config)#**access-list 100 permit ip 10.0.0.0 0.255.255.255 12.0.0.0 0.255.255.255**

Pour créer une nouvelle « carte de cryptage » de nom « monmap », de numéro 20, et de type IPsec-ISAKMP :

Router(config)#**crypto map monmap 20 ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

Pour définir l'adresse IP du correspondant :

```
Router(config-crypto-map)#set peer 11.0.0.2
```

Pour référencer le transform-set déterminant comment le trafic est protégé :

```
Router(config-crypto-map)#set transform-set montransform
```

Pour référencer l'ACL déterminant le trafic à chiffrer :

```
Router(config-crypto-map)#match address 100
```

Pour appliquer une crypto-map à une interface (ici monmap à Fa0/1) :

```
Router(config)#interface fastEthernet 0/1
```

```
Router(config-if)#crypto map monmap
```

```
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

p – sauvegarde de la configuration du routeur sur un serveur TFTP (puis restauration)

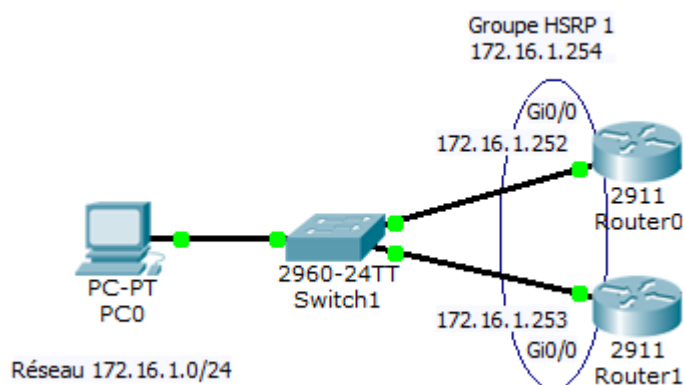
```
Router#copy run tftp: (sauvegarde) Router#copy tftp: run (restauration)
```

Adresse IP du serveur TFTP : **192.168.10.1**

Nom du fichier : **configRouter**

Attention : si un routeur comportant une ACL doit être traversé pour atteindre le serveur TFTP, il faut rajouter à cette ACL une règle de filtrage autorisant le trafic UDP vers ce serveur : **access-list 101 permit udp any host 192.168.10.1**

q – configuration HSRP



HSRP (Hot Standby Routing Protocol) est un protocole propriétaire Cisco qui permet de créer un routeur virtuel à partir de deux routeurs physiques.

Il s'agit de configurer un groupe HSRP (de numéro 1) avec l'interface Gi0/0 de Router0 et l'interface Gi0/0 de Router1.

Sur Router0 :

```
Router(config)#int gi0/0
```

Pour configurer l'adresse IP (réelle) et le masque de cette interface :

```
Router(config-if)#ip address 172.16.1.252 255.255.255.0
```

Pour inclure une interface dans un groupe HSRP de numéro donné, et configurer l'adresse virtuelle du groupe :

```
Router(config-if)#standby 1 ip 172.16.1.254
```

Pour définir la priorité du routeur (100 par défaut) pour un groupe donné (le routeur préemptable qui aura la priorité la plus haute deviendra le routeur actif du groupe) :

```
Router(config-if)#standby 1 priority 100
```

Pour déclarer le routeur préemptable (éligible pour devenir actif si un autre du groupe tombe en panne) :

```
Router(config-if)#standby 1 preempt
```

Le tracking d'interface permet à un routeur de vérifier l'état d'une de ses interfaces et, si elle est down, de décrémenter sa priorité HSRP (par défaut de 10) de telle sorte qu'elle devienne inférieure à celle d'un routeur en standby qui deviendra alors actif. Pour configurer le tracking d'une interface d'un groupe :

```
Router(config-if)#standby 1 track GigabitEthernet0/1
```

Pour visualiser si le routeur est actif ou passif :

```
Router(config-if)#do show standby
```

Sur Router1, faire la configuration similaire :

```
Router(config)#int gi0/0
```

```
Router(config-if)#ip address 172.16.1.253 255.255.255.0
```

```
Router(config-if)#standby 1 ip 172.16.1.254
```

```
Router(config-if)#standby 1 priority 95
```

```
Router(config-if)#standby 1 preempt
```

```
Router(config-if)#standby 1 track GigabitEthernet0/1
```

r – procédure pour que le routeur démarre bien avec la configuration que l'on a enregistrée (si besoin)

Dans certains cas, il se peut que le routeur ne démarre pas avec la configuration que l'on a précédemment enregistrée. Par exemple, lorsque le registre de configuration contient la valeur 0x2142, le routeur contourne la configuration de démarrage stockée en NVRAM pendant la phase de boot. Cette caractéristique est normalement utilisée pendant une procédure de récupération de mot de passe.

Pour un démarrage normal du routeur, le registre de configuration doit contenir la valeur 0x2102 (pour qu'il charge la configuration de démarrage depuis la NVRAM/ROM dans la RAM).

Pour rétablir la bonne valeur du registre de configuration :

- Mettre le routeur sous tension en maintenant appuyées les touches CTRL Pause (pendant 10 à 15 secondes) ; le routeur rentre en mode ROMmon (ROMmon est un système de restauration du routeur Cisco en cas de problème majeur ne pouvant être réparé).
- Modifier la configuration du registre comme suit :

```
rommon1>confreg 2102
```

```
rommon1>reset
```

Autre possibilité

```
Router#configure terminal
```

```
Router(config)#config-register 0x2102
```

```
Router(config)#end
```

```
Router#reload
```

<https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html>

s – procédure pour réinitialiser le mot de passe du routeur (si besoin)

<http://www.supinfo.com/articles/single/1171-reinitialiser-mot-passe-votre-routeur-cisco>

3 – Principales commandes de configuration de la borne wifi Air-Lap1142n-e-k9

a – configuration de l'interface virtuelle BVI du point d'accès

Dans le point d'accès sans fil qui relie les clients à interface filaire (Ethernet) et les clients à interface non-filaires (802.11), nous devons relier (ponter) l'interface radio sans fil (Dot11Radio0 ou

Dot11Radio1) utilisée par les clients wifi, et l'interface filaire Ethernet (Gi0) utilisée par les clients filaires pour que ces deux interfaces soient dans le même domaine de diffusion de couche 2.

Ce pontage se fait grâce à l'interface BVI (Bridge Virtual Interface) qui agit comme une interface routée entre l'interface radio et l'interface filaire de la borne wifi. Elle permet d'établir un pont entre ces deux interfaces.

Une interface BVI est une interface virtuelle routée qui représente un pont entre deux interfaces d'un routeur ou d'une borne wifi. Tous les paquets échangés entre un client filaire et un client non-filaire, et donc entrant ou sortant sur ces interfaces pontées de la borne wifi devront passer par cette BVI.

À une interface BVI, on peut attribuer une adresse de couche trois, des politiques de QoS, des listes d'accès ou tout autre « service » que l'on peut attribuer à n'importe quelle interface physique. Les bornes wifi Cisco utilisent la technologie Cisco Integrated Routing and Bridging (IRB) et les commandes bridge pour activer ce pont (activées par défaut).

L'IP du point d'accès, si on veut en configurer une, doit être configurée sur le pont BVI et non sur l'interface Ethernet.

Nous allons configurer l'adresse IP de la borne sur l'interfaces BVI1 qui sera le pont (numéroté 1) entre l'interface radio (Dot11Radio0 ou Dot11Radio1) et l'interface Ethernet (Gi0).

Ap# **conf ter**

Ap(config)# **interface BVI 1**

Ap(config-if)# **ip address 192.168.211.151 255.255.255.0**

Ap(config-if)# **no shutdown**

Ap(config-if)# **exit**

Ap# **ip default-gateway 192.168.211.254**

b - Création des SSID sur le point d'accès et mappage d'un SSID à chaque VLAN

Il s'agit de mapper un SSID à chaque VLAN ; pour chacun, il faut configurer une méthode d'authentification des clients.

Les clients s'authentifieront avec une clé statique WPA2.

La commande *authentication open* autorise la connexion des équipements.

Pour prendre en charge la gestion des clés d'authentification, il faut utiliser la commande *authentication key-management*. Il faut ensuite définir la valeur de la clé.

Si on souhaite rendre le réseau wifi visible et donc diffuser le SSID, il faut utiliser la commande *mbssid guest-mode* (mbssid : Multiple Basic Service Set Identifier).

```
Ap(config)#dot11 ssid BTSSIO
```

```
Ap(config-ssid)# vlan 1
```

```
Ap(config-ssid)# authentication open
```

```
Ap(config-ssid)# authentication key-management wpa version 2
```

```
Ap(config-ssid)# wpa-psk ascii springfield
```

```
Ap(config-ssid)# mbssid guest-mode
```

```
Ap(config-ssid)# exit
```

c - Configuration d'une sous-interface Ethernet et d'une sous-interface radio pour chaque VLAN sur le point d'accès

Le switch est connecté au Point d'Accès wifi par un seul câble. Sur l'interface Ethernet Gi0 du Point d'Accès, peuvent passer plusieurs VLAN ; il faut donc créer une sous-interface Ethernet pour chaque VLAN.

D'autre part, le Point d'Accès wifi peut diffuser plusieurs SSID, vers plusieurs VLAN, depuis une seule interface radio ; sur cette interface radio Dot11Radio0, il faut donc créer une sous-interface radio pour chaque VLAN.

Chaque sous-interface radio doit être mappée à un numéro de pont. Chaque sous-interface Ethernet doit aussi être mappée à un numéro de pont (le même que celui mappé pour la sous-interface radio correspondante).

Enfin, pour chaque sous-interface, il faut activer le taguage de trames (*encapsulation dot1Q*).

```
Ap(config)# interface Dot11Radio0.1
```

```
Ap(config-subif)# encapsulation dot1Q 1 native
```

```
Ap(config-subif)# bridge-group 1
```

```
Ap(config-subif)# exit
```

```
Ap(config)# interface Gi0.1
```

```
Ap(config-subif)# encapsulation dot1Q 1 native
```

```
Ap(config-subif)# bridge-group 1
```

Ap(config-subif)# **exit**

d - Configuration de l'interface radio du point d'accès et mappage des SSID à cette interface radio

Les SSID sont créés, mais restent inutilisables, car ils ne sont liés à aucune interface radio ; nous allons donc configurer chaque interface radio qui va servir à diffuser un ou plusieurs SSID afin de les rendre accessibles.

L'interface radio 2.4ghz porte souvent le numéro 0 et l'interface radio5ghz porte le numéro 1.

La commande *mbssid* permet la diffusion de plusieurs SSID.

Pour prendre en charge la gestion des clés d'authentification, il faut activer une suite de chiffrement à l'aide de la commande *encryption mode ciphers*, et définir le cryptage utilisé sur l'interface radio. Pour s'aligner sur les meilleurs standards de sécurité et avec les meilleurs débits de données, combiner l'authentification WPA2 (configurée sur le SSID) avec le cryptage AES (configuré sur l'interface radio).

La commande *channel least-congested 1 6 11* renseigne le canal sur lequel la borne va diffuser ; celle-ci va choisir le meilleur canal entre le 1, le 6 et le 11 afin d'être le moins impactée par d'éventuelles interférences.

Ap(config)# **int dot11radio0**

Ap(config-if)# **mbssid**

Ap(config-if)# **encryption vlan 1 mode ciphers aes-ccm**

Ap(config-if)# **ssid BTSSIO**

Ap(config-if)# **channel least-congested 1 6 11**

Ap(config-if)# **no shutdown**

Remarques :

- La commande *show dot11 bssid* permet de voir les SSID diffusés par la borne.

- La commande *copy run start* permet de sauvegarder la configuration de la borne WiFi !

- Attention : penser à configurer un serveur DHCP avec un pool pour chaque VLAN pour que chaque client wifi obtienne une adresse IP dans le bon VLAN (ainsi que l'adresse de la passerelle et éventuellement du serveur de noms).

4 – Principales commandes de configuration du routeur Windows

a – configuration de la fonction de routage

1. installer le rôle *Services de stratégie et d'accès réseau*, avec le service de rôle *Routage* ;
2. activer le routage avec *Démarrer / Outils d'administration / Routage et accès distant* ; cliquer droit sur l'icône du serveur et sélectionner *Configurer et activer le routage et l'accès distant* ; cocher le service *Routage réseau*

b – commandes de configuration de routes

Pour configurer une route statique (et persistante, c'est à dire qui reste même si la machine est réinitialisée) :

Router(config)#**route -p add 192.168.2.0 mask 255.255.255.0 192.168.50.2**

Pour configurer une route par défaut :

Router(config)#**route -p add 0.0.0.0 mask 0.0.0.0 192.168.50.2**

Pour supprimer une route statique :

Router(config)#**route delete 192.168.2.0**

Pour afficher la table de routage :

Router#**route print**

c – configuration d'une règle de filtrage

1. sélectionner *Démarrer / Outils d'administration / Routage et accès distant* ; cliquer droit sur l'icône de l'interface sur laquelle on souhaite créer une règle de filtrage et sélectionner *Propriétés* ;
2. sous l'onglet *Général*, cliquer sur *Filtres d'entrée* ou *Filtres de sortie*, puis sur *Nouveau* ; entrer et valider la règle ;
3. dans **Action de filtrage**, sélectionner l'action de filtrage appropriée, puis cliquer sur **OK**

d – configuration du relais DHCP

1. sélectionner *Démarrer / Outils d'administration / Routage et accès distant* ; dans la branche *IPv4*, cliquer droit sur *Général*, puis sélectionner *Nouveau protocole de routage* ; sélectionner ensuite *Agent de relais DHCP* puis *OK* ;
2. dans la branche *IPv4*, cliquer droit sur *Agent de relais DHCP*, puis sélectionner *Nouvelle interface* ;
3. sélectionner l'interface qui sera utilisée pour la réception des requêtes DHCP de la part des clients DHCP puis cliquer sur *OK* ;
4. S'assurer que la case *Relayer les paquets DHCP (Dynamic Host Configuration Protocol)* est cochée, puis cliquer sur *OK* ;
5. dans la branche *IPv4*, cliquer droit sur *Agent de relais DHCP*, puis sélectionner *Propriétés* ; spécifier l'adresse IP du serveur DHCP, puis cliquer sur *OK*.

5 - Principales commandes de configuration du routeur- parefeu Pfsense

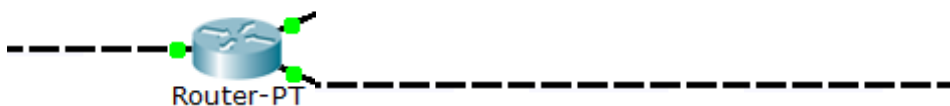
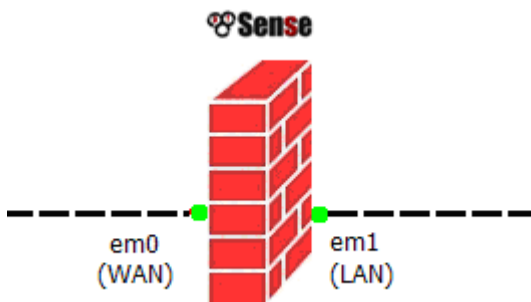
a - présentation du Pfsense

Un routeur-parefeu Pfsense comporte toujours au moins deux interfaces :

- une interface logique externe WAN (correspondant à l'interface physique *em0*) sur **laquelle la fonction NAT automatique est implantée** par défaut.
- une interface logique interne LAN (correspondant à l'interface physique *em1*)

Une interface physique correspond à une carte réseau ; elle possède toujours une adresse MAC.
Une interface logique est toujours associée à une interface physique ; elle possède toujours une adresse IP.

Dans le cas des VLAN plusieurs interfaces logiques peuvent être associées à une même interface physique (notion correspondante aux sous-interfaces CISCO).



192.168.1.253

192.168.4.253

192.168.4.254

192.168.1.254

La configuration d'un routeur-parefeu PfSense se fait depuis le navigateur d'un poste connecté à ce PfSense en tapant l'adresse IP de l'interface LAN.

b – configuration de routes

Pour configurer une route statique :

1. entrer d'abord la passerelle à utiliser pour joindre le réseau pour lequel on veut créer une route :

1ère solution : entrer cette passerelle lors de la saisie de l'adresse IP de l'interface du PfSense concernée (*Gateway : add a new one*) :

Exemple : pour l'interface LAN, créer une passerelle 192.168.4.254 :

Interfaces: LAN

General configuration

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 configuration

IPv4 address /

Gateway - or **add a new one.**
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Add new gateway:

Default gateway: ☒

Gateway Name:

Gateway IPv4:

Description:

2ème solution : entrer cette passerelle avec la commande *System Routing*, onglet *Gateways* :

System: Gateways



Gateways Routes Groups				
Name	Interface	Gateway	Monitor IP	Description
GW_LAN_2	LAN	192.168.4.254	192.168.4.254	Interface lan Gateway

1. créer ensuite la route avec la commande *System Routing*, onglet *Routes* ;

Exemple : Créer une route vers le réseau 192.168.2.0/24 utilisant la passerelle 192.168.4.254 :

System: Static Routes



Gateways Routes Groups			
Network	Gateway	Interface	Description
192.168.2.0/24	GW_LAN_2 - 192.168.4.254	LAN	

Pour configurer une route par défaut :

entrer simplement la passerelle à utiliser par défaut pour l'interface WAN en précisant que cette passerelle est la passerelle par défaut :

1ère solution : entrer cette passerelle lors de la saisie de l'IP de l'interface WAN (*Gateway : add a new one*) :

Exemple : pour l'interface WAN, créer une passerelle par défaut 192.168.1.254 :

Interfaces: WAN

General configuration

Enable

☒ **Enable Interface**

Description

WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 configuration

IPv4 address

192.168.1.253

X

/ 24

Gateway

None

- or add a new one.

If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Add new gateway:

Default gateway:

☒

Gateway Name:

GW_WAN_2

Gateway IPv4:

192.168.1.254

Description:

Interface wan Gateway

Save Gateway

Cancel

2ème solution : entrer cette passerelle par défaut avec la commande *System Routing*, onglet *Gateways* :

System: Gateways



Gateways Routes Groups				
Name	Interface	Gateway	Monitor IP	Description
GW_WAN_2 (default)	WAN	192.168.1.254	192.168.1.254	Interface wan Gateway

c – configuration d'une règle de filtrage

Fonctionnement des règles de filtrage sous PfSense :

1. On crée toujours les règles **en entrée** d'une interface donnée.

Exemple : pour autoriser une machine du LAN à envoyer des mails, il faut créer une règle d'autorisation en entrée de l'interface LAN, pour cette machine.

2. On ne crée une règle que pour autoriser ou interdire **des demandes initiées, émises par un ou plusieurs postes**, jamais pour les réponses (qui sont toutes **implicitement autorisées quelque soit le type de trafic, en entrée et en sortie sur toutes les interfaces**).

Exemple : pour autoriser une machine du LAN à consulter le Web, il faut créer une règle d'autorisation en entrée de l'interface LAN, pour cette machine ; la réponse HTTP du trafic retour en entrée de l'interface WAN (en en sortie sur l'interface LAN) vers cette machine est **implicitement autorisée**.

Ainsi lorsqu'une connexion est établie par un poste, cette connexion est ajoutée par le routeur dans sa table de gestion d'état des connexions (*established*) puisqu'il s'agit un parefeu stateful. **Le trafic retour est alors automatiquement autorisé par le firewall quelque soit le type de trafic, en entrée et en sortie sur toutes les interfaces.**

Les règles équivalentes à *permit tcp ... established*, et *permit icmp ... echo-reply* sont donc implicites et n'ont pas être écrites.

3. Les règles de NAT s'appliquent avant les règles de filtrage.

4. Les règles sont lues de bas en haut

5. Dès qu'une règle est évaluée positivement, elles est appliquée et l'évaluation des règles cesse. Le paquet est traité selon la règle.

6. Sur chaque interface, la dernière règle est toujours l'instruction implicite de blocage qui est automatiquement ajoutée et qui bloque l'ensemble du trafic.

Pour configurer une règle de filtrage, sélectionner la commande *Firewall Rules*, puis l'onglet correspondant à l'interface en entrée de laquelle on veut créer une règle de filtrage (LAN, WAN, ...).

Interface WAN :

Firewall: Rules



Floating WAN LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	RFC 1918 networks	*	*	*	*	*		Block private networks
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.
Click the button to add a new rule.

pass block reject log
 pass (disabled) block (disabled) reject (disabled) log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Par défaut, PfSense bloque tout trafic émis en entrée sur l'interface WAN (sauf bien sûr les réponses à des demandes établies par des postes du LAN qui sont toujours implicitement autorisées à entrer). Les règles concernant le WAN ne doivent être modifiées que pour laisser passer du trafic entrant (VPN, DMZ, ...).

Interface LAN :

Floating WAN LAN VPN IPsec OpenVPN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

Par défaut, PfSense autorise tout trafic en entrée sur l'interface LAN.

Concernant les trois règles par défaut du LAN, il ne faut surtout pas désactiver la règle *Anti-Lockout*, qui permet de se connecter à l'interface Web de PfSense via un autre PC (sous peine de reconfigurer voire de réinstaller PfSense).

La seconde et la troisième règles sont celles qui autorisent tout trafic.

Attention : l'emploi de *LAN net* dans la case *Source* n'autorise que les communications à partir des postes appartenant à la même plage d'adresses que celle de l'interface LAN !

S'il y a routeur, ou un switch de niveau 3, entre le PfSense et le réseau local, les réseaux accessibles par ce routeur n'appartiendront plus à la même plage d'adresses que celle de l'interface LAN. Les règles de filtrage en entrée de l'interface LAN les empêchent donc de communiquer avec l'extérieur, sauf si on modifie les règles comme suit pour l'interface LAN :

<div>FloatingWANLANVPNIPsecOpenVPN</div>										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
<input type="checkbox"/>		IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>		IPv6 *	*	*	*	*	*	none		Default allow LAN IPv6 to any rule

d -configuration de la redirection de port

Pour configurer le port forward, sélectionner la commande *Firewall NAT*, puis l'onglet *Port forward*.

e -configuration du serveur DHCP du routeur

Pour configurer le DHCP, sélectionner la commande *Services DHCP Server*.

f - commandes de configuration de relais DHCP

Pour configurer le relais DHCP, sélectionner la commande *Services DHCP Relay*.