BTS SIO Gap (option SISR)

Lycée Dominique Villars 05000 Gap

Conçu et rédigé en collaboration par les étudiants SIO SISR 2014 ;) et leur professeur G.Thomassin

Utiliser des routeurs cisco 1941

Table des matières:

Bibliographie **3**

Accès au routeur **4**

Par la console 4

Accès par ssh 5

par http/https 6

par telnet: 7

Reconfiguration du routeur en cas de perte du mot de passe **7**

La Commande Setup 9

Administrer le routeur. **10**

Voir la configuration actuelle 11

Enregistrer la configuration du routeur 11

Enregistrer config-->flash du routeur 11

Restaurer configuration à partir d'un fichier dans la mémoire flash du routeur 11

Export config Packet Tracer 12

Sauvegarder config ->trivial ftp: 12

Installation du démon tftpd sur un serveur linux 12

Sauvegarde tftp 13

Restaurer la configuration du routeur à partir de la sauvegarde sur le serveur 13

Export de packet tracer vers un vrai routeur avec serveur http 14

Activation d'une interface réseau du routeur 15

Configurer l'accès SSH à un routeur 15

Commandes de diagnostic STP 17

Routage 17

définir la passerelle par défaut d'un routeur 17

Entrer une route statique: 18

Activer le routage 18

Masquer un réseau interne 18

Redirection routeur vers dmz 20

Manque d'interface réseau: 20

Convertir Switchport en Routerport 21

Définir une interface virtuelle (sub address) 21

Routeur en serveur DHCP: 22

relais DHCP 23

Access Control List (ACL) 24

ACL Standard 24

Bloquer l'accès d'un réseau à un autre réseau: 24

ACL étendues 24

Solution de tolérance de panne pour passerelle 26

VRRP 26

GLBP 28

VPN 29

Agrégations de lien 32

Vlans 35

Divers 35

Etude de cas : 2 Cisco 1941 avec DHCP sur un seul routeur 36

Bibliographie

Une documentation ici :
http://www.cisco.com/en/US/docs/routers/access/1900/software/configuration/guide/routconf.html#wp1056709

Reset de la configuration :

http://www.cisco.com/en/US/products/ps5855/products_password_recovery09186a0080b3911d.shtml

Les possibles adresses ip, mot de passe et utilisateur initiales:

http://www.router-defaults.com/Router/Cisco--1941-ip-password-username

---

Accès au routeur

Il y a plusieurs façons de se connecter au routeur: soit par la console soit par ssh soit par http/https ou même telnet :(

Par la console

On utilise l'accès par la console lorsque le routeur n'a pas encore d'adresse ip ou que l'on n'a pas encore configuré l'accès par ssh.

Matériel utilisé: Un cable console (câble bleu db9-rj45) connecté d'un côté au port série de votre pc et de l'autre au port bleu marqué console sur le routeur.

Logiciel nécessaire: Si votre linux est en mode texte utilisez minicom ou screen sinon vous pouvez utiliser gtkterm.

Attention ces logiciels doivent être lancés en tant que root sinon l'accès au port série

du pc sera refusé par le système.

Accès par ssh

Branchez le port GE0/0 du routeur à un switch avec un câble droit et repartez du switch toujours avec un câble droit pour atteindre l'interface réseau de votre pc.

Vous pouvez aussi utiliser un câble croisé pour connecter directement le routeur à votre pc. Il se peut aussi que votre carte réseau soit capable de détecter qu'un croisement est nécessaire et l'effectue automatiquement.

Depuis votre pc si vous êtes en mode graphique, il vous faut ouvrir un terminal: konsole ou gnome-terminal.

Une fois le prompt obtenu:

ssh root@adresseIpDuRouteur

Il faut que votre configuration réseau vous permette d'atteindre le routeur.

Au besoin vous pouvez créer une interface virtuelle temporaire sur votre pc dans le réseau du routeur pour pouvoir communiquer avec lui:

```
#ifconfig eth0:1 10.10.10.5/24

#exit

$ping 10.10.10.1  …..success

$ ssh cisco@10.10.10.1
```

Le mot de passe initial est *cisco* il doit obligatoirement être modifié à la première connexion.

par http/https

Remarque: C'est décevant, maintient dans la médiocrité et dangereux au moins pour http.

```
Router# conf t

Router(config)# ip http server

Router(config)# ip http secure-server

Router(config)# ip http authentication local

Router(config)# ip http timeout-policy idle 600 life 86400 requests 10000

Router(config)# username yourname privilege 15 secret 0 yourpassword
```

par telnet:

c'est dangereux

```
Router(config)# line vty 0 4
```

```
Router(config-line)# privilege level 15
Router(config-line)# transport input telnet
Router(config-line)# exit
```

Reconfiguration du routeur en cas de perte du mot de passe

- Brancher le routeur à votre port série grâce au câble console (câble bleu db9-rj45) lancer gtkterm ou minicom ou screen en tant que root.

Les paramètres suivants de votre logiciel doivent être renseignés:

port série à utiliser: /dev/ttyS0

Bits:8

Parity: N

Stop bit:1

- Allumer le routeur, suivre le démarrage du routeur sur GtkTerm ou minicom et attendre le message

READ ONLY ROMON INITIALISED

“program load complete, entry point...”

- A l’affichage de ce message, il faut envoyer un signal “break” au routeur

appuyer

- soit sur CTRL + B si vous êtes sur gtkterm attention au b en majuscule
- soit F si vous êtes sous minicom

- Entrer “confreg 0x2142” en tant que rommon1>

rommon1>confreg 0x2142

- Entrer ensuite “reset” en tant que rommon2>, le routeur redémarre

- Une fois le routeur redémarré, vous pouvez soit suivre la procédure de configuration initiale en tapant Yes soit l’éviter en tapant No

Cas ou vous n’utilisez pas le programme de setup:

- En entrant “enable”, nous avons maintenant accès à l’invite de commande en tant qu’administrateur “Routeur#”

- Nous pouvons voir la configuration actuelle du routeur grâce à la commande *show running-config*

- Entrer “Routeur#conf t,

puis “Routeur(config)#enable secret <mot de passe>” pour choisir le mot de passe qui servira à l’accès à la connexion en tant qu’administrateur.

Router#enable secret passf101
IMPORTANT:

Ne pas oublier de remettre le confreg en 0x2102

Router(config) # config-register 0x2102

Router(config) # exit

- Enfin, entrez la commande

Router# *copy run start* pour sauvegarder la configuration

Changer le nom du routeur :

Router(config)#hostname <sonNom>

La Commande Setup

Elle permet de faire une configuration simplifiée des informations suivantes :

-hostname

-mot de passe (3 mots de passe sont à fournir)

-configuration de l’interface réseau d’administration

choix de l'interface, adresse ip et masque

-snmp(simple network management protocol inutile pour l'instant)

Administrer le routeur.

Affichage de la configuration des interfaces du Cisco :

cisco#enable
cisco#show interface GigabitEthernet <le numéro de votre interface>

Si l'on veut voir l'ensemble des configurations des interfaces

cisco#show ip interfaces brief

Voir la configuration actuelle

routeur# show run

On tape "espace" ensuite pour passer d'une page à l'autre.

Enregistrer la configuration du routeur

Pour que la configuration soit retrouvée après redémarrage du routeur, il faut en mode enable sauver la configuration en tapant : copy run start et valider lorsque le routeur propose de sauver la configuration dans le fichier startup-config.

Enregistrer config-->flash du routeur

Sauvegarde la configuration courante dans un fichier appelé “backupconfig”
routeur#copy running-config flash:backupconfig

Restaurer configuration à partir d’un fichier dans la mémoire flash du routeur

Remplace la configuration courante par celle du fichier “backupconfig”
copy flash:backupconfig running-config

Export config *Packet Tracer*

Sur Packet Tracer: Sélectionnez le routeur allez dans config, puis export la config qui

s'appelle "running config" et faire une sauvegarde dans un dossier sur votre pc.

Ensuite toujours sur Packet Tracer, créer un autre routeur du même modèle, aller sur le routeur dans config puis cliquez sur "Merge" et sélectionner le fichier que nous avons précédemment sauvegardé sur le pc.

Sauvegarder config ->trivial ftp:

Installation du démon tftpd sur un serveur linux

pc#ssh root@adServTftp

serv#apt-get install tftpd

serv#mkdir /srv/tftp

serv#vim nomFichier // on crée le fichier de sauvegarde vide pour le moment

esc:wq // on peut y copier la config du routeur de packet tracer

serv#chmod -R u+rwx /srv/tftp

serv#chown -R nobody /srv/tftp

serv#/etc/init.d/openbsd-inetd restart

Sauvegarde tftp

pc#ssh cisco@adRouter

cisco>enable

cisco#copy run tftp // on sauvegarde la config dans le fichier du serveur TFTP

Address or name of remote host [? ipserveur

Destination filename [cisco-confg]? nomFichier //le nom du fichier doit etre le meme que celui créé sur le serveur TFTP

nettoyage pour réutilisation

pc# ssh root@adServTftp

serv#vim /srv/tftp/nomFichier *//supprimer les lignes avec **'aaa'** '*

Restaurer la configuration du routeur à partir de la sauvegarde sur le serveur

pc#ssh en cisco@adRouter

cisco>enable

cisco#copy tftp run // on prend la sauvegarde comme configuration

Address or name of remote host [? ipserveur

Destination filename [cisco-confg]? nomFichier

Export de packet tracer vers un vrai routeur avec serveur http

Sur Packet Tracer: Aller sur le routeur allez dans config, puis export la config qui s'appelle "running config" et faire une sauvegarde.

Vous la copiez ensuite avec scp dans le dossier publié d'un serveur web /var/www/htdocs/mesConfigs/

Ensuite connectez vous sur le routeur puis tapez les commandes suivantes:
enable
copy http://ipdevotreserveur/mesConfigs/nomdevotresauvegarde running-config

Tester et si c'est ok
copy run start

Activation d'une interface réseau du routeur

//on configure depuis le terminal

rpiolit#conf t

//on choisit l'interface à configurer

rpiolit(config)#interface gigabitEthernet0/1/0

//on lui donne une adresse ip

piolit(config-if)# ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy

où xxx.xxx.xxx.xxx est une adresse ipv4 et yyy.yyy.yyy.yyy est un masque de réseau

//on la démarre

rpiolit(config-if)#no shutdown

Puis on n'oublie pas d'enregistrer/écrire la configuration en mémoire ou dans la mémoire flash de démarrage.

Configurer l'accès SSH à un routeur

Router>enable

Password:

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname <nomDuRouteur>

cisco(config)#ip domain-name btsinfogap.org

cisco(config)#crypto key generate rsa general-keys modulus 2048

The name for the keys will be: rNomDeMontagne

% The key modulus size is 2048 bits

% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

cisco(config)#ip ssh time-out 60

cisco(config)#ip ssh authentication-retries 3

cisco(config)#ip ssh version 2

cisco(config)#line vty 0 4

cisco(config-line)#transport input ssh telnet

cisco(config-line)#exit

cisco(config)#aaa new-model

ici on crée un user et on lui affecte un mot de passe

cisco(config)#username root password <sonMotDePasse>

cisco(config)#exit

sans oublier le copy run start sinon c'est à refaire.

cisco# copy run start

Commandes de diagnostic STP

Pour le diagnostic STP d'une interface :

#show spanning-tree interface *interface*

Pour des informations détaillées :

#show spanning-tree detail

Pour vérifier uniquement les interfaces actives :

#show spanning-tree active

Activer le spanning tree protocole sur les ports du module switch

#spanning-tree mode rapid-pvst

Routage

définir la passerelle par défaut d'un routeur

Pour permettre au routeur d'accéder à internet il faut spécifier au routeur sa passerelle par défaut :
Ici la passerelle par défaut est 172.16.255.254

rpiolit(conf t)#ip route 0.0.0.0 0.0.0.0 172.16.255.254

Entrer une route statique:

ip route réseau masque passerelle

exemple:

routerSio(config)#ip route 192.168.0.0 255.255.255.0 193.254.19.2

qui se lit ainsi: pour atteindre le réseau 192.168.0.0/24 on utilisera la passerelle qui a pour adresse 193.254.19.2

Activer le routage

routerSio(config)#ip routing

Masquer un réseau interne

Redirection d'un paquet et masquerading

1) Configuration de l'interface externe (côté internet)

interface externe ip nat outside

//si l'interface externe est g0/0

router(config)# interface g0/0

router(config-if)#ip nat outside

router(config-if)#end

2) puis configurer l'interface interne avec un **ip nat inside**

//activer le masquerading

//le 1 est l'identifiant de la liste il s'agit d'une source list standard et son numéro doit être donc inférieur à 100

ip nat inside source list <1> interface <nom de l'interface externe> overload

exemple:

si la g0/0 est l'interface externe:

routeur(config)#ip nat inside source list 1 interface g0/0 overload

//il faut autoriser les adresses locales à être natées (remplacées, masquées)

//on définit donc la source list 1

Router(config)#ip access-list standard 1

Je rappelle que 1 est l'identifiant de la liste.

Router(config-std-nacl)#permit 10.np.ne.0 0.0.0.255

//exemple:pour le réseau à masquer 10.25.15.0/24 on écrit 10.25.15.0 0.0.0.255

Router(config-std-nacl)#deny any

Router(config-std-nacl)#end

Router(config)#exit

Router#write memory

Router# copy run start

Redirection routeur vers dmz

DMZ : Une DMZ est un réseau interne à l'intérieur duquel se trouvent des serveurs proposant des services à l'extérieur.

Exemple : Lorsque le routeur reçoit une requête HTTP sur son interface externe il doit la transmettre au serveur web caché dans la DMZ puis lors de la réponse au serveur web remplacer dans le paquet l'adresse du serveur par son ip externe.

WAN |----------|ROUTEUR |----------| DMZ

syntaxe de redirection des requêtes vers un serveur de la dmz:

ip nat inside source static tcp adresseDuServeur port adresse du routeur port

CISCO (config)# ip nat inside source static tcp 192.168.52.51 80 172.16.55.50 80

Evidemment on peut avoir des ports différents sur le routeur et le serveur

---

Manque d'interface réseau:

Convertir Switchport en Routerport

Vous avez un module switch dans votre routeur et vous manquez d'interfaces routables voici la solution.

interface vlan 500

ip address 172.16.50.1 255.255.240.0

int f0/1/0

switchport mode access

switchport access vlan 500

no shutdown

Définir une interface virtuelle (sub address)

Vous n'avez pas de module switch mais vous avez un switch en plus du routeur.

Sur le routeur on crée une sous-interface de l'interface physique qui est connectée au switch.

Le switch a son port connecté au routeur en trunk.

Par contre un des ports sera mis en mode access dans le même vlan que la sous

interface. Plus qu'à y brancher un poste ou un switch il sera dans le nouveau réseau.

Config du routeur:

interface f0/0.1

ip address xxx.xxx.xxx.xxx

Il faut ensuite la mettre dans un vlan ici 500

enc dot1q 500

et la relier à un switch bien configuré(vlan)

à compléter...

Routeur en serveur DHCP:

---

http://www.manzainfo.fr/index.php/reseaux/cisco/53-configurer-dhcp-sur-un-routeur-cisco#.UkRCQYZT7A1

Configuration du routeur (1941) :

```
#Configuration mode Terminal
Router>enable
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
#Paramétrage de l'interface réseau 0/0
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
#Création d'un Pool DHCP (nom : pool dhcp1)
Router(config-if)#ip dhcp pool pool dhcp1
#Définition du réseau ou le DHCP délivrera les adresses
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
#Adresse IP de la passerelle par défaut
Router(dhcp-config)#default-router 192.168.10.1
#Adresse IP du ou des serveurs DNS
Router(dhcp-config)#dns-server 192.168.10.2
#On quitte la configuration du pool
Router(dhcp-config)#exit
#Ici on empêche le DHCP de fournir les 10 premières IP. (pour une réservation par exemple).
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
```

relais DHCP

Sur le routeur qui doit relayer les requêtes dhcp des clients on renseigne l'adresse ip du serveur à qui il doit les transmettre comme ceci:

routeur(config)#ip helper-address <ip du serveur dhcp>

Access Control List (ACL)

Elles peuvent être standard ou étendues.

ACL Standard

Bloquer l'accès d'un réseau à un autre réseau:

Le réseau Organisateurs ne souhaite pas que les visiteurs puissent y pénétrer:

Router(config)#access-list 1 deny 172.31.1.0 0.0.0.255 *(liste réseau visiteurs)*

Router(config)#interface fa0/1 *(interface du réseau 10.10.10.0 Organisateurs)*

Router(config-if)#ip access-group 1 out *(bloque la liste du réseau visiteurs)*

Router(config-if)#exit

ACL étendues

Elles permettent de définir les protocoles et les ports utilisés.

cours sur les acl:

http://www.nolot.eu/Download/Cours/reseaux/m2pro/ACL-Cisco.pdf

G0/0 → interface 172.16.x.x (externe) ip nat outside

G0/1 → interface 10.2.x.x (serveurs)

G0/1/0 → interface192.168.x.x (clients)

 # Appliquer l'ACL client sur l'interface g0/0

ip nat inside source list client interface GigabitEthernet0/0 overload

 # Appliquer l'ACL serveur sur l'interface g0/0

ip nat inside source list serveur interface GigabitEthernet0/0 overload

 # Passerelle du routeur

ip route 0.0.0.0 0.0.0.0 172.16.48.152

 # ACL du réseau client qui autorise toutes les communications sur le port 80 ou le port 53 ou l'icmp

ip access-list extended client

permit tcp 192.168.0.0 0.0.0.255 host 0.0.0.0 eq www

permit tcp 192.168.0.0 0.0.0.255 host 0.0.0.0 eq domain

permit icmp any any

 # ACL du réseau serveur qui autorise toutes les communications ip

ip access-list extended serveur

permit ip 10.2.0.0 0.0.255.255 any

Solution de tolérance de panne pour passerelle

Nous verrons ici deux méthodes vrrp et glbp

VRRP

virtual redundancy routing protocol

Activer le protocole Vrrp

Voilà comment se déroule la mise en place du protocole VRRP sur une interface:

Router(config)#interface <interface>

Router(config-if)#ip address <ip> < masque>

Router(config-if)#no shutdown

Router(config-if)#vrrp 1 priority <entre 1 et 255> (200 pour R1 et 100 pour R2)

Router(config-if)#vrrp 1 preempt

Configuration de R1 :

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ip address 10.10.10.xx 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#vrrp 1 ip <définir une ip virtuelle>

Router(config-if)#vrrp 1 priority 200 <entre 1 et 255> (200 pour R1 et 100 pour R2)

Router(config-if)#vrrp 1 preempt

Configuration de R2 :

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ip address 10.10.10.xx 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#vrrp 1 ip <définir une ip virtuelle la même que R1>

Router(config-if)#vrrp 1 priority 100 <entre 1 et 255> (200 pour R1 et 100 pour R2)

Router(config-if)#vrrp 1 preempt

R1(config-if)# **vrrp 10 timers advertise 3** **!**Réglage du timer “advertise”

R1(config-if)# **vrrp 10 timers learn** ! Réglage du timer “learn”

R1(config-if)# **vrrp 10 enable** ! Facultatif

Vérification de la configuration :

Routeur# show vrrp

Ne pas oublier configurer les routes sur les routeurs et les postes

GLBP

Activer le protocole Glbp:

glbp permet le load balancing pour routeur

http://www.itsyourip.com/cisco/how-to-configure-glbp-in-cisco-ios-routers/

Routeur 1:

Cisco(config)#interface g0/1

Cisco(config-if)#ip address 10.10.10.x 255.255.255.0

 # Définir une ip virtuelle

Cisco(config-if)#glbp 1 ip <ip virtuelle>

 # Intervalle de temps de 5 secondes entre lesquels la passerelle virtuelle active redirige les clients vers un expéditeur virtuel actif dans le cas d'un échec

 # 3600 secondes pour régler le délai d'attente en secondes avant qu'un expéditeur virtuel secondaire devient invalide

Cisco(config-if)# glbp 1 timers redirect 5 3600

Cisco(config-if)#glbp 1 preempt

 # Délai minimum

Cisco(config-if)# glbp 1 preempt delay minimum 60

Cisco(config-if)#glbp 1 load-balancing round-robin

Cisco(config-if)#glbp 1 priority 150

Routeur 2:

Cisco(config)#interface g0/1

Cisco(config-if)#ip address 10.10.10.x 255.255.255.0

 # Définir une ip virtuelle

Cisco(config-if)#glbp 1 ip <ip virtuelle>

 # Intervalle de temps de 5 secondes entre lesquels la passerelle virtuelle active redirige les clients vers un expéditeur virtuel actif dans le cas d'un échec

 # 3600 secondes pour régler le délai d'attente en secondes avant qu'un expéditeur virtuel secondaire devient invalide

Cisco(config-if)# glbp 1 timers redirect 5 3600

Cisco(config-if)#glbp 1 preempt

 # Délai minimum

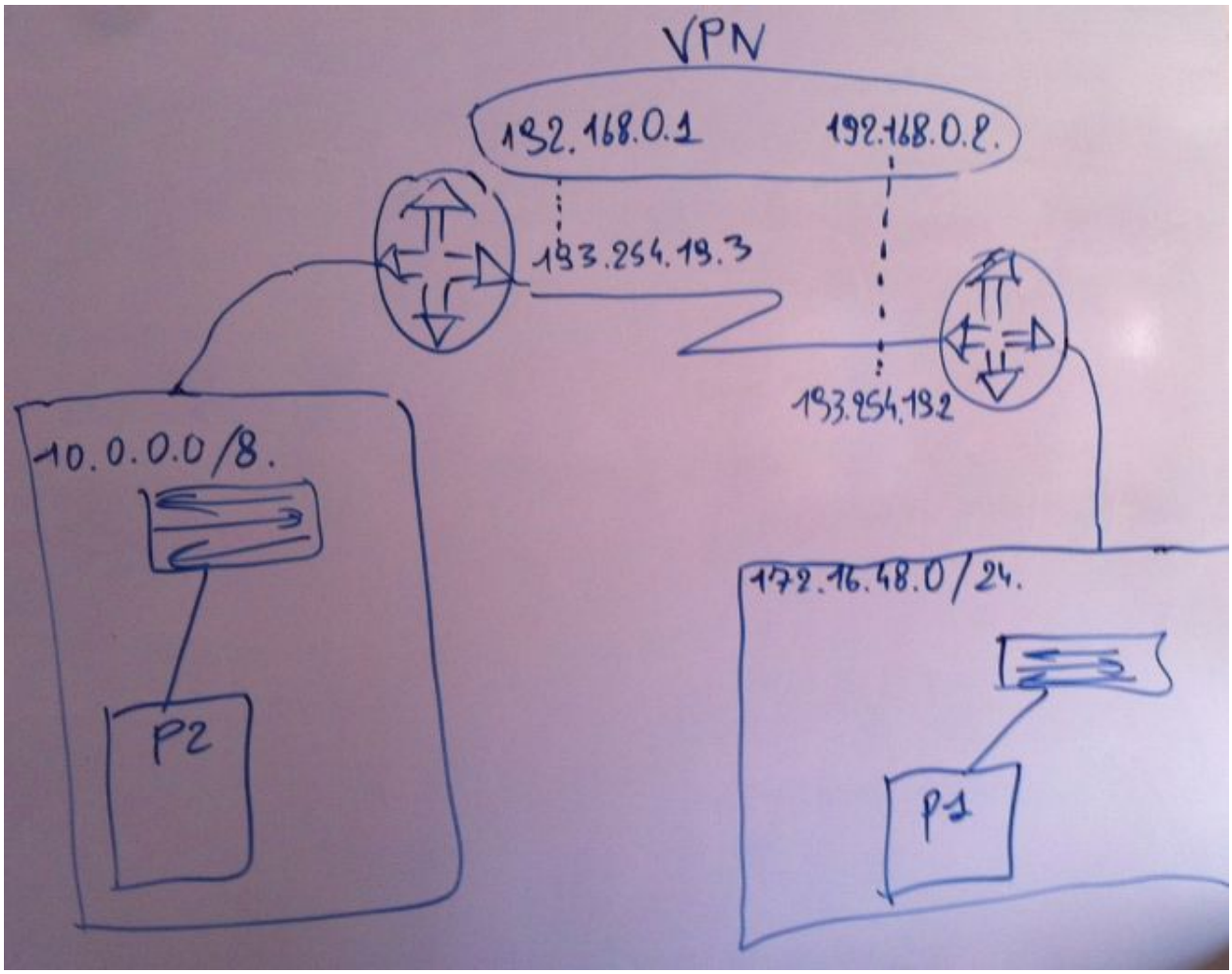
Cisco(config-if)# glbp 1 preempt delay minimum 60

Cisco(config-if)#glbp 1 load-balancing round-robin

Ne pas oublier configurer les routes sur les routeurs et les postes

---

VPN



<u>On active les interfaces serial sur les deux routeurs Cisco</u>

rpiolit#enable

rpiolit#conf t

Enter configuration commands, one per line. End with CNTL/Z.

rpiolit(config)#int s0/0/0

rpiolit(config-if)#no shutdown

rpiolit(config-if)#ip address 193.254.19.2 pour l'autre routeur 193.254.19.3

On test le ping entre les deux interfaces sérial

Mise en place du VPN sur les deux interfaces serial

rpiolit(config-if)#

Configure a Site-to-Site GRE Tunnel

suivre les 9 étapes du lien ci-dessous:

chercher Configure a Site-to-Site GRE Tunnel dans

http://www.cisco.com/en/US/docs/routers/access/1900/software/configuration/guide/Secconf1.html#wp1056232

Licence : (il faut l'activer)

license boot module c1900 technology-package securityk9

Agrégations de lien

L'objectif:

Doubler la bande passante entre deux serveurs qui par exemple sont synchronisés et nécessitent donc un meilleur débit.

Sur cisco deux protocoles permettent l'agrégation de lien:

Link agrégation control protocol (ouvert)
http://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html et

http://www.cisco.com/c/en/us/td/docs/server_nw_virtual/2-10-0_release/configuration/guide/swcg210/3link.html#wp951304

ou pagp (propriétaire cisco).

Un peu de culture:

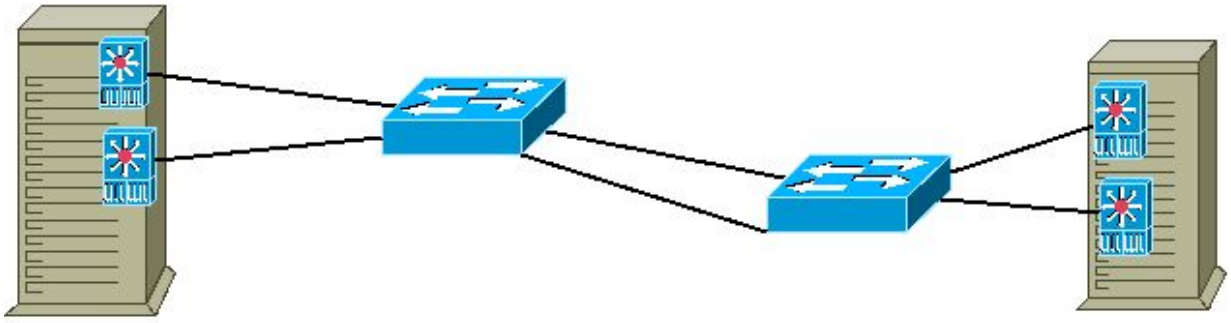
Link Aggregation Control Protocol sur wikipédia

LACP est un protocole standardisé par l'IEEE et est implémenté par différents constructeurs. Il fournit un mécanisme permettant de contrôler le groupement de plusieurs ports physiques en un canal logique de communication.
Le principe de fonctionnement consiste à émettre des paquets LACP vers l'équipement partenaire, directement connecté et configuré pour utiliser LACP. Le mécanisme LACP

va permettre d'identifier si l'équipement en face prend LACP en charge, et groupera les ports configurés de manière similaire (vitesse, mode duplex, VLAN, trunk de vlan, etc.)
Un équipement configuré pour utiliser LACP peut fonctionner en trois modes :
passif : l'équipement n'initiera pas de négociation LACP. Il répondra uniquement aux sollicitations des équipements « partenaires ».
actif : l'équipement initiera les négociations LACP.
on : l'équipement suppose que l'équipement partenaire est également dans ce mode et fera de l'agrégation de liens
Port Aggregation Protocol (PAgP)PAgP est un protocole propriétaire Cisco, de ce fait disponible sur les commutateurs Cisco ainsi que sur les équipements disposant de la licence adéquate. Son utilisation permet de faciliter et d'automatiser la configuration des agrégats de liens (EtherChannel chez Cisco) en échangeant les informations nécessaires entre les ports Ethernet, à la manière de LACP.
Un équipement configuré pour utiliser PAgP peut fonctionner en trois modes :
auto : négociation passive avec le second équipement
desirable : négociation active avec le second équipement
on : aucun protocole n'est utilisé, on suppose que le second équipement est configuré pour utiliser l'agrégation de liens.

Le matériel

- 2 serveurs linux multidomiciliés dont les interfaces sont agrégées en une seule (n'est alors visible qu'une seule adresse ip).
- 6 câbles
- 2 switchs cisco ou compatibles LACP (un seul est nécessaire mais on suppose les serveurs dans deux salles différentes chacune étant distribuée par un switch.



TAF:

a) Mettre en place un service apache sur un des serveurs et placer dans le répertoire public un fichier dont la taille permettra de bien mesurer le débit entre les deux machines.

b) Depuis le client mesurer le temps nécessaire à la récupération du fichier sur le serveur.

c) Configurer le bounding sur les interfaces réseau des deux machines linux.

d) Configurer les ports des switchs(par paires) en agrégation de lien

e) tester le nouveau débit.

un tuto:

http://www.nolot.eu/Download/Cours/reseaux/m2pro/CRC-0809/crc-cours4-etherchannel.pdf

---

Vlans

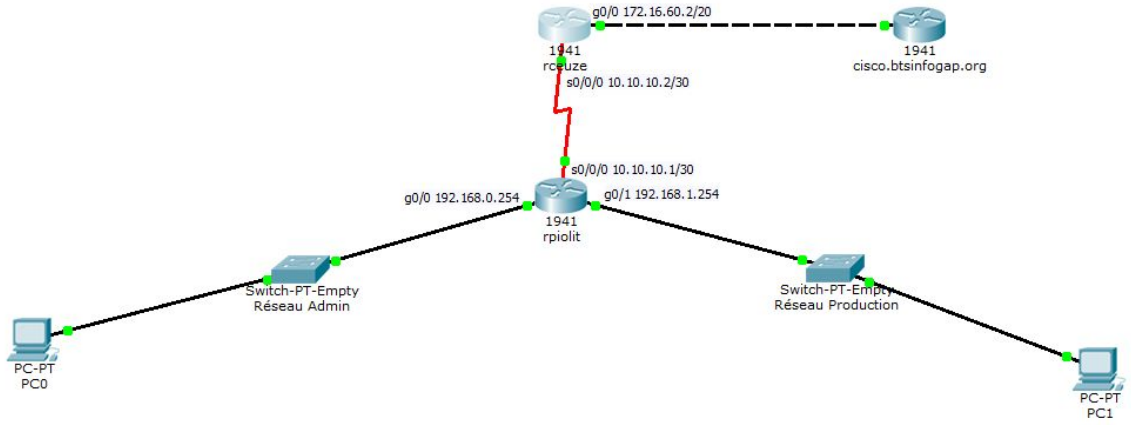
http://www.clemanet.com/switch-vlan-cisco.php

Divers

Commande magique snmp

if index percist

Etude de cas : 2 Cisco 1941 avec DHCP sur un seul routeur



On applique les “pool” dhcp sur le cisco **tout en haut** :

ip dhcp pool pooldhcpradmin

network 192.168.0.0 255.255.255.0

default-router 192.168.0.254

dns-server 8.8.8.8

ip dhcp pool pooldhcprprod

network 192.168.1.0 255.255.255.0

default-router 192.168.1.254

dns-server 8.8.8.8

Puis on configure le NAT

interface GigabitEthernet0/0

ip nat outside

interface Serial0/0/0

ip nat inside

ip nat inside source list 1 interface GigabitEthernet0/0 overload

access-list 1 permit any < Pas très recommandé mais fonctionne.

et on rajoute les lignes pour que les réseaux communiquent :

ip route 192.168.0.0 255.255.255.0 10.10.10.1

ip route 192.168.1.0 255.255.255.0 10.10.10.1

On active le DHCP helper **sur le routeur au milieu** :

interface GigabitEthernet0/0

ip address 192.168.0.254 255.255.255.0

ip helper-address 10.10.10.2 <- Correspond au serveur DHCP (rpiolit sur le schéma)

interface GigabitEthernet0/1

ip address 192.168.1.254 255.255.255.0

ip helper-address 10.10.10.2 <- Correspond au serveur DHCP (rpiolit sur le schéma)

Et on rajoute la route par défaut pour rejoindre internet

ip route 0.0.0.0 0.0.0.0 10.10.10.2

Les clients ont accès au net, et disposent d'un serveur DHCP.