DUMONT ADRIEN

IRIS

2016-2017

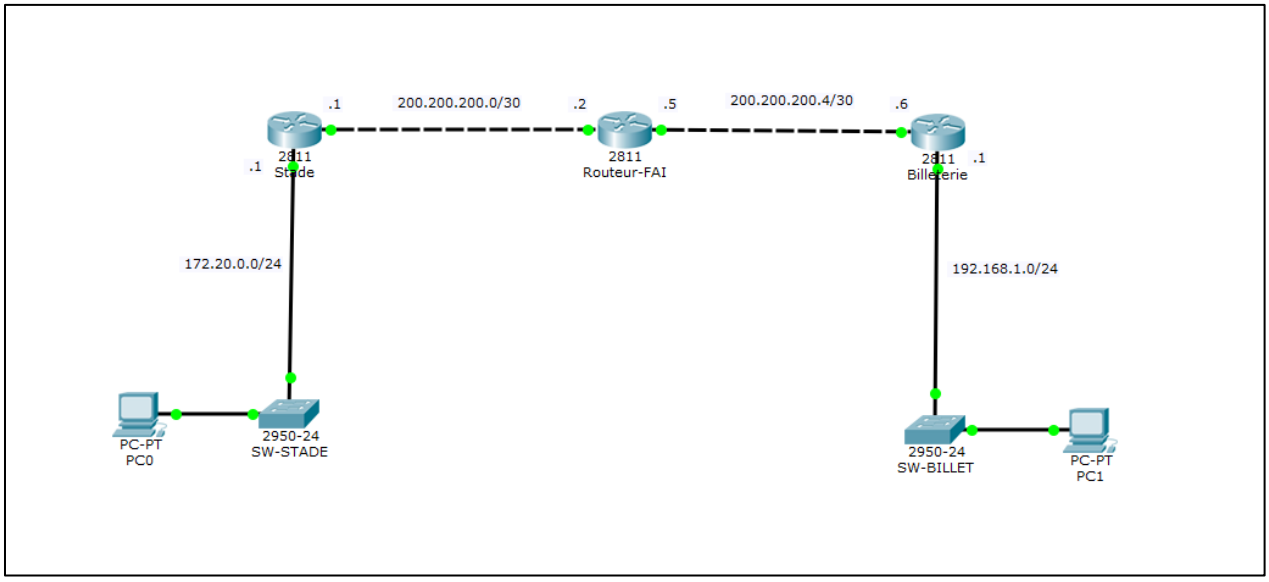
Sommaire

1-Cahier des charges

StadiumCompany compte actuellement deux sites distants : une billetterie en centre-ville et une boutique de souvenirs dans une galerie marchande locale. Les sites distants sont connectés via un service DSL à un FAI local.

Pour rendre les communications plus simple et plus sécurisé, on souhaite mettre en place un VPN entre le stade et la billeterie.

Un shéma du projet a été realisé sur Cisco Packet tracer :



Le VPN sera mis en place entre le Routeur R1 « Stade » et le routeur R2 « Billeterie » afin de permettre la communication entre les deux réseaux locaux du stade et de la billeterie.

2-Solutions

Comparatif des solutions

VPN

Il existe plusieurs types de VPN fonctionnant sur différentes couches réseau, voici les VPN que nous pouvons mettre en place sur un serveur dédié ou à la maison :

PPTP

Facile à mettre en place, mais beaucoup d'inconvénients liés à la lourdeur du protocole de transport GRE, le matériel réseau (routeur ADSL, wifi, doit être compatible avec le PPTP)

Ipsec

Plus efficace que le PPTP en termes de performance, mais aussi très contraignant au niveau de la mise en place

OpenVPN

La mise en place est plus compliquez que Ipsec et PPTP, mais son utilisation est très souple.

Routage

EIGRP

EIGRP est un protocole de routage interne, il est capable de calculer une route de secours.
Le protocole va donc garder deux routes pour chaque destination : la route principale (celle avec la meilleure métrique), et une route secondaire.
Nous verrons plus tard qu'il faut remplir une condition pour garder une route de secours.
Autre avantage, EIGRP est capable de faire du Load Balancing s'il connait plusieurs liens équivalents.
L'EIGRP est peu gourmand en ressource, et très rapide.

OSPF

Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau.
En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur.

Choix de solutions

VPN

Nous allons utiliser le protocole IPSEC pour mettre en place le VPN, ce choix a été fait par soucis de performance.

Le protocole IPSEC est plus efficace que PPTP mais plus compliqué à mettre en place, cependant, le projet de liaison entre le stade et la billeterie n'est pas un projet très lourd, l'infrastructure est assez simple pour se tourner vers IPSEC

OpenVPN est trop compliqué à mettre en place pour un projet de ce type.

Routage

Le routage sera effectué grace au protocole EIGRP, cette solution présente des avantages en terme de sécurité et de continuité de service avec la gestion des routes de secours.

EIGRP consomme peu de bande passante et ce toujours grâce à une basse fréquence de ses mises à jour des tables de routage, cette fréquence de mise à jour est idéale dans une petite infrastructure comme celle-ci car les modifications de la topologie seront rare.

3- Projet

Objectif et but du projet

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe.

Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions sans tenir compte des objectifs commerciaux généraux ni de la conception de l'infrastructure à long terme. Certains projets ont été menés sans souci des conditions de bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe.

À présent, la direction de StadiumCompany veut améliorer la satisfaction des clients en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction de StadiumCompany sait qu'elle ne dispose pas du savoir-faire voulu en matière de réseau pour prendre en charge cette mise à niveau. StadiumCompany décide de faire appel à des consultants réseau pour prendre en charge la conception, la gestion du projet et sa mise en œuvre. Ce projet sera mis en œuvre suivant trois phases.

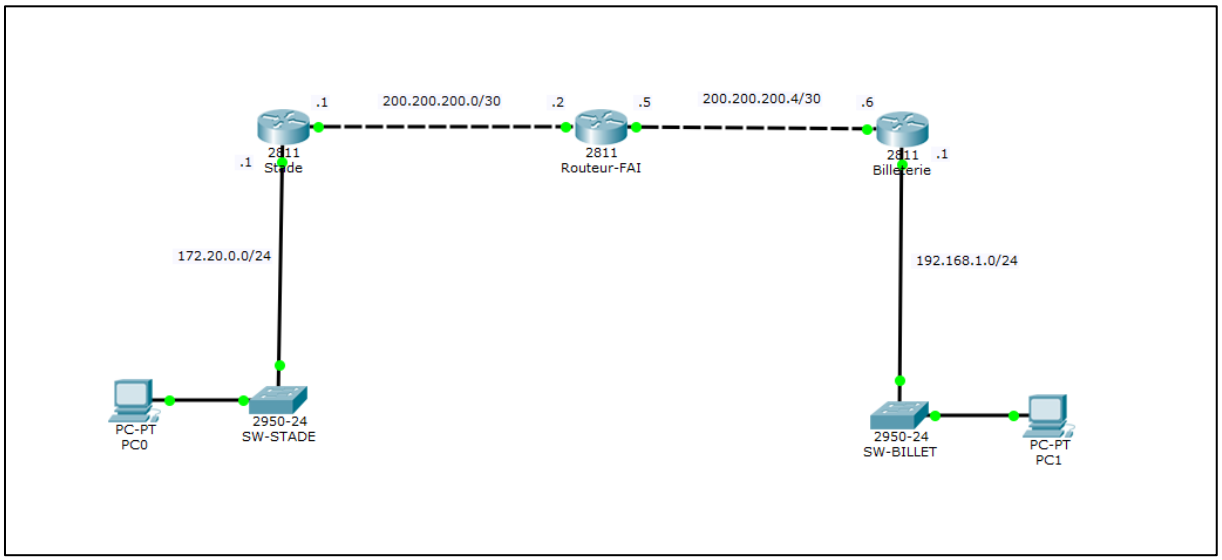
La première phase consiste à planifier le projet et préparer la conception réseau de haut niveau.

La deuxième phase consiste à développer la conception réseau détaillée.

La troisième phase consiste à mettre en œuvre la conception.

Shema du projet

Le schéma a été realisé sur CiscoPacket tracer, il permet de se rendre compte de la topologie réseau du projet.



Configuration des interfaces

Routeur R1

Le routeur R1 correspond au routeur du stade.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip address 172.20.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip address 200.200.200.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

Routeur R2

Le routeur R2 correspond au routeur FAI

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 200.200.200.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface FastEthernet 0/1
R2(config-if)#ip address 200.200.200.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

Routeur R3

Le routeur R3 correspond au routeur de la billetrrie

```
R3(config)#interface FastEthernet 0/0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface FastEthernet 0/1
R3(config-if)#ip address 200.200.200.6  255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
```

Routage EIGRP

Routeur R1

```
R1(config)#router eigrp 1
R1(config-router)#network 172.20.0.0 0.0.0.255
R1(config-router)#network 200.200.200.0 0.0.0.3
R1(config-router)#exit
```

Routeur R2

```
R2(config)#router eigrp 1
R2(config-router)#network 200.200.200.0 0.0.0.3
R2(config-router)#network 200.200.200.4 0.0.0.3
R2(config-router)#exit
```

Routeur R3

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.1.0 0.0.0.255
R3(config-router)#network 200.200.200.4 0.0.0.3
R3(config-router)#exit
```

Configuration VPN

Il faut savoir que le VPN se configure juste sur les Routeurs d'extrémités dans notre cas R1 et R3, aucune modification à faire sur R2.

Routeur R1

Activation de la fonction crypto

R1(config)#crypto isakmp enable

Configuration de la police de securité

R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit

Configuration de la clé

R1(config)#crypto isakmp key iris123 address 200.200.200.6

Options de transformations des données

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1(config)#crypto ipsec security-association lifetime seconds 1800

Access Control List (ACL)

R1(config)#access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0255

Association de l'ACL à la crypto map

R1(config)#crypto map stade 10 ipsec-isakmp
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit

Association crypto map et interface de sortie

R1(config)#interface fastEthernet 0/1
R1(config-if)#crypto map stade
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

Routeur R3

Activation de la fonction crypto

R3(config)#crypto isakmp enable

Configuration de la police de securité

R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#hash md5
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit

Configuration de la clé

R3(config)#crypto isakmp key iris123 address 200.200.200.1

Options de transformations des données

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(config)#crypto ipsec security-association lifetime seconds 1800

Access Control List (ACL)

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0. 0.0.0.255

Association de l'ACL à la crypto map

R3(config)#crypto map billetterie 10 ipsec-isakmp
R3(config-crypto-map)#set peer 200.200.200.1
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#exit

Association crypto map et interface de sortie

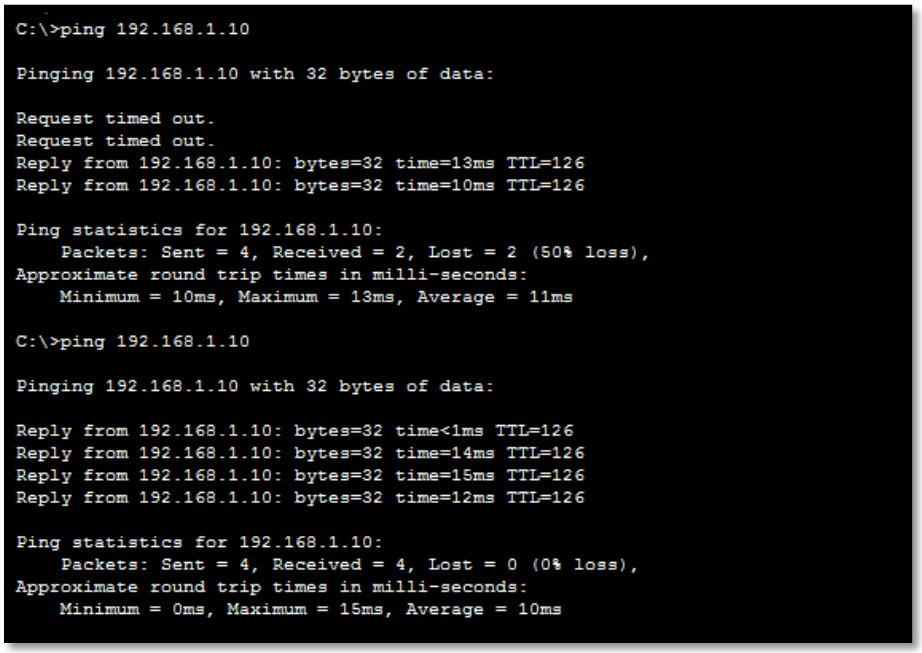
R3(config)#interface FastEthernet 0/1
R3(config-if)#crypto map billetterie
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

Validation

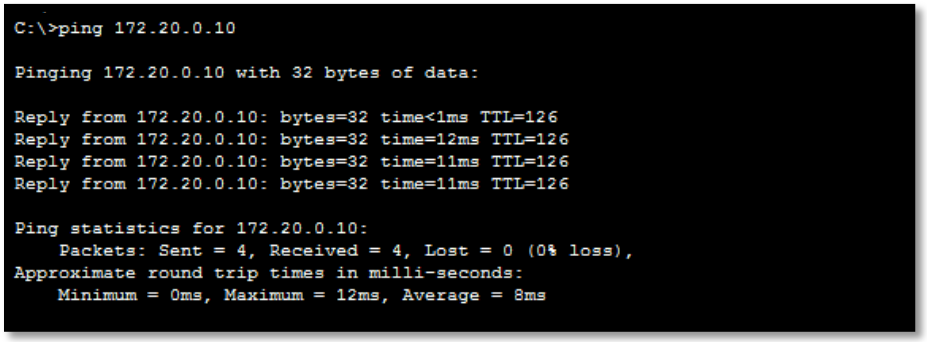
Ping

Un PC est connecté au réseau local Stade (172.20.0.0) avec l'adresse IP 172.20.0.10, un autre PC lui est connecté au réseau local Billeterie (192.168.1.0) avec l'adresse IP 192.168.1.10.

Un premier ping est effectué depuis le PC du Stade vers le PC de la billeterie :



Un deuxiéme ping est effectué dans l'autre sens, du PC billeterie vers le PC Stade



Informations retournées par le VPN

Routeur R1

```
R1#show crypto ipsec transform-set

Transform set 50: {    { esp-3des esp-sha-hmac  }

  will negotiate = { Tunnel,  },
```

Routeur R3

```
R1#show crypto ipsec transform-set

Transform set 50: {    { esp-3des esp-sha-hmac  }

  will negotiate = { Tunnel,  },
```

Verification map

Routeur R1

```
R3#show crypto map
Crypto Map billeterie 10 ipsec-isakmp
      Peer = 200.200.200.1
      Extended IP access list 101
         access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
      Current peer: 200.200.200.1
      Security association lifetime: 4608000 kilobytes/900 seconds
      PFS (Y/N): N
      Transform sets={
            50,
      }
      Interfaces using crypto map billeterie:
            FastEthernet0/1
```

Routeur R3

```
R3#show crypto map
Crypto Map billeterie 10 ipsec-isakmp
      Peer = 200.200.200.1
      Extended IP access list 101
         access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
      Current peer: 200.200.200.1
      Security association lifetime: 4608000 kilobytes/900 seconds
      PFS (Y/N): N
      Transform sets={
            50,
      }
      Interfaces using crypto map billeterie:
            FastEthernet0/1
```

Vérification des association de sécurité (SA)

Routeur R1

R1#show crypto ipsec sa

```
interface: FastEthernet0/1
    Crypto map tag: stade, local addr 200.200.200.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (172.20.0.0/255.255.255.0/0/0)
  remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  current_peer 200.200.200.6 port 500
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 0
  #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

    local crypto endpt.: 200.200.200.1, remote crypto endpt.:200.200.200.6
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
    current outbound spi: 0x0(0)
```

R1#show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
200.200.200.6   200.200.200.1   QM_IDLE           1006    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Routeur R3

R3#show crypto ipsec sa

```
interface: FastEthernet0/1
    Crypto map tag: billeterie, local addr 200.200.200.6

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.20.0.0/255.255.255.0/0/0)
   current_peer 200.200.200.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 0
   #pkts decaps: 22, #pkts decrypt: 22, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 200.200.200.6, remote crypto endpt.:200.200.200.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)
```

R3#show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
200.200.200.1   200.200.200.6   QM_IDLE           1058    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

4-Conclusion

Pour conclure, ce projet nous a permis d'avoir une approche un peu moins théorique et plus axée dans la pratique en configurant du matériel cisco, sur des problématique d'entreprise comme la mise en place de VPN entre routeur

De plus, ce projet nous a permis de revoir et d'apprendre certaines notions sur les configurations routeur et protocole de routage

Ce projet nous a aussi permis de mettre en application les différents cours sur les ACL

Enfin, nous avons pu apprendre à communiquer et à travailler en groupe, en séparant les taches et en s'organisant pour au final fournir un travail équivalent chacun de notre côté.

5-Annexe

Show run R1

```
R1#show run
Building configuration...
Current configuration : 1159 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
ip cef
no ipv6 cef
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key iris123 address 200.200.200.6
crypto ipsec security-association lifetime seconds 1800
crypto ipsec transform-set 50 esp-3des esp-md5-hmac
crypto map stade 10 ipsec-isakmp
 set peer 200.200.200.6
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
spanning-tree mode pvst
interface FastEthernet0/0
 ip address 172.20.0.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 200.200.200.1 255.255.255.252
 duplex auto
 speed auto
 crypto map stade
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 172.20.0.0 0.0.0.255
 network 200.200.200.0 0.0.0.3
 auto-summary
ip classless
ip flow-export version 9
access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
line con 0
line aux 0
line vty 0 4
 login
end
```

Show run R2

```
R2#show run
Building configuration...
Current configuration : 674 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
ip cef
no ipv6 cef
spanning-tree mode pvst
interface FastEthernet0/0
 ip address 200.200.200.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 200.200.200.5 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 200.200.200.0 0.0.0.3
 network 200.200.200.4 0.0.0.3
 auto-summary
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

Show run R3

```
R3#show run
Building configuration...
Current configuration : 1161 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R3
ip cef
no ipv6 cef
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key iris123 address 200.200.200.1
crypto ipsec security-association lifetime seconds 1800
crypto ipsec transform-set 50 esp-3des esp-md5-hmac
crypto map billeterie 10 ipsec-isakmp
 set peer 200.200.200.1
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
spanning-tree mode pvst
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 200.200.200.6 255.255.255.252
 duplex auto
 speed auto
 crypto map billeterie
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 192.168.1.0
 network 200.200.200.4 0.0.0.3
 auto-summary
ip classless
ip flow-export version 9
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
line con 0
line aux 0
line vty 0 4
 login
end
```