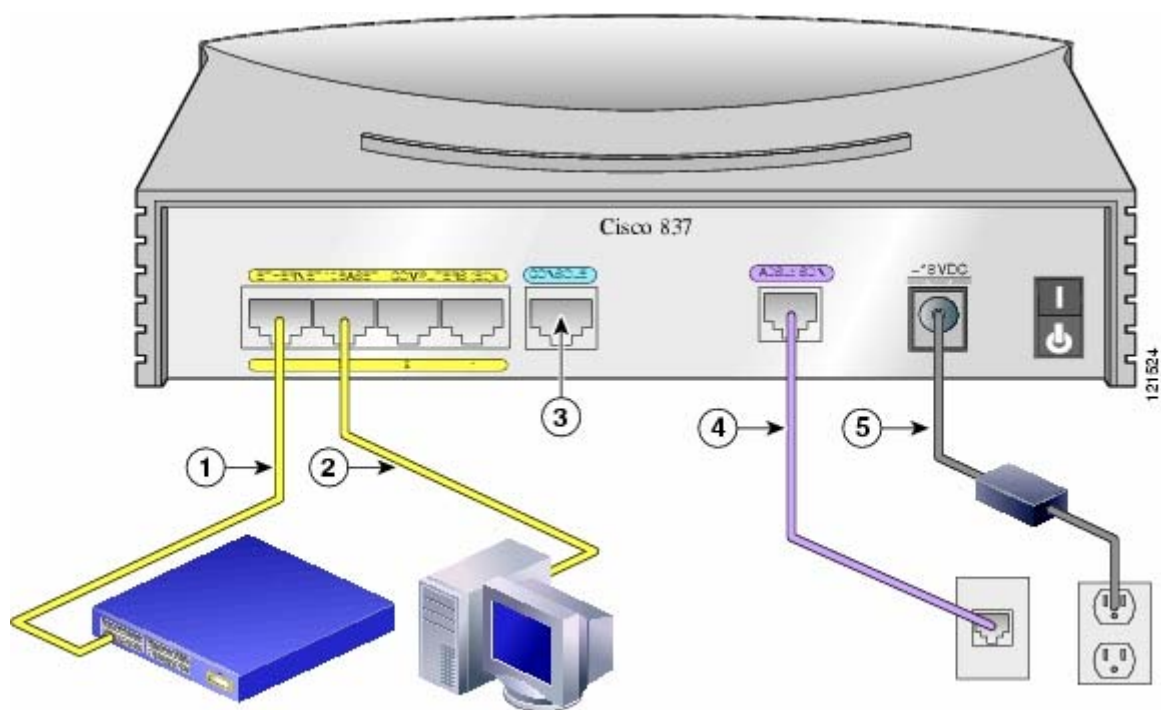


comment paramétrer une connexion ADSL sur un modem-router CISCO 837



Sommaire

Introduction

1 Connexion au routeur Cisco

1.1 Attribution d'un mot de passe par CRWS

1.2 Connexion avec Teraterm pro web

1.3 Changement du nom du routeur

2 Configuration des interfaces du routeur

2.1 ATM0

2.2 DIALER0

2.3 ETHERNET0

2.4 Paramétrer la route par défaut

2.5 Configuration de la NAT

3 Configuration des services supplémentaires

3.1 Serveur DHCP

3.2 Service DynDNS

3.3 Serveur SSH

4 Sécuriser le routeur

4.1 Le serveur HTTP

4.2 Antispoofing

4.3 ICMP et IP

5 Sauvegarde de la configuration et de l'IOS

5.1 Sauvegarder sur un serveur TFTP distant

5.2 Fichier de configuration final

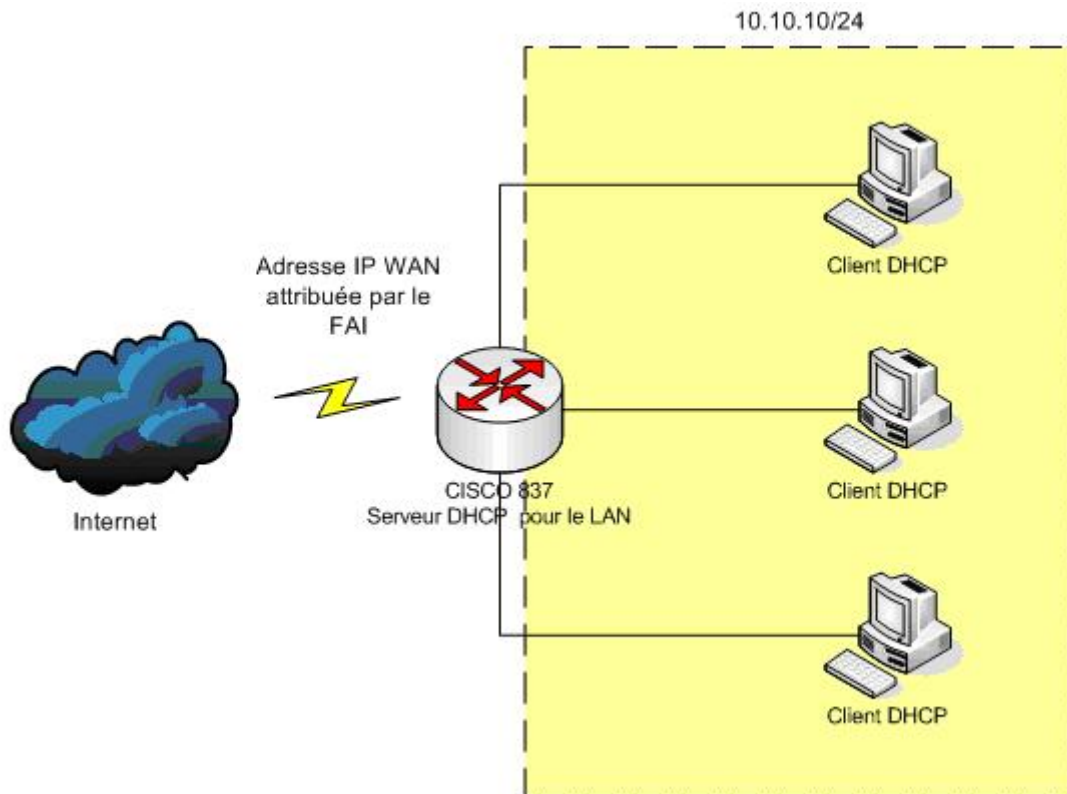
Conclusion

Introduction

Cet article va vous expliquer comment paramétrer une connexion ADSL sur un modem-routeur CISCO 837.

Le routeur utilisé est équipé d'IOS 12.4.

La connexion Internet est une Wanadoo haut-débit max (8Mb/s en débit montant et 256k/s en débit descendant). L'adresse IP WAN est fournie par un serveur DHCP de Wanadoo.



1 Connexion au routeur Cisco

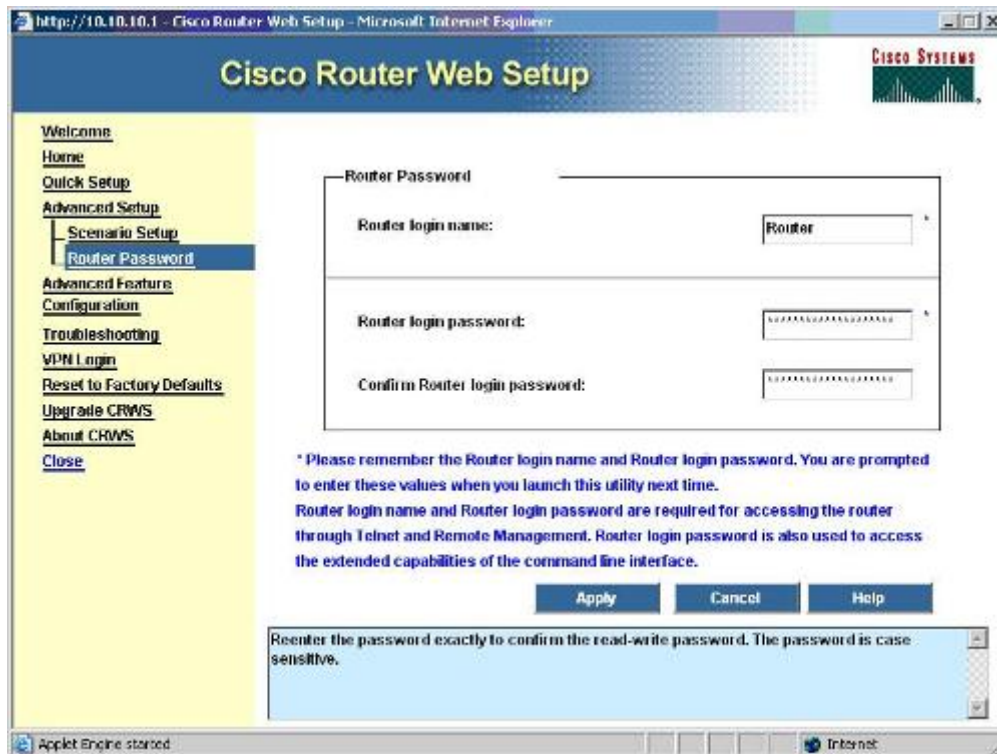
1.1 Attribution d'un mot de passe par CRWS

Ouvrez votre navigateur web sur l'adresse <http://10.10.10.1>

Lorsque vous êtes sur la page principale, cliquez sur Router password et entrez un mot de passe de connexion.

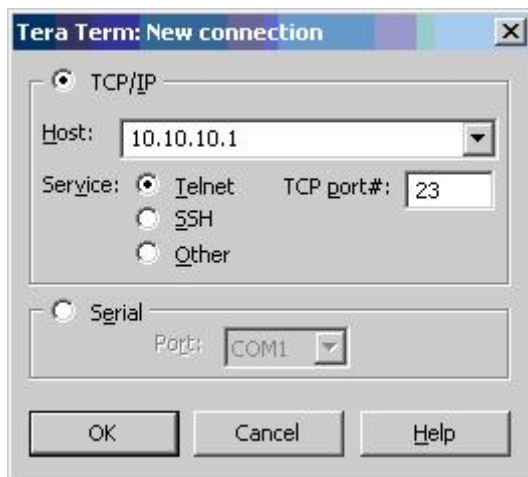
Cliquez sur Apply pour terminer le paramétrage.

Fermer la fenêtre.



1.2 Connexion avec Teraterm pro web

La connexion se fait par TELNET. Connectez-vous sur l'adresse IP 10.10.10.1. En username entrez Router et en mot de passe celui que vous avez enregistré.



1.3 Changement du nom du routeur

En premier lieu, nous changeons le nom du routeur en CISCOADSL.

```
Router>en
Password:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CISCOADSL
CISCOADSL(config)#
```

2 Configuration des interfaces du routeur

2.1 ATM0

On indique que l'on souhaite utiliser une adresse IP fournie par un serveur DHCP du fournisseur d'accès et qu'elle soit positionnée sur l'interface dialer0.

On paramètre l'interface ATM pour utiliser le circuit virtuel 8/35.
On spécifie que l'on utilise PPPOE et que l'on utilisera les paramètres du pool 1.

```
CISCOADSL(config)#interface ATM0
CISCOADSL(config-if)#ip dhcp client client-id dialer0
CISCOADSL(config-if)#pvc 8/35
CISCOADSL(config-if-atm-vc)#pppoe-client dial-pool-number 1
CISCOADSL(config-if-atm-vc)#exit
CISCOADSL(config-if)#exit
```

2.2 DIALERO

L'adresse IP de dialer0 sera négociée par PPP.
On configure l'authentification PPP CHAP en utilisant le nom d'utilisateur et le mot de passe fourni par le fournisseur d'accès. L'option callin réalise une one-way authentication. Cela veut dire que pour la connexion s'établie, il suffit que notre équipement s'authentifie vis-à-vis de l'équipement du fournisseur d'accès.

On récupère les adresses des serveurs DNS Wanadoo avec la commande ppp ipcp dns request.

L'interface dialer0 est définie comme l'interface outside pour la configuration du NAT.

```
CISCOADSL(config)#interface dialer0
CISCOADSL(config-if)#ip address negotiated
CISCOADSL(config-if)#ip mtu 1492
CISCOADSL(config-if)#ip nat outside
CISCOADSL(config-if)#encapsulation ppp
CISCOADSL(config-if)#ip tcp adjust-mss 1452
CISCOADSL(config-if)#dialer pool 1
CISCOADSL(config-if)#dialer remote-name wanadoo
CISCOADSL(config-if)#dialer-group 1
CISCOADSL(config-if)#ppp authentication chap callin
CISCOADSL(config-if)#ppp chap hostname login_FAI
CISCOADSL(config-if)#ppp chap password 0 password_FAI
CISCOADSL(config-if)#ppp ipcp dns request
CISCOADSL(config-if)#exit
```

2.3 ETHERNETO

L'interface ethernet0 est définie comme l'interface inside pour la configuration du NAT.

```
CISCOADSL(config)#interface ethernet0
CISCOADSL(config-if)#ip nat inside
CISCOADSL(config-if)#exit
```

2.4 Paramétrer la route par défaut

On configure la route par défaut sur l'interface dialer0

```
CISCOADSL(config)#ip route 0.0.0.0 0.0.0.0 dialer0
```

2.5 Configuration de la NAT

La première ligne définit que les adresses inside autorisés sont définies par l'access-list 101.

L'access 101 autorise tout les paquets IP provenant du sous-réseau 10.10.10.0/24.

Dialer-list autorise le protocole IP sur le dialer group numéro 1 (ATM0).

```
CISCOADSL(config)#ip nat inside source list 101 interface dialer0 overload
CISCOADSL(config)#access-list 101 permit ip 10.10.10.0 0.255.255.255 any
CISCOADSL(config)#dialer-list 1 protocol ip permit
```

3 Configuration des services supplémentaires

3.1 Serveur DHCP

On crée un pool DHCP qui porte le nom CLIENT.

La commande import all permet d'ajouter la liste des serveurs DNS reçues par le fournisseur d'accès dans la configuration du serveur DHCP.

Le sous-réseau attribuable est 10.10.10.0/24.

La passerelle par défaut des clients sera 10.10.10.1.

Le bail est positionné à 50 jours.

```
CISCOADSL(config)#ip dhcp pool CLIENT
CISCOADSL(dhcp-config)#import all
CISCOADSL(dhcp-config)#network 10.10.10.0 255.0.0.0
CISCOADSL(dhcp-config)#default-router 10.10.10.1
CISCOADSL(dhcp-config)#lease 50 0
```

```
CISCOADSL(dhcp-config)#exit
```

3.2 Service DynDNS

Si vous possédez un dyndns et que vous souhaitez le mettre à jour depuis votre routeur CISCO, définissez la méthode de mise à jour par HTTP.

Spécifiez l'adresse HTTP avec testlogin qui est votre login et testpassword votre mot de passe chez dyndns. La variable myip est volontairement laissée à vide pour que ce soit l'adresse IP de dialer0 qui soit automatiquement positionné.

Les mises à jour sont effectuées toutes les 6 heures.

Pour faire le ?, taper simultanément sur les touches CTRL et v puis taper ?

```
CISCOADSL(config)#ip ddns update method myupdate
CISCOADSL(DDNS-update-method)# http
CISCOADSL(DDNS-HTTP)# add http://testlogin:testpassword@cisco.dyndns.org/nic/update?
system=dyndns&hostname=cisco.gotdns.org&myip=
CISCOADSL(DDNS-HTTP)# interval maximum 0 6 0 0
CISCOADSL(DDNS-update-method)# exit
CISCOADSL(config)# interface dialer0
CISCOADSL(config-if)# ip ddns update hostname cisco.dyndns.org
CISCOADSL(config-if) ip ddns update myupdate
CISCOADSL(config-if)# exit
```

3.3 Serveur SSH

On veut que le serveur SSH de la machine 10.10.10.2 soit accessible depuis Internet.

On mappe le port 22 (SSH) de l'interface dialer0 sur l'adresse 10.10.10.2 en inside.

```
CISCOADSL(config)#ip nat inside source static tcp 10.10.10.2 22 interface dialer0 22
```

4 Sécuriser le routeur

4.1 Le serveur HTTP

Par défaut, l'interface de configuration CRWS est disponible depuis n'importe quel réseau.

On crée une access-list qui autorise seulement les administrateurs du réseau 10.10.10.0/24 à s'y connecter.

```
CISCOADSL(config)#access-list 24 permit 10.10.10.0 0.0.0.255
CISCOADSL(config)#access-list 24 deny any
CISCOADSL(config)#ip http access-class 24
```

4.2 Antispoofing

On active la protection uRPF contre le spoofing.

5.2 Fichier de configuration final

Current configuration : 2577 bytes

```
!  
version 12.4  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
!  
hostname CISCOADSL  
!  
boot-start-marker  
boot-end-marker  
!  
memory-size iomem 5  
enable secret 5 PASSWORD  
!  
no aaa new-model  
!  
resource policy  
!  
ip subnet-zero  
no ip source-route  
!  
!  
no ip dhcp use vrf connected  
ip dhcp excluded-address 10.10.10.1  
!  
ip dhcp pool CLIENT  
  import all  
  network 10.0.0.0 255.0.0.0  
  default-router 10.10.10.1  
  lease 50  
!  
!  
ip cef  
no ip ips deny-action ips-interface  
ip ddns update method myupdate  
  HTTP  
  add  
  http://testlogin:testpassword@cisco.gotdns.org/nic/update?system=dyndns&hostname=cisc  
o.gotdns.org&myip=  
  interval maximum 0 6 0 0  
!  
!  
!  
!  
username Router password 7 PASSWORD  
!  
!  
!  
!  
interface Ethernet0  
  ip address 10.10.10.1 255.255.255.0  
  ip nat inside  
  ip virtual-reassembly  
  hold-queue 100 out  
!  
interface Ethernet2
```



```
no ip address
shutdown
hold-queue 100 out
!
interface ATM0
ip dhcp client client-id Dialer0
no ip address
no atm ilmi-keepalive
dsl operating-mode auto
pvc 8/35
pppoe-client dial-pool-number 1
!
!
interface FastEthernet1
duplex auto
speed auto
!
interface FastEthernet2
duplex auto
speed auto
!
interface FastEthernet3
duplex auto
speed auto
!
interface FastEthernet4
duplex auto
speed auto
!
interface Dialer0
ip ddns update hostname cisco.gotdns.org
ip ddns update myupdate
ip address negotiated
ip access-group 102 in
ip verify unicast reverse-path
no ip redirects
no ip unreachable
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
ip tcp adjust-mss 1452
dialer pool 1
dialer remote-name wanadoo
dialer-group 1
ppp authentication chap callin
ppp chap hostname login_FAI
ppp chap password 7 password_FAI
ppp ipcp dns request
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
!
ip http server
ip http access-class 24
no ip http secure-server
!
ip nat inside source list 101 interface Dialer0 overload
ip nat inside source static tcp 10.10.10.2 30777 interface Dialer0 30777
!
```

```
access-list 23 permit 10.10.10.0 0.0.0.255
access-list 24 permit 10.10.10.0 0.0.0.255
access-list 24 deny any
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
access-list 102 permit icmp any any packet-too-big
access-list 102 deny icmp any any
access-list 102 permit ip any any
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
line con 0
  exec-timeout 120 0
  no modem enable
  stopbits 1
line aux 0
line vty 0 4
  access-class 23 in
  exec-timeout 120 0
  login local
  length 0
!
scheduler max-task-time 5000
end
```

Conclusion

En suivant chaque étape de l'article, votre routeur cisco 837 sera opérationnel pour un accès ADSL et disposera d'une sécurité minimum contre les attaques provenant de votre réseau local et d'Internet. Un serveur SSH est accessible pour vous permettre d'administrer votre réseau depuis la connexion ADSL de votre routeur.