Authentification PPP

>>> PAP, CHAP, PAP-CHAP, CHAP-PAP

Description :

Dans ce cours, nous allons étudier les différentes authentifications sur une liaison PPP entre deux routeurs. Nous allons mettre en place les authentifications PAP, CHAP, PAP-CHAP et CHAP-PAP pour observer le fonctionnement.

Authentification PPP

>>> PAP, CHAP, PAP-CHAP, CHAP-PAP

Sommaire :

I) Introduction

1) Fonctionnement du PPP

PPP signifie Point to Point Protocol ou protocole point à point. Il s'agit d'un protocole beaucoup plus élaboré que SLIP (c'est la raison pour laquelle il l'a supplanté), dans la mesure où il transfère des données supplémentaires, mieux adaptées à la transmission de données sur Internet.

2) Fonctionnement du PAP

PAP signifie Password Authentication Protocol est un protocole d'authentification pour PPP. Les données sont transmises en texte clair sur le réseau ce qui le rend par conséquent non sécurisé.

L'avantage de PAP est qu'il est extrêmement simple à implémenter, lui permettant d'être utilisé dans des systèmes embarqués très légers. Sur des systèmes de taille raisonnable on préférera sans doute le protocole CHAP.

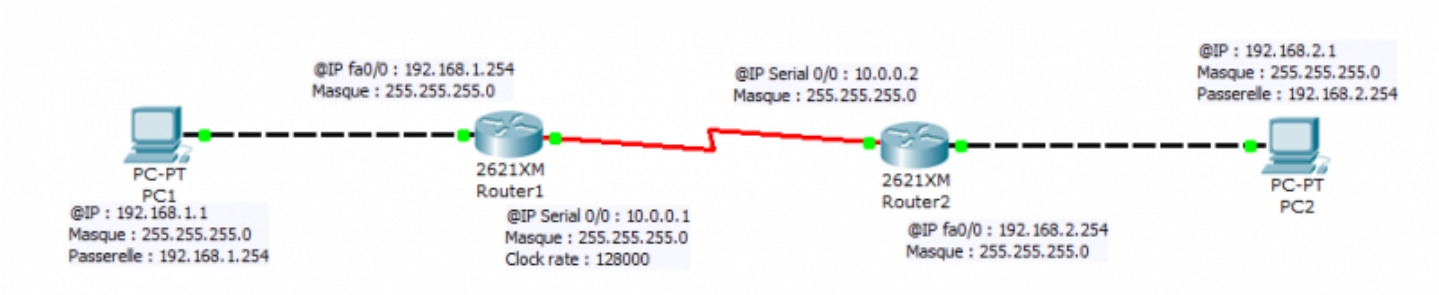
3) Fonctionnement du CHAP

CHAP signifie Challenge Handshake Authentication Protocol est un protocole d'authentification pour PPP à base de challenge, ce qui le rend bien plus sûr que son pendant PAP. Ce protocole est défini dans la RFC 1994. Il est aussi utilisé par le protocole iSCSI afin qu'Initiator et Target iSCSI s'authentifient éventuellement mutuellement.

L'objectif de CHAP est que le pair s'authentifie auprès d'un authentificateur sans échange de mot de passe en clair sur le réseau et sans que l'échange puisse être rejoué par un tiers à l'écoute. La contrainte est que

chaque partie partage un « secret » (mot de passe) commun. Microsoft a développé la variante MS-CHAP qui supprime cette contrainte.

II) Schéma réseau



III) Configuration de base

1) Configuration routeur 1

On commence par une chose simple mais qui va nous simplifier la vie, la configuration du hostname pour identifier nos deux routeurs dans les différents logs :

```
configure terminal
hostname Router1
end
```

On configure ensuite l'interface connecté à notre PC1 :

```
configure terminal
interface fastethernet 0/0
ip address 192.168.1.254 255.255.255.0
no shutdown
end
```

On configure maintenant l'interface série qui sera connecté sur le deuxième routeur :

```
configure terminale
interface serial 0/0
ip address 10.0.0.1 255.255.255.0
encapsulation ppp
clock rate 128000
no shutdown
end
```

Pour finir on ajoute une route statique :

```
configure terminal
ip route 192.168.2.0 255.255.255.0 10.0.0.2
end
```

Voilà notre premier routeur est configuré.

2) Configuration routeur 2

On reproduit la même chose sur le deuxième routeur :

```
configure terminal
hostname Router2
end
```

On configure ensuite l'interface connecté à notre PC2 :

```
configure terminal
interface fastethernet 0/0
ip address 192.168.2.254 255.255.255.0
no shutdown
end
```

On configure maintenant l'interface série qui sera connecté sur le premier routeur :

```
configure terminale
interface serial 0/0
ip address 10.0.0.2 255.255.255.0
encapsulation ppp
no shutdown
end
```

On ne configure pas de clock rate sur le routeur 2 car le routeur 1 est le routeur maitre.

Pour finir on ajoute une route statique :

```
configure terminal
ip route 192.168.1.0 255.255.255.0 10.0.0.1
end
```

On vérifie que les deux machines communiquent bien :

```
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=11ms TTL=126
Reply from 192.168.2.1: bytes=32 time=16ms TTL=126
Reply from 192.168.2.1: bytes=32 time=15ms TTL=126
Reply from 192.168.2.1: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 24ms, Average = 16ms
```

Cliquez ci-dessous pour télécharger le fichier Packet Tracert, comprenant une démonstration du réseau :

IV) Mise en place de l’authentification PAP

Premier cas d’authentification, nous allons configurer une authentification PAP.

1) Configurations

a) Configuration du routeur 1

On commence par activer le service de chiffrement :

```
configure terminal
service password-encryption
```

On crée un nouvel utilisateur :

```
configure terminal
username USER-R1 password 0 AQW
end
```

Ensuite on configure l’interface série, pour activer l’authentification PAP ainsi que le login et le password :

```
configure terminal
interface serial 0/0
ppp authentication pap
ppp pap sent-username USER-R2 password 0 AQW
end
```

- USER-R2 étant le login crée sur le routeur distant, avec lequel nous nous authentifions pour la communication PPP.

Si vous essayez de pinger de PC1 vers PC2 vous remarquerez que la connexion entre les deux routeurs ne fonctionne plus.

b) Configuration du router2

On commence par activer le service de chiffrement :

```
configure terminal
service password-encryption
```

On crée un nouvel utilisateur :

```
configure terminal
username USER-R2 password 0 AQW
end
```

Ensuite on configure l’interface série, pour activer l’authentification PAP ainsi que le login et le password :

```
configure terminal
interface serial 0/0
ppp authentication pap
```

```
ppp pap sent-username USER-R1 password 0 AQW
end
```

- USER-R1 étant le login crée sur le routeur distant, avec lequel nous nous authentifions pour la communication PPP.

2) Test de fonctionnement

On teste la communication entre nos deux pc :

```
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=62ms TTL=126
Reply from 192.168.2.1: bytes=32 time=88ms TTL=126
Reply from 192.168.2.1: bytes=32 time=94ms TTL=126
Reply from 192.168.2.1: bytes=32 time=94ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 94ms, Average = 84ms
```

Vous pouvez observer la négociation et l'authentification PPP avec les commandes suivantes :

- debug ppp authentication ----> Pour voir les messages de chaque étape du processus l'authentification PAP ou CHAP se déroule
- debug ppp negotiation ----> Génère des messages pour le processus de négociation LCP et NCP qui a lieu entre les équipements

Cliquez ci-dessous pour télécharger le fichier Packet Tracert, comprenant une démonstration du réseau :

V) Mise en place de l'authentification CHAP

Deuxième cas d'authentification, nous repartons de la configuration de base et nous configurons maintenant une authentification CHAP.

1) Configuration

a) Configuration du router1

On commence par activer le service de chiffrement :

```
configure terminal
service password-encryption
```

On crée un nouvel utilisateur :

```
configure terminal
username USER-R1 password 0 AQW
end
```

Ensuite on configure l'interface série, pour activer l'authentification CHAP ainsi que le login et le password :

```
configure terminal
interface serial 0/0
ppp authentication chap
ppp chap hostname USER-R2
ppp chap password 0 AQW
end
```

- USER-R2 étant le login crée sur le routeur distant, avec lequel nous nous authentifions pour la communication PPP.

Si vous essayez de pinger de PC1 vers PC2 vous remarquerez que la connexion entre les deux routeurs ne fonctionne plus.

b) Configuration du router2

On commence par activer le service de chiffrement :

```
configure terminal
service password-encryption
```

On crée un nouvel utilisateur :

```
configure terminal
username USER-R2 password 0 AQW
end
```

Ensuite on configure l'interface série, pour activer l'authentification CHAP ainsi que le login et le password :

```
configure terminal
interface serial 0/0
ppp authentication chap
ppp chap hostname USER-R1
ppp chap password AQW
end
```

- USER-R1 étant le login crée sur le routeur distant, avec lequel nous nous authentifions pour la communication PPP.

2) Test de fonctionnement

On teste la communication entre nos deux pc :

```
R1#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/98/277 ms
```

VI) Authentification PAP-CHAP et CHAP-PAP

- PAP-CHAP : Lors d’une connexion, le routeur va commencer par essayer de s’authentifier avec le protocole PAP si celui-ci échoue alors il essayera avec CHAP.
- CHAP-PAP : Lors d’une connexion, le routeur va commencer par essayer de s’authentifier avec le protocole CHAP si celui-ci échoue alors il essayera avec PAP.