Les protocoles d'authentification CHAP et PAP

Par Dr RIAHLA Mohamed Amine

Les protocoles CHAP et PAP

- Fonctionnement du PPP
- Fonctionnement du PAP
- Fonctionnement du CHAP
- Mise en place de l'authentification PAP
  - Configuration
  - Test de fonctionnement
- Mise en place de l'authentification CHAP
  - Configuration
  - Test de fonctionnement
- Authentification PAP-CHAP et CHAP-PAP

Fonctionnement du PPP

Point to Point Protocol

- Un protocole WAN de couche 2 (L-D),
- Basé sur HDLC, permet d'établir une connexion entre deux hôtes sur une liaison point à point.
- **Composants:**
  - L'encapsulation des datagrammes.
  - Le contrôle de la liaison avec LCP (Link Control Protocol).
  - Le contrôle de la c rx avec NCP (Network Control Protocol).
- **Caractéristiques principales** :
  - Multiplexage de protocole réseau (IP, IPX, AppleTalk),
  - Agrégation de lien (on parle de PPP Multilink).
  - Compression,
  - Gestion de la connexion
  - **Authentification**.

Fonctionnement du PPP

Point to Point Protocol

- Il est massivement utilisé pour les connexions Internet dédiées aux particuliers:
  - Soit directement basé sur HDLC (connexion RTC),
  - Soit encapsulé (par exemple PPPoX, utilisé par les connexions ADSL et câble).

Fonctionnement du PAP

- Est un protocole d'authentification pour PPP.
- Une méthode simple utilisant un contact bi-directionnelle.
- Après établissement de la liaison PPP, une paire de nom d'utilisateur et mot de passe est à plusieurs reprises envoyée par le nœud distant à travers le lien jusqu'à ce que l'authentification soit reconnue,
- Les noms d'utilisateur et mot de passe sont envoyés en clair dans le réseau informatique (non sécurisé)
- L'avantage de PAP: il est très simple à implémenter, donc utilisé dans des systèmes embarqués très légers.
- Sur des systèmes de taille raisonnable on préférera sans doute le protocole CHAP.

Fonctionnement du PAP

- Le PAP prend en charge l'authentification **bidirectionnelle** (bi-directionnel) et **unidirectionnelle,**
- Avec l'authentification **unidirectionnelle**, seulement le côté recevant l'appel (NAS) authentifie le côté distant (client). Le client distant n'authentifie pas le serveur.
- Avec l'authentification **bidirectionnelle**, chaque côté envoie indépendamment une Authentifier-demande (AUTHENTIC-REQ) et reçoit une Authentifier-reconnaissance (AUTHENTIC-ACK) ou l'authentifie-Non reconnu (AUTHENTIC-NAK).
- Ceux-ci peuvent être vus avec la commande de **debug ppp authentication,**

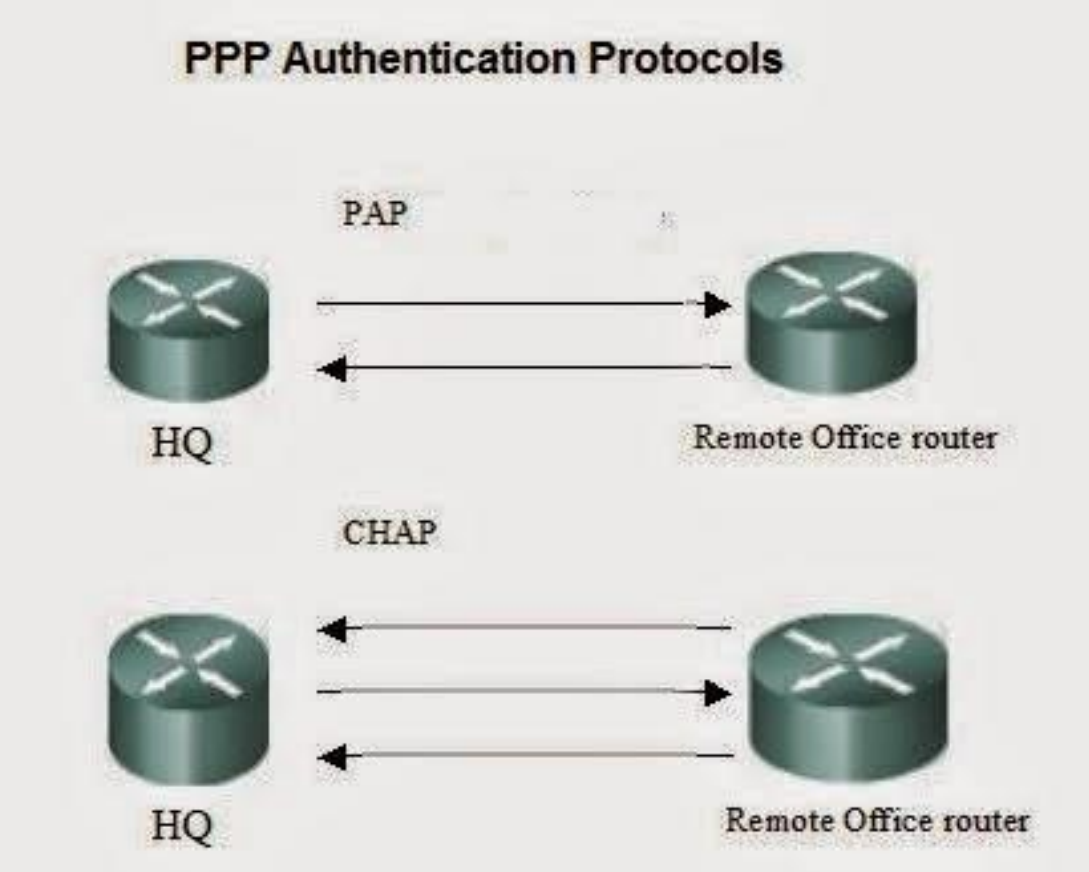
Fonctionnement du CHAP

- **CHAP:** Challenge Handshake Authentication Protocol
- Un protocole d'authentification PPP à base de challenge,
- 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.
- Le protocole CHAP effectue des vérifications régulières pendant l'existence de la liaison.

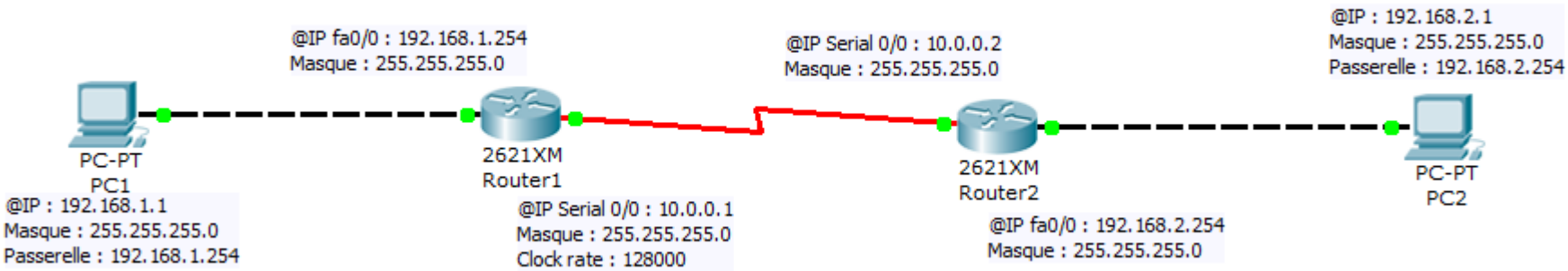
Fonctionnement du CHAP

- Le routeur R1 souhaite établir une connexion CHAP avec le routeur R2. Une fois l'établissement de la liaison terminée, un échange en trois étapes a lieu :
- **Demande CHAP** : R1 demande une confirmation à R2.
- **Réponse CHAP** : R2 répond en envoyant son nom d'utilisateur et son mot de passe à R1. R2 répond par une valeur hachée en MD5, basé sur le mot de passe et le message de demande de confirmation.
- **Finalisation CHAP** : R1 compare ceux-ci avec ceux de sa base de données. S'ils sont identiques, il accepte la connexion, sinon il la refuse. R1 compare la réponse hachée avec son proche calcul de la valeur hachée attendue.

PAP/CHAP


PPP Authentication Protocols
PAP
HQ
Remote Office router
CHAP
HQ
Remote Office router

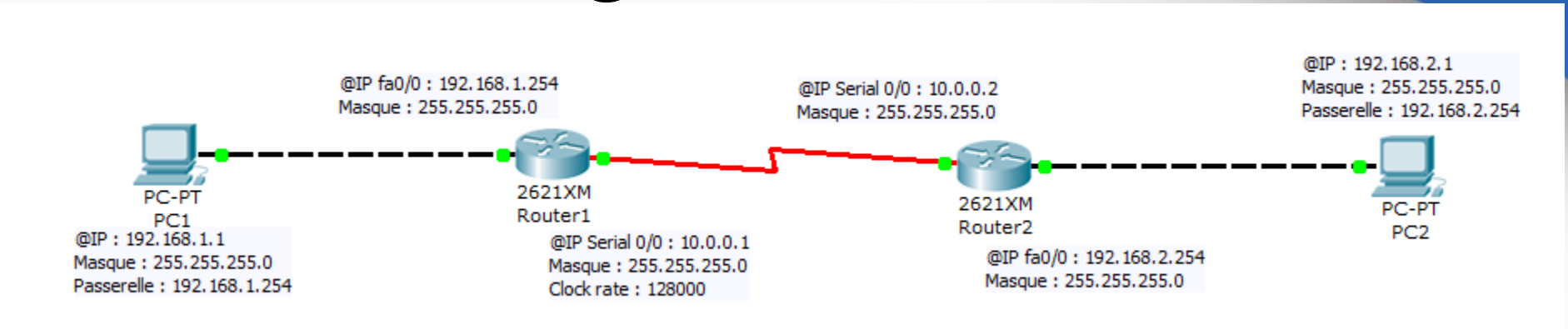
Configuration PAP



Configuration de base

- R1 Hostname
- R1 Configurer Les interfaces
- R1 Configurer l'interface série qui sera connecté sur le deuxième routeur :
  - interface serial 0/0
    ip address 10.0.0.1 255.255.255.0
    encapsulation ppp/***configurer une interface série avec le protocole PPP**
      clock rate 128000
      no shutdown
      end
- Ajouter une route statique :
  - ip route 192.168.2.0 255.255.255.0 10.0.0.2

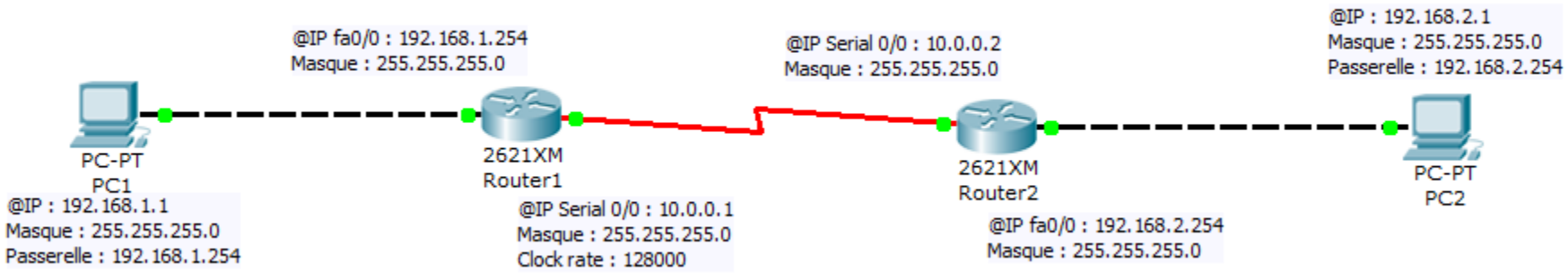
Configuration PAP



Configuration de base

- R2 Hostname
- R2 Configurer Les interfaces
- R2 Configurer l'interface série qui sera connecté sur le deuxième routeur :
  - interface serial 0/0
    ip address 10.0.0.2 255.255.255.0
    encapsulation ppp/***configurer une interface série avec le protocole PPP**
  - clock rate 128000
    no shutdown
    end
- Ajouter une route statique :
  - ip route 192.168.1.0 255.255.255.0 10.0.0.1

Configuration PAP



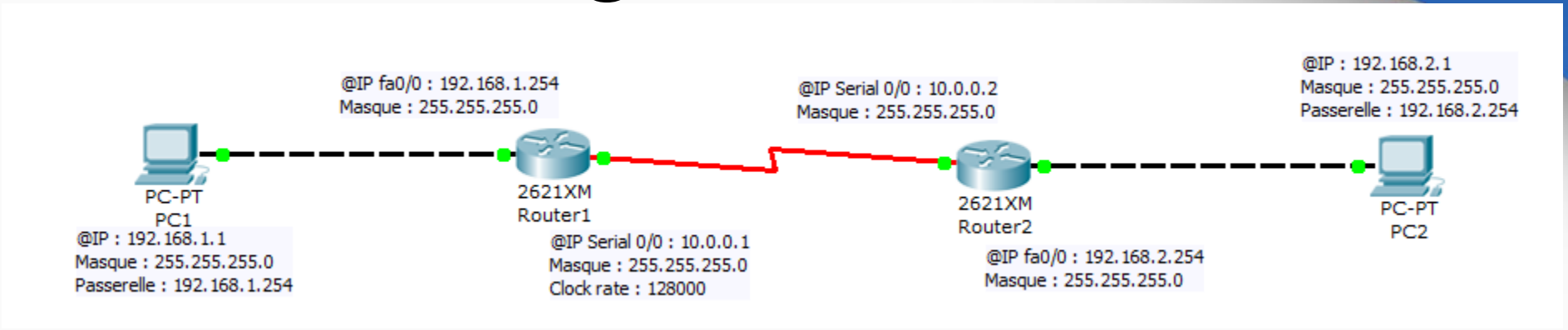
Mise en place de l'authentification PAP (R1)

- Activer le service de chiffrement :
  - **service password-encryption**
- Créer un nouvel utilisateur :
  - **username USER-R1 password 0 AQW**
- Configure l'interface série, pour activer l'authentification PAP et le login et le pass:
  - **interface serial 0/0**
    ppp authentication pap
    ppp pap sent-username USER-R2 password 0 AQW

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

- Pinger de PC1 vers PC2 la connexion entre R1 et R2: ne fonctionne plus!

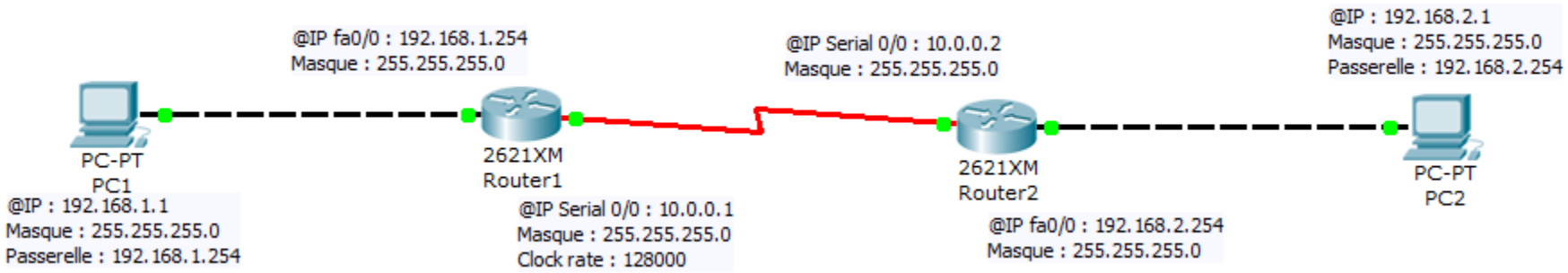
Configuration PAP



Mise en place de l'authentification PAP (R2)

- Activer le service de chiffrement :
  - **service password-encryption**
- Créer un nouvel utilisateur :
  - **username USER-R2 password 0 AQW**
- Configure l'interface série, pour activer l'authentification PAP et le login et le pass:
  - **interface serial 0/0**
    ppp authentication pap
    ppp pap sent-username USER-R1 password 0 AQW
- USER-R1 étant le login crée sur le routeur distant, avec lequel nous nous authentifions pour la communication PPP.

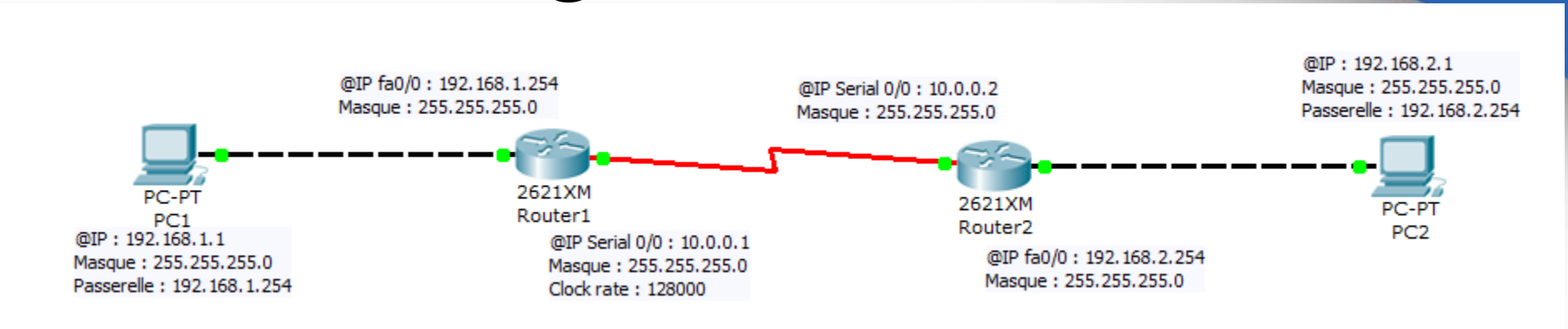
Configuration PAP



Test de fonctionnement

- Ping PC1 et PC2,
- 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

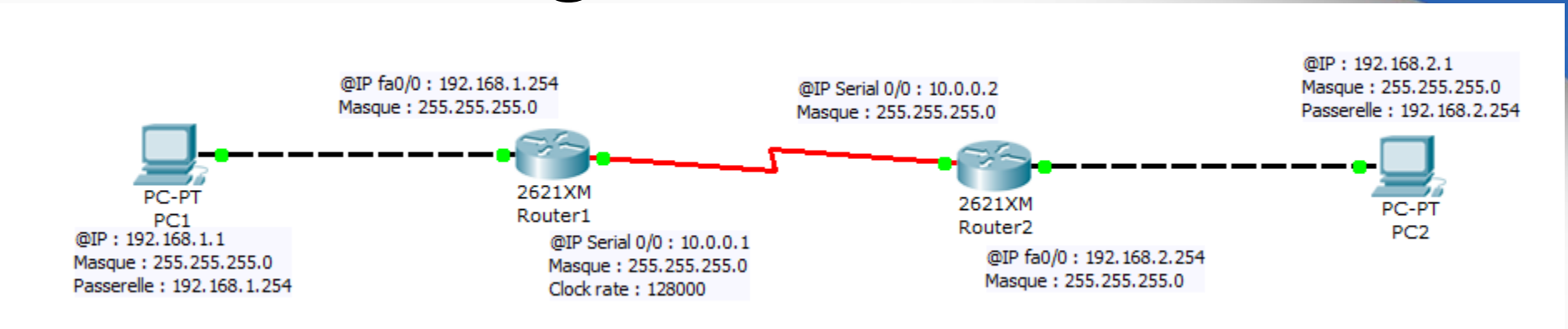
Configuration CHAP



Mise en place de l'authentification PAP (R1)

- Activer le service de chiffrement :
  - **service password-encryption**
- Créer un nouvel utilisateur :
  - **username USER-R1 password 0 AQW**
- Configure l'interface série, pour activer l'authentification PAP et le login et le pass:
  - **interface serial 0/0**
    ppp authentication chap
    ppp chap hostname USER-R2
  - **ppp chap password 0 AQW**
- USER-R2 étant le login crée sur le routeur distant, avec lequel nous nous authentifions pour la communication PPP.
- Pinger de PC1 vers PC2 la connexion entre R1 et R2: ne fonctionne plus!

Configuration CHAP



Mise en place de l'authentification PAP (R2)

- Activer le service de chiffrement :
  - **service password-encryption**
- Créer un nouvel utilisateur :
  - **username USER-R2 password 0 AQW**
- Configure l'interface série, pour activer l'authentification PAP et le login et le pass:
  - **interface serial 0/0**
    ppp authentication chap
    ppp chap hostname USER-R1
  - **ppp chap password AQW**

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

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.

Commandes de configuration PPP

configurer une interface série avec le protocole PPP

R1(config)#interface serial 0/0
R1(config-if)#encapsulation ppp

c**onfigurer la compression sur PPP**

R1(config-if)#compress [predictor | stac]
Pour spécifier le seuil de qualité de la liaison :
R1(config-if)#ppp quality pourcentage
Si le pourcentage de la qualité de la liaison n'est pas maintenu, alors la liaison est désactivée.

Equilibrer le charge sur plusieurs liaisons

R1(config-if)#ppp multilink