A **PAP (Password Authentication Protocol)** és a **CHAP (Challenge-Handshake Authentication Protocol)** két különböző protokoll, amelyeket hitelesítésre használnak hálózati kapcsolatokban. A fő különbség köztük az, hogyan kezelik a jelszóbiztonságot és az ellenőrzési folyamatot. Az alábbiakban részletesen bemutatom a különbségeket:

PAP (Password Authentication Protocol)

1. **Működési mód**:
   - A PAP egy egyszerű hitelesítési protokoll, amely a felhasználónév és jelszó egyértelmű (titkosítatlan) továbbításán alapul.
   - A kliens elküldi a felhasználónevet és a jelszót a szervernek, amely összehasonlítja azokat a saját adatbázisában tárolt értékekkel.
2. **Biztonság**:
   - **Gyenge biztonság**: A jelszó titkosítatlan formában kerül átvitelre, így könnyen lehallgatható, ha a kapcsolat nem titkosított.
   - Nem nyújt védelmet az ismételt támadásokkal (replay attack) szemben.
3. **Használat**:
   - Ritkán használják modern hálózatokban, mivel elavult és nem biztonságos.
   - Csak olyan helyzetekben alkalmazzák, ahol a kapcsolat biztonságát más módon (pl. VPN, SSL/TLS) garantálják.

CHAP (Challenge-Handshake Authentication Protocol)

1. **Működési mód**:
   - A CHAP egy fejlettebb protokoll, amely kihívás-válasz (challenge-response) mechanizmust használ.
   - A szerver küld egy véletlenszerű kihívást (challenge) a kliensnek.
   - A kliens a jelszót egy hash-függvény segítségével kombinálja a kihívással, majd visszaküldi a szervernek a hash-értéket.
   - A szerver ugyanazt a hash-függvényt használja a kihívás és a jelszó alapján, hogy ellenőrizze a kliens válaszát.
2. **Biztonság**:
   - **Erősebb biztonság**: A jelszó soha nem kerül közvetlenül átvitelre a hálózaton, csak a hash-elt érték.
   - Ellenáll az ismételt támadásoknak, mivel minden hitelesítési ciklushoz új kihívás-válasz párost használ.
   - Az időszakos hitelesítés révén ellenőrzi a kliens folyamatos jelenlétét.
3. **Használat**:
   - Gyakrabban használják, mint a PAP, különösen PPP (Point-to-Point Protocol) alapú kapcsolatokban.
   - Biztonságosabb, de még mindig nem a legmodernebb megoldás (pl. EAP vagy RADIUS protokollokhoz képest).

PAP konfigurálása

1. Globális felhasználónév és jelszó beállítása

Add meg a távoli eszköz felhasználónevét és jelszavát, amelyet a PAP használ hitelesítéskor.

```
Router(config)# username <távoli_eszköz_neve> password <jelszó>
```

2. Lépj be a soros interfész konfigurációs módba

```
Router(config)# interface Serial0/0/0
```

3. Engedélyezd a PPP protokollt

```
Router(config-if)# encapsulation ppp
```

4. Engedélyezd a PAP hitelesítést

```
Router(config-if)# ppp authentication pap
```

5. Add meg a PAP hitelesítési adatokat

```
Router(config-if)# ppp pap sent-username <saját_nev> password <jelszó>
```

Példa teljes konfigurációra

Router 1 Konfigurációja:

```
Router1(config)# username Router2 password mysecret
Router1(config)# interface Serial0/0/0
Router1(config-if)# encapsulation ppp
Router1(config-if)# ppp authentication pap
Router1(config-if)# ppp pap sent-username Router1 password mysecret
Router1(config-if)# no shutdown
```

Router 2 Konfigurációja:

```
Router2(config)# username Router1 password mysecret
Router2(config)# interface Serial0/0/0
Router2(config-if)# encapsulation ppp
Router2(config-if)# ppp authentication pap
Router2(config-if)# ppp pap sent-username Router2 password mysecret
Router2(config-if)# no shutdown
```

Hitelesítés ellenőrzése

1. **Ellenőrizd az interfész állapotát**: `Router# show interfaces Serial0/0/0`
2. **Ellenőrizd a PPP állapotát**: `Router# show ppp all`
3. **Ellenőrizd a hitelesítési folyamatot**: `Router# debug ppp authentication`

CHAP konfigurálása:

1. Globális felhasználónév és jelszó beállítása

Add meg a távoli eszköz felhasználónevét és a hitelesítéshez használt jelszót. A felhasználónévnek meg kell egyeznie a távoli router hosztnevével.

```
Router(config)# username <távoli_eszköz_neve> password <jelszó>
```

2. Lépj be a soros interfész konfigurációs módba

```
Router(config)# interface Serial0/0/0
```

3. Engedélyezd a PPP protokollt

```
Router(config-if)# encapsulation ppp
```

4. Engedélyezd a CHAP hitelesítést

```
Router(config-if)# ppp authentication chap
```

5. Kapcsold be az interfészt

```
Router(config-if)# no shutdown
```

Példa Teljes Konfiguráció

Router 1 Konfigurációja:

```
Router1(config)# hostname Router1
Router1(config)# username Router2 password mysecret
Router1(config)# interface Serial0/0/0
Router1(config-if)# encapsulation ppp
Router1(config-if)# ppp authentication chap
Router1(config-if)# no shutdown
```

Router 2 Konfigurációja:

```
Router2(config)# hostname Router2
Router2(config)# username Router1 password mysecret
Router2(config)# interface Serial0/0/0
Router2(config-if)# encapsulation ppp
Router2(config-if)# ppp authentication chap
Router2(config-if)# no shutdown
```

Hitelesítés Tesztelése

1. **Ellenőrizd az interfész állapotát**: `Router# show interfaces Serial0/0/0`
2. **Ellenőrizd a PPP állapotát**: `Router# show ppp all`
3. **Ellenőrizd a CHAP hitelesítési folyamatot**: `Router# debug ppp authentication`