

# Hálózatok építése és üzemeltetése



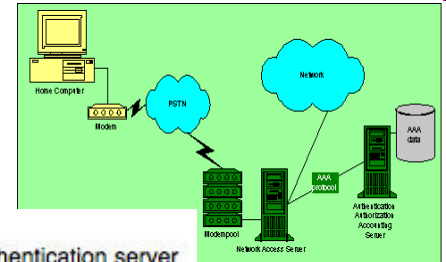
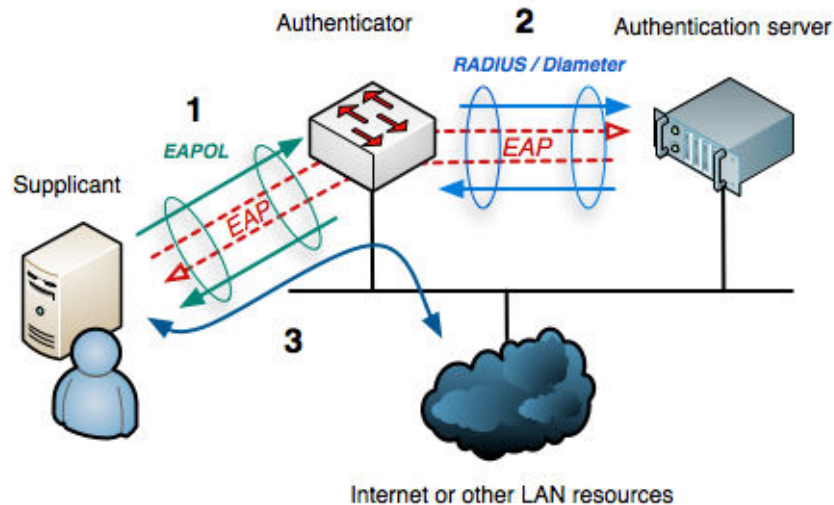
EAP - RADIUS

# Szolgáltatás / hálózat elérés

- ▶ NAS (Network Access Server)  
Hálózat/szolgáltatás biztosítása
  - ▶ Távoli szolgáltatás elérése

## ▶ Kapcsolat

- ▶ Modemes (PSTN/GSM)
- ▶ Vezetékes
  - ▶ Lokális
  - ▶ Távoli
- ▶ Vezetéknélküli



# RADIUS

---

- ▶ **Remote Authentication Dial In User Service**
  - ▶ Eredetileg a betárcsázós felhasználóknak (Merit Networks és Livingston Enterprises)
  - ▶ Ma már széleskörű használat
    - ▶ Azonosítás nem csak dial-in felhasználáskor
    - ▶ xDSL felhasználó azonosítás
    - ▶ Nagyvállalati WiFi
    - ▶ Távközlésben számlázáshoz
  
- ▶ **AAA szolgáltatás nyújtása**
  - ▶ Authentication - Hitelesítés
  - ▶ Authorization - Jogosultság kezelés
  - ▶ Accounting - Számlázás

# RADIUS tulajdonságok

---

## ▶ Legfőbb tulajdonságok

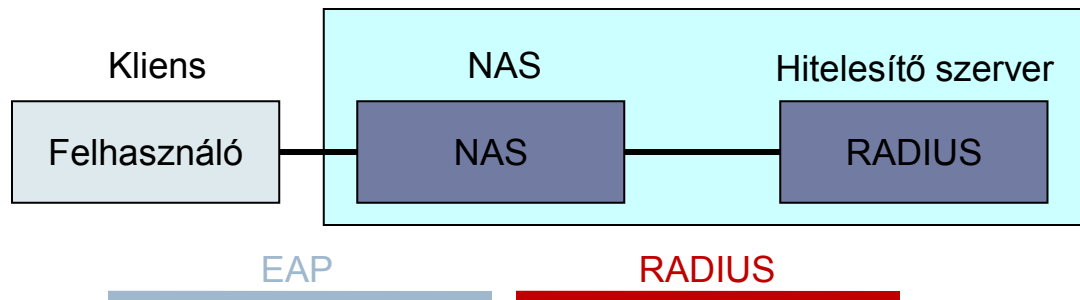
- ▶ UDP alapú (kapcsolatmentes)
  - ▶ 1812 –es port
  - ▶ Hálózati hiba kezelése a RADIUS részéről
- ▶ Állapotmentes
  - ▶ Multithread támogatás
- ▶ Hop by hop biztonság

## ▶ Hiányosságok

- ▶ End to end biztonság támogatása
- ▶ Skálázhatósági problémák (főleg torlódás esetén)

# RADIUS kapcsolat

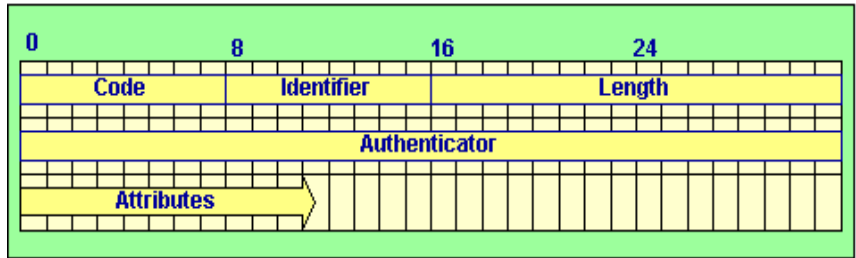
## ▶ Kliens - NAS - RADIUS



- ▶ Sok esetben a kliens és a hitelesítő szerver kommunikál (hitelesít)
  - ▶ A NAS csak továbbítja az üzeneteket
- ▶ De van RADIUS – RADIUS kapcsolat is (proxy)

# RADIUS üzenetek

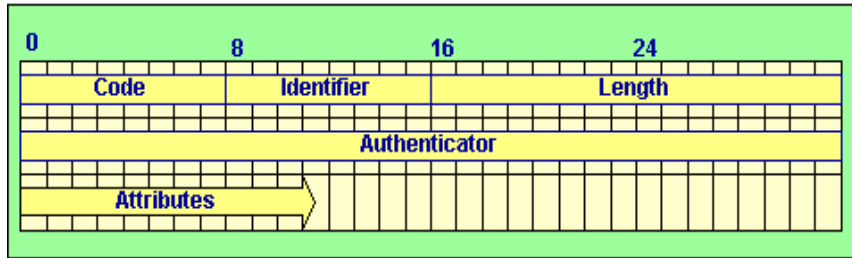
- ▶ Kérés/válasz üzenetek
- ▶ Code
  - ▶ 1: acces-request, 2: acces-accept, 3: access-reject
  - ▶ 4: accounting-request, 5: accounting-response
  - ▶ 11: access-challenge
  - ▶ 12: status-server, 13: status-client
  - ▶ 255: reserved
- ▶ Identifier
  - ▶ Üzenetváltás azonosítója
    - ▶ A kérés válasz összerendelése
  - ▶ Egyszerre csak max. 256 üzenetváltás
- ▶ Length
  - ▶ Üzenet hossza: 20 – 4096 bájtt



# Radius üzenetek (folyt.)

## ▶ Authenticator

- ▶ 16 bájt hitelesítés
- ▶ Request authenticator:
  - ▶ Hitelesítés kérés: 16 bájt véletlen érték
  - ▶ Lehet egyben a CHAP kihívás is
  - ▶ Jelszó elrejtése
- ▶ Response authenticator:
  - ▶ Hitelesítés válasz: MD5(Code, ID, Length, hit. kérés, AVs, közös titok)
  - ▶ Hitelesítés és integritás védelem



# RADIUS üzenetek - AVP

---

- ▶ **Attribútum-érték párok (AVP)**
  - ▶ Attribútum (1 bájt) – hossz (1 bájt) - érték mezőhármas
  - ▶ Az attribútum csak számmal jelölve
    - ▶ Típusok:
      - Integer, Enumeration, IP Address, String, Date, Binary
    - ▶ Előre definiált attribútumok
    - ▶ 26:Vendor-specific attribute
      - VSA mező, hasonló az AVP –hez
      - Gyártó – típus – hossz - érték
- ▶ **Attribútumok:**
  - ▶ User-Name, User-Password, CHAP-Password, NAS-IP-Address, NAS-Port, Service-Type, ...
  - ▶ Szótár az attribútum név és száma (típus) megfeleltetéséhez

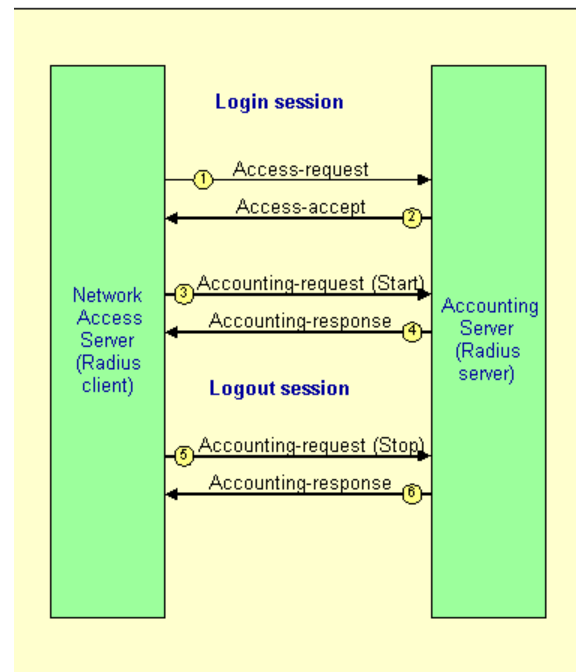


# Attribútum szótár példa

▶ #	ATTRIBUTE-NAME	TYPE
▶ #	-----	
▶ 1	User-Name	STRING
▶ 2	User-Password	STRING
▶ 3	CHAP-Password	STRING
▶ 4	NAS-IP-Address	IPADDR
▶ 5	NAS-Port	INT
▶ 6	Service-Type	ENUM
▶ 7	Framed-Protocol	ENUM
▶ 8	Framed-IP-Address	IPADDR
▶ 9	Framed-IP-Netmask	IPADDR
▶ 10	Framed-Routing	ENUM
▶ #	VALUE-MEANING	FOR ATTRIBUTE
▶ #	-----	
▶ 1	PPP	7
▶ 2	SLIP	7
▶ 3	AppleTalk Rem. Acc. Protocol (ARAP)	7
▶ 4	Gandalf SingleLink/MultiLink	7
▶ 5	Xylogics proprietary IPX/SLIP	7
▶ 6	X.75 Synchronous	7

# RADIUS üzenetváltás

- ▶ Kérdés-válasz típusú
- ▶ Hitelesítés esetén
  - ▶ Kérés:
    - ▶ access-request
  - ▶ Válasz:
    - ▶ acces-accept
    - ▶ access-reject
    - ▶ access-challenge
- ▶ Számlázás esetén
  - ▶ késedelmi idő
  - ▶ viszony idő
  - ▶ küldött és fogadott bájtok, csomagok
  - ▶ magyarázat a bontásra



# Feladatok

# Password Authentication Protocol (PAP)

---

- ▶ **Password Authentication Protocol (PAP)**
  - ▶ Egyszerű, nyílt szöveges
  - ▶ A hitelesítő kéri a felhasználó nevet és a jelszót, amit a kliens kódolás nélkül megküld
- ▶ **Nem biztonságos**
  - ▶ A hálózat figyelésével megvan a felhasználónév és a jelszó
  - ▶ Nincs védelem az üzenet visszajátszása ellen

# RADIUS alap hitelesítés

---

- ▶ Alapból jelszavas hitelesítés (PAP) vagy kihívás alapú hitelesítés (CHAP)
- ▶ A felhasználó jelszavát ismeri a RADIUS szerver: *password*
- ▶ A NAS és a RADIUS szerver között egy jelszó van az üzenetek hitelesítése végett: *S*
  
- ▶ A hitelesítés típusai bővíthetők

# RADIUS PAP hitelesítés lépései

---

## 1. NAS – Access-request

- ▶ A NAS generál egy azonosítót: *NAS Authenticator*
- ▶ User-password attribute értéke (védett jelszó):  
`MD5(S, NAS Authenticator) XOR password`

## 2. RADIUS – Access-accept vagy Access-reject

- ▶ *Response authenticator* generálása:  
`MD5(Code, Identifier, Length, NAS Authenticator, Attributes, S)`

# 1. feladat

RADIUS szerver életre keltése

Teszt kapcsolat a RADIUS szerverrel

Jelszavas hitelesítés

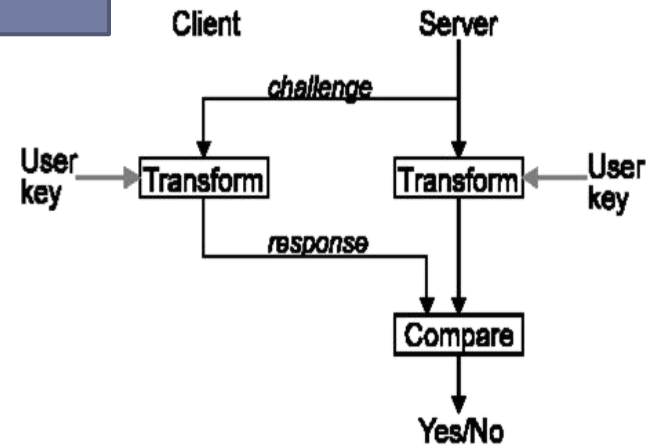
# Challenge Handshake Authentication Protocol (CHAP)

## ▶ Challenge Handshake Authentication Protocol (CHAP)

- ▶ A hitelesítő küld egy kihívást, ami tartalmazza a viszony azonosítóját, valamint egy tetszőleges értéket

kihívás

- ▶ A felhasználó válaszában elküldi a felhasználó nevét és egy egyirányú hash algoritmussal (pl. MD5) a szervertől kapott kihívást, a viszony azonosítóját és a jelszavát.





# CHAP tulajdonságok

---

- ▶ **Jobb mint a PAP**
  - ▶ A jelszó nem utazik a hálózaton
  - ▶ Véd az üzenet visszajátszása ellen is
  - ▶ Véd a megszemélyesítés ellen, az azonosítás többszöri megismétlésével
  
- ▶ **Még mindig nem tökéletes...**
  - ▶ A szervernek ismernie kell a felhasználó jelszavát. (Minden NAS -nak)
  - ▶ A kihívás és a válasz ismeretében off-line jelszó találgatással sebezhető

# RADIUS CHAP hitelesítés lépései

---

## ▶ NAS – CHAP

- ▶ Kihívás generálása: *CHAP Authenticator*
- ▶ Felhasználó név, jelszó bekérése CHAP séma alapján

## ▶ NAS – Access-request

- ▶ *NAS Authenticator*
  - ▶ Ha a CHAP Authenticator 16 bájt hosszú, akkor ide jön
- ▶ CHAP mezők kitöltése (CHAP password)

## ▶ RADIUS – Access-accept vagy Access-reject

## 2. Feladat

### CHAP hitelesítés

# Extensible Authentication Protocol (EAP)

---

- ▶ **Hitelesítő keretprotokoll, mely egy konkrét metódus alapján hitelesít**
  - ▶ Plusz információk kicserélésének lehetősége
- ▶ **A NAS szerepe**
  - ▶ Nem hitelesít, továbbítja az EAP hitelesítési üzeneteket
    - ▶ EAP beágyazása RADIUS üzenetekbe
  - ▶ A NAS nem feltétlenül ismeri az azonosítás módját  
DE: Muszáj ismerni, hogy sikerült-e vagy sem!
- ▶ **Hitelesítési lehetőségek (metódusok)**
  - ▶ Pl.: MD-5 kihívás, egyszeri jelszavak (OTP), nyilvános kulcsok
  - ▶ Bővíthető!

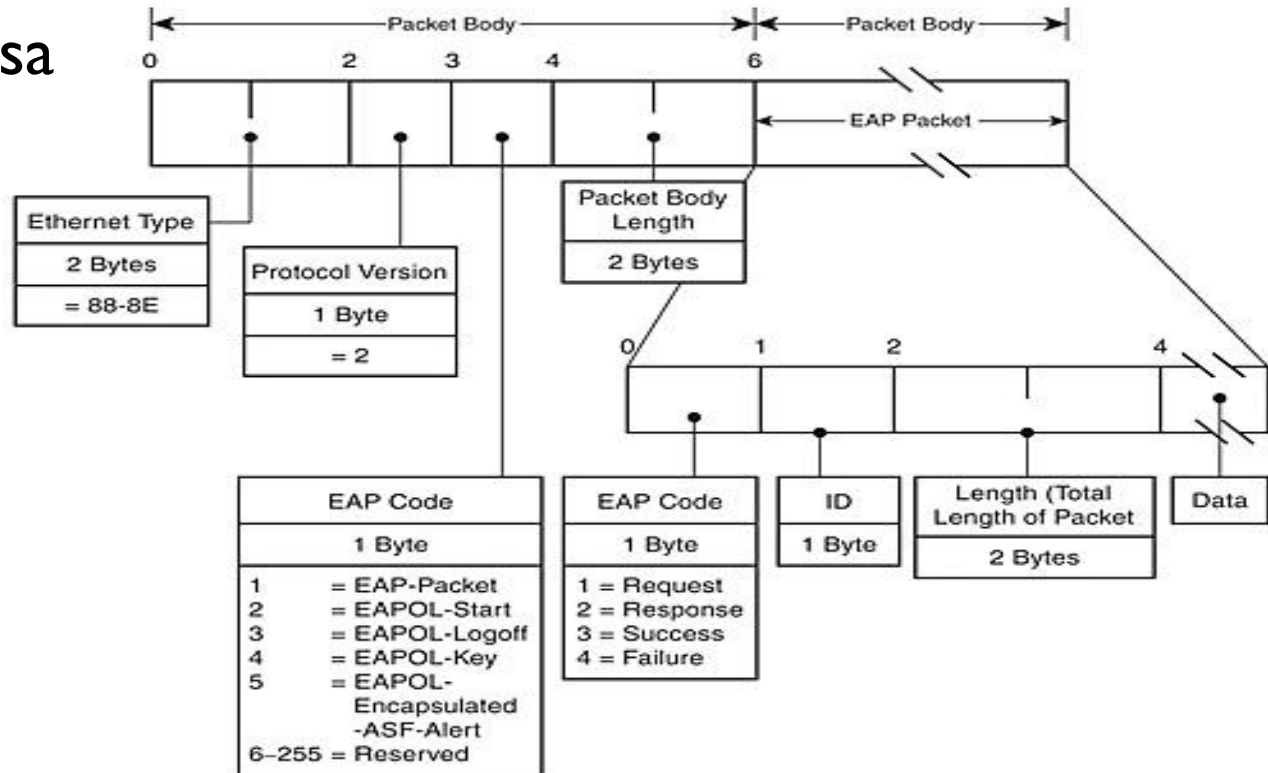
# EAP tulajdonságok

---

- ▶ Duplikált üzenetek elnyomása és újraküldés szükséges
  - ▶ Elhelyezkedhet a lokális linken és az AAA stackjében is
- ▶ Az alsóbb rétegnek kell biztosítania az üzenetek hitelességét
  - ▶ Pl.: Hamis EAP-Success üzenetek veszélye

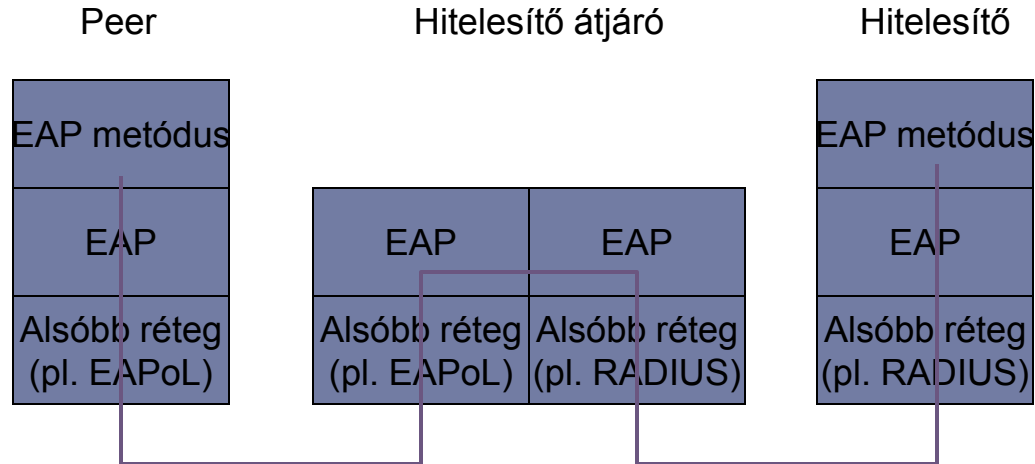
# EAPoL – EAP a linken

## ▶ EAP szállítása



# Hitelesítő EAP segítségével

- ▶ Nem a NAS végzi a hitelesítést!



# EAP üzenetek

---

- ▶ **Több kérdés és válasz ciklus**
  - ▶ Az authenticator kérdez, supplicant válaszol
  - ▶ Egyszerre csak 1 aktív kérdés
  - ▶ Egy viszonyban csak egyetlen hitelesítési mód
  
- ▶ **A kérdések ismételve, ha nem érkezik válasz**
  - ▶ Kivéve sikeres és sikertelen üzenetek
  
- ▶ **Kérés (request) és válasz (response)**
  - ▶ Code (1 byte) – Azonosító (1 byte) – Hossz, beleértve a fejléct is (2 byte) – Adat/hitelesítő típus (1 byte) – Adatok a megadott hosszúságban
  
- ▶ **Sikeres és sikertelen üzenet**
  - ▶ Code (1 byte) – Azonosító (1 byte) – Hossz (2 byte)
  - ▶ A hossz itt 4 bájtt



# EAP code, type

---

## ▶ Code

1: kérés, 2: válasz, 3: siker, 4: sikertelen, 5: Inicializálás, 6: Befejezés

## ▶ Type

### ▶ 1: Identitás (Identity)

▶ A végpont identitásának lekérdezése

### ▶ 2: Figyelmeztetés (Notification)

▶ Megjelenítendő üzenet

### ▶ 3: Elutasítás (Nak)

▶ Érvénytelen vagy értelmezhetetlen típus

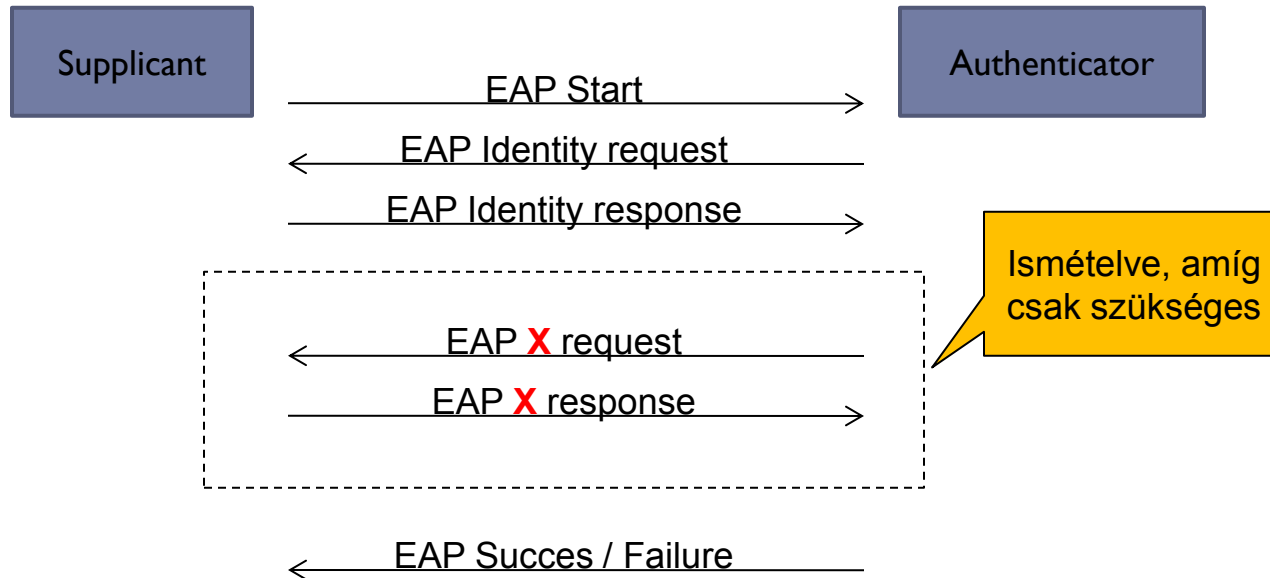
▶ Csak válasz esetén

# EAP hitelesítő típusok

---

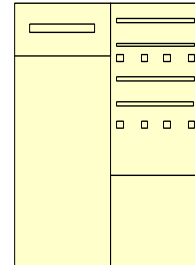
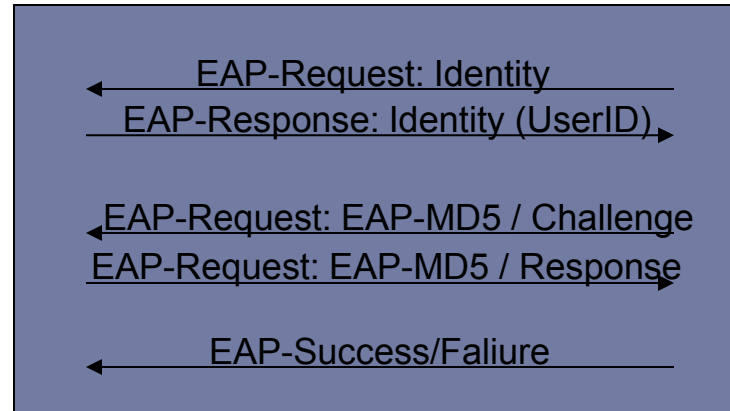
- ▶ 4: MD5-Challenge
  - ▶ A CHAP megfelelője
- ▶ 5: Egyszeri jelszó (One-Time Password - OTP)
  - ▶ OTP kihívás és válasz
- ▶ 6: Általános jelkártya (Generic Token Card)
  - ▶ üzenet és válasz
- ...
- ▶ 13: EAP-TLS
- ▶ 21: EAP-TTLS
- ▶ 25: PEAP, Protected EAP
- ▶ 26: MS-EAP-Authentication (EAP/MS-CHAPv2)

# EAP üzenetciklus



# EAP-MD5

- ▶ IETF RFC 3748
- ▶ Analóg a CHAP hitelesítéssel



## 3. Feladat

802.1X környezet összerakása

supplicant – authenticator – authentication server

EAP-MD5 hitelesítés

# Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)

---

- ▶ Hasonló a CHAP -hez, de
  - ▶ Mindkét fél azonosítva van
  - ▶ A hitelesítő nem ismeri a nyílt jelszót:  
NTHASH használata
  - ▶ plusz hiba kódok
    - ▶ lejárt jelszavak
    - ▶ jelszóváltoztatás

# MS-CHAPv2 működése – kliens oldal

---

1. A felhasználó kéri a hitelesítést
2. **Szerver oldal:** A hitelesítő 16 bájtos véletlen kihívást küld: *authenticator challenge*
3. A felhasználó válasza:
  1. 16 bájtos *peer challenge* generálása
  2. Kihívás (*challenge*) generálása:  
SHA(*authenticator challenge*, *peer challenge*, *user name*)  
Csak az első 8 bájtot használja
  3. Jelszó átalakítása 3 db DES kulccsá (NTHASH-en keresztül)
  4. **NTRResponse:** A *challenge* kódolása a DES kulcsokkal
  5. Válasz a hitelesítésre: **NTRResponse** + *peer challenge* + *user name*

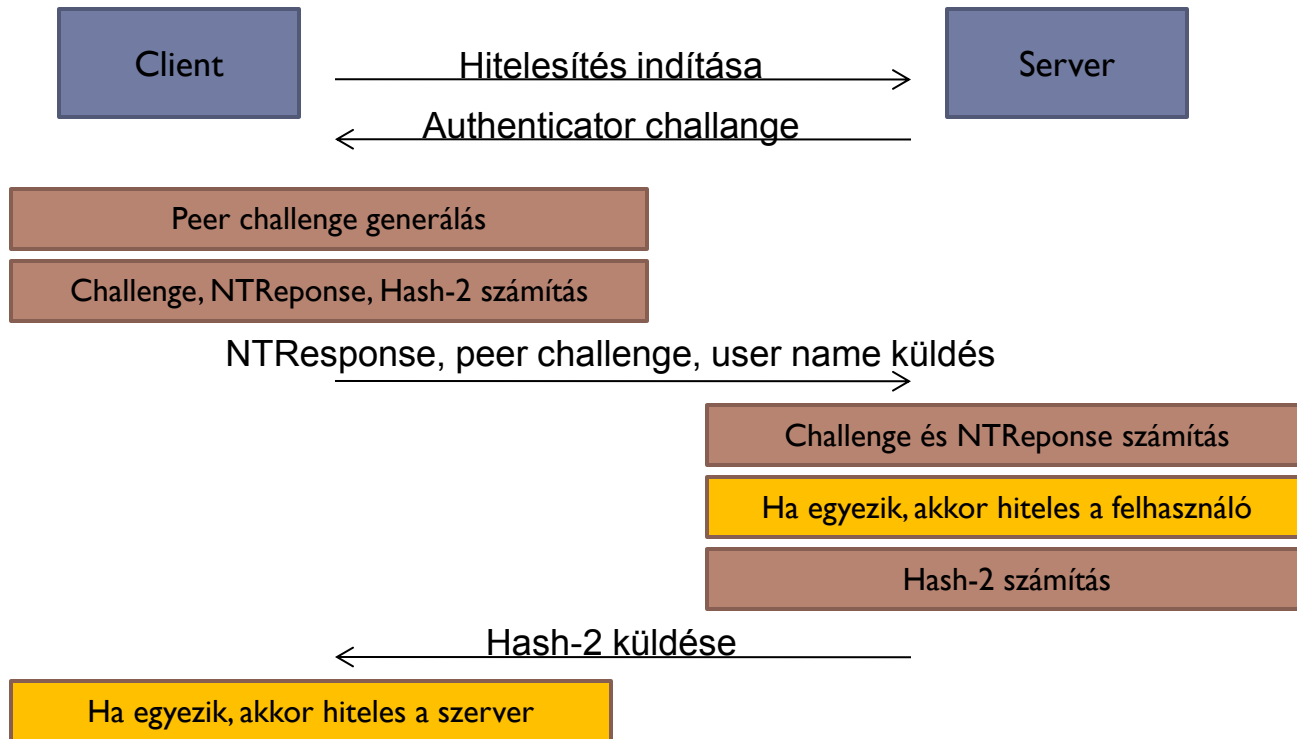
# MS-CHAPv2 működése – szerver oldal

---

1. A felhasználó által küldött válasz ellenőrzése (NTHASH ismerete szükséges)
  - ▶ Ugyanazok a lépések, mint a felhasználó esetén
  - ▶ Ha egyezik, akkor jó a jelszó a felhasználónál
2. Pozitív hitelesítés esetén (NTResponse és peer challenge a korábbi válaszból):
  1. Password-hash-hash előállítása az NTHASH –es passwordból MD4 algoritmussal
  2. Hash-1 előállítása:  
SHA(password-hash-hash, NTResponse, „Magic server to client signing constant”)
  3. Hash-2 előállítása:  
SHA(hash-1, peer challenge, „Pad to make it do more than one iteration”)
3. Hash-2 visszaküldése a felhasználónak
4. **Kliens oldal:** A felhasználó ellenőrzi a hitelesítő válaszát
  - ▶ Ugyanazok a lépések, mint a szerver esetén
  - ▶ Ha egyezik, akkor a szervernél is jó a jelszó



# MS-CHAPv2 működése



# MS-CHAPv2 gyengeségei

---

- ▶ A 8 bájtos kihívás előállítása nem jelent plusz biztonságot. A támadó is elő tudja állítani, mert ezek nyíltan mennek
- ▶ A 3 db DES kulcs előállítása és használata
  - ▶ *A DES algoritmus mai alkalmazhatatlansága*

**Microsoft Security Advisory (2743314)**

Unencapsulated MS-CHAP v2 Authentication Could Allow Information Disclosure

Published: Monday, August 20, 2012

Version: 1.0

# 4. Feladat

## MSCHAPv2 Hitelesítés

# EAP-TLS

---

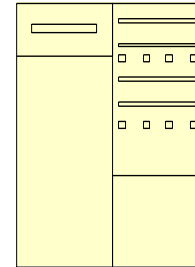
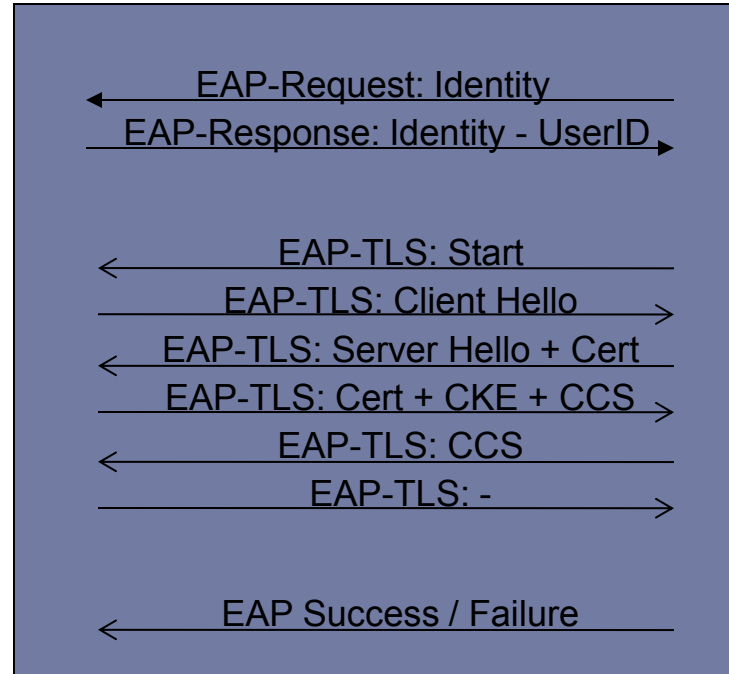
- ▶ **TLS – Transport Layer Security**

- ▶ Kölcsönös azonosítás
  - ▶ Certificate: Nyilvános kulcsú azonosítás
  - ▶ Kliens és szerver tanúsítványok
- ▶ Integritás védelem
- ▶ Kulcscsere

- ▶ **EAP-TLS**

- ▶ IETF RFC 2716
- ▶ A TLS funkcióinak átültetése PPP hitelesítéshez
- ▶ Csak a „handshake” funkció, nem a titkosítás!

# EAP-TLS üzenetek



C/SKE: Client/Server Key Exchange, CCS: Change Cipher Spec

# EAP-TTLS

---

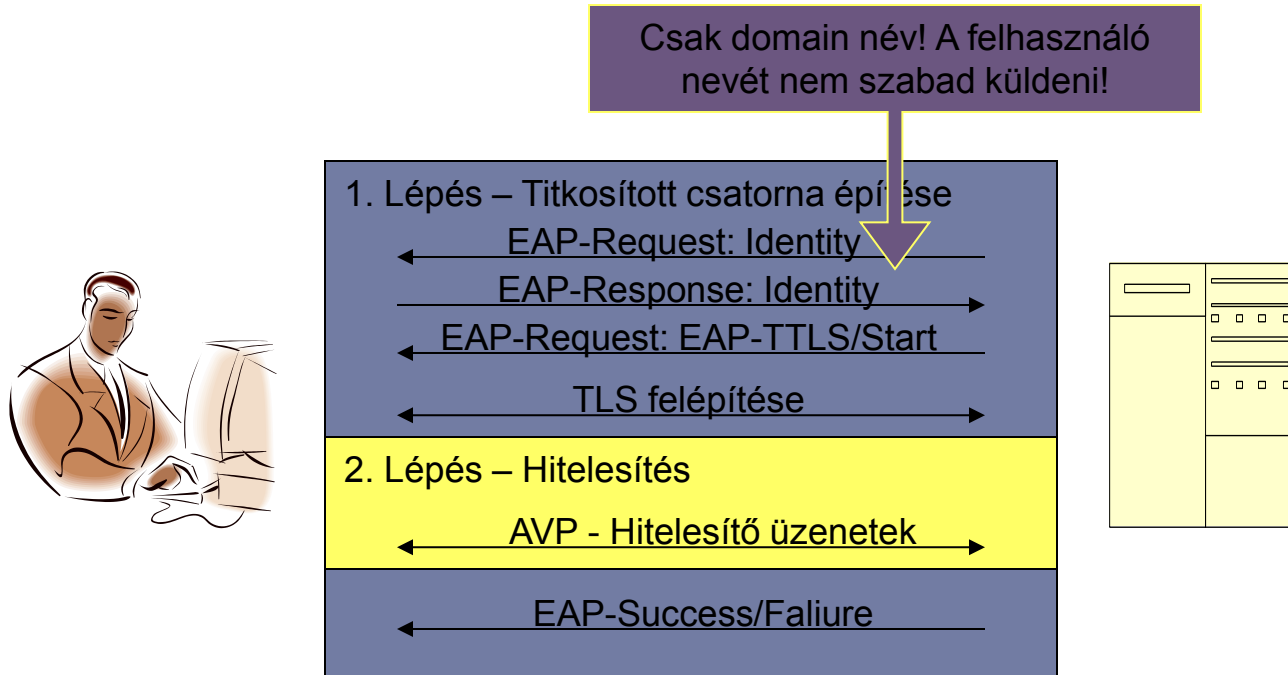
## ▶ EAP-TTLS

- ▶ Tuneled Transport Layer Security
- ▶ IETF draft: Funk, Meetinghouse

## ▶ Hitelesítés

- ▶ 1. lépés: Titkos csatorna felépítése (TLS)
  - ▶ Csak a szerver azonosítja magát
- ▶ 2. lépés: Aktuális hitelesítés
  - ▶ AVP üzenetek, a RADIUShoz hasonlóan
- ▶ Támogatott hitelesítések:
  - ▶ EAP módszerek, PAP, CHAP, MS-CHAP, MS-CHAPv2

# EAP-TTLS üzenetek



# 5. Feladat

## EAP-TTLS-PAP hitelesítés



# PEAP

---

## ▶ PEAP

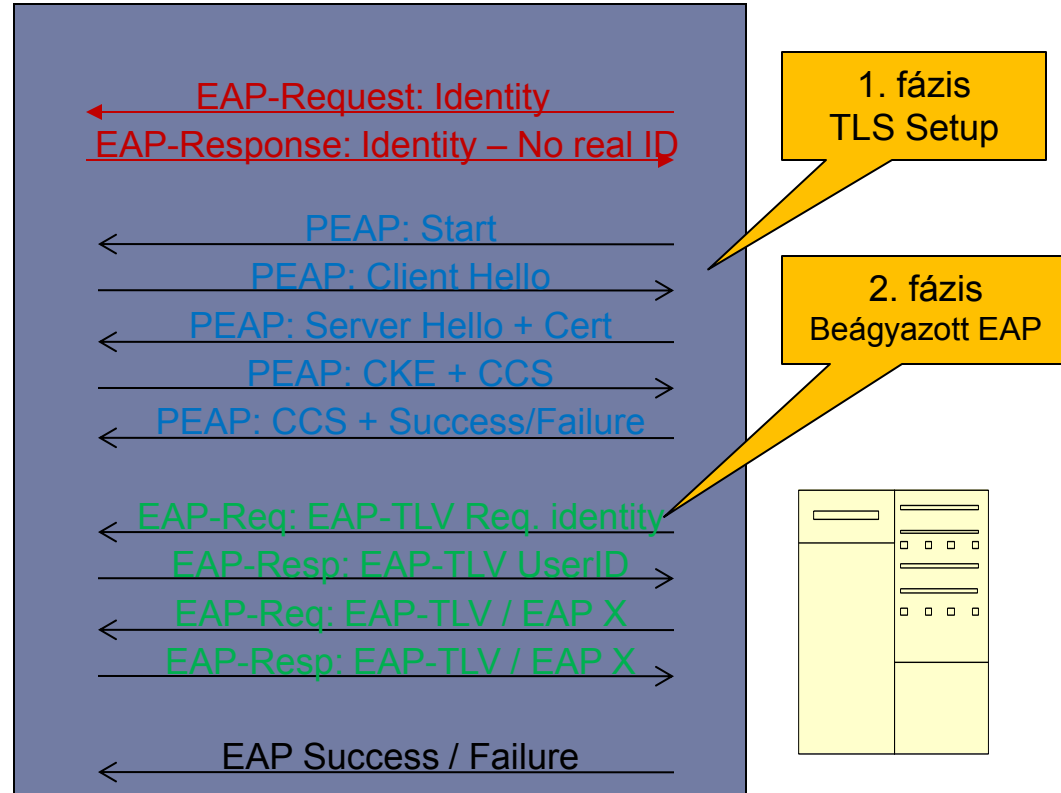
- ▶ Protected EAP
- ▶ IETF draft: Microsoft (+ Cisco és RSA)

## ▶ Hitelesítés

(hasonlóan az EAP-TTLS-hez)

- ▶ 1. lépés: Titkos csatorna felépítése (TLS)
  - ▶ Csak a szerver azonosítja magát
- ▶ 2. lépés: Aktuális hitelesítés
- ▶ Támogatott hitelesítések:
  - ▶ Csak EAP módszerek + MSCHAPv2
  - ▶ EAP esetén az üzenetek beágyazva EAP-TLV –be (type-length-value)

# PEAP üzenetek



# 6. Feladat

## PEAP-MSCHAPV2 hitelesítés

# EAP összehasonlítás

## ▶ EAP protokollok összehasonlítása

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Kliens hitelesítés	MD5	Tanúsítvány	Bármilyen	EAP
Szerver hitelesítés	-	Tanúsítvány	Tanúsítvány*	Tanúsítvány*
Hitelesítés iránya	Kliens hitelesítése	Kölcsönös	Kölcsönös	Kölcsönös
Felhasználó identitásának védelme	Nincs	Nincs	TLS	TLS

- ▶ Az EAP-TTLS hitelesítésnek több ingyenesen elérhető változata van. A PEAP protokoll egyelőre Microsoft specifikus
  - ▶ Mindkettő szabványos szeretne lenni