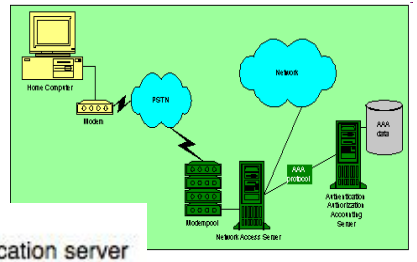
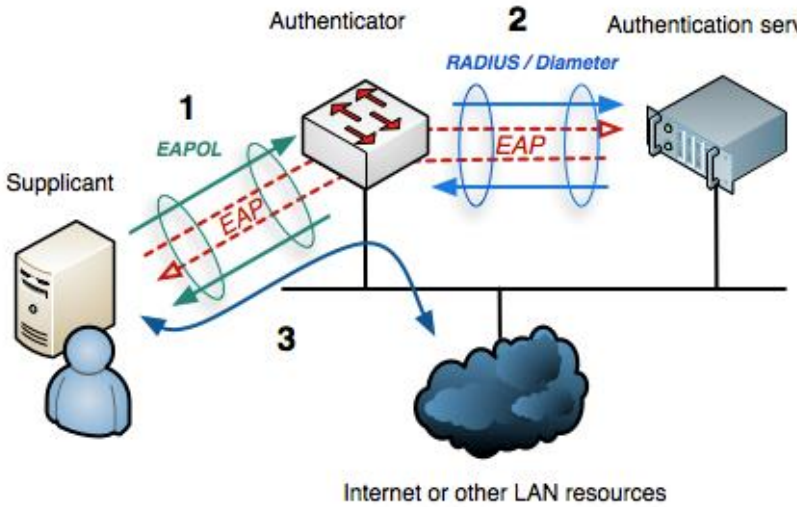
Hálózatok építése, konfigurálása és működtetése

Extensible Authentication Protocol

Szolgáltatás/hálózat elérés

- Felhasználó gépe
  - Távoli szolgáltatás elérése
- NAS (Network Access Server)
  Hálózat/szolgáltatás biztosítása
- AAA központ
  - Hitelesítés, jogosultság, számlázá
- Kapcsolat
  - Modemes (PSTN/GSM)
  - Vezetékes
    - Lokális
    - Távoli
  - Vezetéknélküli





Felhasználó kapcsolat a NAS-hoz

- PPP (Point to Point Protocol)
  - kapcsolat egy direkt összeköttetésen keresztül (point to point)
  - Cél IP, IPX és NetBEUI + egyéb csomagok szállítása (Multi-protocol)
  - A kapcsolat irányításához:
    LCP (Link Control Protocol)
  - Titkosítás
    - DES vagy 3DES
    - Microsoft Point-to-Point Encryption
      - RC4 titkosítás (40, 56 vagy 128 bites kulcsok)
      - Gyakran változtatott kulcsok

LCP működése

1. Fázis - Establishment
   - Egyeztetés
     - Hitelesítés: Authentication Protocol
     - Tömörítés: Compression Control Protocol
     - Titkosítás: Encryption Control Protocol

2. Fázis - Authentication
   - Felhasználó azonosítása
     - Password Authentication Protocol (PAP)
     - Challenge-Handshake Authentication Protocol (CHAP)
     - Microsoft Challenge-Handshake Authentication Protocol (MSCHAP)
     - Extensible Authentication Protocol (EAP)

LCP működése 2.

3. Fázis – MS specifikus
   - Microsoft implementációk
   - Callback Control Protocol (CBCP)
     - A felhasználó visszahívása, további biztonság

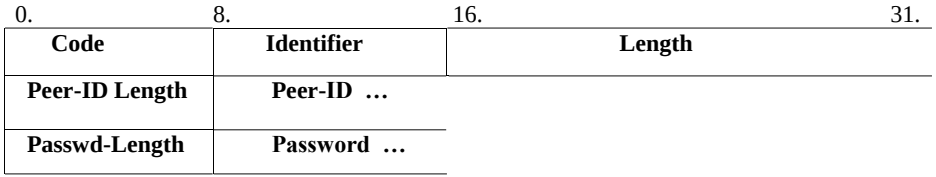
4. Fázis – Network Layer Protocol
   - Network Control Protocols (NCPs)
   - Az 1. fázis során egyeztetett protokollok használata.
   - IP esetén pl. hálózati adatok elküldése

Hitelesítési protokollok

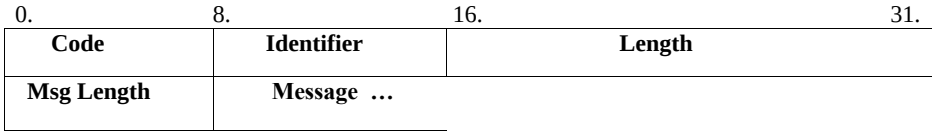
- Password Authentication Protocol (PAP)
  - Egyszerű, nyílt szöveges
  - A hitelesítő kéri a felhasználó nevet és a jelszót, amit a kliens kódolás nélkül megküld
- Nem biztonságos
  - A hálózat figyelésével megvan a felhasználónév és a jelszó
  - Nincs védelem az üzenet visszajátszása ellen

PAP üzenetek

- Azonosítás kérelem



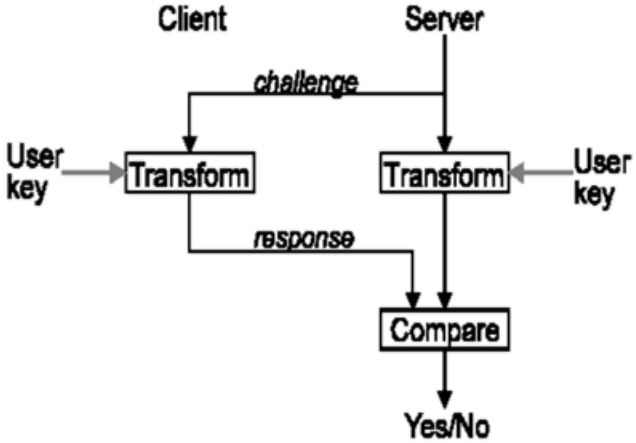
- Azonosítás válasz (Ack vagy Nak)



code: 1 kérelem, 2 Ack, 3 Nak

Hitelesítési protokollok 2.

- Challange Handshake Authentication Protocol (CHAP)
  - A hitelesítő küld egy kihívást, ami tartalmazza a viszony azonosítóját, valamint egy tetszőleges értéket
  - A felhasználó válaszában elküldi a felhasználó nevét és egy egyirányú hash algoritmussal (pl. MD5) a szervertől kapott kihívást, a viszony azonosítóját és a jelszavát.



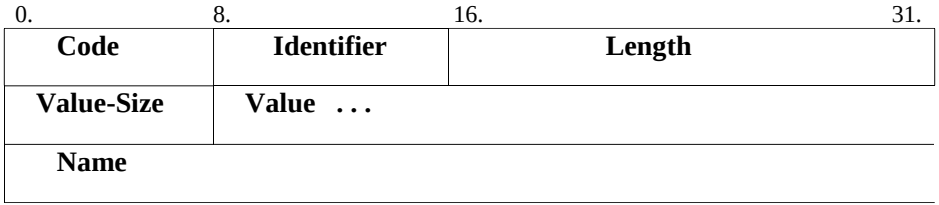
CHAP tulajdonságok

- Jobb mint a PAP
  - A jelszó nem utazik a hálózaton
  - Véd az üzenet visszajátszása ellen is
  - Véd a megszemélyesítés ellen, az azonosítás többszöri megismétlésével

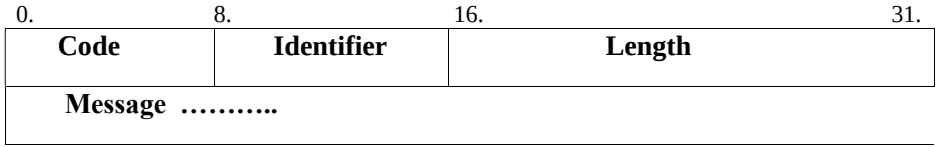
- Még mindig nem tökéletes...
  - A szervernek ismernie kell a felhasználó jelszavát. (Minden NAS -nak)
  - A kihívás és a válasz ismeretében off-line jelszó találgatással sebezhető

CHAP üzenetek

- Kézfogás (Kihívás és válasz)



- Azonosítás (Success vagy Fail)



code: 1 kihívás, 2 válasz, 3 siker, 4 sikertelen

Hitelesítési protokollok 3.

- Microsoft CHallange 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: *authetnicator challange*

3. A felhasználó válasza:
   1. 16 bájtos peer challange generálása
   2. Kihívás (challenege) generálása:
      SHA(authenticator challange, peer challange, user name)
      Csak az első 8 bájtot használja
   3. Jelszó átalakítása 3 db DES kulccsá (NTHASH-en keresztül)
   4. NTResponse: A challenge kódolása a DES kulcsokkal
   5. Válasz a hitelesítésre: NTResponse + peer challange + user name

MS-CHAPv2 működése – szerver oldal

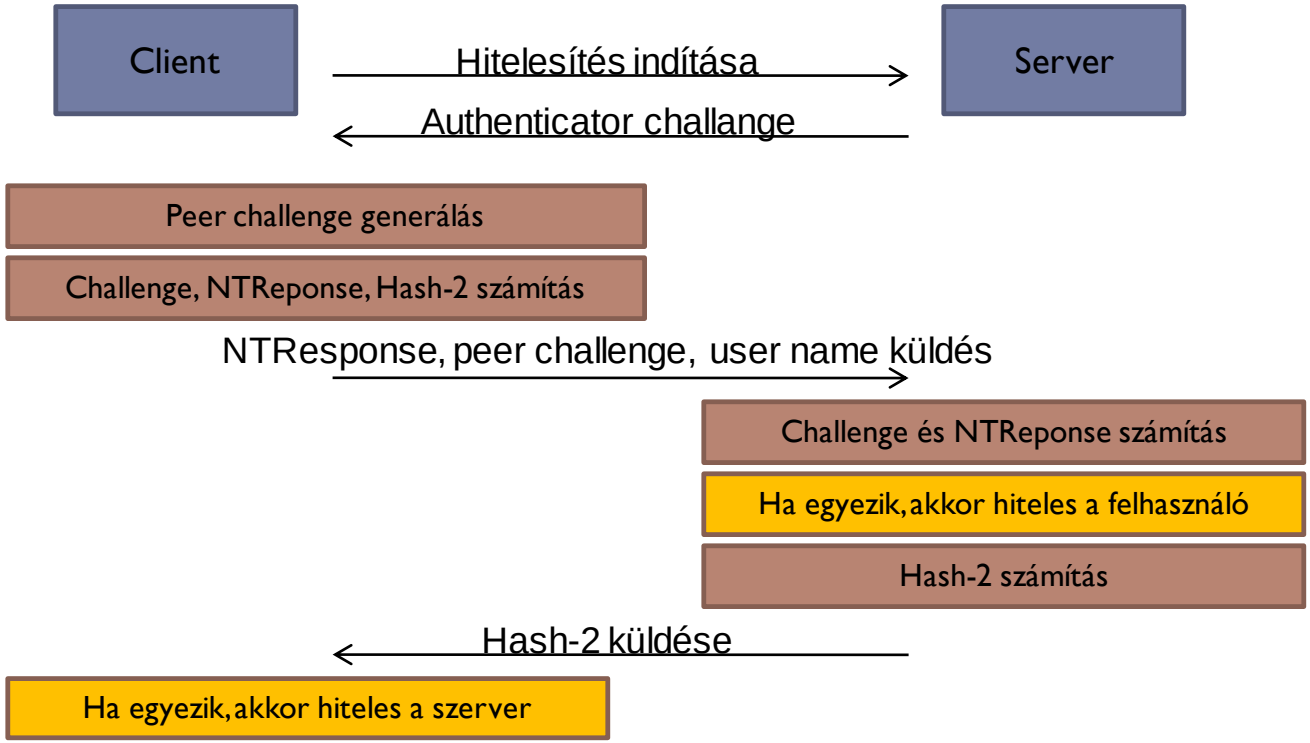
1. A felhasználó által küldött válasz ellenőrzése (NTHASH ismerete szükséges)
   - Ugyanazok a lépések, mint a felhasználó esetén
   - Ha egyezik, akkor jó a jelszó a felhasználónál

2. Pozitív hitelesítés esetén (NTResponse és peer challenge a korábbi válaszból):
   1. Pasword-hash-hash előállítása az NTHASH –es passwordből 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

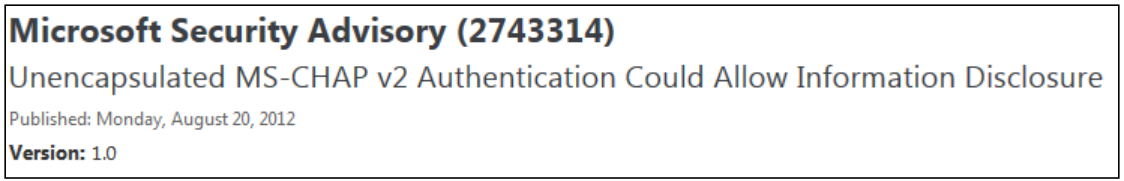
4. **Kliens oldal:** A felhasználó ellenőrzi a hitelesítő válaszát
   - Ugyanazok a lépések, mint a szerver esetén
   - Ha egyezik, akkor a szervernél is jó a jelszó

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

Hitelesítési protokollok 4.

- Extensible Authentication Protocol (EAP)

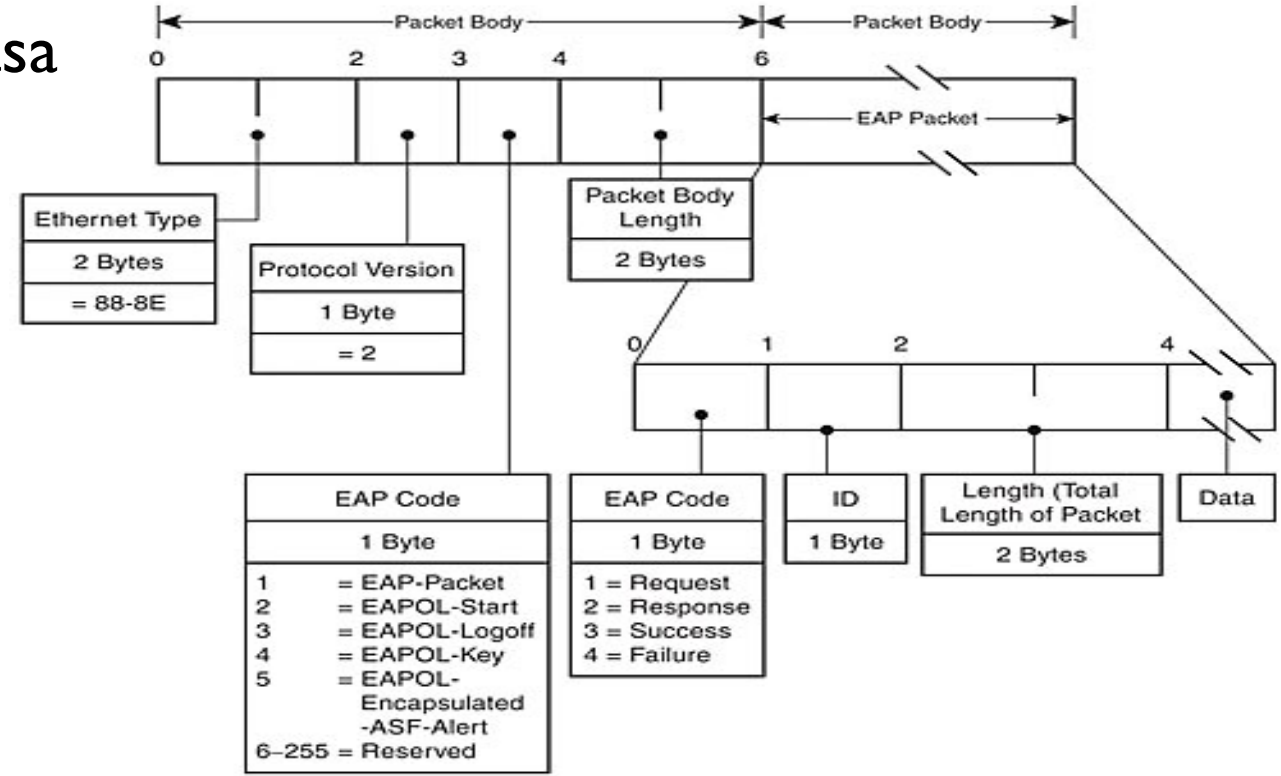
- A hitelesítés kiválasztása csak az Authentication fázisban történik
  - Plusz információk kicserélése
  - A NAS nem feltétlenül ismeri az azonosítás módját
    DE: Muszáj ismerni, hogy sikerült-e vagy sem!
  - A NAS más hitelesítők szolgáltatását (pl.: RADIUS) is igénybe veheti
- Hitelesítési lehetőségek
  - 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

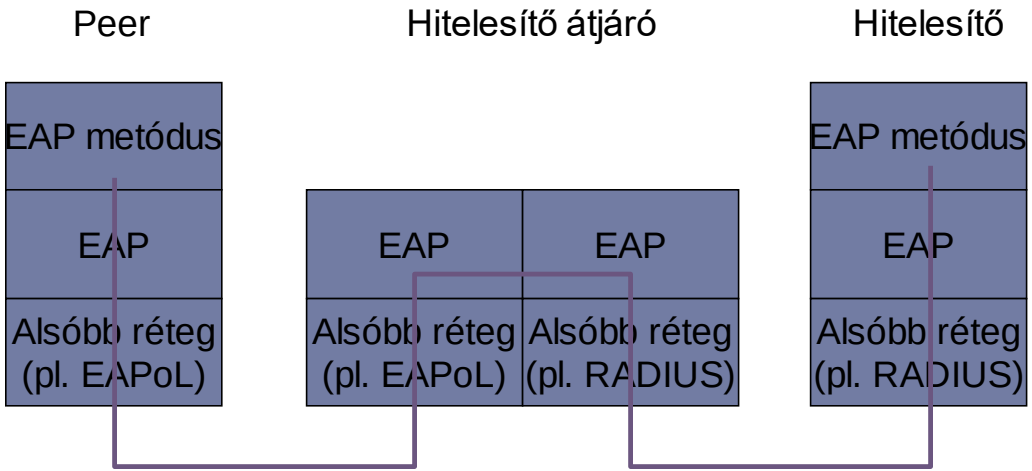
EAPoL – EAP a linken

- EAP szállítása



Hitelesítő EAP segítségével

- Sokszor nem a NAS végzi a hitelesítést



EAP üzenetek

- Több kérdés és válasz ciklus
  - Az authenticator kérdez, peer 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 fejlécet 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 bájt

Code

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

EAP adat típusok

- 1: Identitás (Identity)
  - A végpont identitásának lekérdezése
- 2: Figyelmeztetés (Notification)
  - Megjelenítendő üzenet
- 3: Elutasítás (Nak)
  - Érvénytelen vagy értelmezhetetlen típus
  - Csak válasz esetén

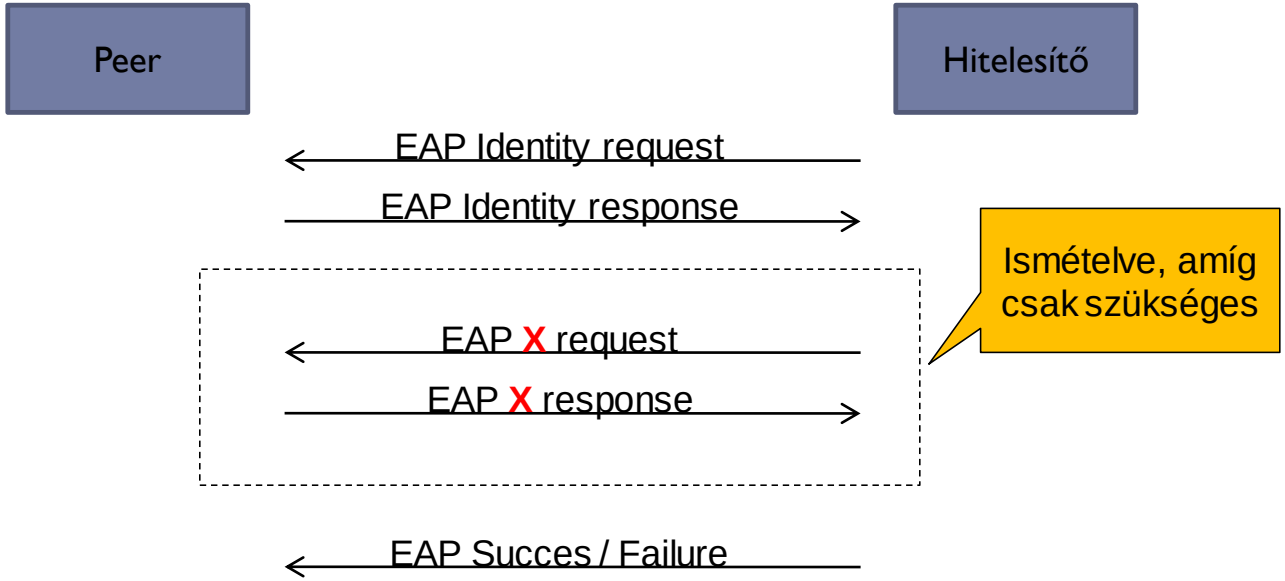
EAP hitelesítő típusok

- 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

…

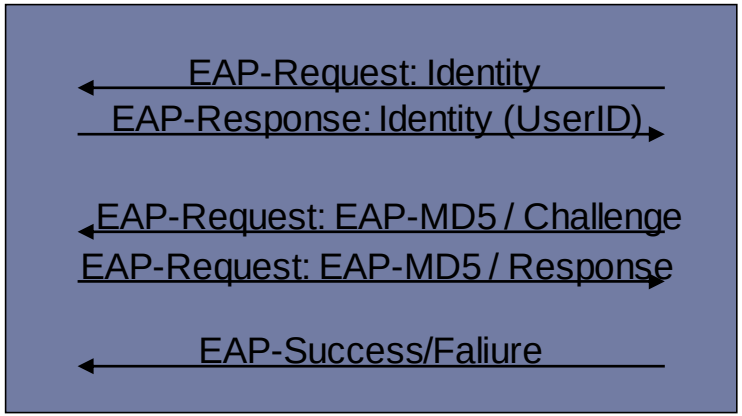
- 13: EAP-TLS
- 21: EAP-TTLS
- 25: PEAP
- 29: EAP-MSCHAP-V2

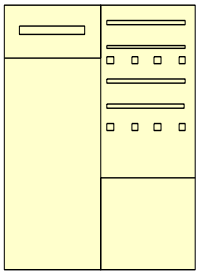
EAP üzenetciklus



EAP-MD5

- IETF RFC 3748
- Analóg a CHAP hitelesítéssel

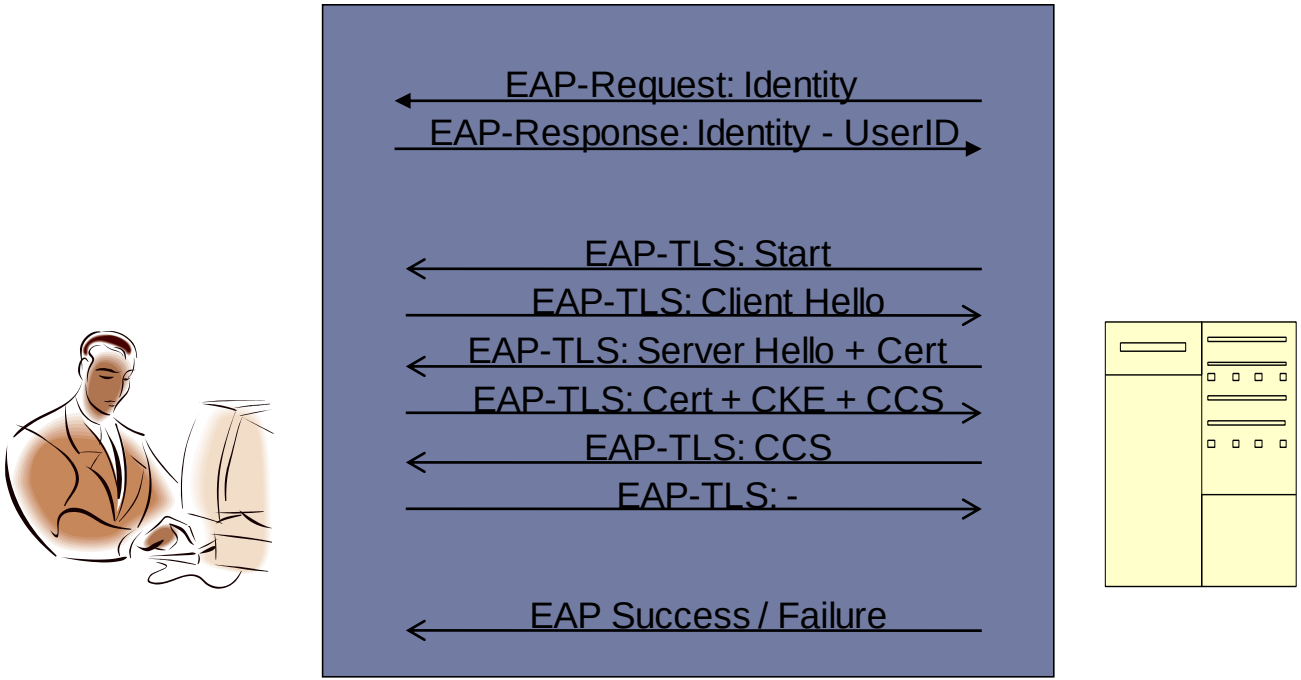




EAP-TLS

- 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



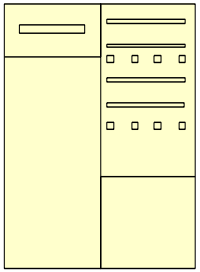
C/SKE: Client/Server Key Exchange, CCS: Change Cipher Spec

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



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

EAP-Request: Identity

EAP-Response: Identity – No real ID

PEAP: Start

PEAP: Client Hello

PEAP: Server Hello + Cert

PEAP: CKE + CCS

PEAP: CCS + Success/Failure

EAP-Req: EAP-TLV Req. identity

EAP-Resp: EAP-TLV UserID

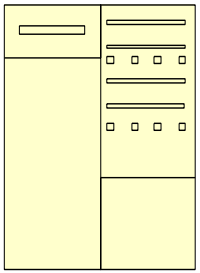
EAP-Req: EAP-TLV / EAP X

EAP-Resp: EAP-TLV / EAP X

EAP Success / Failure

1. fázis
TLS Setup

2. fázis
Beágyazott EAP



EAP összehasonlítás

- EAP protokollok összehasonlítása

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Kliens hitelesítés	MD5	Tanúsítvány	Bármi	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 leni

RADIUS

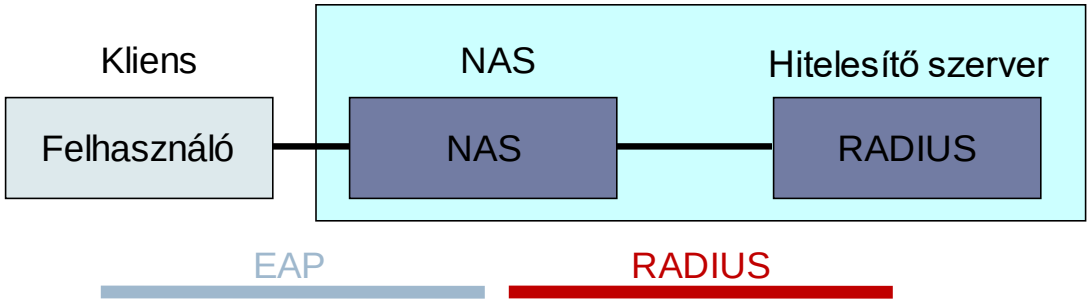
- Remote Authentication Dial In User Service
  - Eredetileg a betárcsázós felhasználóknak (Merit Networks és Livingston Enterprises)
  - Ma már széleskörű használat
    - Azonosítás nem csak dial-in felhasználáskor
    - Távközlésben számlázáshoz
- AAA szolgáltatás nyújtása

RADIUS tulajdonságok

- Legfőbb tulajdonságok
  - UDP alapú (kapcsolatmentes)
  - Állapotmentes
  - Hop by hop biztonság
- Hiányosságok
  - End to end biztonság támogatása
  - Skálázhatósági problémák

RADIUS kapcsolat

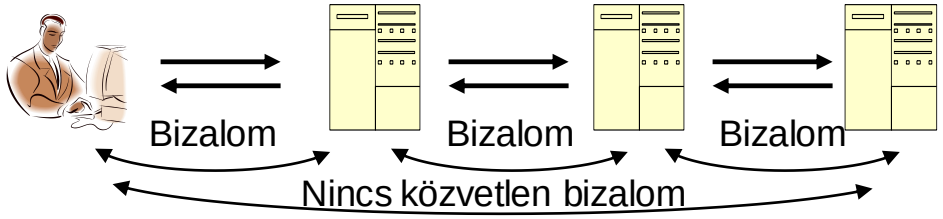
- Kliens - NAS - RADIUS



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

RADIUS proxy

- Több RADIUS szerver is részt vehet a hitelesítésben
  - A szerver, aki a kérést kapja képtelen a hitelesítést elvégezni, ezért továbbítja a kérést
  - Egymás között is kliens-szerver viszony
  - Hop by hop bizalom



  - A felhasználó csak az első szerverben bízik

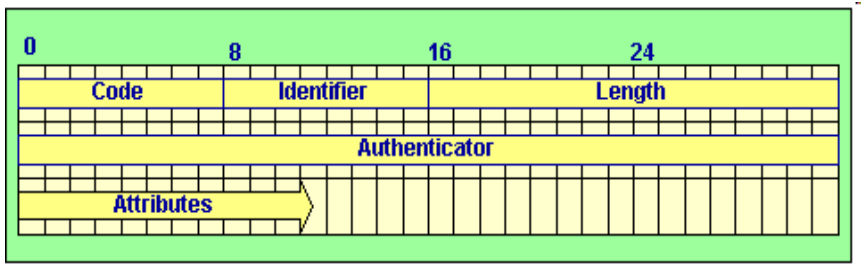
- RADIUS tartományok (realm)

RADIUS kacsolat

- UDP forgalom
  - 1812 –es port (De használatos a 1645 is)
  - Hiba esetén az üzeneteket meg kell ismételni (retransmission timers)
- Jól illeszkedik az állapotmentes működéshez
  - Multithread támogatás

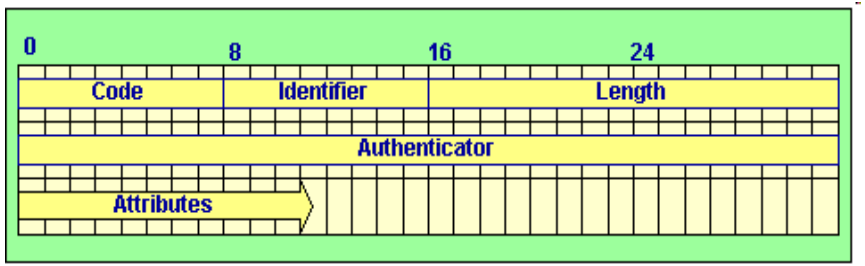
RADIUS üzenetek

- 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 bájt

Radius üzenetek (folyt.)



- Authenticator
  - 16 bájt hitelesítés
  - Request authenticator:
    - Hitelesítés kérés: 16 bájt véletlen érték
    - Lehet 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

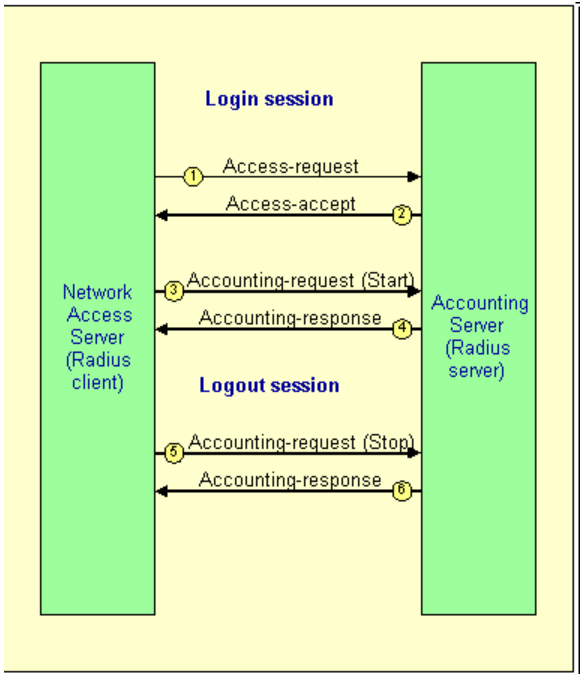
Attribútum szótár példa

```
#  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



RADIUS alap hitelesítés

- Alapból jelszavas hitelesítés vagy kihívás alapú hitelesítés
- 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 bővíthetőek

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)

RADIUS CHAP hitelesítés lépései

- NAS – CHAP / EAP Identity + EAP-MD5
  - Kihívás generálása: *CHAPAuthenticator*
  - Felhasználó név, jelszó bekérése
- 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

RADIUS Jogosultságok

- A jogosultságok alapján
  - Magánhálózatok felépítése a felhasználó azonosítása alapján
  - Különböző forgalmi osztályokba sorolás

- Legtöbb esetben csak NAS hozzáférés engedélyesése/tiltása

RADIUS számlázás

- Hálózati számlázás
  - A használt szolgáltatás, eltelt idő, küldött/fogadott csomagok és bájtok a viszony alatt, átlagsebesség, stb…
- Kapcsolat naplózása
- Parancsok naplózása

RADIUS számlázás üzenetek

- Kliens/szerver modell
  - A kliens számlázási adatokat küld a szerver számára, hogy az feldolgozza
  - A szerver akár proxyzhatja is az adatokat
- Biztonságos kommunikáció – hasonló a hitelesítéshez és jogosultságokhoz
- AVP mezők az adatok számára

- Az üzeneteket nyugtázni kell
  - Ha nem érkezik nyugta, akkor újraküldés
  - Ha sokáig nem jön nyugta, akta a küldés leáll, inkonzisztencia léphet fel!

Egyéb AA(A) lehetőségek

- Idősorrendben:
  - TACACS (AA)
  - XTACACS
  - TACACS+ (Cisco)
  - *RADIUS*
  - DIAMETER

Diameter

- Kétszer nagyobb mint a RADIUS
  - IMS (IP Multimedia Subsystem)
  - IETF RFC 3588 (Diameter Base Protocol)

- A RADIUS hibák javítása
  - Skálázható
  - Biztonságos
  - Könnyen adminisztrálható

RADIUS – Diameter
Felek viszonya

- RADIUS
  - Tiszta kliens-szerver protokoll. A RADIUS csak válaszol (csak kliens szerepben kérdez)
- Diameter
  - Peer-to-peer jelleg. Működik a kliens-szerver kapcsolat is, de bármelyik résztvevő kérdezhet is
  - Pl.: újrahitelesítés kérése

- RADIUS
  - Állapotmentes protokoll. Legalábbis minimális információt tárol (pl. üzenetek azonosítója)
  - Egyszerű több szálú implementáció
- Diameter
  - Állapotokat tárol

RADIUS – Diameter Üzenetek

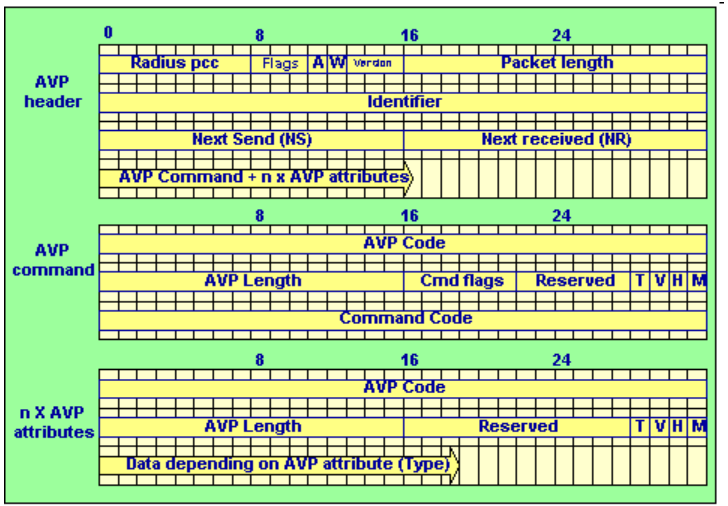
- RADIUS
  - Minimális fejléc (kód, azonosító, hossz, hitelesítő) + AVP csomagok
- Diameter
  - Alapvetően hasonló a RADIUS üzenetekhez
  - + fejléc információk: verziószám, alkalmazás ID, end-to-end azonosító, jelzőbitek
  - + AVP információk: Gyártó azonosító, kontroll bitek

- RADIUS
  - UDP csomagolás. Újraküldés, ha szükséges
- Diameter
  - Kapcsolatorientált szállító protokoll. SCTP vagy TCP. Megbízható szállító protokoll, nem az alkalmazás kezeli a duplikált üze neteket vagy az újraküldést. 3868 port
  - Sokszor az ACK üzenetek miatt nagyobb a forgalom, mint RADIUS esetben

- RADIUS
  - Nincs hibaüzenet. Ha hibás az üzenet, akkor csendben eldobja
- Diameter
  - Hibaüzenetek. Hibabit (E bit)

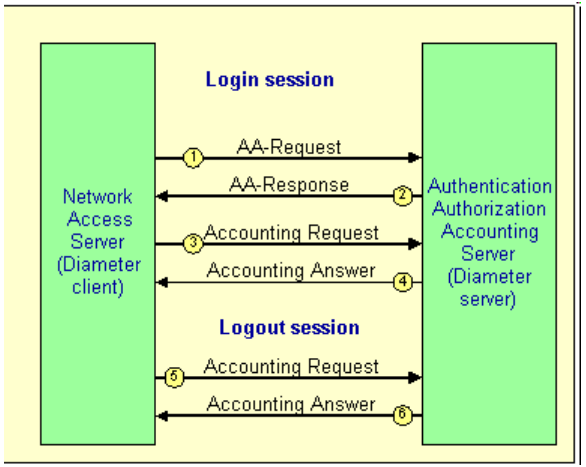
Diameter üzenetek

- Kérés/válasz:



Diameter üzenetváltás

- Számlázás esetén
  - Accounting Data Interchange Format - ADIF



RADIUS – Diameter Együttműködés

- RADIUS
  - Proxy szerverek, amelyek láncot alkothatnak
- Diameter
  - Agents (ügynökök), amelyek láncot alkothatnak
    - Relay agent: routing információk
    - Proxy agent: üzenetek proxyzása
      - Hasonló a realy-hez, de módosíthat is
      - End-to-end biztonság kizárva
    - Redirect agent: A kérés átirányítása
    - Translation ügynökök: Átjáró más protokollokhoz

RADIUS – Diameter Kompatibilitás, bővíthetőség

- RADIUS
  - Nincs támogatás a kompatibilitáshoz (Nem jó üzenetek csendes eldobása)
- Diameter
  - Képesség egyeztetés
  - Mandatory (M) bit az AVP csomagokban
  - RADIUS együttműködés. Működnek a RADIUS AVP és parancskódok

- RADIUS
  - Bővíthető AVP üzenetek (26:VSA)
- Diameter
  - Bővíthető AVP üzenetek (VSA) + 32 bites parancskódok
  - Új AAA alkalmazások, új procedúrák

RADIUS – Diameter Skálázhatóság

- RADIUS
  - UDP üzenetek. Egyfelől jó, de nincs torlódás vezérlés. Adatvesztés is lehet miatta
  - Az egyik fő ok, hogy új protokoll kellet!
  - 8 bites azonosító: mindössze 256 függőben lévő üzenetcsere (Bár létezik megoldás: az IP paramétereket kell változtatni)
- Diameter
  - Torlódásvezérlés
  - 32 bites azonosító
  - 32 bitre igazított üzenetek a gyorsabb feldolgozás miatt
  - Sok állapot (szállítási rétegben + viszonyrétegben)

RADIUS - Diameter Biztonság

- RADIUS
  - Közös titok, hop-by-hop
  - Gondok a közös titkok kezelésével (túl sok adminisztráció) és az authenticator helyes előállítása is kérdéses (kiszámíthatatlan és ismétlés nélkülinek kell lennie)
  - Legtöbbször csak a jelszó titkosított
  - Proxyk használatával mindenki belenyúl az üzenetbe
- Diameter
  - Kötelező IPSec támogatás, opcionális TLS. Szerverek számára mindkettő kötelező. Üzenetváltásnál kötelező használni.
  - Hop-by-hop mellett end-to-end biztonság is

RADIUS - Diameter

- Diameter jobb: (Nem csoda, ezért csinálták)
  - Jobb skálázhatóság
  - Jobb üzenetkezelés (hibaüzenetek)
  - Együttműködés, kompatibilitás, bővíthetőség
  - Nagyobb biztonság
    - IPSec (+ TLS)
    - End-to-end titkosítás
- RADIUS
  - még használható, de lassan már kár ragaszkodni hozzá
- Diameter hátránya:
  - nagy komplexitás