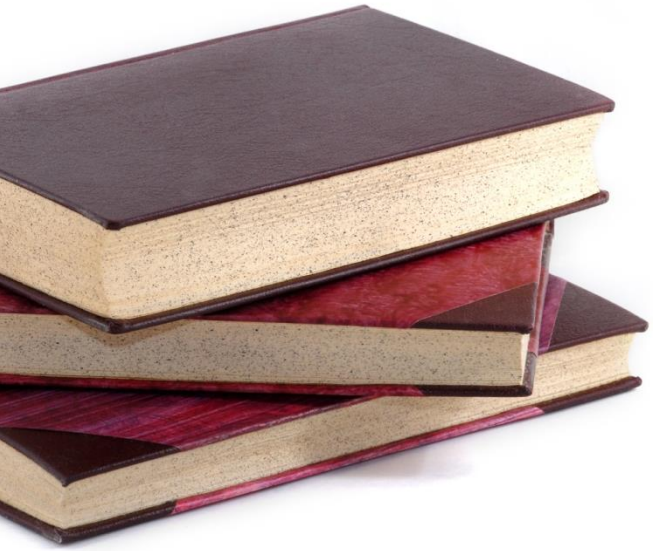
RL
crunch it connected

Cursul 11



11

Autentificare

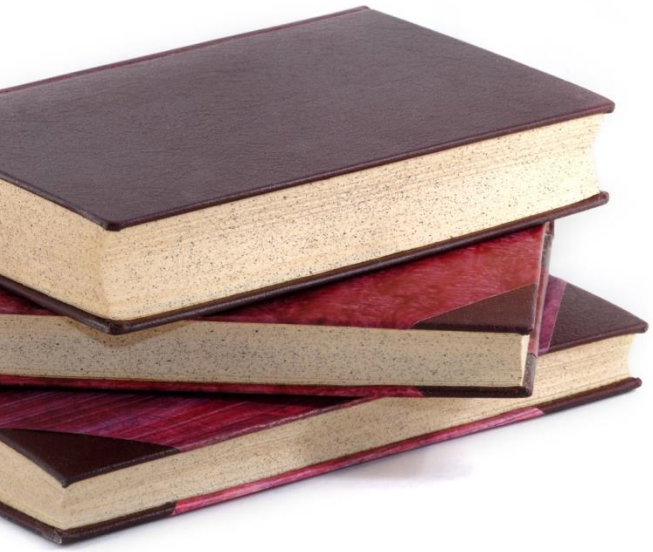
12-13 ianuarie 2016

Obiective

- Recapitulare: Securitatea în rețele
- Metode de autentificare
- EAP
- PPP
- PPPoE
- 802.1X
- RADIUS

RL
crunch it connected

Cursul 11

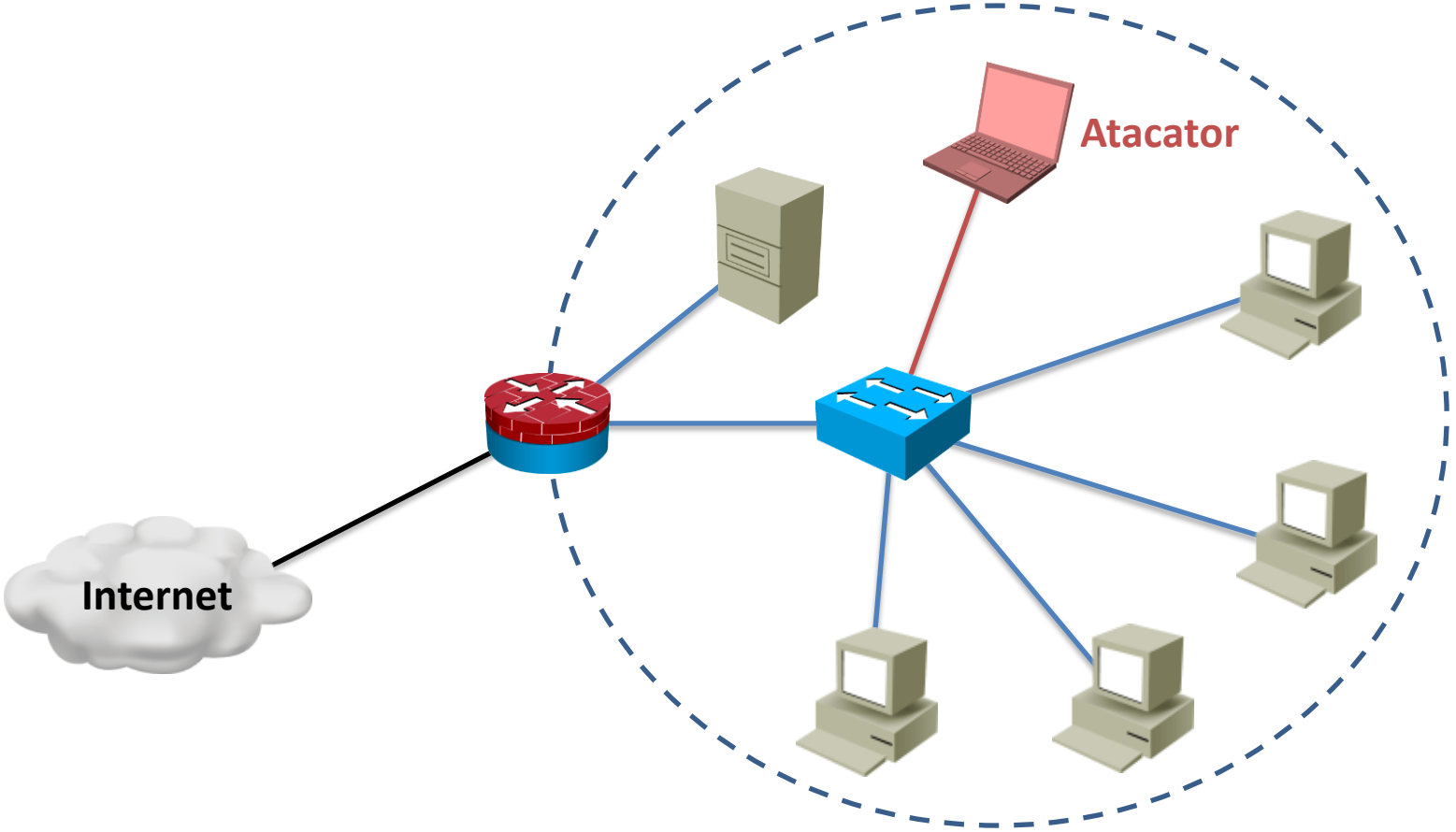


Recapitulare

- Riscuri de securitate
- Calitățile securității
- AAA

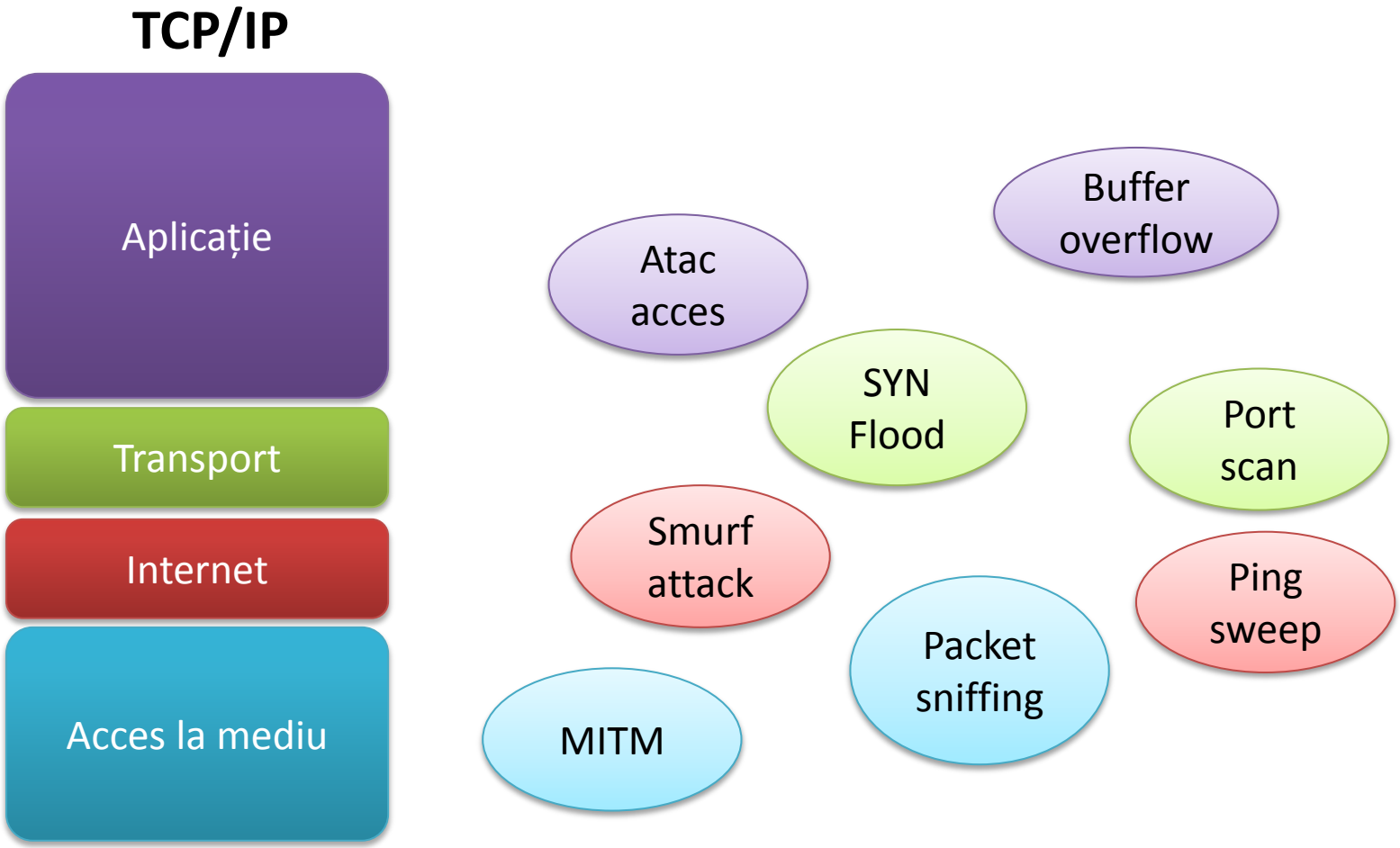
Riscuri de securitate

- Un firewall dedicat protejează rețeaua de atacuri din exterior
- Dacă un atacator obține acces fizic la rețea, ce atacuri poate efectua? La ce nivel sunt situate aceste atacuri?



Nivele de atac

- 802.1x încearcă să protejeze rețeaua de atacurile de la toate nivelele superioare prin securizarea nivelului **Acces la mediu**



Recapitulare: Concepte de securitate

- Autentificare
  - Sursa și destinația sunt cine spun că sunt

- Confidențialitate
  - Doar sursa și destinația pot vizualiza informația

- Integritate
  - Mesajul ajuns la destinație nu a fost modificat pe parcurs

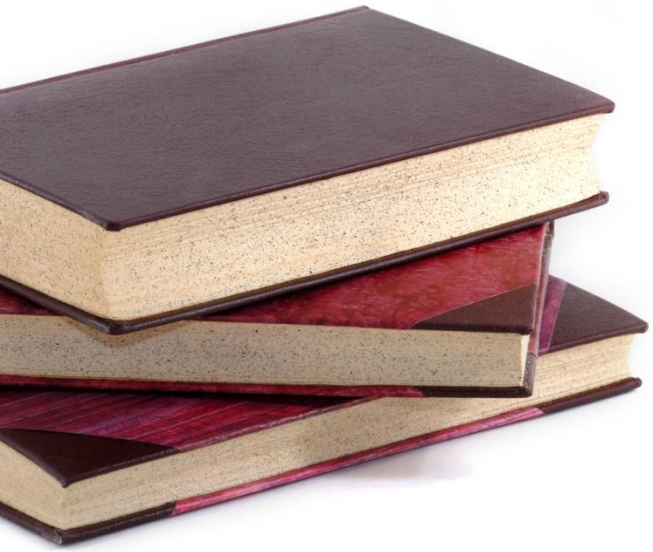
AAA

- Un sistem de securitate trebuie să ofere suport pentru trei operații de bază:

Authentication	• Clientul este cine spune că este și poate accesa sistemul • Exemplu: Utilizatorul student cu parola student poate accesa un anumit sistem Linux
Authorization	• Clientul are dreptul să facă operația pe care o încearcă • Exemplu: Utilizatorul student poate crea fișiere în /home/student/ dar autorizarea va eșua dacă încearcă să creeze în /root/
Accounting	• Acțiunile clientului sunt contabilizate • Exemplu: Log-uri de acces

RL
crunch it connected

Cursul 11

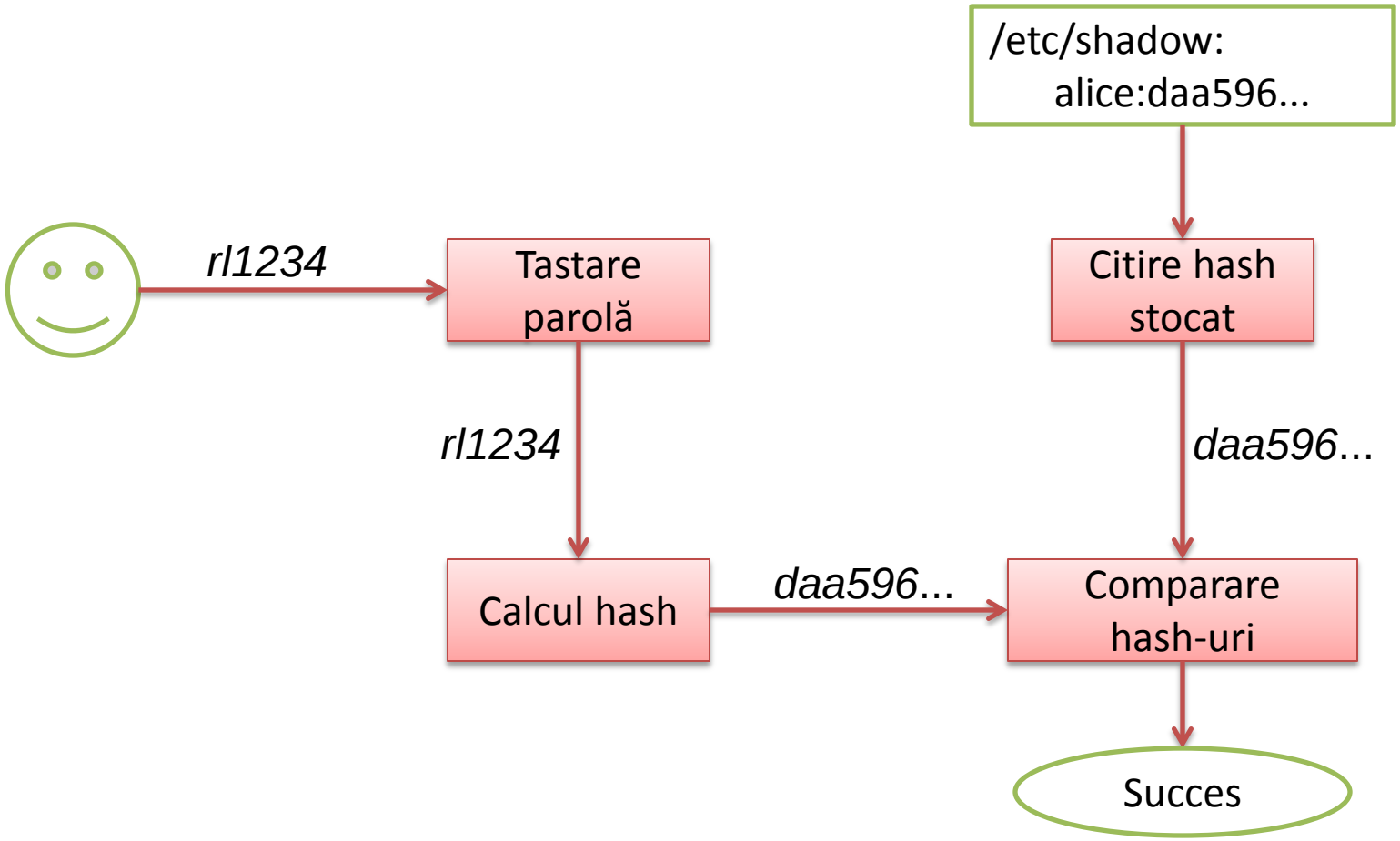


Metode de autentificare

- Autentificare cu parole
- Autentificare cu challenge-uri
- Autentificare TLS
- EAP
- EAPOL

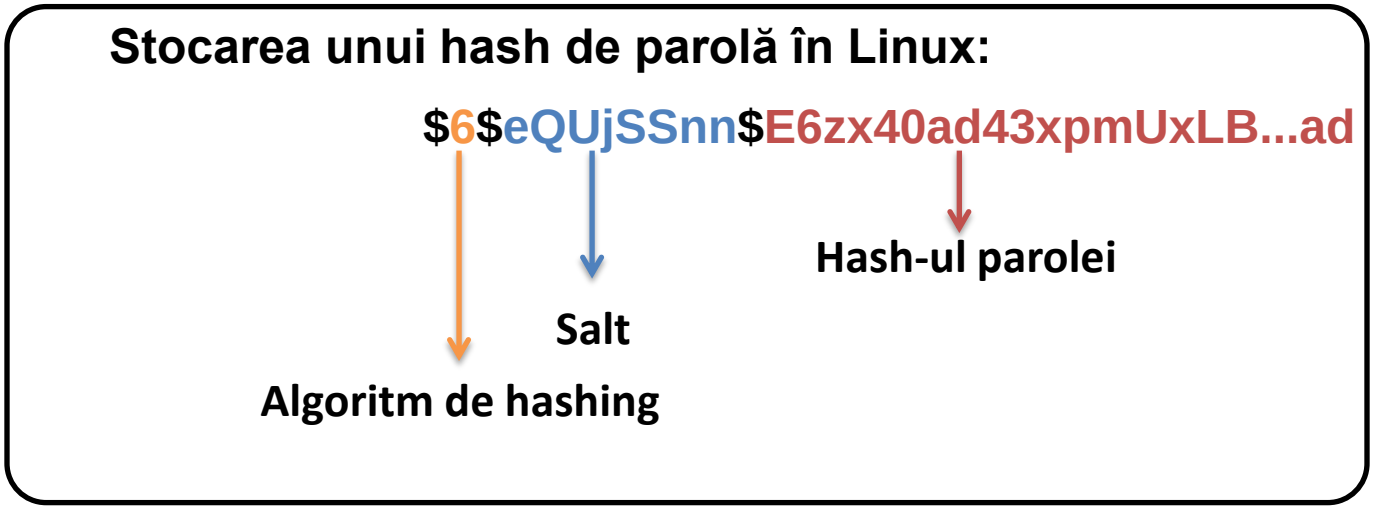
Autentificare cu parole

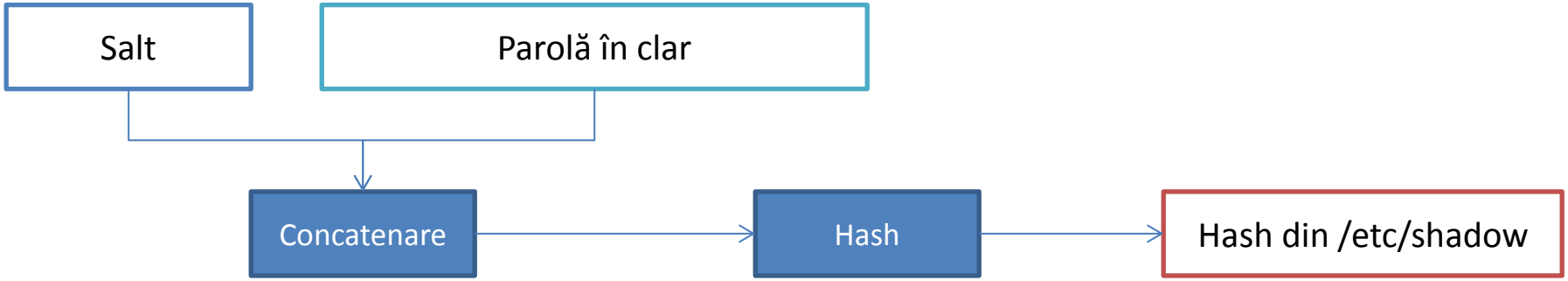
- Stocarea directă a parolelor nu este recomandată
  - Dacă un atacator accesează parolele, acestea sunt compromise imediat



Autentificare cu parole

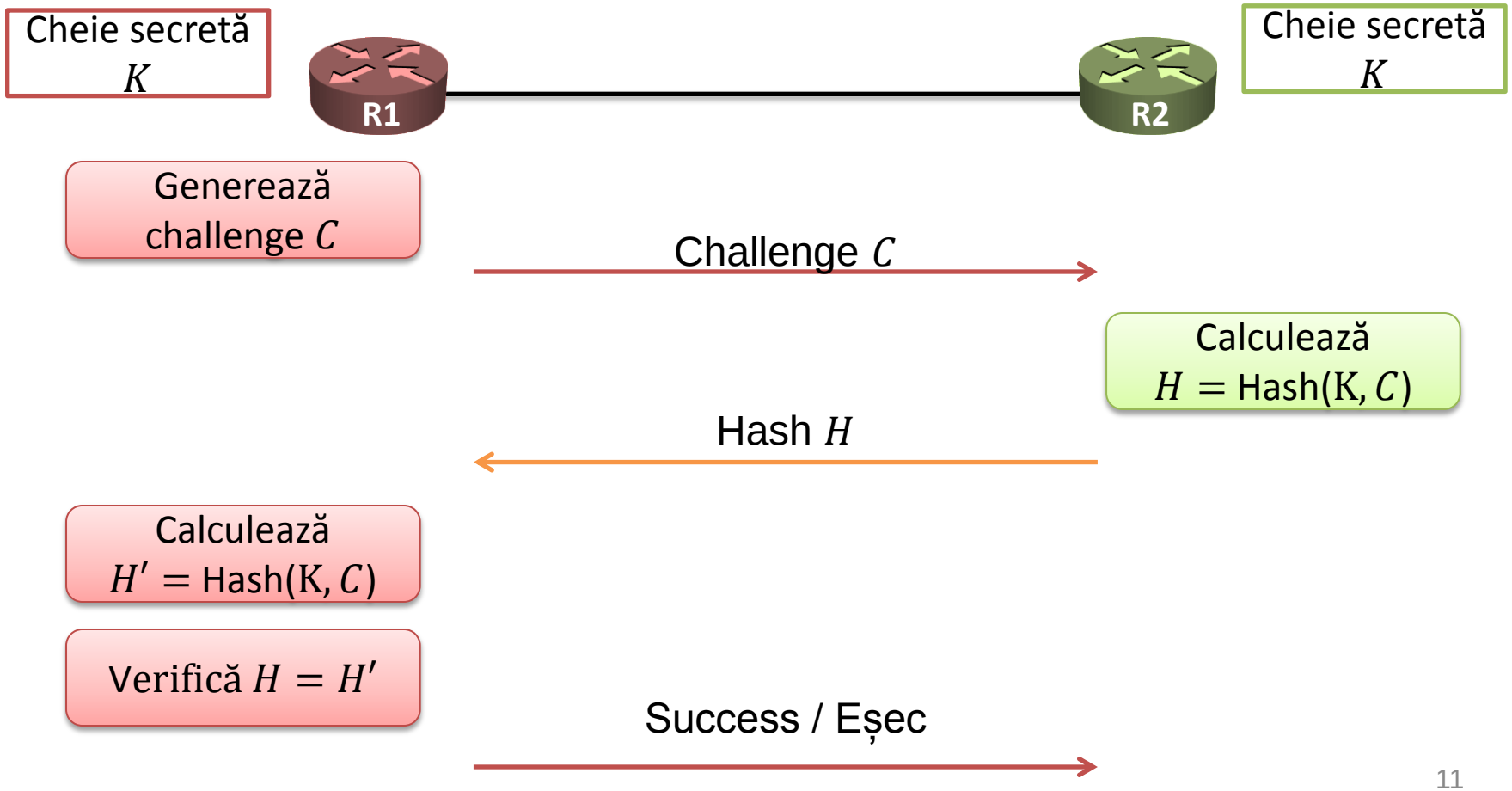
- Parolele sunt stocate sub formă de hash
- Adăugarea unui salt îmbunătățește securitatea hash-ului
  - Îngreunează folosirea de baze de date de hash-uri precalculate





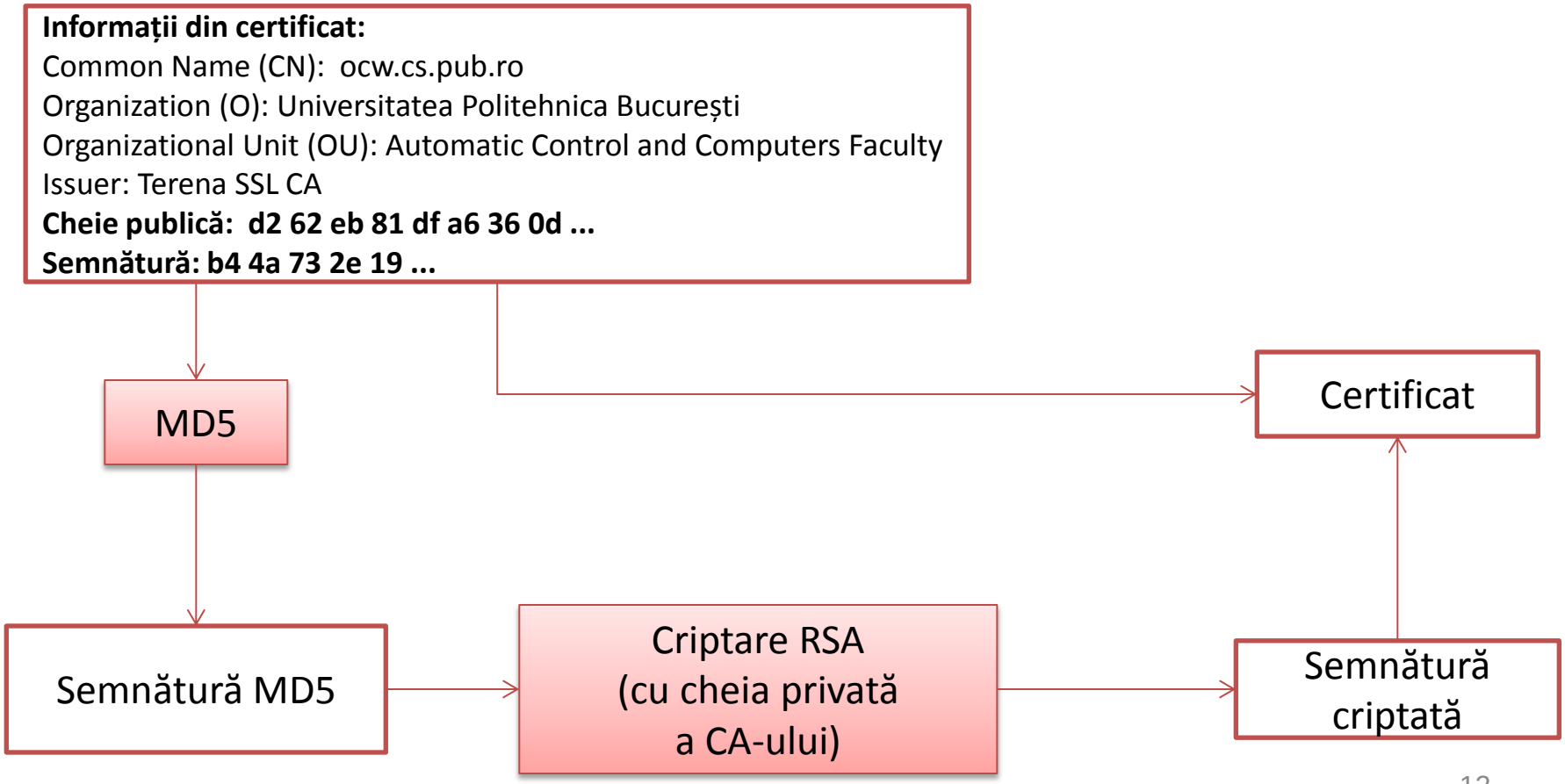
Autentificare cu challenge

- Solves the problem of authenticating endpoints when a secret key is pre-shared, without transmitting the key over the wire



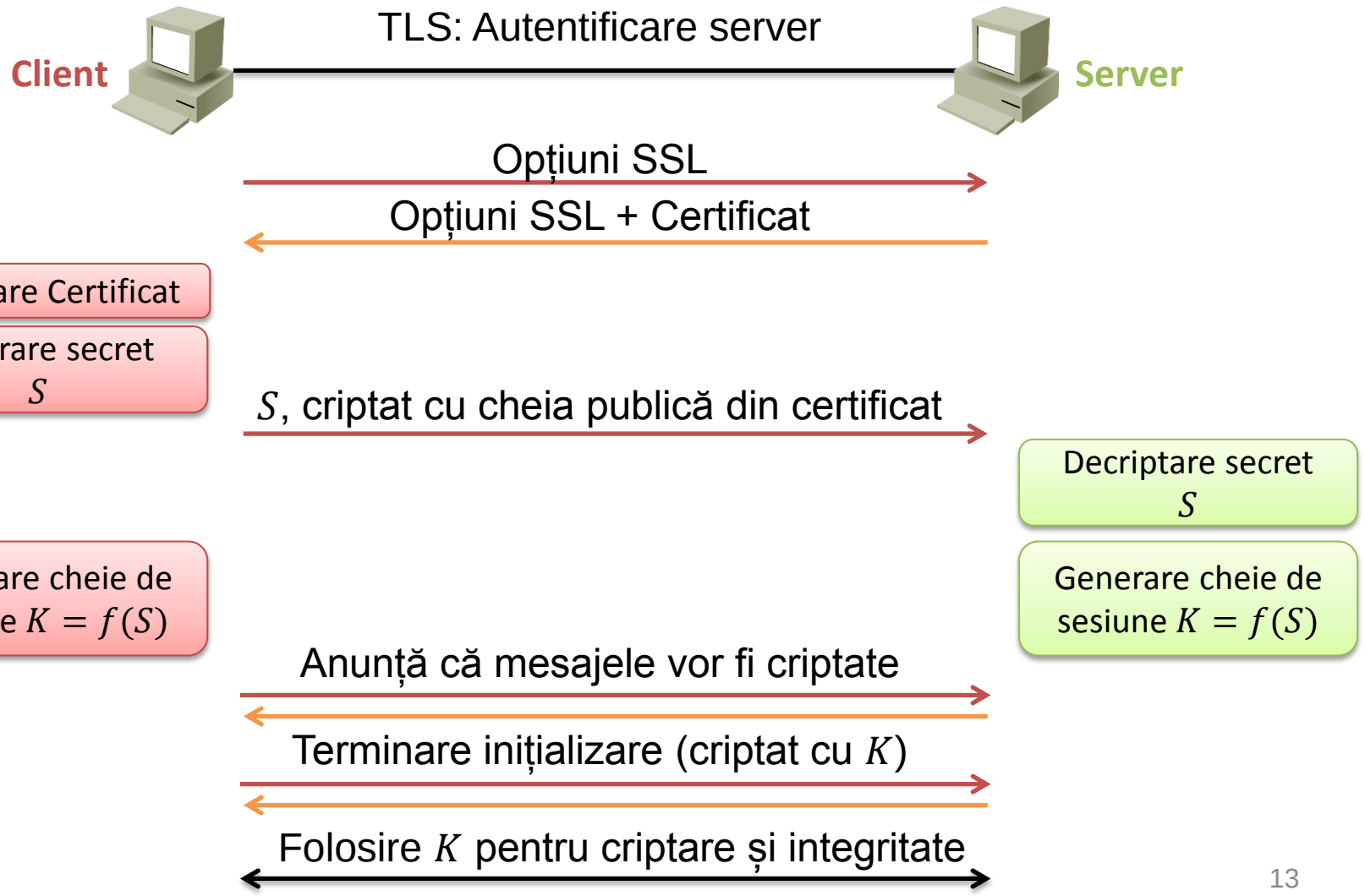
Autentificare cu certificate

- Certificatele conțin cheia publică a unei entități, semnată cu cheia privată a unui CA (Certificate authority)

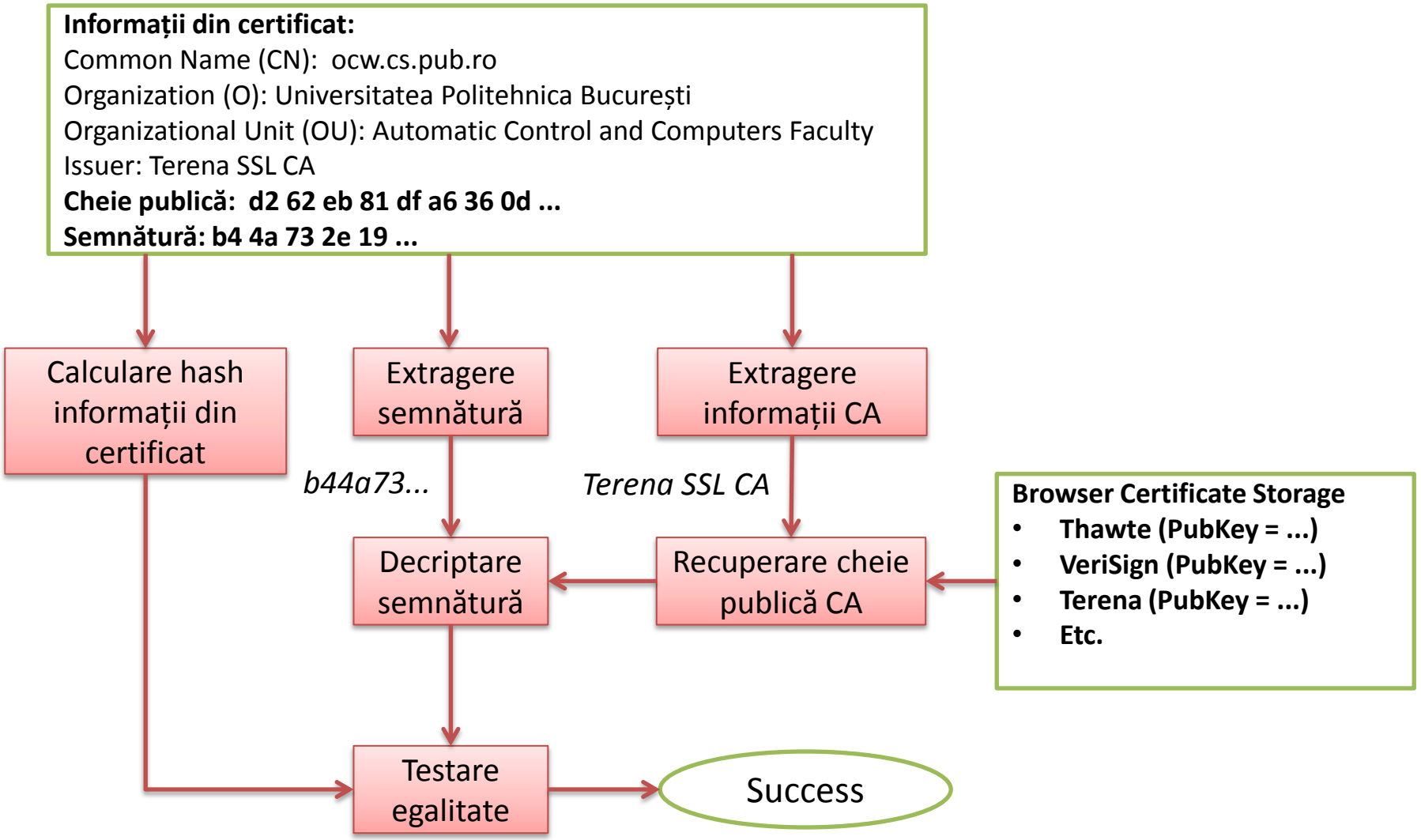


TLS

- TLS este folosit de numeroase servicii (inclusiv HTTPS)



TLS: Verificare certificat



EAP

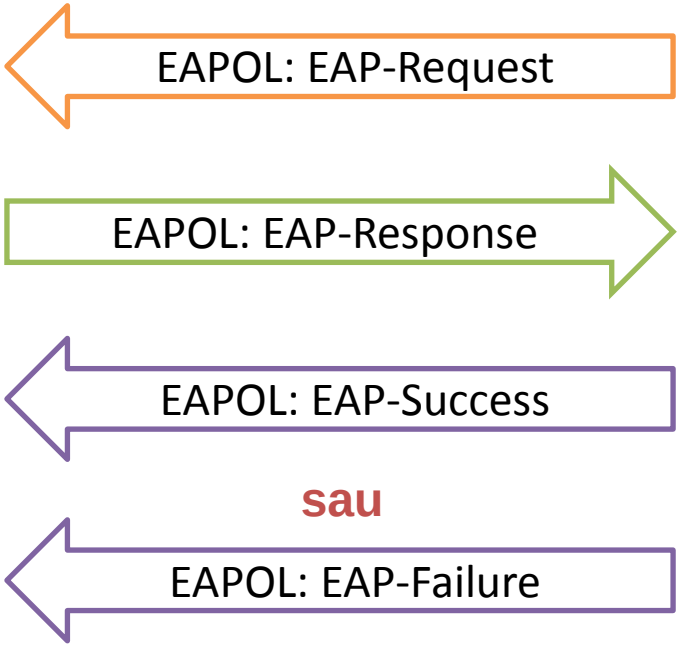
- EAP este un format de mesaje care poate încapsula diferite protocoale de autentificare
- Nu e folosit doar pentru 802.1X
  - 802.11n folosește EAP în WPA și WPA2
- EAP nu poate fi folosit direct pentru transmiterea cadrelor
  - Este necesar un alt protocol care să transmită informația EAP
- Antetul EAP specifică doar metoda ce va fi folosită pentru autentificare

EAP

- Informația utilă protocolului de autentificare este situată în **EAP-Method**
- Există 4 mesaje EAP:
  - Request: un nod cere informații de autentificare altui nod
  - Response: un nod oferă informații de autentificare altui nod
  - Success: anunță că autentificarea s-a făcut cu succes
  - Failure: anunță că autentificarea a eșuat

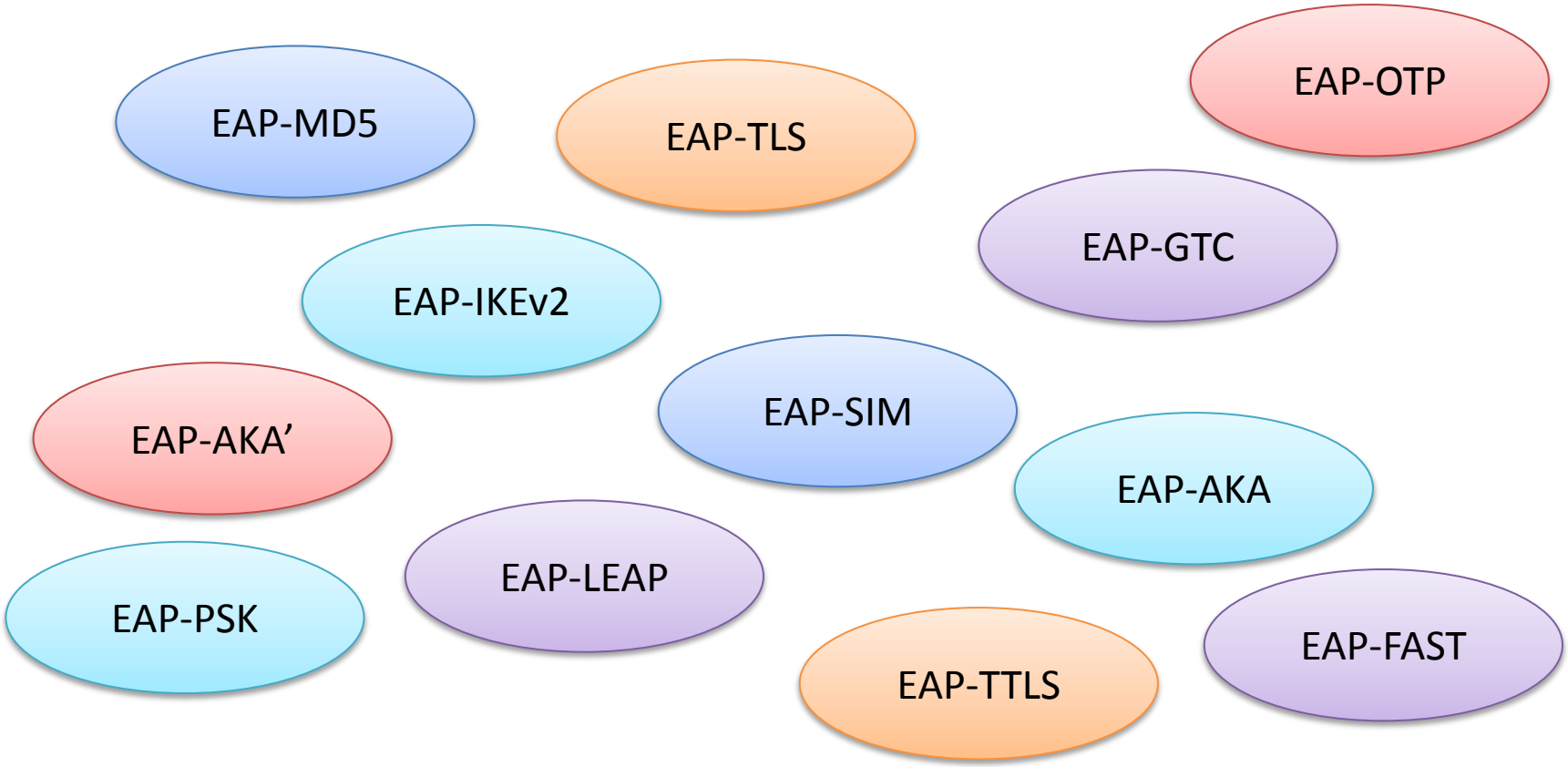
EAP – Exemplu de comunicație

- EAPOL este folosit pentru transportul mesajelor EAP



Exemple EAP-Method

- În interiorul mesajului EAP sunt incluse datele metodei de autentificare
- EAP suportă un număr mare de metode:



Exemple EAP-Method

- Dintre metodele EAP, trei sunt definite de RFC-ul EAP
- Pentru fiecare dintre acestea, solicitatorul poate refuza metoda și sugera autentificatorului alte metode

EAP-MD5

- Mesajul de EAP-Request conține un Challenge
- Autentificatorul așteaptă un EAP-Response cu challenge-ul hash-uit cu HMAC-MD5 (cheia pentru HMAC e parola utilizatorului)

EAP-GTC

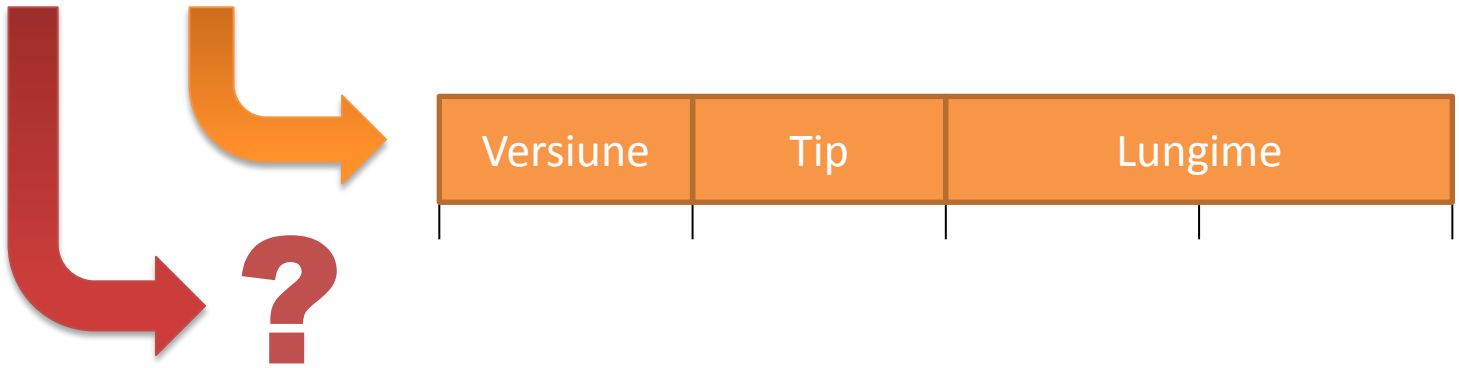
- Generic Token Card

EAP-OTP

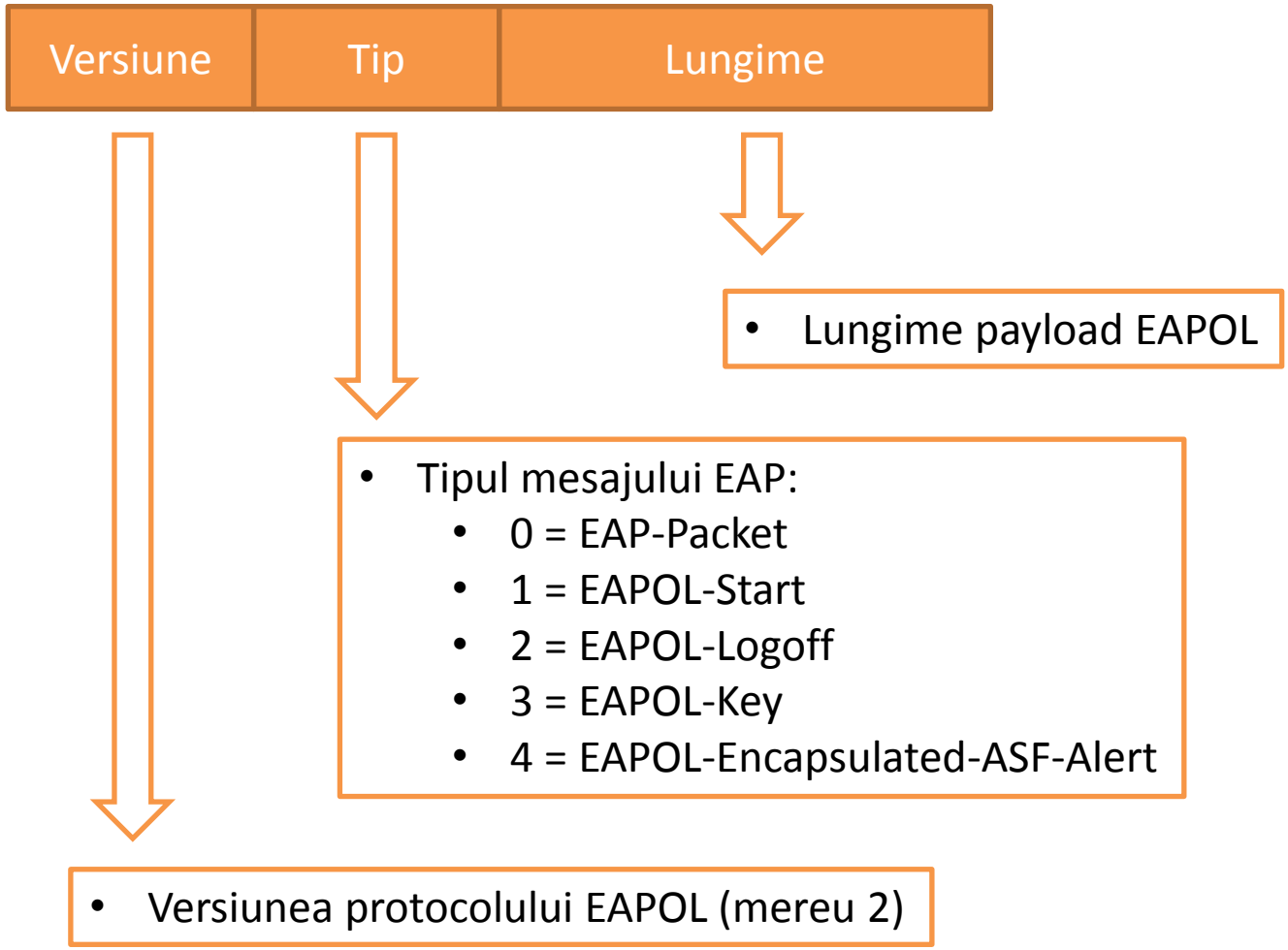
- One Time Password

EAPOL

- EAPOL este încapsularea folosită peste informația EAP pentru a putea funcționa peste rețele 802.3 și 802.11

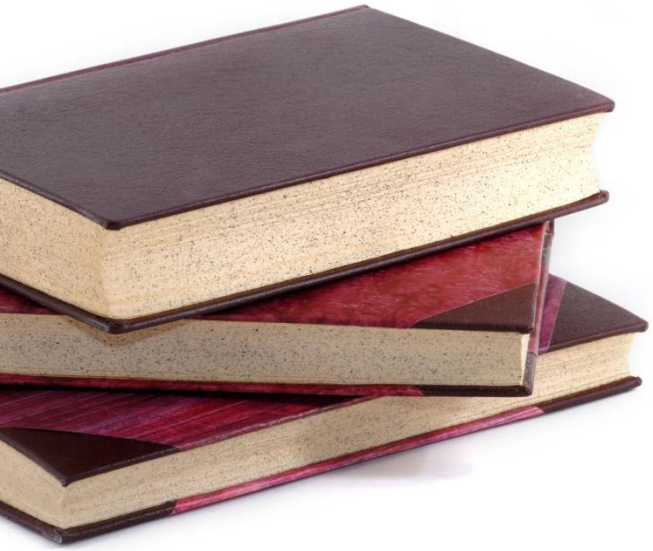


EAPOL


Versiune
Tip
Lungime
• Lungime payload EAPOL
• Tipul mesajului EAP:
• 0 = EAP-Packet
• 1 = EAPOL-Start
• 2 = EAPOL-Logoff
• 3 = EAPOL-Key
• 4 = EAPOL-Encapsulated-ASF-Alert
• Versiunea protocolului EAPOL (mereu 2)

RLO
crunch it connected

Cursul 11

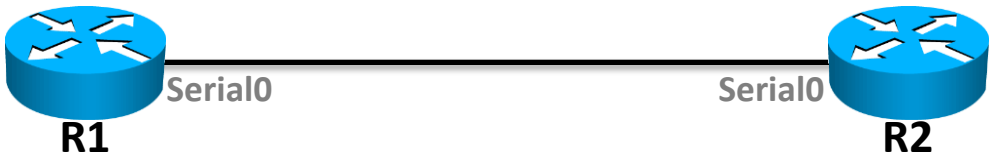


PPPoE

- Istorie
- Componente
- EAP
- EAP-Methods
- EAPOL

PPP

- Point to Point Protocol
- Protocol de nivel legătură de date, folosit pentru legături punct la punct
  - Linii seriale, linii telefonice, fibră optică, etc.
- Ethernet folosește adrese MAC la nivel 2; are sens folosirea adresării pe o linie punct la punct?
  - R: Nu, și PPP nu include adrese în antet
- Are sens implementarea de autentificare pe o linie punct la punct?

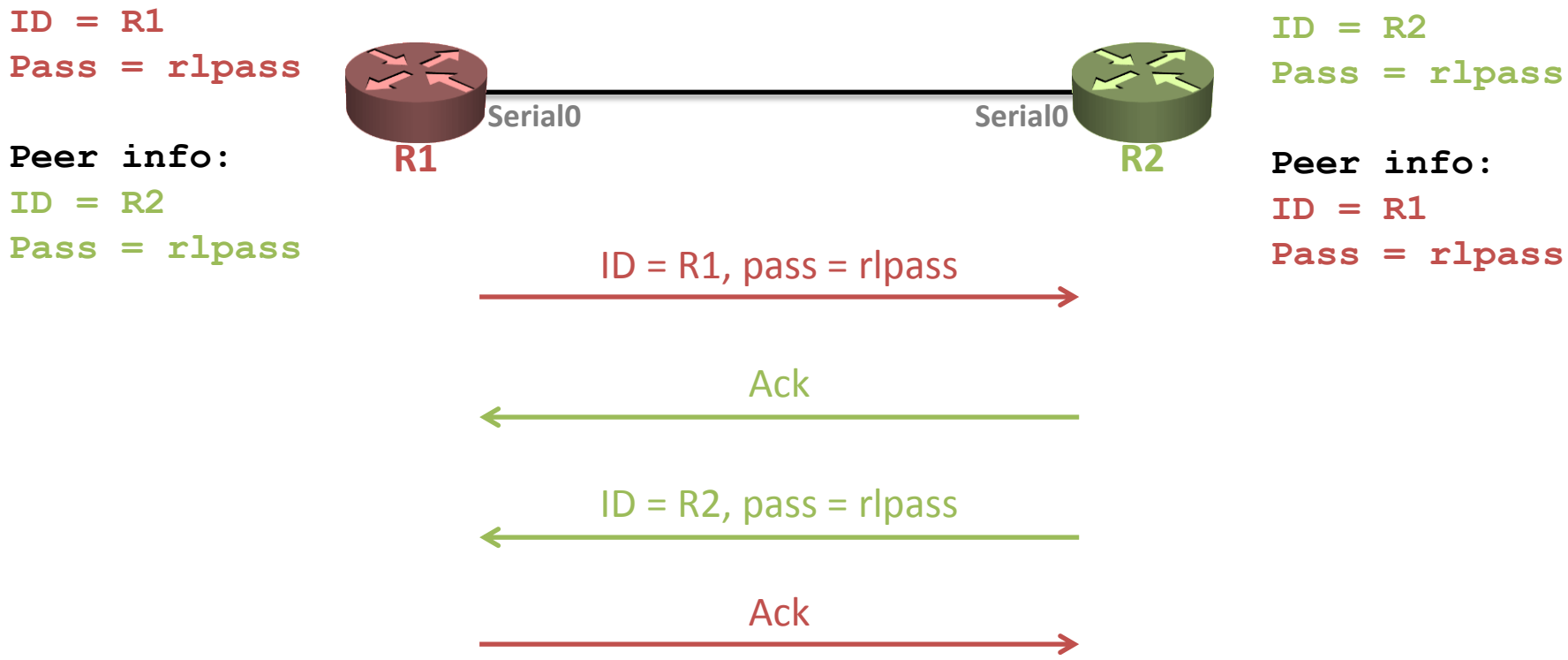


PPP

Autentificare	Stabilește cu succes conexiunea doar după o autentificare realizată cu succes
Compresie	Datele pot fi comprimate înainte de trimiterea pe fir pentru a reduce consumul de trafic
Criptare	Datele pot fi trimise criptat

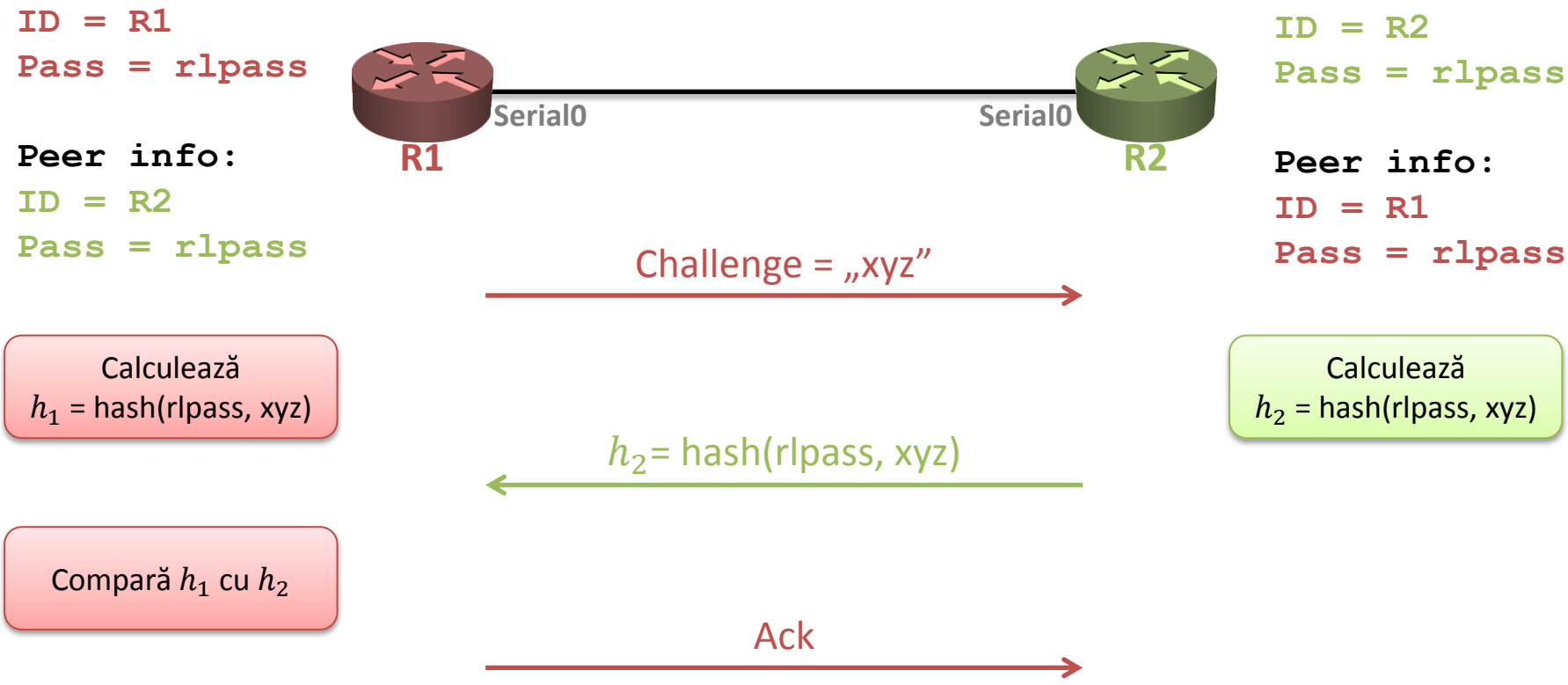
PPP – Autentificare PAP

- Plain Authentication Protocol
- Care sunt riscurile folosirii metodei de autentificare PAP?



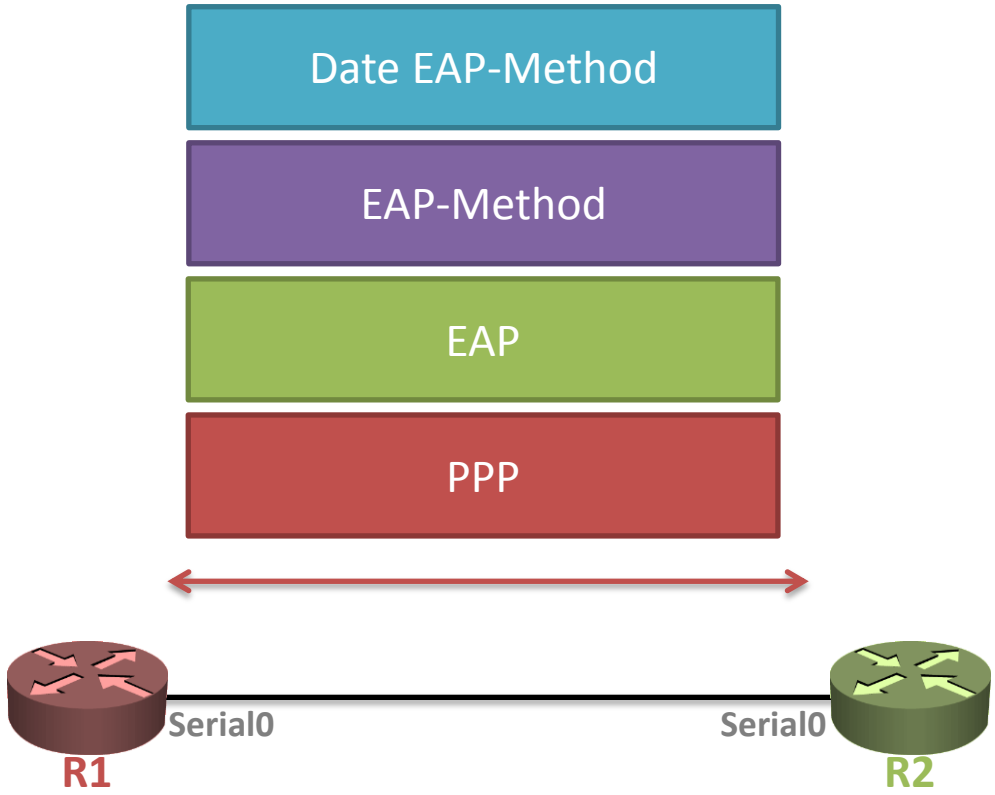
PPP – Autentificare CHAP

- Challenge Authentication Protocol
- Challenge-ul se trimite la stabilirea legăturii și după intervale aleatoare de timp



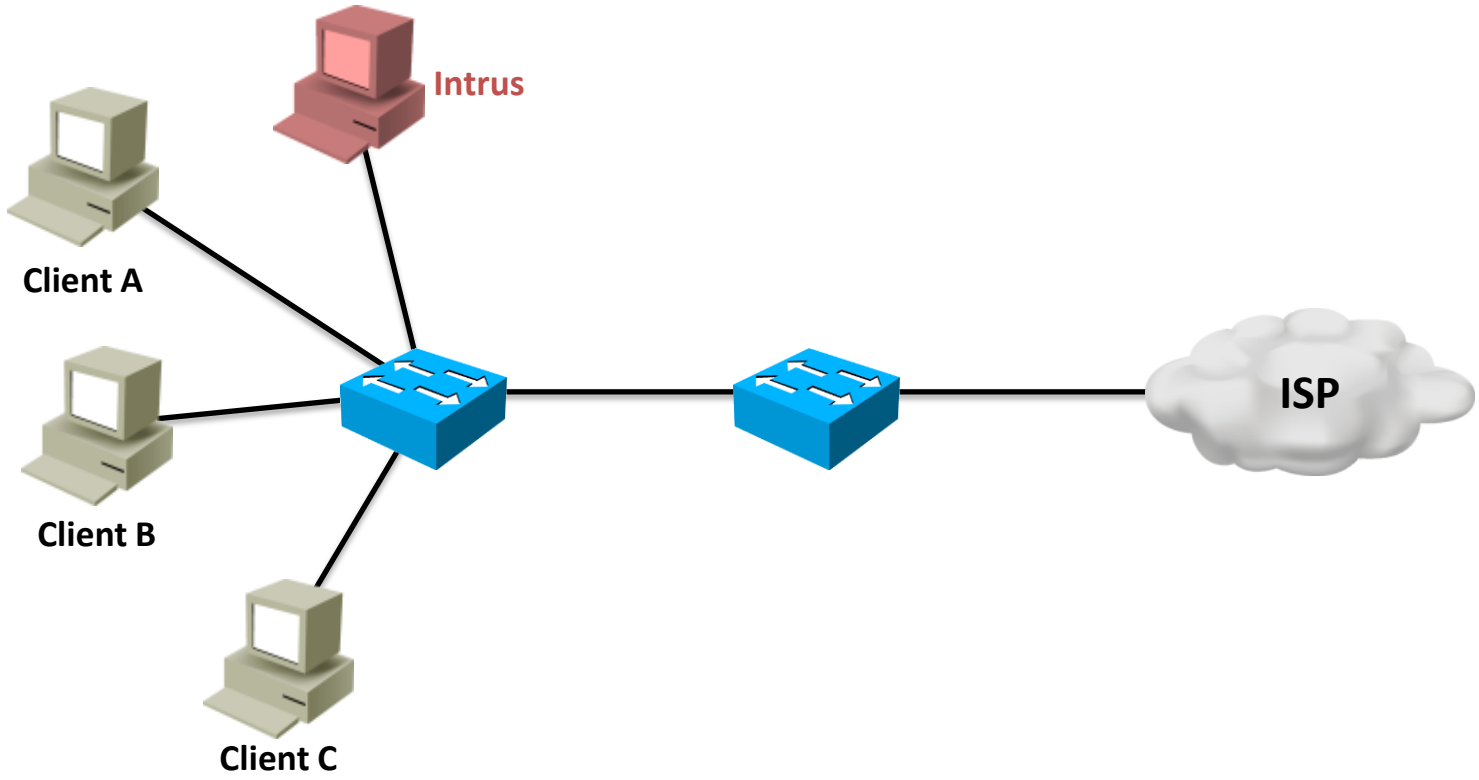
PPP – Autentificare EAP

- Orice metodă EAP poate fi folosită pe post de autentificare în PPP



Autentificare în rețele Ethernet

- Rețelele Ethernet sunt folosite inclusiv de ISP-uri pentru a asigura conectivitate la Internet
- Ethernet = mediu multiacces fără mecanism de autentificare
  - Oricine se poate conecta la rețea
  - Este necesar un mecanism de autentificare

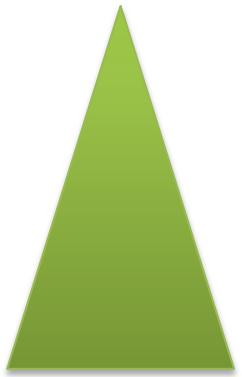


Soluții autentificare în rețele Ethernet

- Înlocuim rețeaua Ethernet cu alt mediu fizic cu autentificare
  - Prea scump
- Folosim autentificare la nivel de port pe switch (802.1X)
  - Switch-urile trebuie să fie compatibile 802.1X, ceea ce înseamnă switch-uri mai scumpe
- Folosim un proxy cu autentificare HTTP (captive portal)
  - Clientul trebuie să facă manual autentificarea printr-o pagină web
  - Clientul nu poate fi un ruter
- Folosim un protocol de nivel 2 cu autentificare peste protocolul de nivel 2 Ethernet

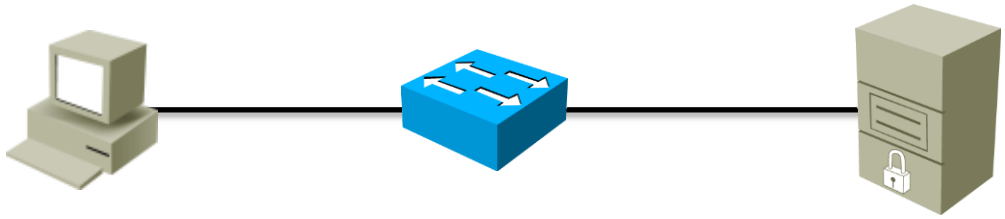
PPPoE – Avantaje

- Folosește infrastructura Ethernet existentă
- Pentru switch-urile din rețea PPP-ul este transparent
  - Ele transmit în continuare cadre standard Ethernet
- Multe infrastructuri de ISP au putut fi migrate ușor către PPPoE deoarece foloseau PPP (pentru Dial-up, DSL, etc.)



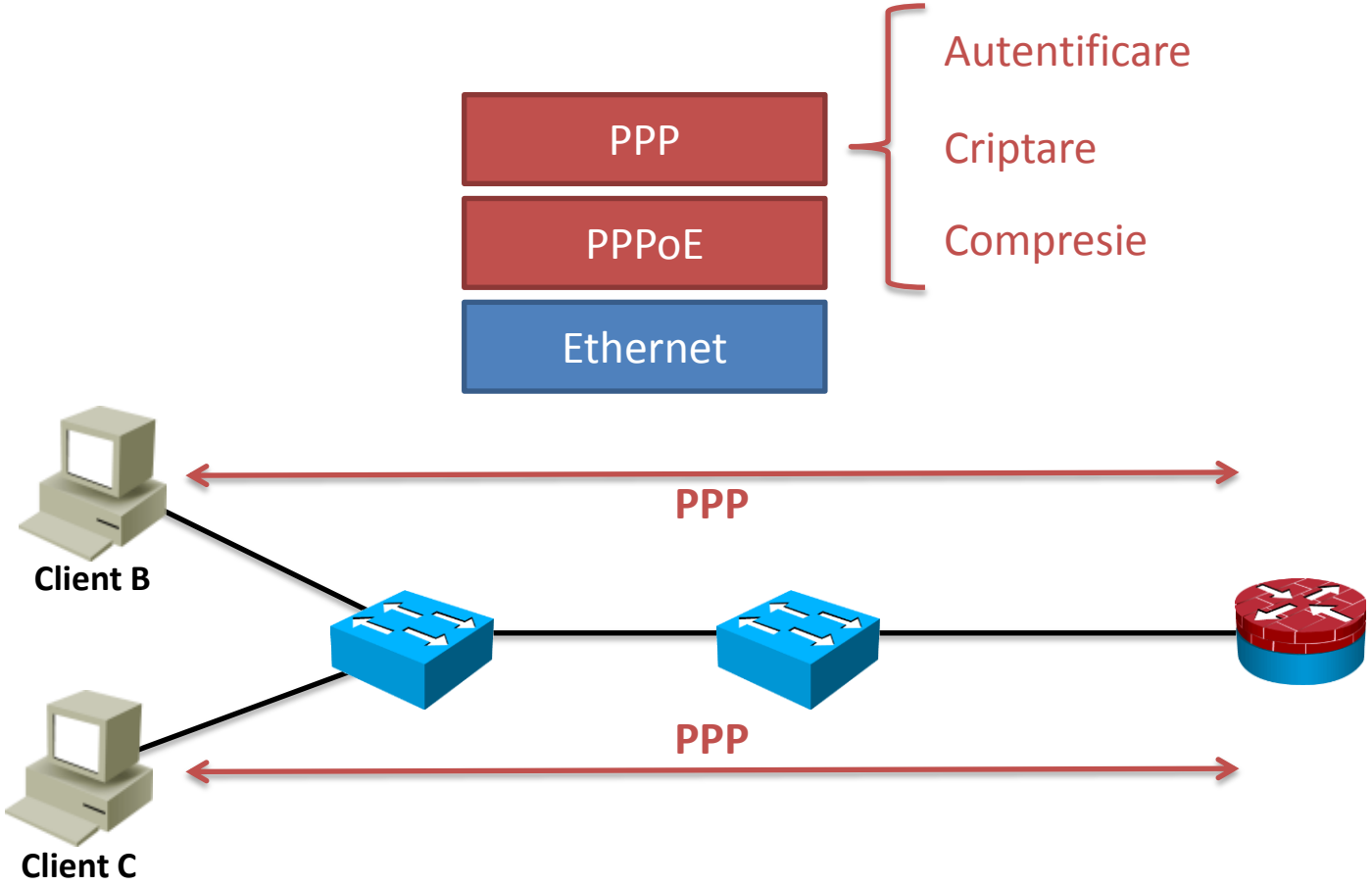
PPPoE – Cerințe

- Clientul trebuie să poată înțelege protocol PPPoE
  - O mare parte din sistemele de operare și echipamentele de rețea sunt compatibile PPPoE
- Provider-ul de Internet trebuie să aibă un server capabil să primească și să gestioneze conexiunile de la utilizatori
- Este necesar un mecanism de gestionare a utilizatorilor
  - Server RADIUS



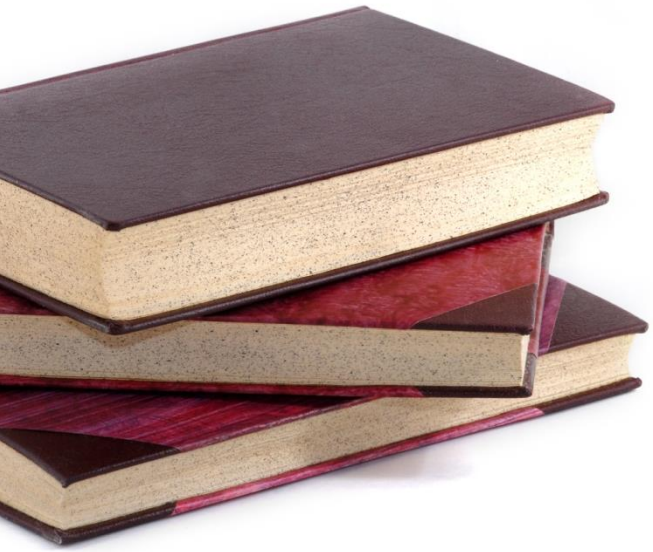
PPPoE

- PPP over Ethernet
- Permite folosirea protocolului PPP peste un mediu multiacces prin stabilirea de comunicații punct la punct



RLO
crunch it connected

Cursul 11

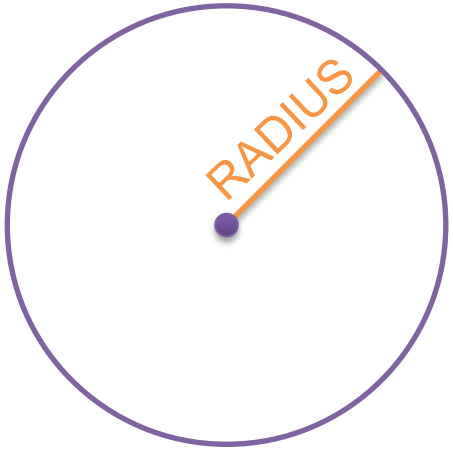


RADIUS

- Descriere
- Tipuri de mesaje
- Autentificare cu RADIUS

RADIUS

- Remote Access Dial-In User Service
- Protocol folosit pentru a oferi servicii de AAA
- RADIUS nu face diferența între autentificare și autorizare, spre deosebire de alte protocoale (TACACS+)
- Folosește UDP port 1812 pentru autentificare și UDP port 1813 pentru contabilizare
- RADIUS nu este o aplicație, ci un protocol
  - Aplicațiile poartă numele de **Servere RADIUS**

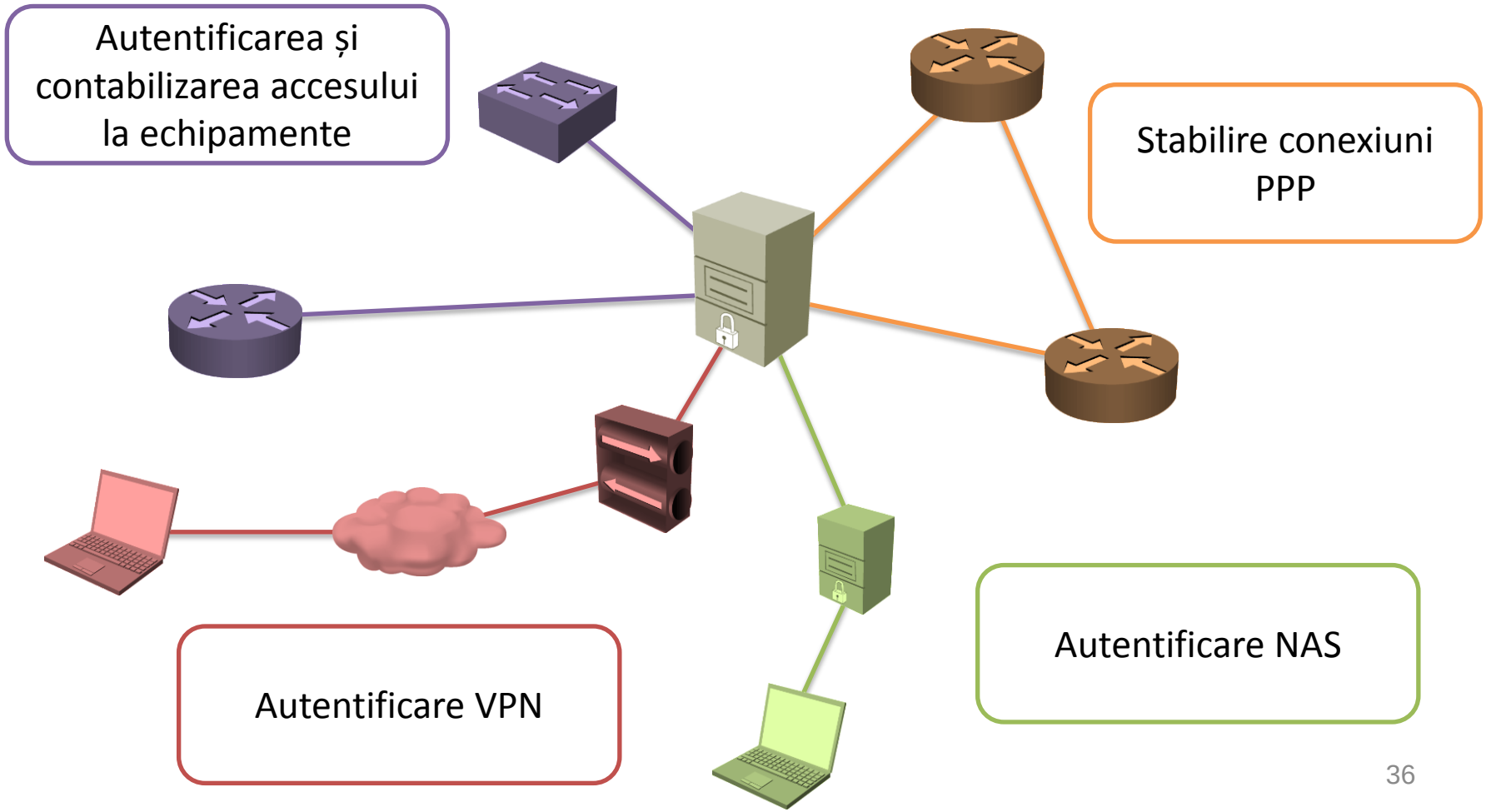


Mesaje RADIUS

Access-Request	• Client → Server • Cerere trimisă pentru realizarea autentificării/autorizării • Poate conține detalii de autentificare (de exemplu numele de utilizator sau parola)
Access-Challenge	• Server → Client • Folosit de server pentru a cere detalii suplimentare de autentificare • Poate fi folosit pentru a trimite un token în vederea autentificării fără a fi transmisă parola pe legătură
Access-Accept	• Server → Client • Semnalează clientului că autentificarea s-a făcut cu succes
Access-Reject	• Server → Client • Semnalează clientului că autentificarea a eșuat

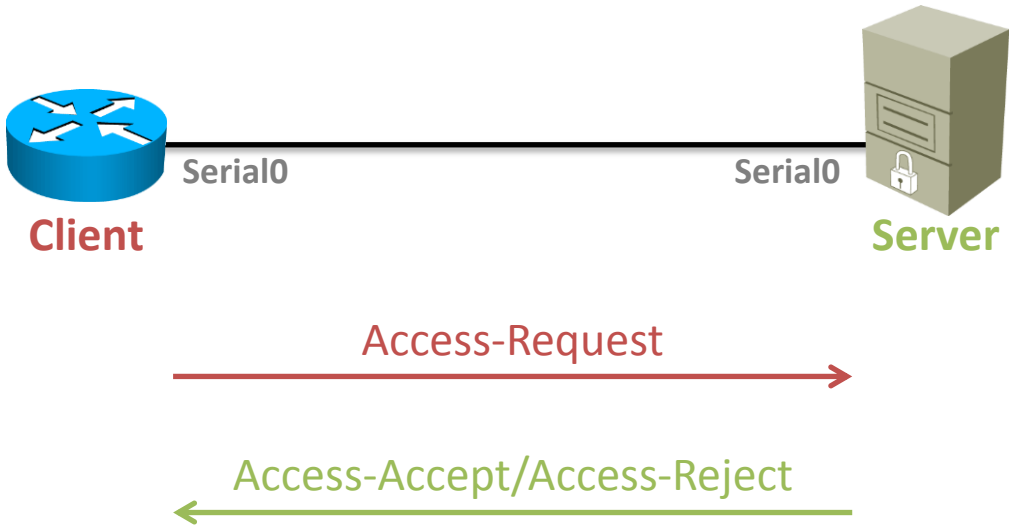
Arhitectură RADIUS

- Serverele RADIUS pot fi folosite pentru a oferi AAA în multiple situații:



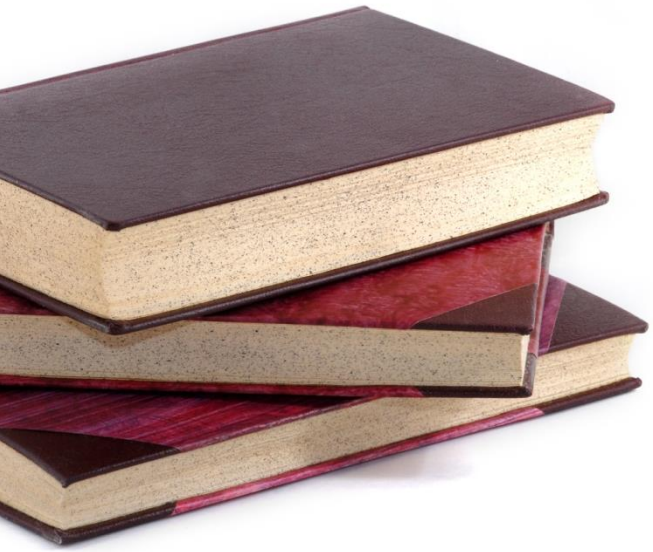
RADIUS – Exemplu de autentificare

- Mesajele RADIUS sunt compatibile cu metode EAP
- Serverul RADIUS va detecta metoda dorită de client direct din mesaj



RLO
crunch it connected

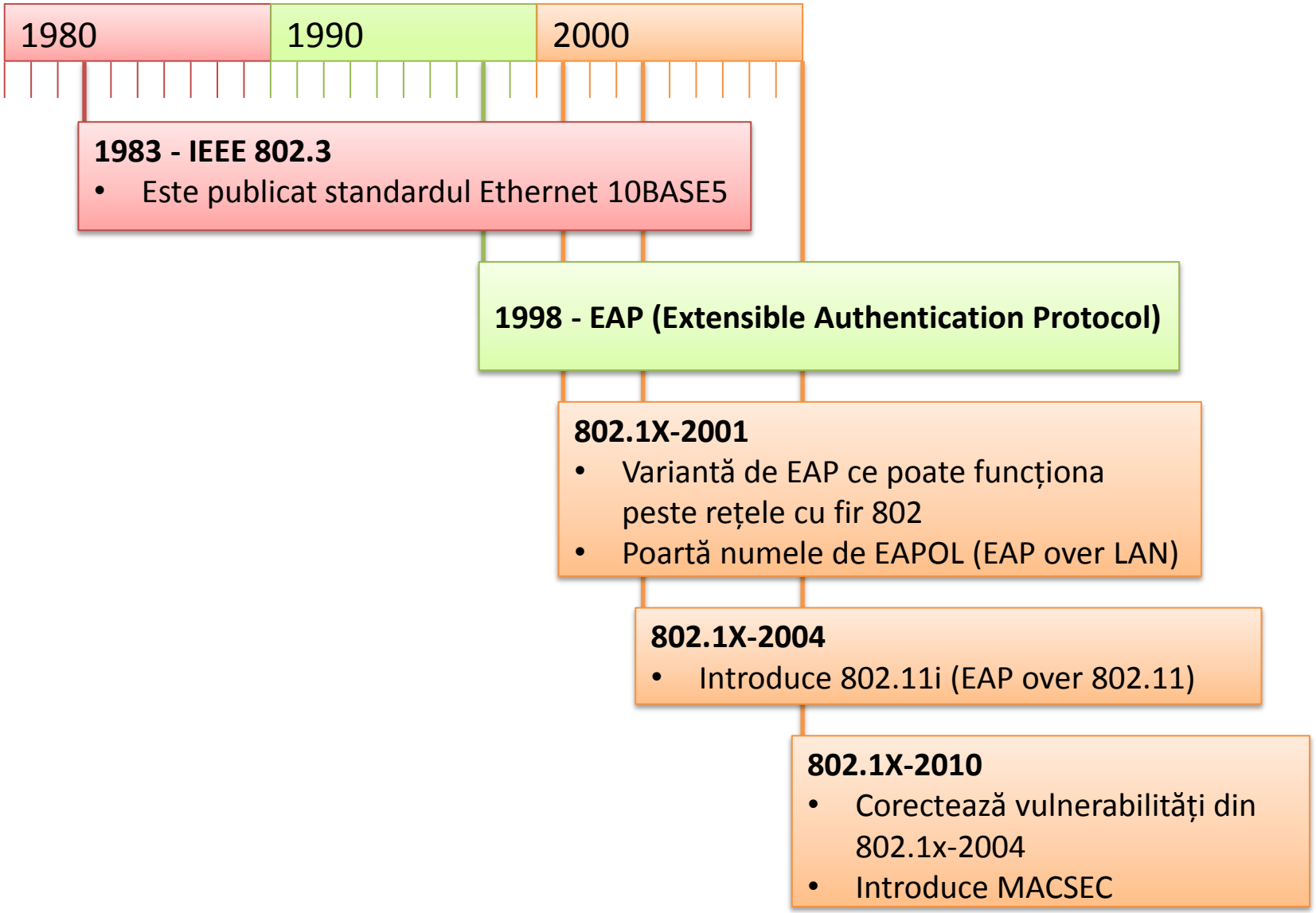
Cursul 11



802.1X

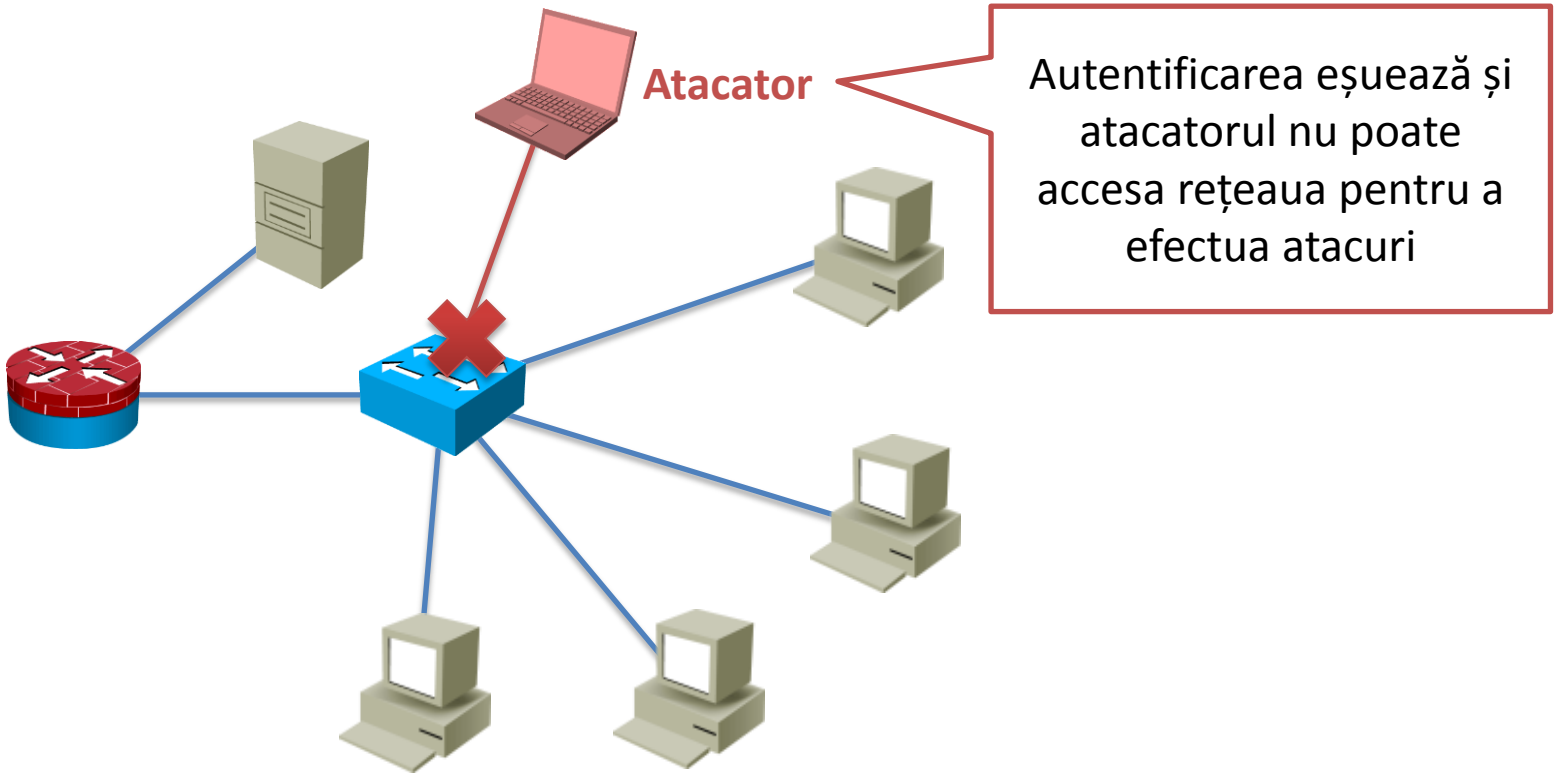
- Istorie
- Componente

Istorie


1980
1990
2000
1983 - IEEE 802.3
• Este publicat standardul Ethernet 10BASE5
1998 - EAP (Extensible Authentication Protocol)
802.1X-2001
• Variantă de EAP ce poate funcționa peste rețele cu fir 802
• Poartă numele de EAPOL (EAP over LAN)
802.1X-2004
• Introduce 802.11i (EAP over 802.11)
802.1X-2010
• Corectează vulnerabilități din 802.1x-2004
• Introduce MACSEC

802.1X

- Permite doar clienților autentificați să acceseze rețeaua
- Autentificarea are loc la nivelul 2 din stiva OSI
- Dacă autentificarea clientului eșuează, acesta nu poate trimite sau primi trafic din rețeaua fizică



Recapitulare: 802.3 și 802.11

- 802.1X funcționează peste rețele 802.3 și 802.11
- În ce tipuri de rețele poate fi configurat 802.1X?

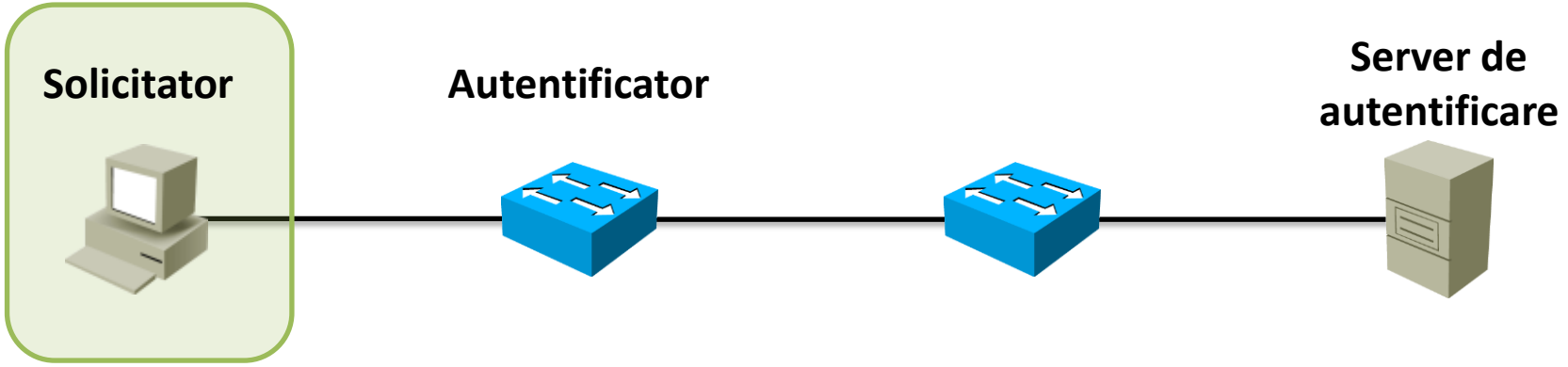
802.3	802.11
Ethernet	802.11a
FastEthernet	802.11b
GigabitEthernet	802.11g
	802.11n

802.1X – Funcții suplimentare

- 802.1X permite și alte funcții pe lângă blocarea accesului stațiilor neautentificate:
  - Poate urmări locația utilizatorilor (de exemplu AP-ul sau switch-ul de unde s-au conectat)
  - Poate contabiliza și taxa activitatea clientului autentificat (pentru servicii de ISP)
  - Poate permite doar accesul la anumite părți din rețeaua fizică în funcție de nivelul de acces al clientului

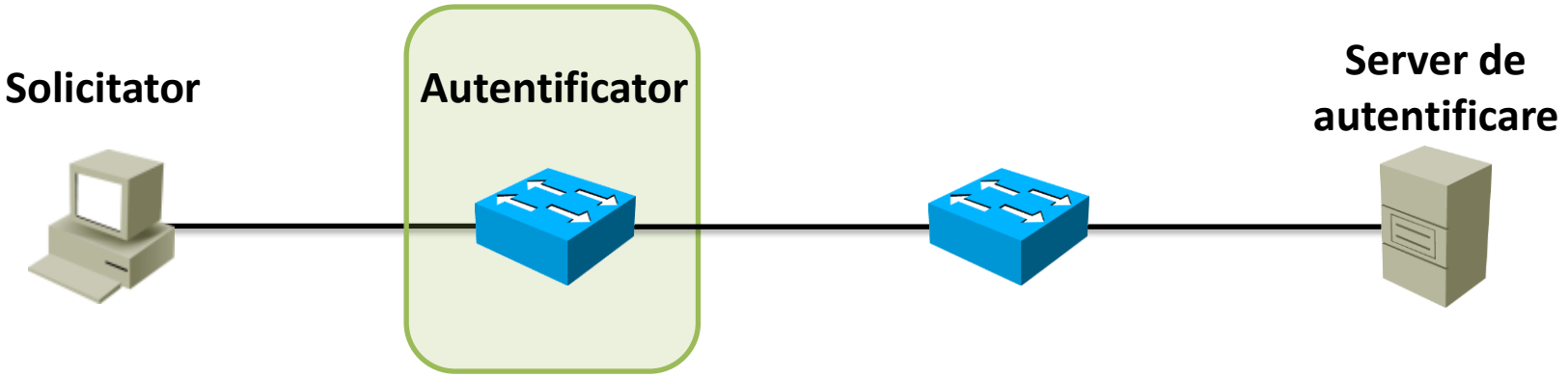
Componente 802.1X

- Solicitator (supplicant)
  - Dispozitiv client care trebuie să se autentifice înainte de a putea accesa rețeaua
  - Dispozitivul trebuie să aibă implementate:
    - 802.1X
    - O **Metodă EAP** (EAP-Method) suportată de server



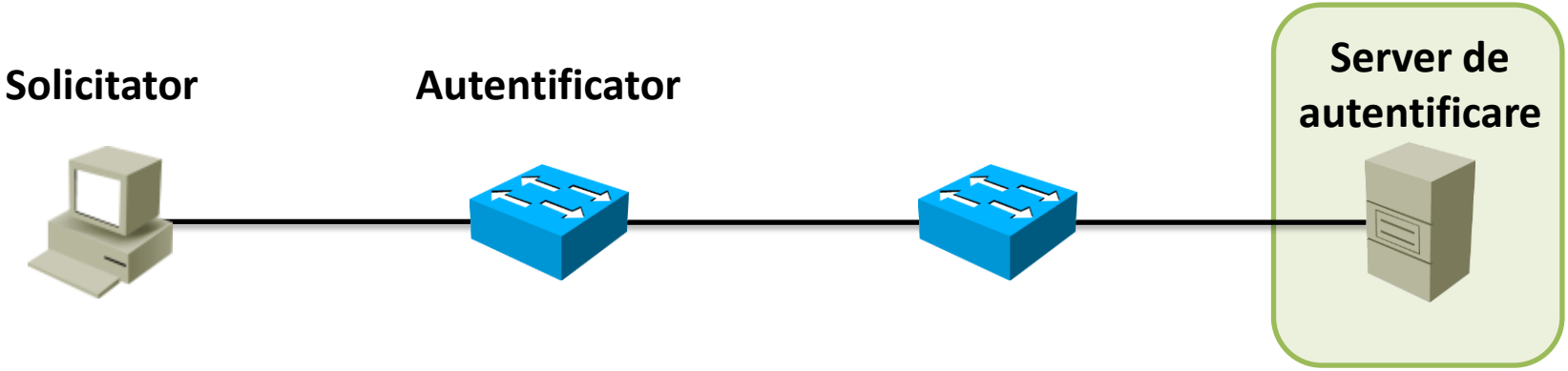
Componente 802.1X

- Autentificator (authenticator)
  - Dispozitiv de nivel 2 (de obicei switch sau access point)
  - Porturile configurate cu 802.1X stau închise până când un solicitator este autentificat
  - Translatează și schimbă mesajele între solicitator și serverul de autentificare



Componente 802.1X

- Server de autentificare (Authentication server)
  - De obicei un server RADIUS
  - Fiecare autentificator are asociat unul sau mai multe servere de autentificare
  - În procesul de intrare în rețea, autentificatorul va valida datele de acces ale solicitatorului interogând serverul de autentificare



Trafic 802.1X

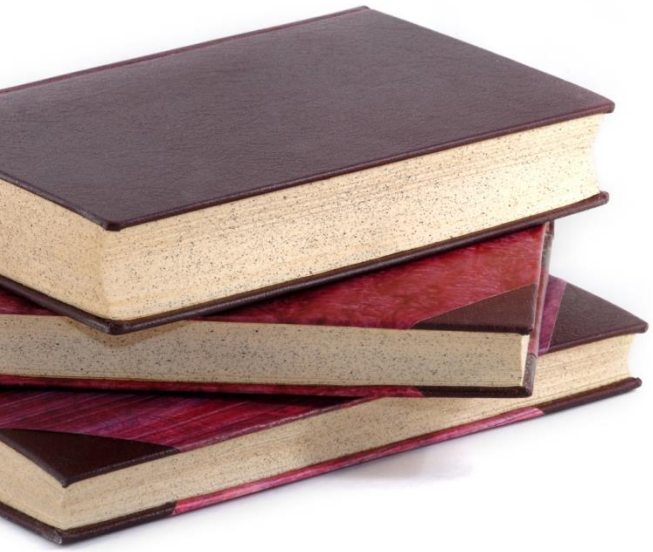
- Procesul de autentificare 802.1X include mai multe tipuri de trafic
- Între solicitator și autentificator: **EAPOL**
  - Funcționează direct peste nivelul 2 (suportate sunt 802.3 și 802.11)
- Între autentificator și serverul de autentificare: **RADIUS**
  - Protocol de nivel aplicație ce funcționează peste UDP

Dialogul solicitator - autentificator

- Singura comunicație descrisă în standardul 802.1X
- Celelalte comunicații sunt necesare pentru 802.1X dar nu sunt definite în standardul propriu-zis
- EAP a fost proiectat ca un protocol point-to-point
  - A fost adaptat pentru funcționarea peste Ethernet prin **EAPOL**

RLO
crunch it connected

Cursul 11



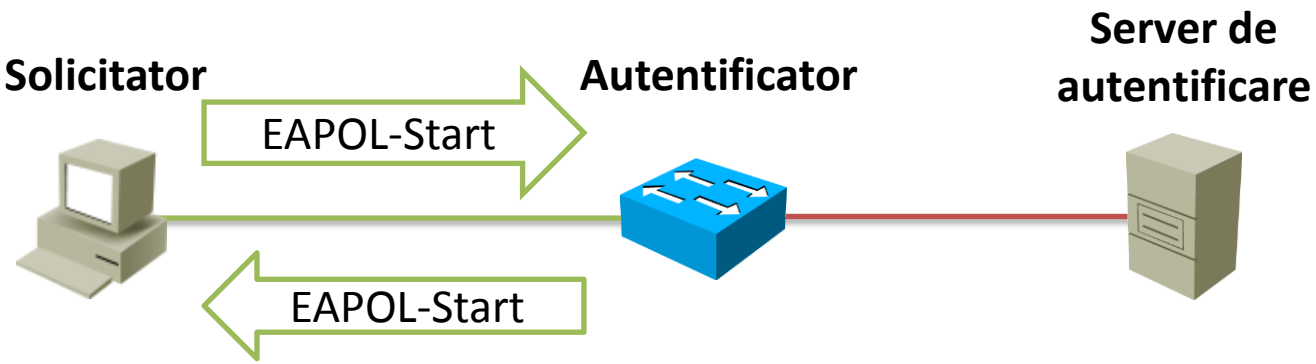
Exemplu de autentificare 802.1X

- Conectare prin EAP-MD5
- Terminarea unei conexiuni

Conectarea unui client – EAP-MD5

Inițiere

- În starea inițială, legătura de pe autentificator este **down**
- La conectarea unui dispozitiv, legătura trece în starea **up**
- Când legătura trece în starea **up**, autentificatorul va trimite un **EAPOL-Start** către solicitator
- Dacă legătura era deja **up** și solicitatorul dorește să se autentifice, poate trimite el mesajul **EAPOL-Start** inițial

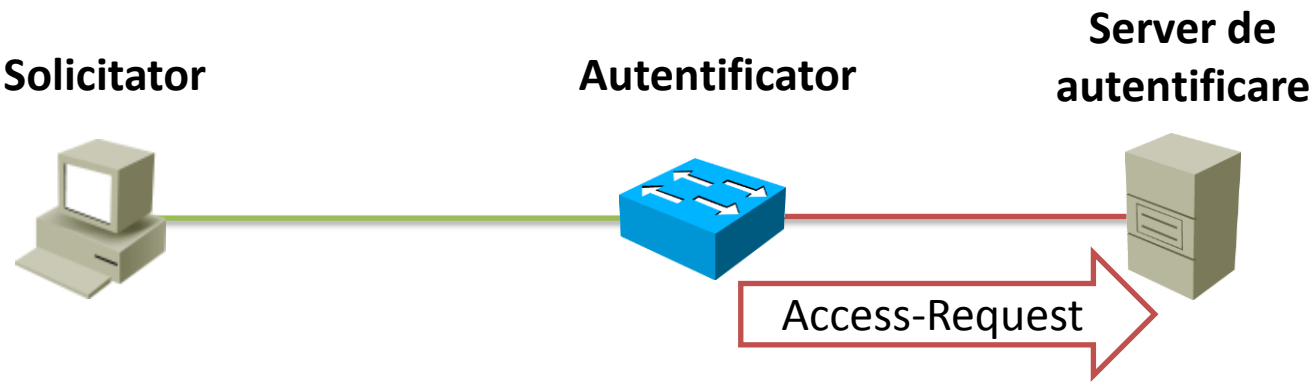


Conectarea unui client – EAP-MD5

Inițiere

Cerere challenge

- Autentificatorul cere un **challenge string** serverului de autentificare
- Mesajul este un mesaj **RADIUS Access-Request** transmis peste UDP
  - Pe acest segment nu se mai folosesc formatele EAPOL/EAP



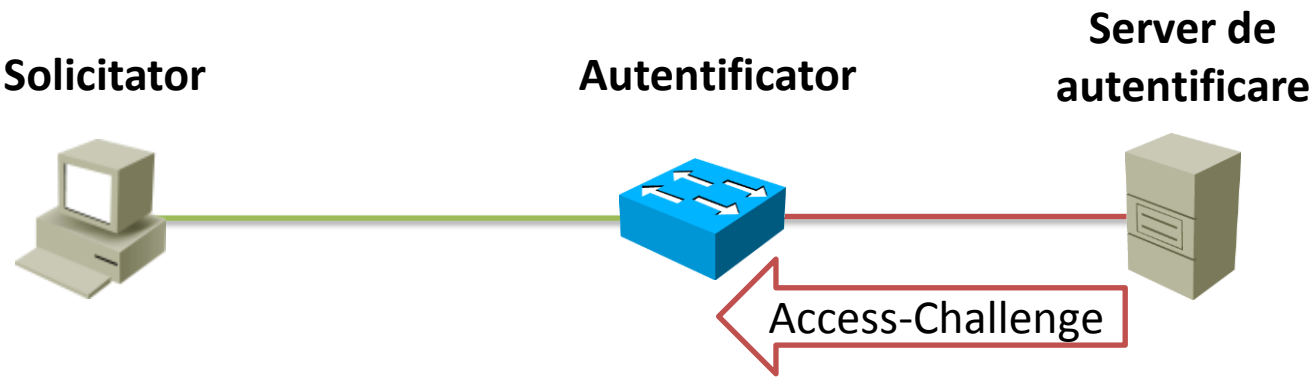
Conectarea unui client – EAP-MD5

Inițiere

Cerere challenge

Primit challenge

- Serverul RADIUS returnează **challenge string**-ul printr-un mesaj **RADIUS** tip **Access-Challenge**



Conectarea unui client – EAP-MD5

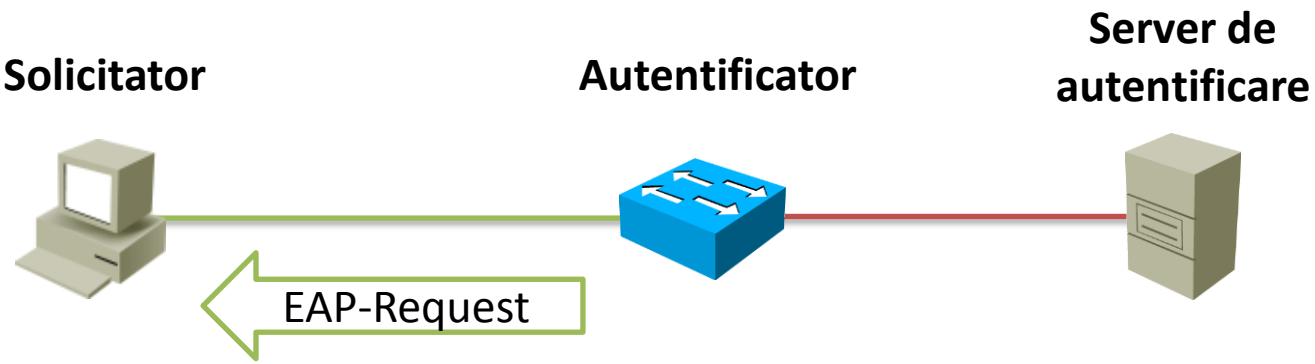
Inițiere

Cerere challenge

Primit challenge

Trimis challenge

- Autentificatorul trimite mai departe **challenge**-ul MD5 către solicitator printr-un **EAP-Request**
- Autentificatorul retrimite **EAP-Request**-ul dacă nu a primit niciun răspuns până la expirarea unui timeout
- Dacă nu primește un răspuns după un număr de încercări, abandonează autentificarea
  - Solicitatorul rămâne blocat în afara rețelei



Conectarea unui client – EAP-MD5

Inițiere

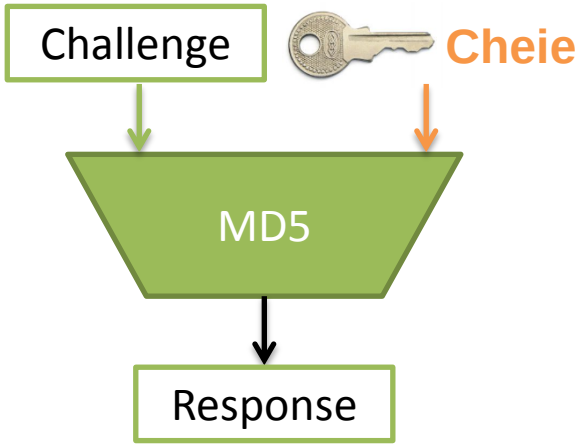
Cerere challenge

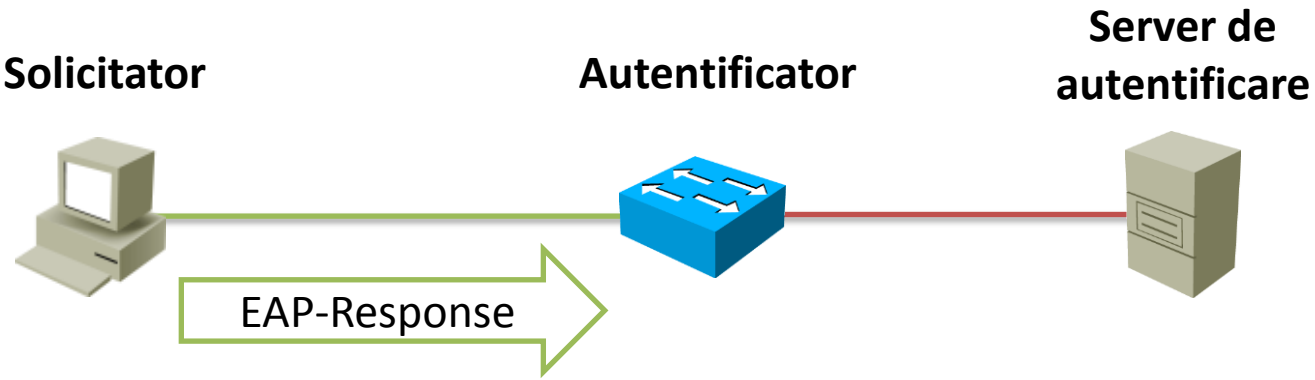
Primit challenge

Trimis challenge

Primit hash

- Solicitatorul preia challenge-ul și calculează un hash pe baza lui și pe baza cheii de acces





Conectarea unui client – EAP-MD5

Inițiere

Cerere challenge

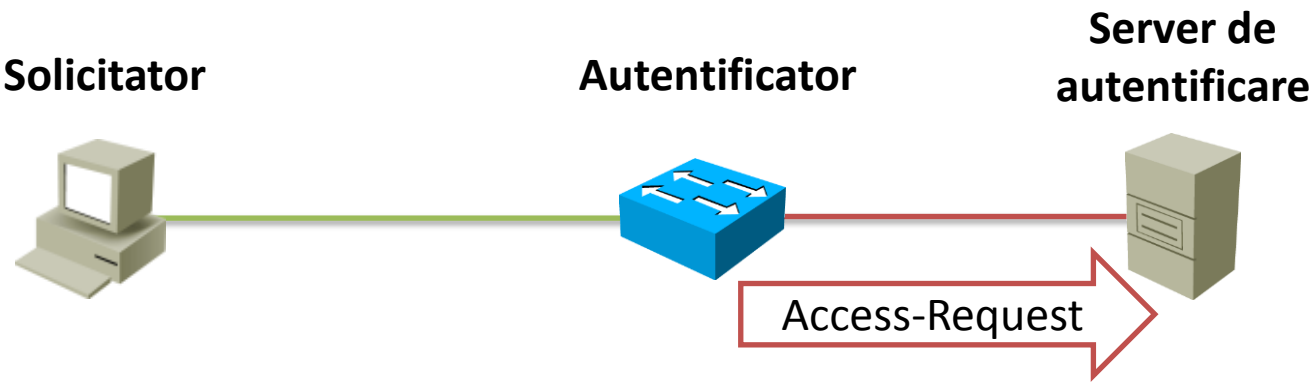
Primit challenge

Trimis challenge

Primit hash

Trimis hash

- Autentificatorul:
  - Primește mesajul **EAP-Response**
  - Extrage datele EAP-Method (care conțin și hash-ul solicitatorului)
  - Trimite datele (hash, username) mai departe serverului de autentificare printr-un mesaj **RADIUS Access-Request**



Conectarea unui client – EAP-MD5

Inițiere

Cerere challenge

Primit challenge

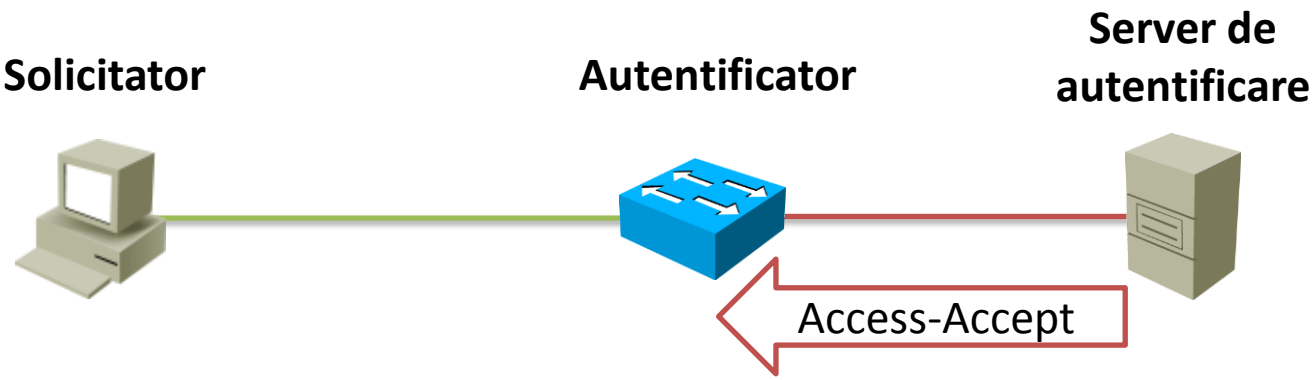
Trimis challenge

Primit hash

Trimis hash

Primit răspuns

- Serverul de autentificare:
  - Folosește cheia din baza de date corespunzătoare solicitatorului și calculează pe baza ei un **hash** al **challenge**-ului trimis anterior
  - Compară **hash**-ul din mesajul **Access-Request** primit anterior cu cel calculat
  - Dacă sunt egale trimite un **RADIUS Access-Accept** către autentificator
  - Dacă nu sunt egale trimite un **RADIUS Access-Reject** către autentificator



Conectarea unui client – EAP-MD5

Inițiere

Cerere challenge

Primit challenge

Trimis challenge

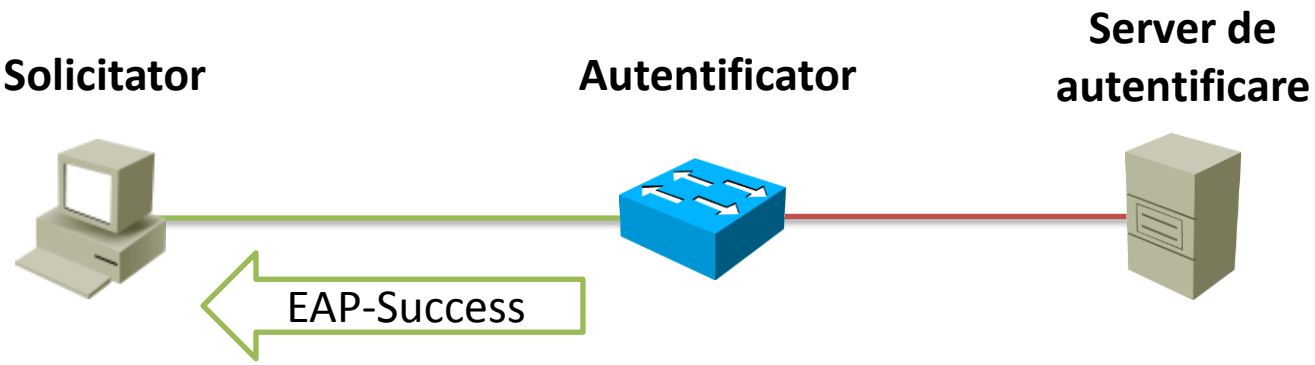
Primit hash

Trimis hash

Primit răspuns

Trimis răspuns

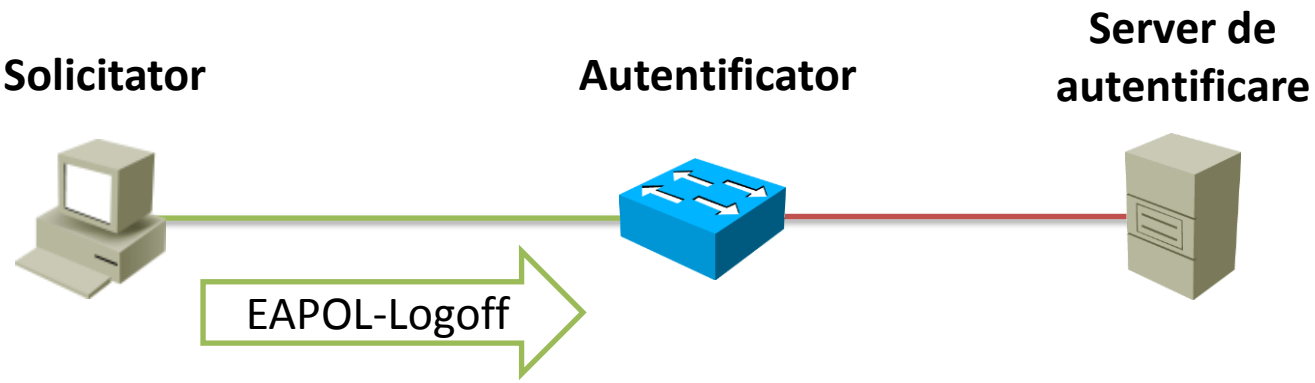
- Dacă autentificatorul a primit un **Access-Accept** de la server:
  - Trimite un **EAP-Success** către solicitator
  - Solicitatorul poate accesa rețeaua
- Dacă autentificatorul a primit un **Access-Reject** de la server:
  - Trimite un **EAP-Failure** către solicitator
  - Solicitatorul **nu** poate accesa rețeaua
  - În cazuri speciale, poate configurat doar un acces parțial al solicitatorului (de exemplu doar un VLAN neprivilegiat)



Terminare sesiune client

- Inițiere
- Cerere challenge
- Primit challenge
- Trimis challenge
- Primit hash
- Trimis hash
- Primit răspuns
- Trimis răspuns
- Terminare

- Când solicitatorul dorește să părăsească rețeaua, acesta poate anunța autentificatorului să închidă sesiunea de autentificare
- Pentru a închide sesiunea solicitatorul trimite un mesaj **EAPOL-Logoff**



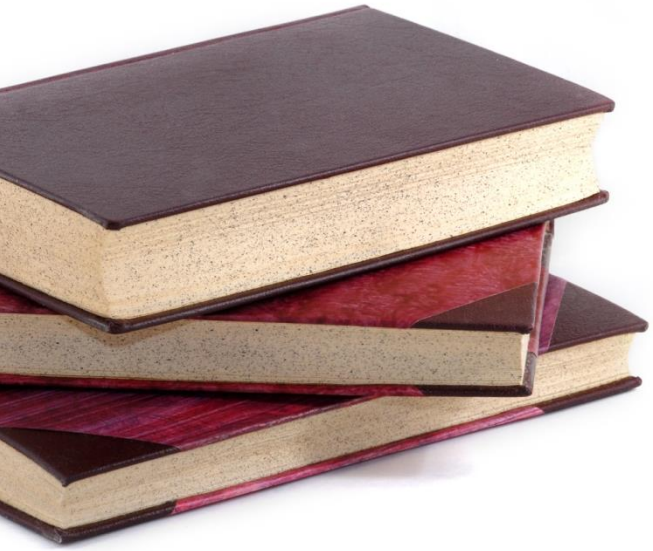
Conectarea unui client – EAP-MD5

- EAP-MD5 nu este o soluție sigură deoarece MD5 este vulnerabil la atacuri brute force
  - Vulnerabilitatea matematică a MD5 poate fi exploatată prin **rainbow tables**
- Pentru 802.1X se recomandă folosirea altor protocoale în loc de EAP-MD5

RLO
crunch it connected

Cursul 11

MACsec



MACsec

- IEEE 802.1AE – publicat în 2006
- Folosit în 802.1X-2010
- Protocol de nivel 2 fără conexiune ce oferă:
  - Confidențialitate
  - Integritate
  - Autentificare

- Protocolul stabilește **asocieri de securitate** (Security Association) unidirecționale la nivel 2 ce sunt grupate în **canale sigure** (Secure Channel)
- Conexiunile LAN neautorizate sunt identificate și izolate de restul rețelei

MACsec

- Similar cu cadrul Ethernet, însă include și:
  - Security Tag, compus din:
    - Numărul asocierii
    - Numărul pachetului (folosit ca vector de inițializare pentru criptare și împotriva replay attack)
    - Identificator de canal sigur
  - MAC (Message authentication code)
    - Similar cu MAC-ul folosit în tunelele SSH
    - Folosit pentru realizarea autentificării

Cuvinte cheie