802.1x, EAP a RADIUS

Martin Stanek

Katedra informatiky
FMFI UK, Bratislava
stanek@dcs.fmph.uniba.sk

2011/12

Obsah

Riadenie prístupu v sieti

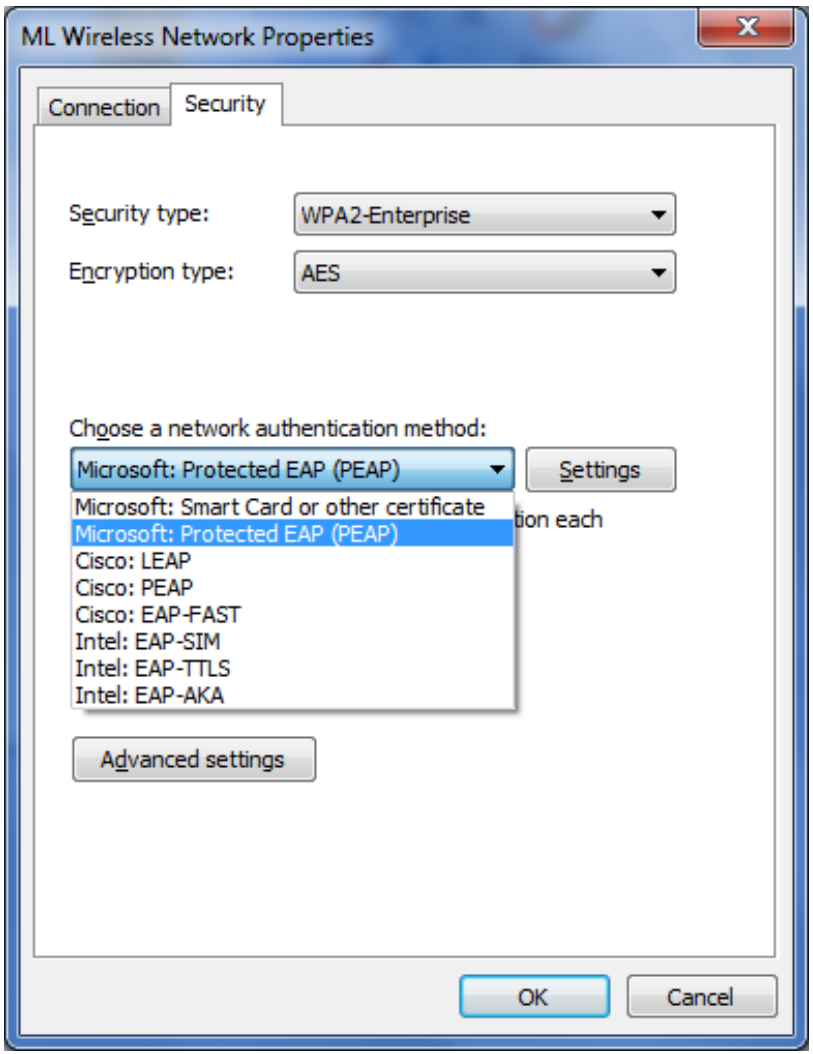
- AAA služby $\sim$ authentication, authorization, accounting
- **autentizácia**: proces dokazovania identity subjektu
- autorizácia: určenie oprávnenia subjektu vykonať danú činnosť
- účtovanie: sledovanie využívania sieťových zdrojov

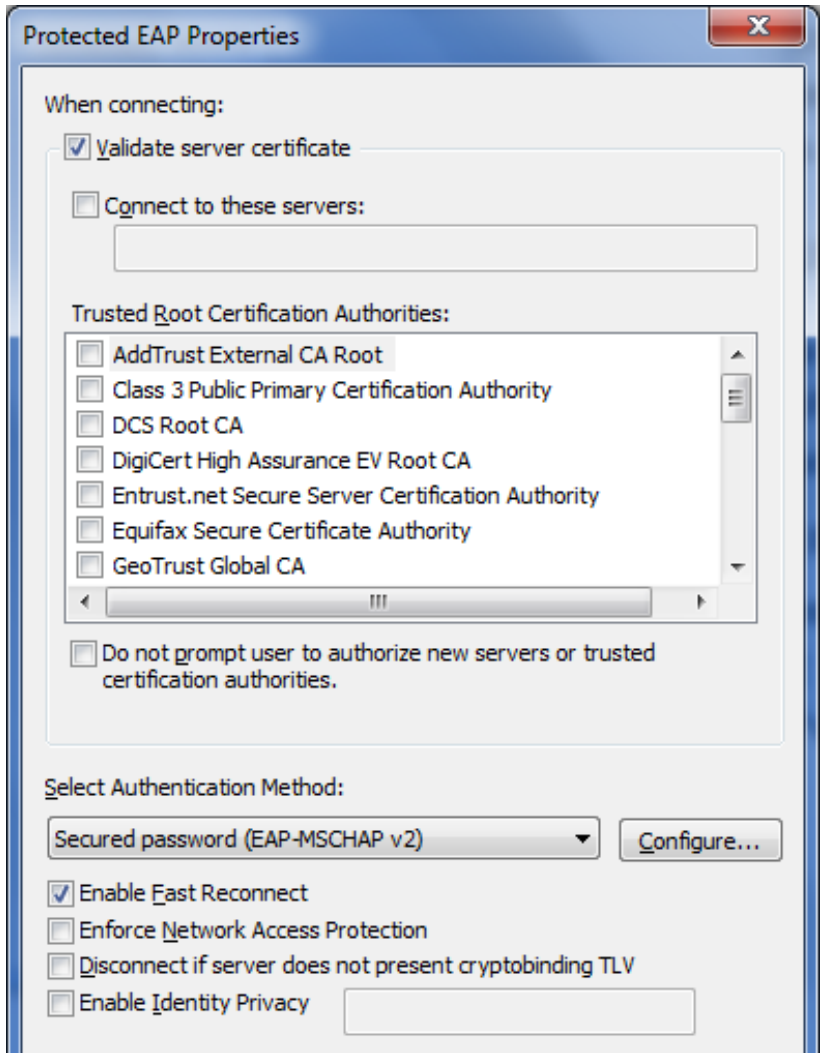
IEEE Std 802.1x

- Port-Based Network Access Control
- IEEE štandard (verzie 2001, 2004, 2010)
  - http://standards.ieee.org/about/get/802/802.1.html, vyše 200 strán
- štandard definuje:
  - spôsob „port-based“ riadenia sieťového prístupu
  - spôsob vytvorenia kľúčov pre IEEE Std 802.1AE MAC Security (MAC – Media Access Control, súčasť linkovej vrstvy v OSI modeli)
  - spôsob použitia štandardných autentizačných a autorizačných protokolov
- použitie napr. WPA2 Enterprise (WPA2-802.1x)
  - cf. WPA2 Personal (WPA2-PSK, Pre-shared key)

Podpora vo Windows 7

- WiFi; pre LAN (služba OS) Wired AutoConfig

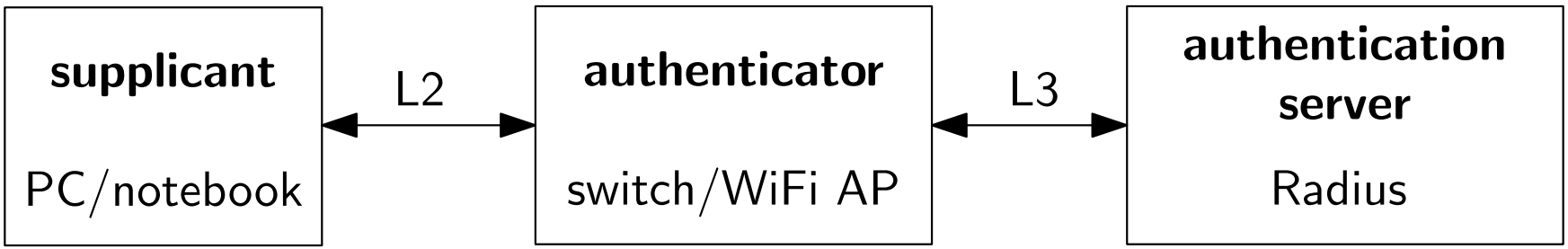




Podpora v Ubuntu (11.10)

- NetworkManager

Subjekty v 802.1x

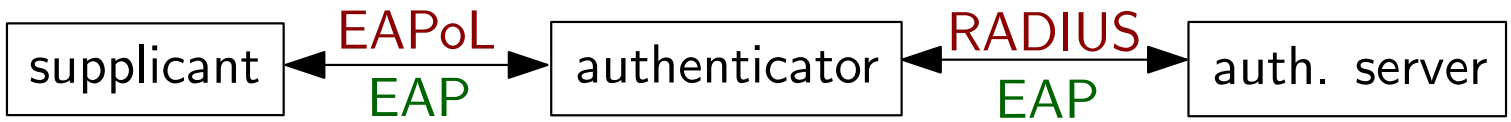


- Supplicant (klient)
  - SW, napr. súčasť operačného systému
  - HW, napr. Intel vPro
- Authenticator (sprostredkovateľ z hľadiska autentizácie)
- Authentication server

Čo sa deje v 802.1x

- úvodný stav: prístupový bod (port) je zavretý pre ľubovoľnú komunikáciu klienta okrem EAPoL
- klient vykoná autentizáciu voči autentizačnému serveru (EAP)
  - úspešne: authenticator otvorí port, priradí VLAN a pod.
  - neúspešne: authenticator neotvorí port / otvorí port a zaradí klienta do guest VLAN a pod.

Protokoly v 802.1x



- EAPoL (EAP over LAN)
  - komunikácia supplicant $\leftrightarrow$ authenticator
  - použitie nad 802.3 (Ethernet), 802.11 (WLAN), ...
  - „zabalenie“ EAP správ do L2 komunikácie
- RADIUS ... detaily neskôr
  - komunikácia authenticator $\leftrightarrow$ autentizačný server
  - tu: EAP „zabalený“ do správ RADIUS protokolu

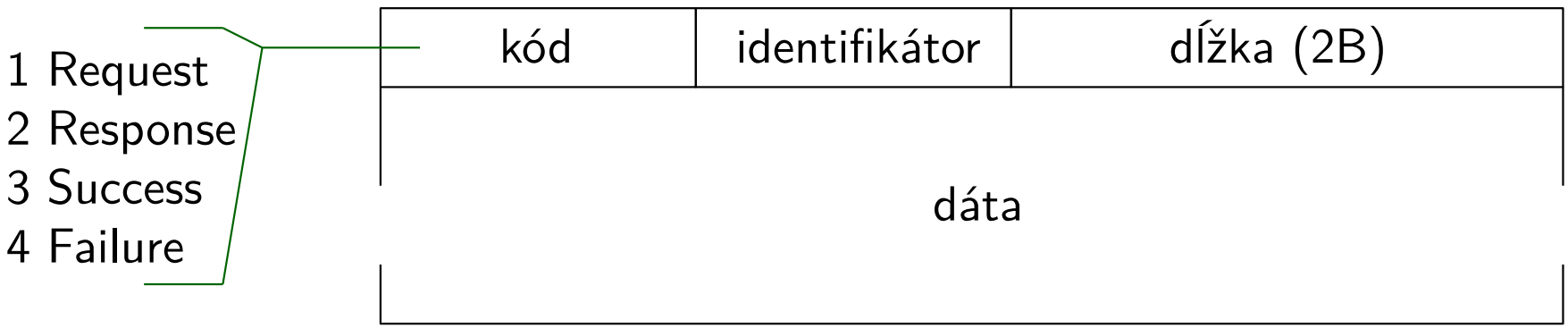
V praxi potrebné riešiť

- pri niektorých EAP metódach – správa certifikátov (serverové, prípadne klientské)
- zaradenia bez podpory 802.1x (napr. tlačiarne)
- Wake on LAN
- viacero zariadení na jeden port (IP telefóny, hub a pod.)
- nedostupný autentizačný server

. . . atď. . . .

EAP (Extensible Authentication Protocol)

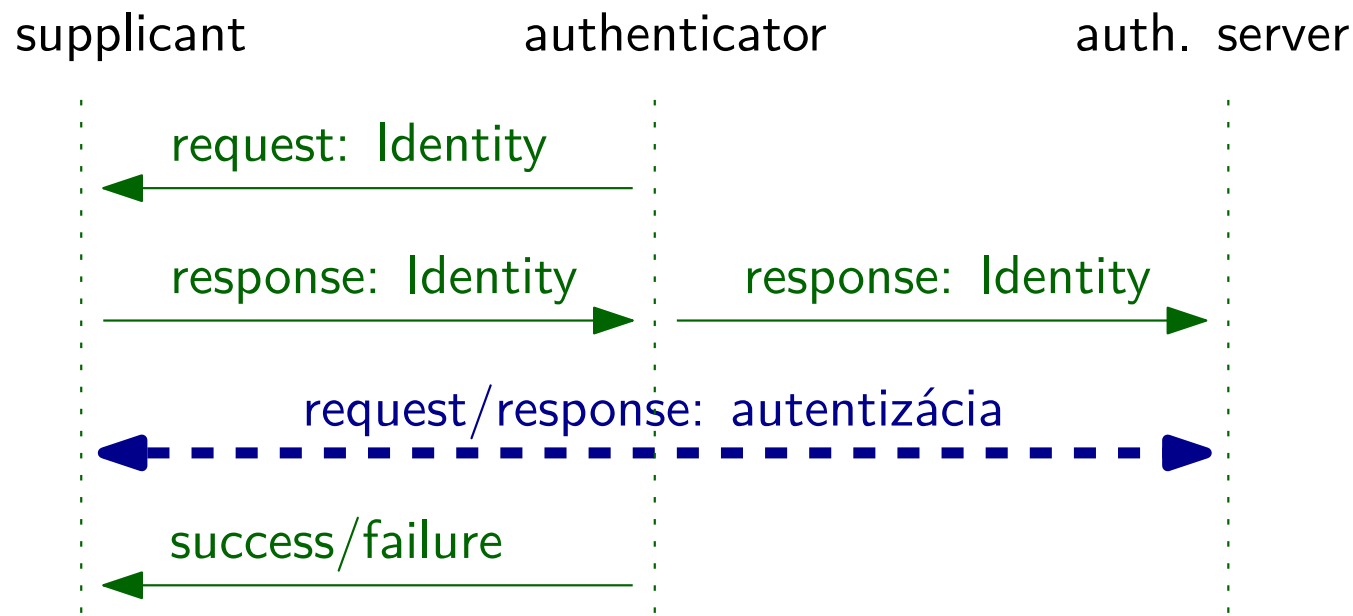
- pôvodne súčasť PPP (Point-to-point protokol), aktuálne RFC 3748
- typicky nad linkovou vrstvou („data link layer“, teda bez IP)
- všeobecný rámec pre rôzne metódy autentizácie
- formát paketov:



  - identifikátor slúži pre párovanie dotazov a odpovedí
  - RFC 5296: nové kódy (5 Initiate, 6 Finish)

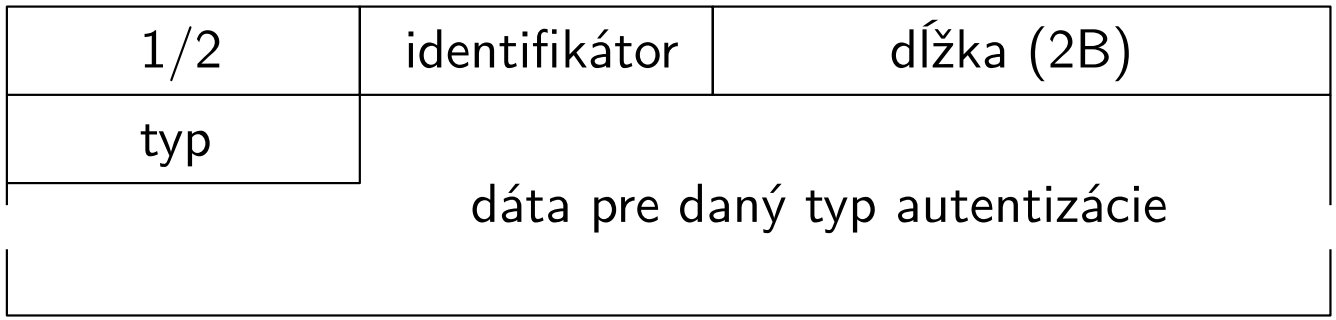
EAP (2)

- veľmi jednoduchý protokol
  - (potenciálne) veľa request/response výmien, obvykle zakončených success/failure
- napríklad:



EAP (3)

- zložitosť prinášajú autentizačné metódy



- príklady autentizačných metód (viac ako 40, možnosť vlastných rozšírení):

4	MD5	21	PEAP
13	TLS	43	FAST
21	TTLS	17	LEAP

EAP-MD5

- povinne implementovaná metóda
- implementácia CHAP (Challenge Handshake Authentication Protocol):
  - Request: *challenge*
  - Response: MD5(identifikátor || *shared secret* || *challenge*)
- nepoužívať – bezpečnostné problémy:
  - len jednostranná autentizácia
  - náchylné na slovníkové útoky a útoky úplným preberaním
  - náchylné na MIM útok . . . správy posielané v otvorenom tvare a bez ochrany integrity
  - nemožnosť skyť identitu
  - nezabezpečená ďalšia komunikácia (neodvádzajú sa kryptografické kľúče)
  - . . .

EAP-TLS, EAP-TTLS a EAP-PEAP

Pointa („vonkajší“ EAP najmä rieši fragmentáciu paketov):

- EAP-TLS: využitie autentizácie v TLS protokole
- EAP-TTLS: tunelovanie klienskej autentizácie v TLS
- EAP-PEAP: tunelovanie vnútornej inštancie EAP v TLS

	EAP-TLS	EAP-TTLS	EAP-PEAP
klientský certifikát	áno	voliteľne	voliteľne
certifikát servera	áno	áno	áno
vzájomná autent.	áno	áno	áno
odvodenie kľúčov	áno	áno	áno
ochrana identity klienta	nie	áno	áno

Niektoré vnútorné metódy autentizácie

- CHAP . . . s MD5 sme už videli
- MS-CHAPv2 . . . variant CHAP (RFC 2759)
  - obojstranná autentizácia
  - bez LAN Managerovej minulosti
  - možnosť meniť heslo ako súčasť protokolu

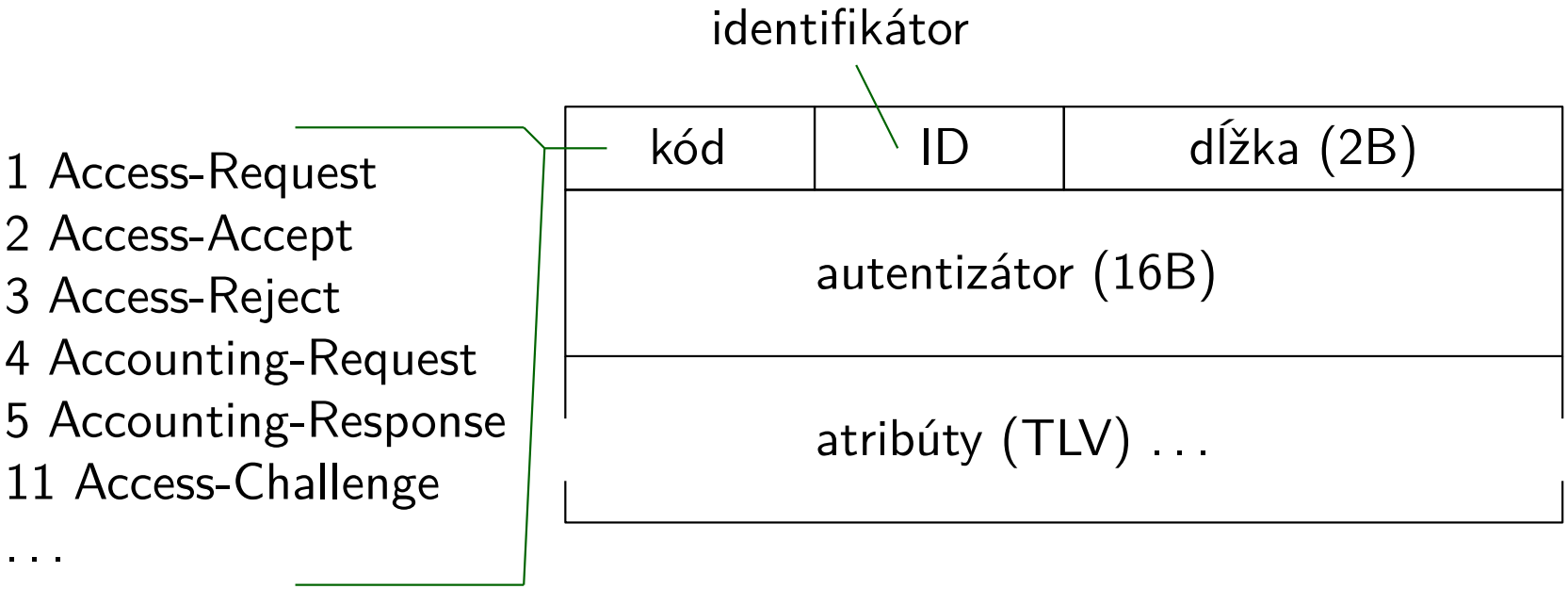
RADIUS

- RADIUS – Remote Authentication Dial In User Service
- RFC 2865, RFC 2866 (Accounting) + niektoré rozšírenia a spresnenia
- obvyklý cieľ: centralizovane riešiť autentizáciu používateľov a systémov
- klient/server protokol
  - klient (NAS – Network Access Server):
    prepínač, smerovač, prístupový bod, VPN server ...
  - server (RADIUS server):
    FreeRADIUS, Network Policy Server (Microsoft), Secure Access Control Server (Cisco)

Základné charakteristiky

- bezstavový protokol (UDP)
- databáza používateľov: SQL databáza, LDAP, textové súbory, ...
- komunikácia klient $\leftrightarrow$ server (iniciuje klient)
- proxy RADIUS server (umožňuje „roaming“ používateľov medzi tzv. realms)

Paket



- autentizátor (authenticator):
  - request auth. (v Access-Request paketoch) – nepredikovateľná a jedinečná hodnota počas života „secret“
  - response auth. (Access-[Accept, Reject, Challenge] paketoch) MD5(kód || ID || dĺžka || request auth. || atrribúty || secret)
  - secret – heslo zdieľané klientom a serverom

Bezpečnosť (1)

- používateľské heslo (P) je posielané „šifrovane“
  - v prípade hesla s max. 16 znakmi (padding hodnotou 0x00 na 16B): $P \oplus \text{MD5}(\text{secret} \,||\, \text{request auth.})$
  - tento mechanizmus je použitý aj pre vybrané ďalšie atribúty
  - ostatné atribúty štandardne v otvorenom tvare (súkromie)
- hodnota *secret*
  - slovníkový útok alebo útok úplným preberaním (z response auth. alebo zo šifrovaného hesla)
  - často rovnaká hodnota pre viacero NAS $\Rightarrow$ falošný NAS, zisťovanie hesiel používateľov

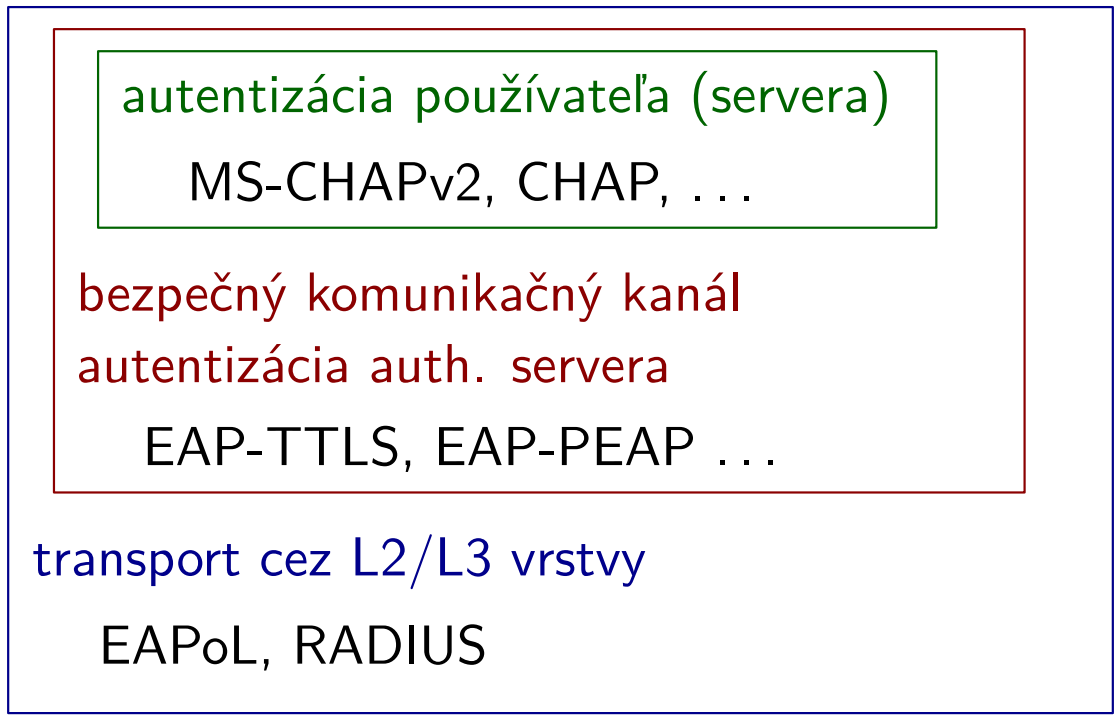
Bezpečnosť (2)

- problémy vyplývajúce z opakovania/predikovateľnosti request auth.
  - možnosť opakovať/vypýtať si dopredu odpovede servera (pozri aj Event-Timestamp atribút)
- Access-Request bez ochrany integrity
  - pozri aj Message-Authenticator atribút (HMAC-MD5)
- niektoré riziká sú eliminované použitím vhodného EAP
- potenciálna ochrana celého protokolu
  - IPSec, RadSec – RADIUS nad TLS (draft)
- RADIUS s EAP (RFC 3579)

Alternatívy a vylepšenia

- TACACS+ (Terminal Access Controller Access-Control System)
  - Cisco, najmä pre prístup k sieťovým prvkom
  - nad TCP, oddelenie autentizácie a autorizácie
  - možnosť šifrovať celé telo paketu (bez hlavičky) . . . synchrónna prúdová šifra skonštruovaná z MD5 (bez zabezpečenia integrity)
- DIAMETER
  - nástupca RADIUS (veľmi pomalý nástup, používa niekto?)
  - základ v RFC 3588
  - nad spoľahlivou transportnou vrstvou (TCP, SCTP)
  - nad zabezpečeným komunikačným kanálom (IPSec, TLS)
  - stavový aj bezstavový model
  - aj server môže iniciovať komunikáciu
  - jednoduchšie rozširovateľný, . . .

Zhrnutie – architektúra (príklad)



Zhrnutie – použitie (príklad)