České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

13. přednáška

Zabezpečení datových sítí

Ing. Tomáš Vaněk, Ph.D.
tomas.vanek@fel.cvut.cz

Osnova

- Zabezpečení v IEEE 802.3 (WiFi)
  - WEP
  - WPA-TKIP
  - IEEE 802.11i (WPA2)
  - IEEE 802.1x
- Zabezpečení v IEEE 802.3 (Ethernet)

Proč je otázka zabezpečení u bezdrátových sítí tak důležitá ?

U bezdrátových sítí nelze dostatečně omezit přístup k fyzickému médiu.

Základní atributy bezpečnosti, které je nutné zajistit:

- Autentizace
- Integrita
- Utajení

Zabezpečení bezdrátových sítí IEEE 802.11

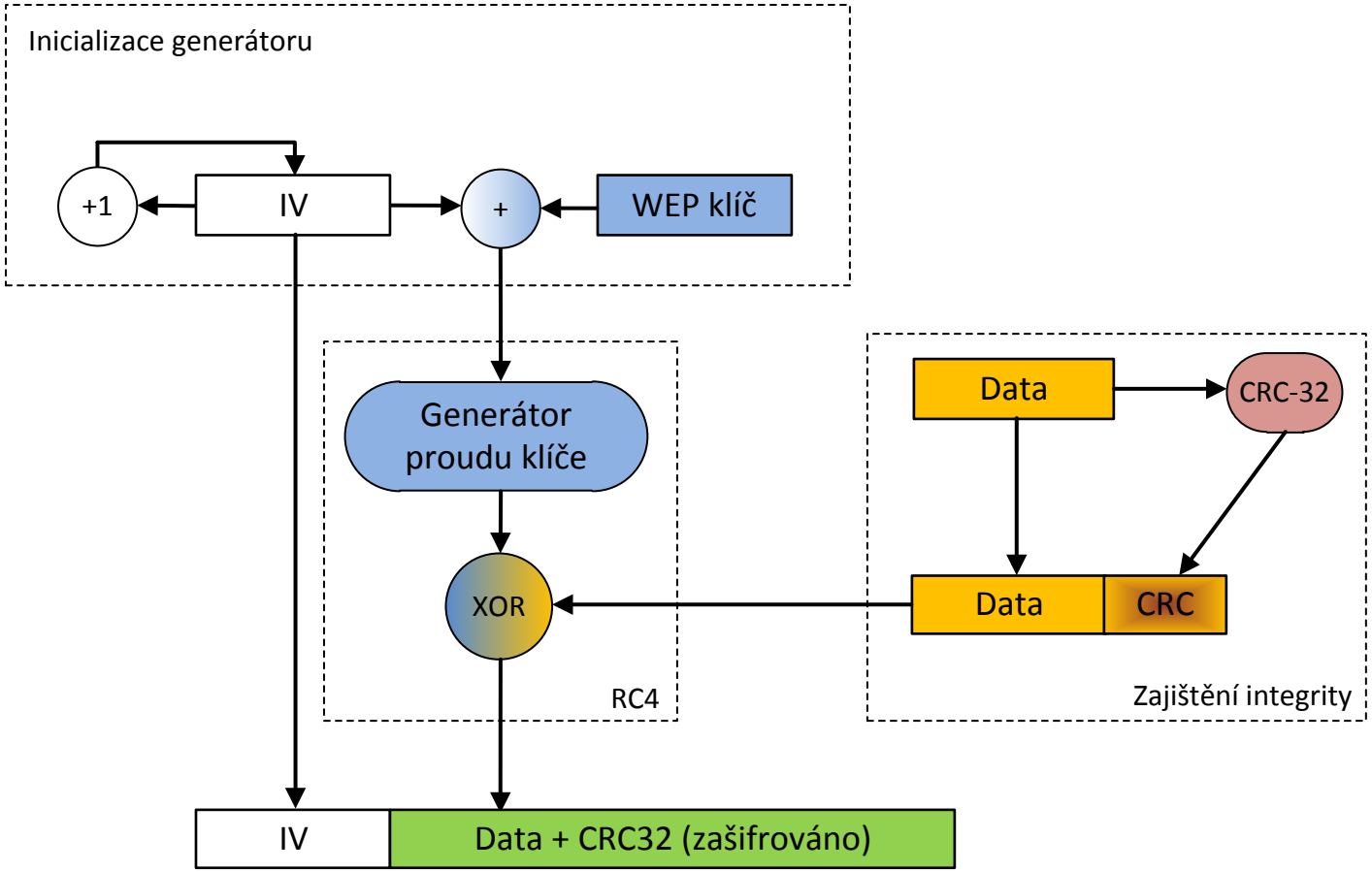
WEP – Wired Equivalent Privacy

- protokol zajišťující **nepovinné** zabezpečení sítí 802.11
- doslova „soukromí jako v drátových sítích“
- hlavní cíl: utajit přenášená data
- obsah datových rámců je zašifrován algoritmem RC4
- datové rámce jsou chráněny před změnou pomocí CRC-32 (Cyclic Redundancy Check)
- **volitelná autentizace** na základě znalosti sdíleného klíče
- široce podporovaný, ale snadno prolomitelný
- délka klíče 64 bitů (dle standardu, v praxi se používají i délky klíče 128 a 256 bitů)

RC4

- symetrická proudová šifra
- základem je tabulka o velikosti 255 bajtů
- v každém kroku RC4 dojde k
  - prohození prvků v současné tabulce
  - výběru bajtu klíče z tabulky
- počáteční nastavení (permutace) je dána klíčem
- RC4 podporuje klíče délky 8-2048 bitů
- v každý krok RC4 produkuje 8 bitů proudu klíče

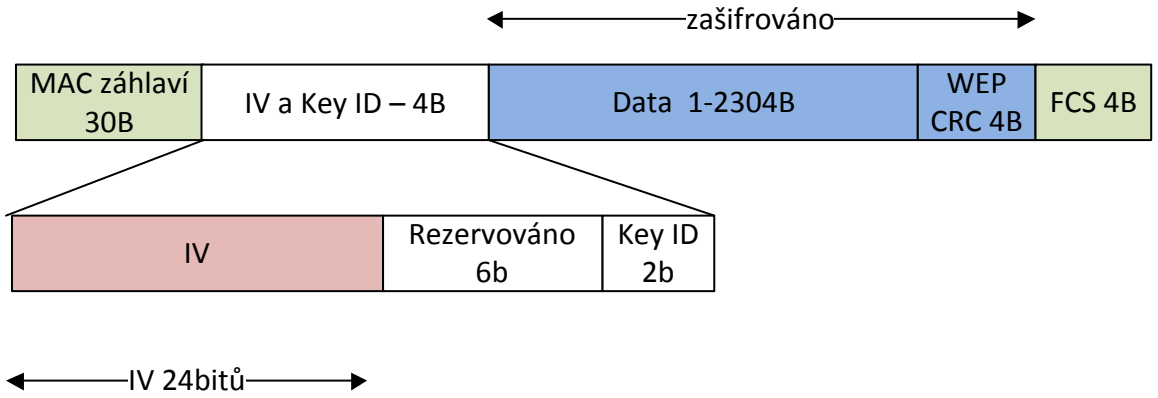
Zabezpečení rámců pomocí protokolu WEP



WEP – bezpečnostní slabiny

- délka klíče 64, 128 nebo 256 bitů
- 24 bitů klíče tvoří vždy Iniciační vektor – IV
  - malá velikost IV (pouze 24 bitů ->2^{24} kombinací)
- reálná délka klíče je tedy 40, 104 nebo 232 bitů
  - klíč je stejný pro každé zařízení v síti
  - klíče jsou statické
- neexistence správy klíčů
  - nutnost manuální výměny na všech zařízeních
- nedostatečná ochrana integrity
  - pouze pomocí CRC-32
- špatná implementace RC4 do WEPu
  - existence slabých klíčů - 9000 z 2^{24} možných
- velmi slabá autentizace pomocí sdíleného klíče

Rámec WEP


zašifrováno
MAC záhlaví 30B
IV a Key ID – 4B
Data 1-2304B
WEP CRC 4B
FCS 4B
IV
Rezervováno 6b
Key ID 2b
IV 24bitů

Vývoj IEEE 802.11i

- Pracovní skupina 802.11 vyvíjela od roku 2001 doporučení 802.11i, které problematiku bezpečnosti řeší komplexně
- Do doby než byla 802.11i přijata byly v roce 2003 uvolněny hotové části 802.11i jako tzv. WPA (WiFi Protected Access)

Útok FMS

- Fluhrer, Mantin, Shamir
- 2001 – popsány slabiny v práci s klíči u algoritmu RC4
- 2004 – popsán útok na protokol WEP schopný získat klíč
- pasivní odposlech provozu
- první byty OT většiny paketů jsou snadno předpověditelné
  - záhlaví SNAP – 0xAA
  - některá pole IP
- IV se přenáší v otevřeném tvaru
  - vhodný tvar IV způsobí kompromitaci některých bitů klíče
- zbývající bity klíče jsou konstantní pro všechny pakety

Útok FMS

- útočník se snaží zrekonstruovat KSA (Key Schedule Algorithm) šifry RC4
- základem útoku je využití slabých IV použitých v RC4
- pro určitou malou skupinu IV existuje asi 5% pravděpodobnost, že budou vyhovovat tzv. podmínce F_{fms} a umožní odhalit další byte klíče
  - (a+3,n-1,x) → (3,255,x)
    - a – KeyID, 2b hodnota, obvykle 0
    - n-1 – prvek o hodnotě rozměru prostoru n ($256 = 2^8$)
    - x - libovolná hodnota
- při zachycení cca $4\text{-}6 \times 10^6$ paketů je 50% pravděpodobnost odhalení klíče

KoreK útok

- 2004
- hacker KoreK
- 16 dalších korelací mezi prvními *L* byty RC4 klíče, prvními dvěma byty generovaného proudu klíče a dalším bytem klíče K[*L*].
- útok je podobný FMS, ale efektivnější
- při zachycení cca 7×10^5 paketů je 50% pravděpodobnost odhalení klíče
- konkrétní hodnoty závisejí na implementaci protokolu
- např. jestli jsou IV generovány nějakým PRNG algoritmem (a jakým), nebo se mění sekvenčně

PTW útok

- 2007
- Tews, Weinmann, Pyshkin
- výrazné urychlení
- při zachycení cca $4x10^4$ paketů je 50% pravděpodobnost odhalení klíče, pro $6x10^4$ paketů je 80% a pro $8,5x10^4$ paketů je 95%.
- v síti s větším provozem lze odchytat dostatečné množství paketů a následně zjistit klíč do 60 s

Chopchop útok

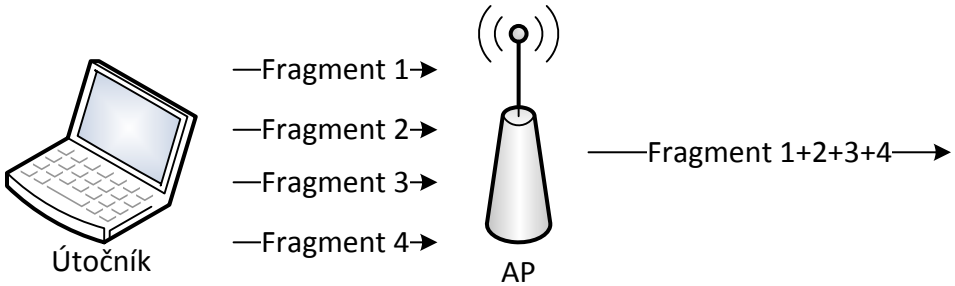
- aktivní útok
- útočník dokáže zjistit *m* posledních bytů OT ze zašifrovaného paketu odesláním průměrně 128*m* paketů (max. 256*m*) do sítě
- útočník nedokáže zjistit klíč
- útok není založen na slabinách implementace algoritmu RC4
- útočník ořízne paket o 1 byte, zrekonstruuje k takto odhadnutému paketu CRC a paket odešle
- pokud byl odhad nesprávný je i CRC špatné a paket je tiše zahozen
- pokud byl odhad správný je správné i CRC a paket je zpracován, ale protože mu poslední byte (nebo více) chybí AP ho zahodí a pošle chybovou zprávu

Padělání zpráv ARP

- ARP injection
- v síti musí být alespoň jeden klient asociovaný s AP
- ARP rámce jsou v provozu snadno rozeznatelné i v zašifrovaných datech
  - délka
  - cílová adresa ARP requestu - FF:FF:FF:FF:FF:FF
- opětovné vysílání ARP request je velmi efektivní způsob jak generovat nové iniciační vektory
- Linux - aircrack-ng, airplay-ng

Útok fragmentací paketů

- aktivní útok
- cíl – získat keystream
- potřebuji zachytit 1 vhodný krátký rámec
  - rámce začínají 0xAAAA0300000008 (LLC/SNAP+zapozdřené IP)
  - prvních 7B bude vždy stejných
  - hodnota 0xAA….⊕ 7B dat = keystream
    - vysílám krátké fragmentované rámce zašifrované známým krátkým keystreamem
  - AP je spojí a odešle jako jeden dlouhý
    - zachytím a provedu XOR s OT jednotlivých fragmentů
    - získám delší keystream
  - lze využít k následné injekci rámce do sítě



WPA – WiFi Protected Access

- publikován v roce 2002
- dočasné řešení od Wi-Fi Alliance před schválením standardu 802.11i (červen 2004)
- stejný algoritmus jako u WEPu – RC4
- autentizace podle 802.1x založená na protokolu EAP
- WEP nahrazen protokolem TKIP
  - Temporary Key Integrity Protocol
- k CRC32 přidán další zabezpečující kód MIC
  - MIC - Message Integrity Check, algoritmus Michael
- kompatibilní se stávajícími zařízeními
  - podporu WPA šlo přidat upgradem firmware

TKIP – Temporary Key Integrity Protocol

- nahrazuje protokol WEP
- stejný šifrovací algoritmus (RC-4)
  - kompatibilita se starším hardware, nutný pouze upgrade ovládacího software
- na rozdíl od WEPu podporuje dynamické klíče
  - klíč se **automaticky** mění každých 10000 paketů

TKIP paket obsahuje

- klíč délky 128 bitů (PK – Packet Key)
- IV délky 48 bitů
- MAC adresu komunikujícího zařízení

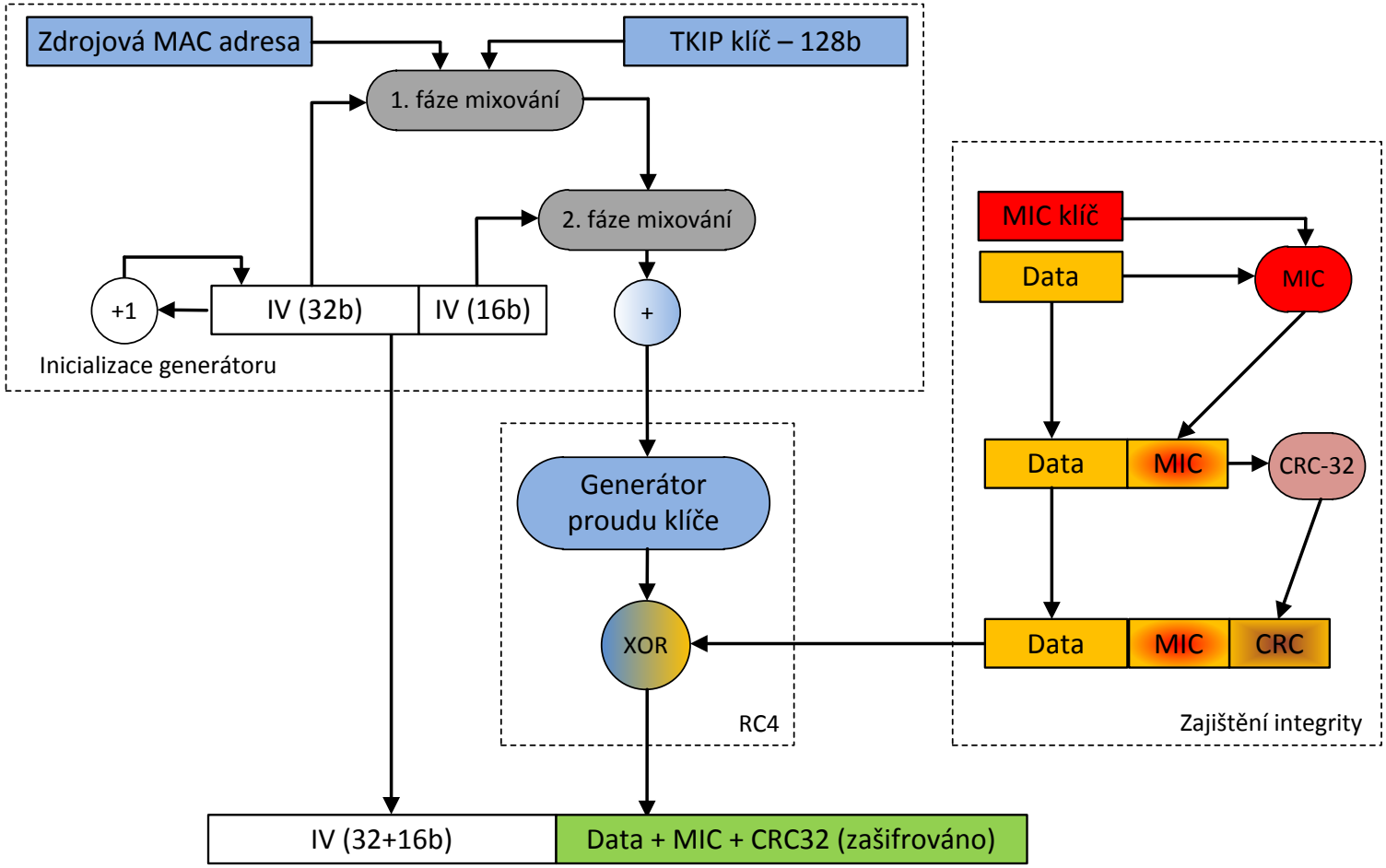
MIC – Message Integrity Check

- algoritmus Michael
  - rychlý
  - 64bitový klíč
- výstup délky 32 bitů
- spočítá se z
  - náhodného čísla
  - datového obsahu rámce
  - záhlaví
  - pořadové číslo rámce (sequence number)
- MIC spolu s CRC-32 řeší problém s možností záměny bitů v rámci
- zabraňuje také vícenásobnému použití IV (replay útoky)
- rámce mimo pořadí jsou zahozeny

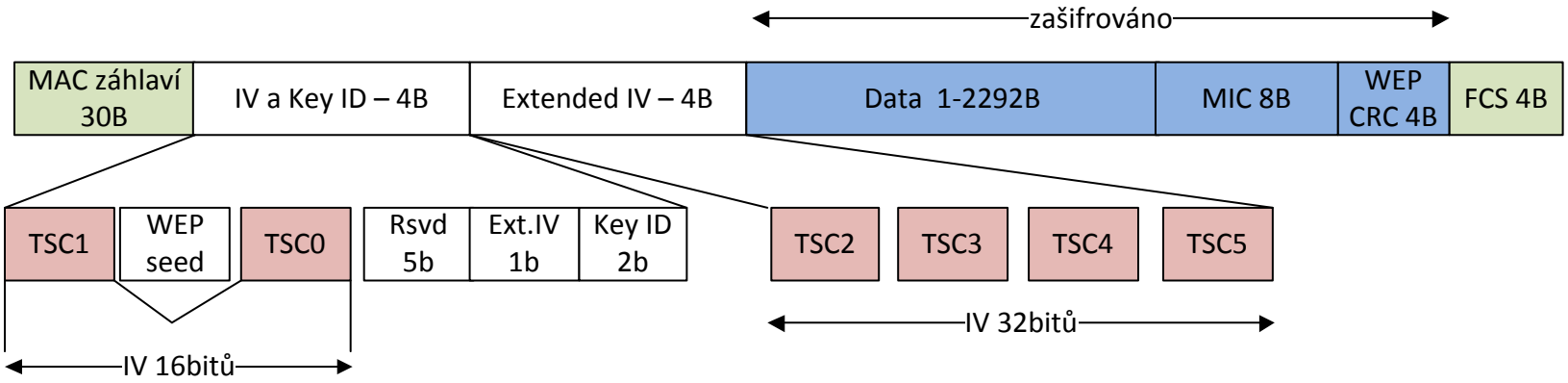
MIC – Message Integrity Check

- MIC vyvinut s cílem udržet kompatibilitu se staršími zařízeními a minimalizovat zpoždění, což se projevilo v jeho nižší bezpečnosti.
- slabá odolnost proti útokům - vyřešeno administrativně
- pokud je v přijatém rámci detekován chybný MIC a současně nebyla detekována chyba v CRC
  - zřejmě o pokus o aktivní útok
- při detekci dvou chyb v MIC za minutu dojde na 60 sekund k přerušení komunikace mezi AP a koncovou stanicí a poté k dojednání nových TKIP klíčů
- platí i pro skupinové klíče GTK (Group Transient Key)
- omezení na 1 narušení za 6 měsíců (MIC má délku 32 bitů, existuje 2^{32} kombinací a lze vyzkoušet 2 kombinace za minutu)

WPA – princip


Zdrojová MAC adresa
TKIP klíč – 128b
1. fáze mixování
2. fáze mixování
+1
IV (32b)
IV (16b)
+
Inicializace generátoru
MIC klíč
Data
MIC
Data
MIC
CRC-32
Generátor proudu klíče
XOR
Data
MIC
CRC
RC4
Zajištění integrity
IV (32+16b)
Data + MIC + CRC32 (zašifrováno)

Rámec TKIP


zašifrováno
MAC záhlaví 30B
IV a Key ID – 4B
Extended IV – 4B
Data 1-2292B
MIC 8B
WEP CRC 4B
FCS 4B
TSC1
WEP seed
TSC0
Rsvd 5b
Ext.IV 1b
Key ID 2b
TSC2
TSC3
TSC4
TSC5
IV 32bitů
IV 16bitů

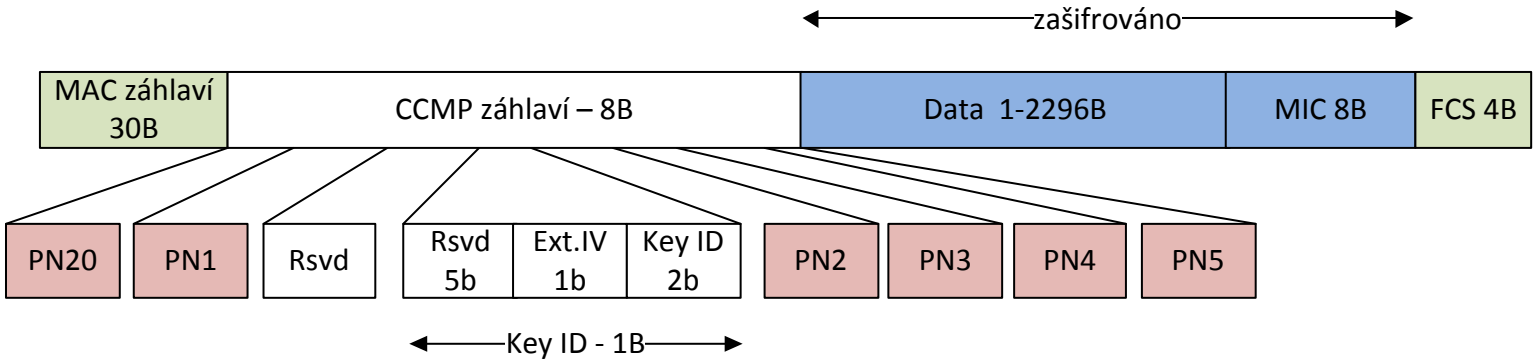
IEEE 802.11i - WPA2, RSN

- řeší komplexně problematiku zabezpečení v sítích IEEE 802.11
- zpětná kompatibilita s WPA
  - WPA je podmnožinou WPA2
- WPA-PSK - alternativní možnost autentizace pro malé sítě
- nový šifrovací algoritmus
  - AES v režimu CCMP
- stávající zařízení nelze upgradovat softwarově
- Broadcast Key Rotation
  - dříve pouze proprietární technologie Cisca

Útoky na PSK u WPA/WPA2

- útok hrubou silou/slovníkový útok
- nutné zachytit 4way handshake
- PMK = PBKDF2 (heslo, SSID, délka SSID, 4096, 256)
  - změna SSID z defaultního zvyšuje bezpečnost
  - délka hesla (min. 10 znaků)
  - odolnost vůči slovníkovému útok
  - útok je relativně pomalý
    - stovky kombinací/s na moderním PC
    - každý pokud = 4096 hashů hledaného hesla
  - TMTO – pro dané SSID lze předgenerovat tabulku
- Nástroje: cowpatty, aircrack-ng

Rámec CCMP (Counter CBC-MAC Protocol)



Autentizace v bezdrátových sítích 802.11

- Otevřená síť
- Autentizace pomocí MAC adresy
- Autentizace na VPN bráně
- Autentizace pomocí webového formuláře
- Autentizace pomocí WEPu (sdílený klíč)
- Autentizace pomocí WPA-PSK
- Autentizace pomocí IEEE 802.1X

Autentizace v bezdrátových sítích 802.11

1. Otevřená autentizace (Open)

- AP autentizuje klienta na základě údajů přijatých ze stanice, ale tyto nijak neověřuje
- Každá stanice, která zná SSID je úspěšně autentizována

2. Autentizace podle MAC adresy

- stejné jako varianta 1) + kontrola zdrojové MAC adresy
- problém s aktualizací databáze MAC adres na více AP
- lze jednoduše padělat

Autentizace v bezdrátových sítích 802.11

3. Autentizace na VPN bráně

- samotná síť autentizaci neřeší
  - k AP se přihlásí kdokoliv
- klient se autentizuje na VPN gatewayi
- na straně klienta je potřeba příslušný SW (VPN klient)
- omezení na konkrétního výrobce
- obtížná rozšiřitelnost
- drahé VPN koncentrátotry
- firemní prostředí
- dnes se už nepoužívá

Autentizace v bezdrátových sítích 802.11

4. Autentizace webovým formulářem

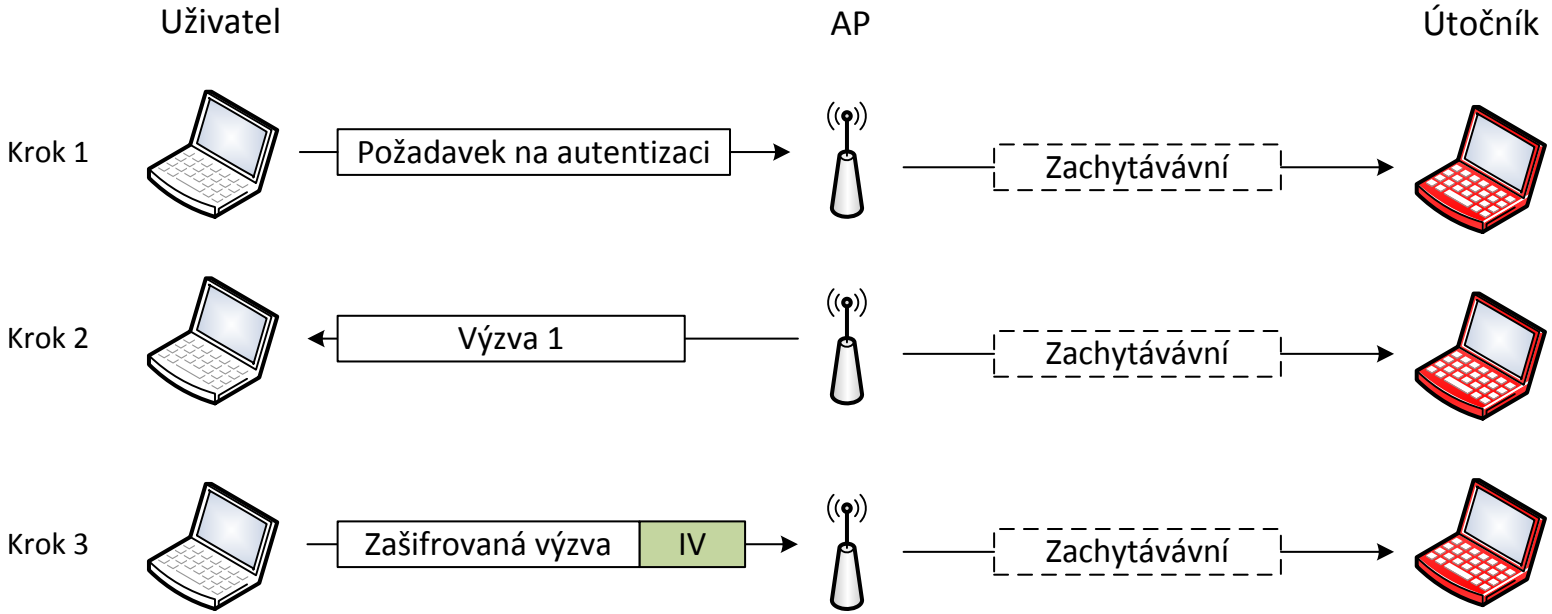
- po připojení do sítě je veškerý provoz přesměrován na přihlašovací stránku
- zde se uživatel autentizuje
- až po úspěšné autentizaci, je možné využívat síťové připojení
- počítač musí být vybavený WWW prohlížečem, který musí být po celou dobu spojení zapnutý
- vhodné pro místa s vysokou fluktuací klientů
  - hotely, letiště

Autentizace v bezdrátových sítích 802.11

5. Autentizace sdíleným klíčem (Shared Key)

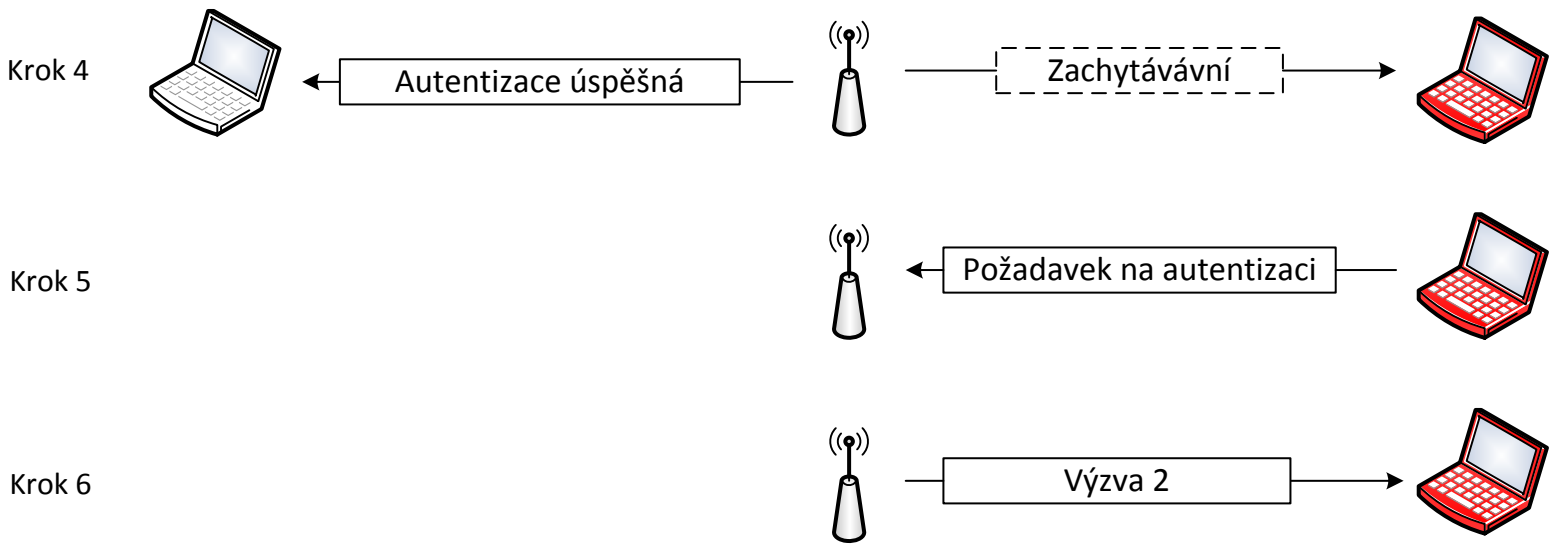
- klient vyzve přístupový bod (AP) k odeslání výzvy
- AP pošle klientovi náhodnou 128-bytovou výzvu
- klient zašifruje výzvu pomocí WEPu a sdíleného klíče
- klient odešle zašifrovanou výzvu odešle do AP
- pokud AP správně dešifruje svoji původní výzvu, povolí klientovi přístup
- **nebezpečné**

Útok na sdílenou autentizaci u WEP



- Útočník spočítá v kroku 3 „Výzva 1“ XOR „Zašifrovaná výzva“ – získá část proudu klíče a konkrétní IV

Útok na sdílenou autentizaci u WEP



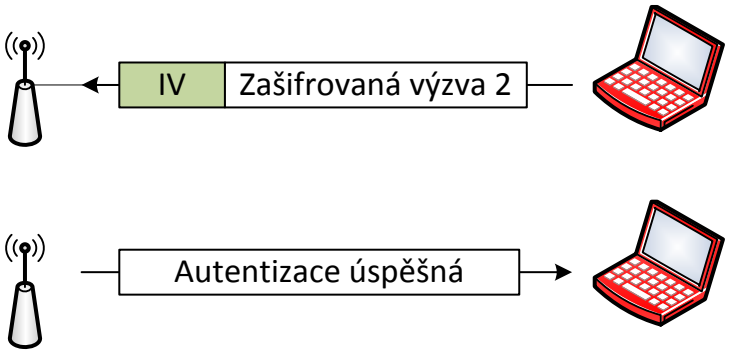
- V kroku 6 útočník spočítá XOR „Výzva 2“ a získaná část proudu klíče.

Útok na sdílenou autentizaci u WEP

- V kroku 7 útočník sestaví rámec obsahující padělanou výzvu a původní IV

Krok 7

Krok 8



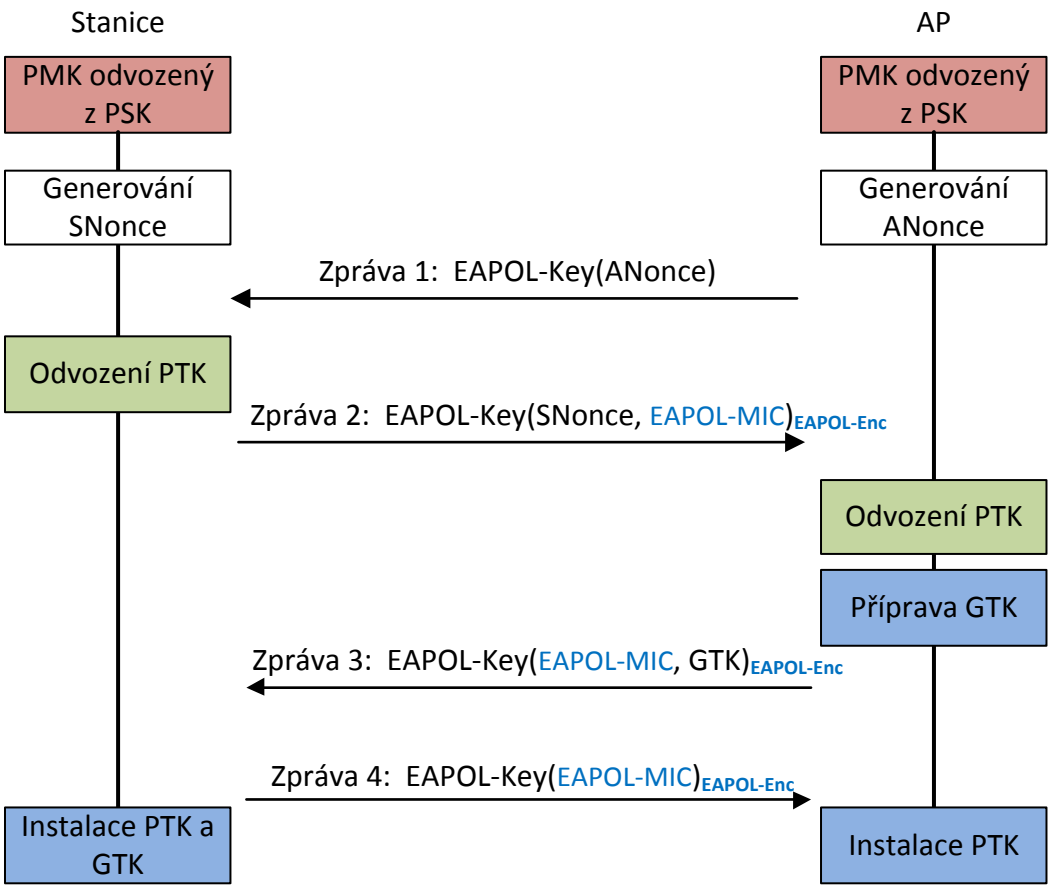
- V kroku 8 je útočník úspěšně autentizován.

Autentizace v bezdrátových sítích 802.11

6. WPA-PSK

- PSK - Pre-shared Key (předsdílený klíč)
- alternativa ke správě klíčů pomocí 802.1X
- vhodné pro menší (domácí) sítě
- PSK je 256 bitové číslo nebo hesla délky 8 - 63 znaků, která se pak na PSK převádí
- náchylné na slovníkové útoky
  - nutno zvolit dostatečně dlouhou a složitou passphrase
- PSK může být různý pro každé zařízení
  - v závislosti na MAC adrese
- standardně výrobci používají jeden PSK pro celou síť
- PMK = PBKDF2 (heslo, SSID, délka SSID, 4096, 256), kde PBKDF2 je metoda z PKCS #5 v2.0

Předání klíčů AP ↔ klient u WPA-PSK

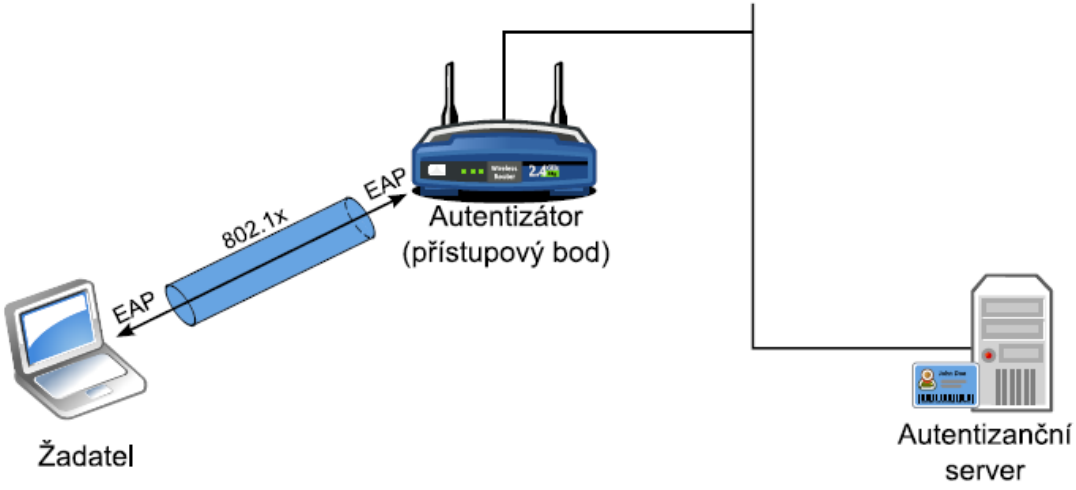


802.1x

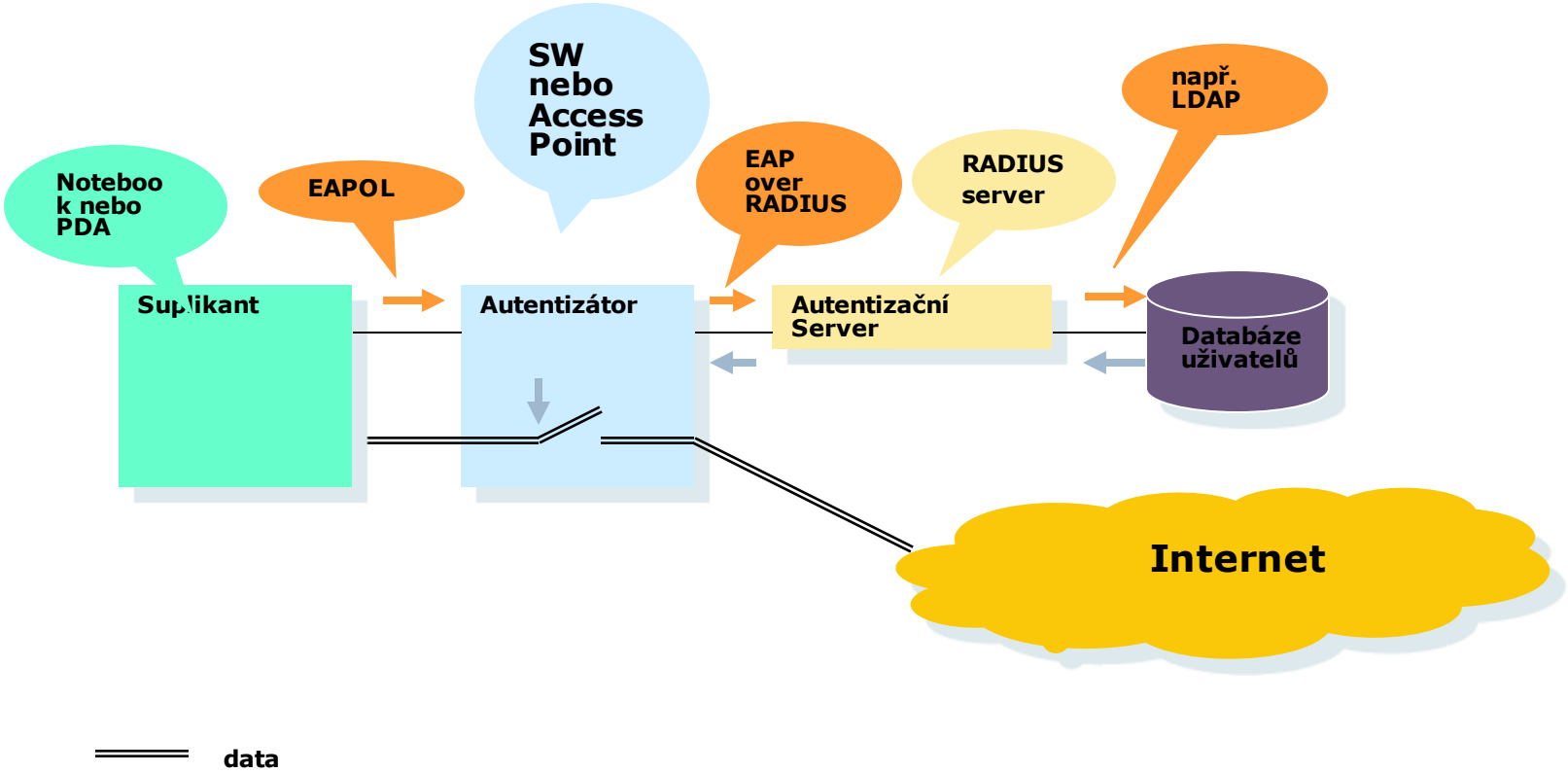
- obecný bezpečnostní rámec pro autentizaci v LAN

Architekturu IEEE 802.1x tvoří tři základní funkční entity:

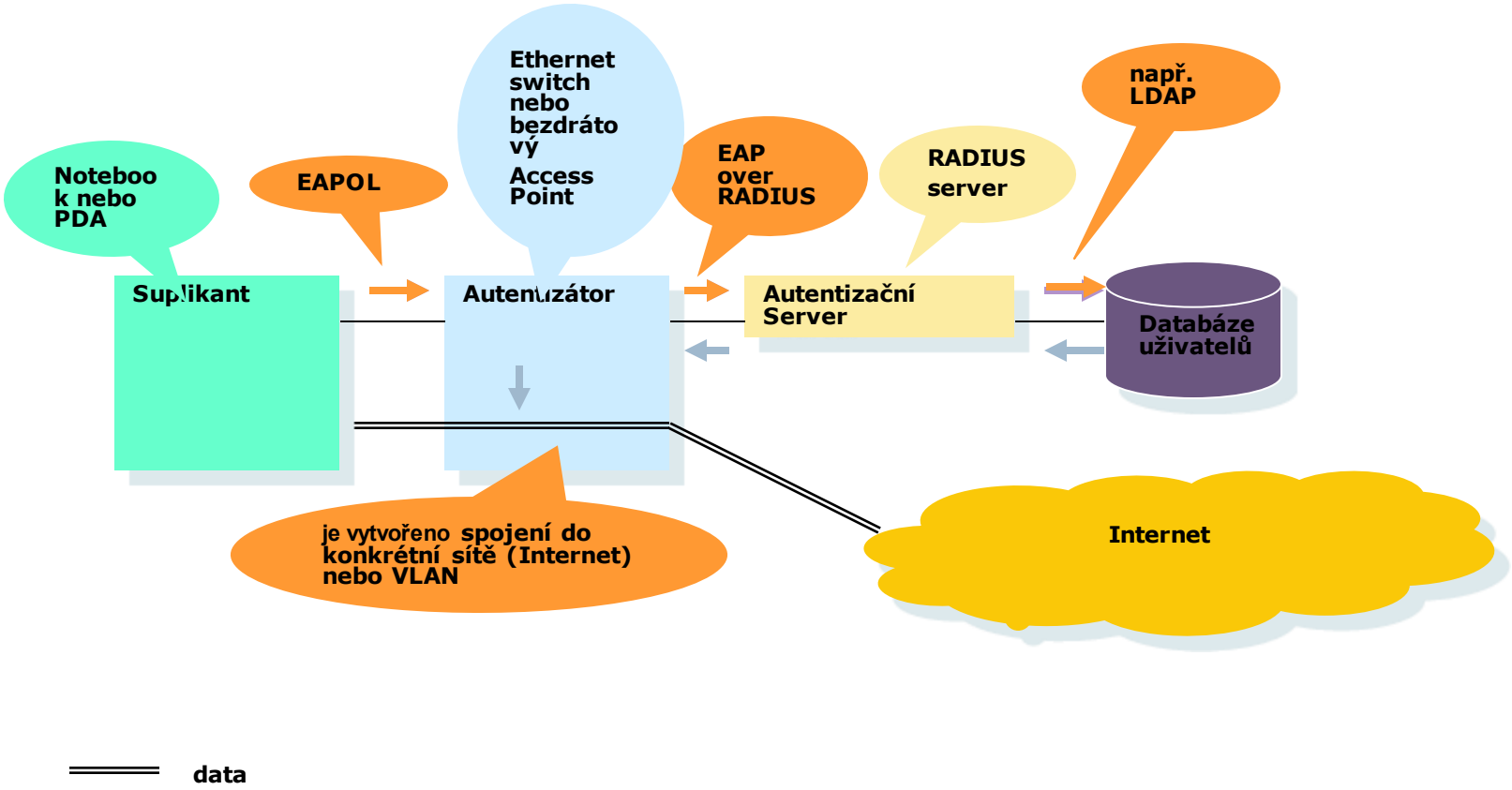
- suplikant (žadatel) připojení k síti,
- autentizátor zajišťující řízení přístupu,
- autentizační server provádějící autorizační rozhodnutí.



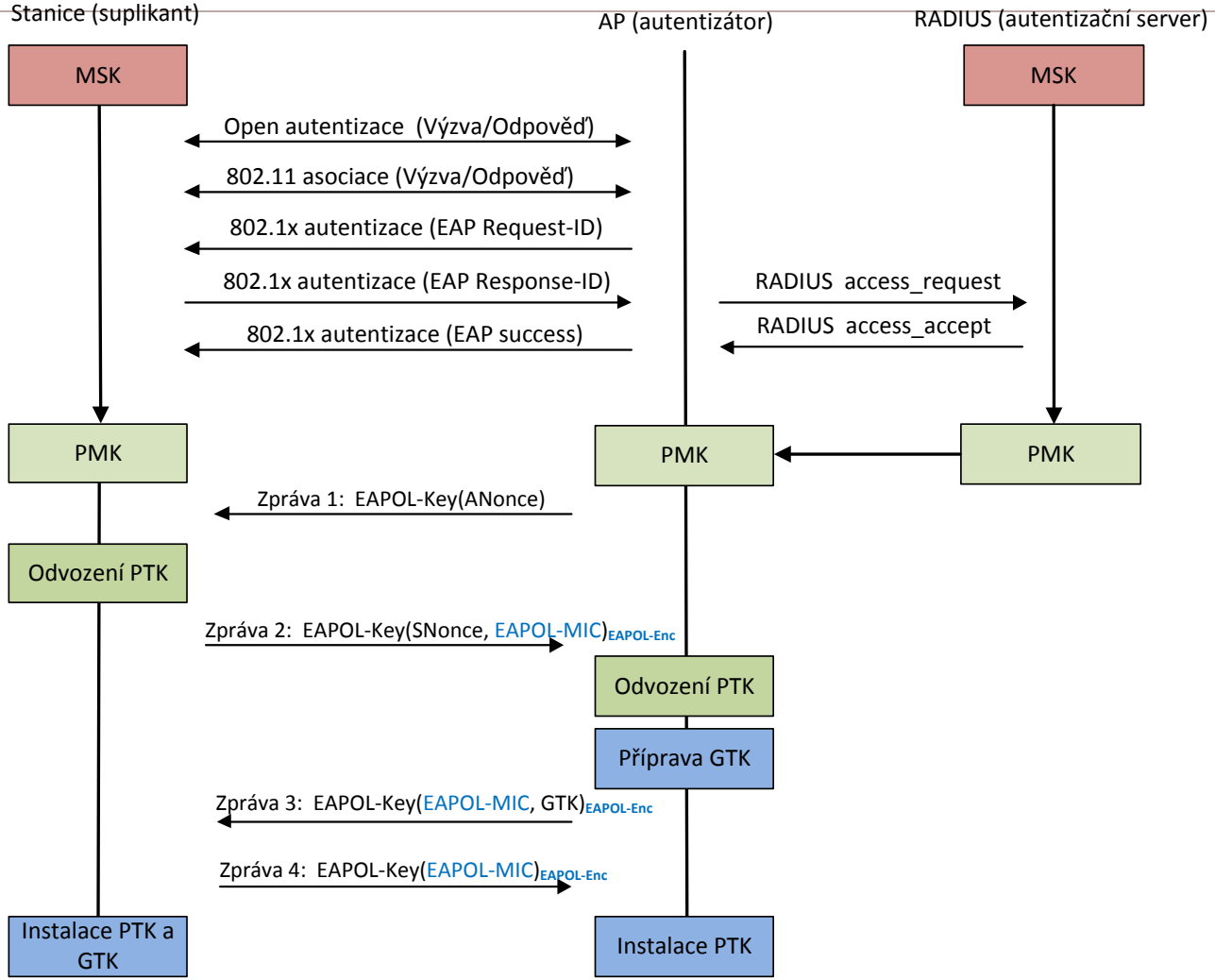
Princip 802.1x



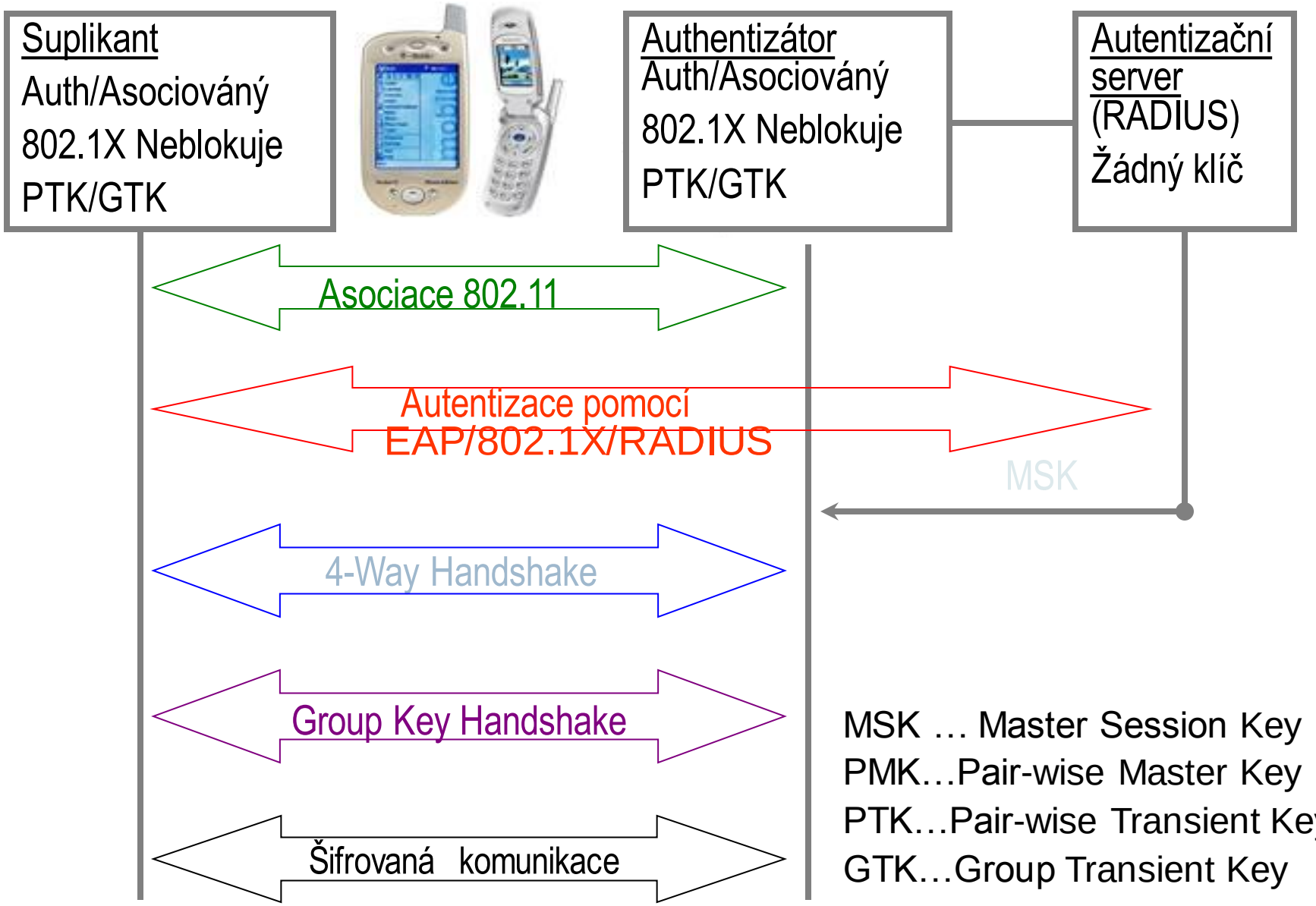
Princip 802.1x



802.1x autentizace



Celý proces výměny klíčů



MSK … Master Session Key
PMK…Pair-wise Master Key
PTK…Pair-wise Transient Key
GTK…Group Transient Key

4-way handshake

- 4-way handske slouží k odvození PTK (Pairwise Transient Key) a GTK (Group TK)
- PTK a GTK se odvozují z PMK (Pairwise Master Key), který se získá následovně:

  1) pokud je autentizace WPA-PSK pak PMK=PSK* pak má délku 512b

  2) pokud je autentizace 802.1x
  odvodí se z 802.1x MSK (Master Session Key) a PMK má délku 384b

PMK obsahuje:

KCK – Key Confirmation Key – 128b – klíč pro zajištění integrity během fáze 4-way handshake

KEK – Key Encryption Key – 128b – klíč pro šifrování dat během 4-way handshake

TK – Temporary Key – 128b – klíč pro šifrování protokolem TKIP nebo AES-CCMP

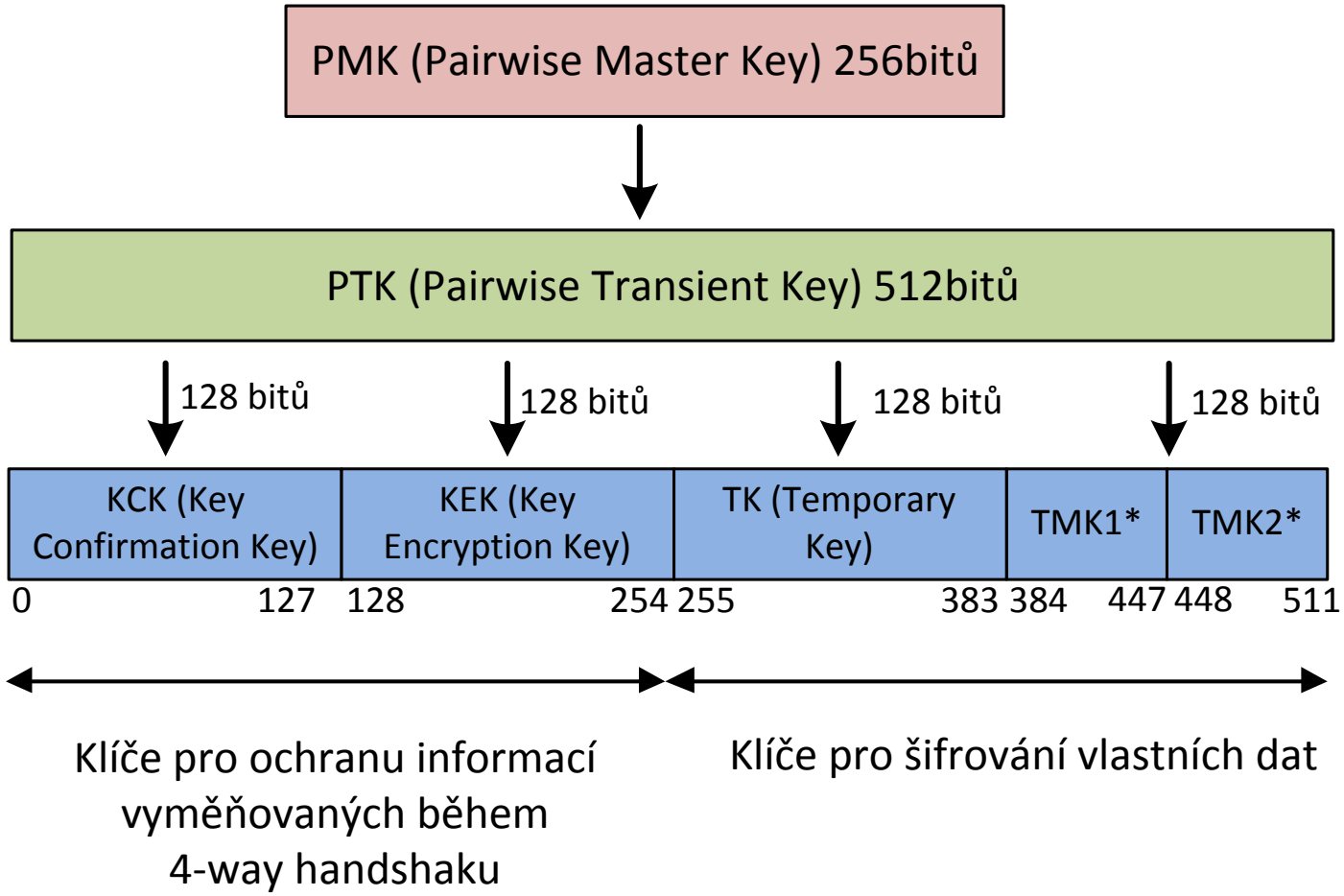
TMK1, TMK2 – Temporary Mic Key – 2x64b – klíč pro MIC – pouze u PSK

*PSK – Pre-Shared Key - generuje se z hesla (8-63 znaků)

4-way handshake

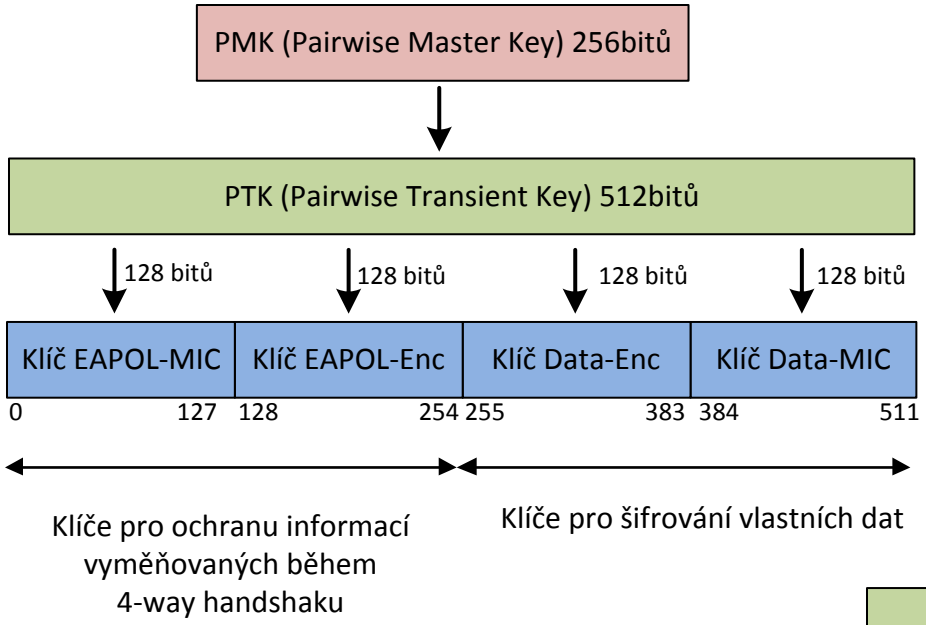
- po 4-way handshaku následuje GK Hansdhake
- po výměnu broadcast a multicast zpráv je nutné si vyměnit GTP (Group Transient Key)
- GTP = GEK + GIK
- GEK – Group Encryption Key – 128b - klíč pro TKIP nebo AES-CCMP
- GIK – Group Integrity Key – 128b - pouze pro algoritmus Michael (u TKIPu)

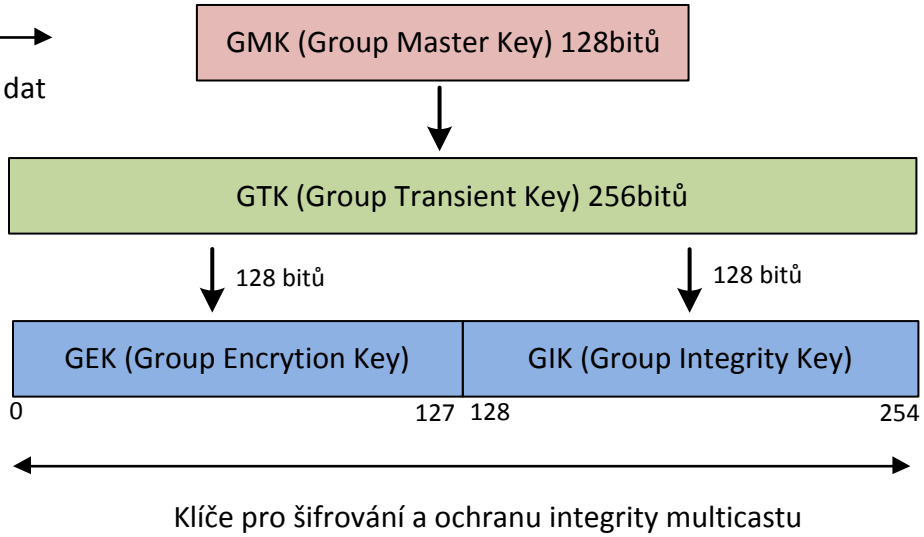
Odvození klíčů pro unicastovou komunikaci



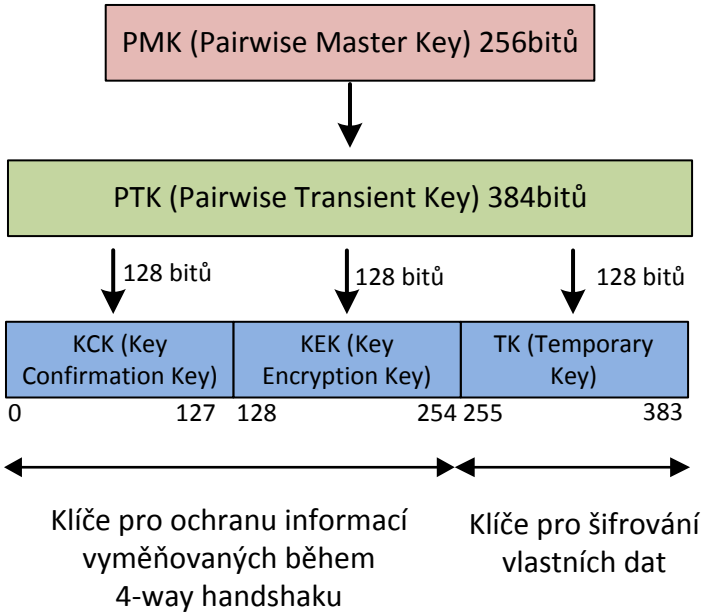
*TMK1, TMK2 – Temporary MIC Key 1,2 – 64bitový klíč pro MIC

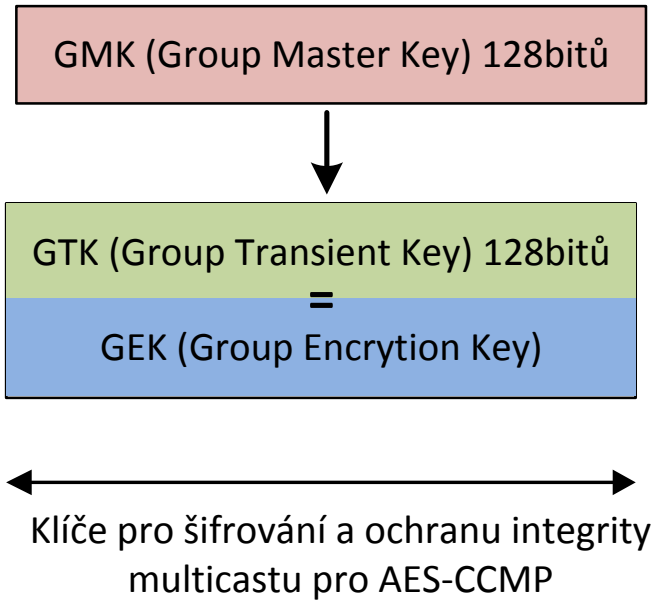
WPA-TKIP hiearchie klíčů





AES-CCMP hiearchie klíčů



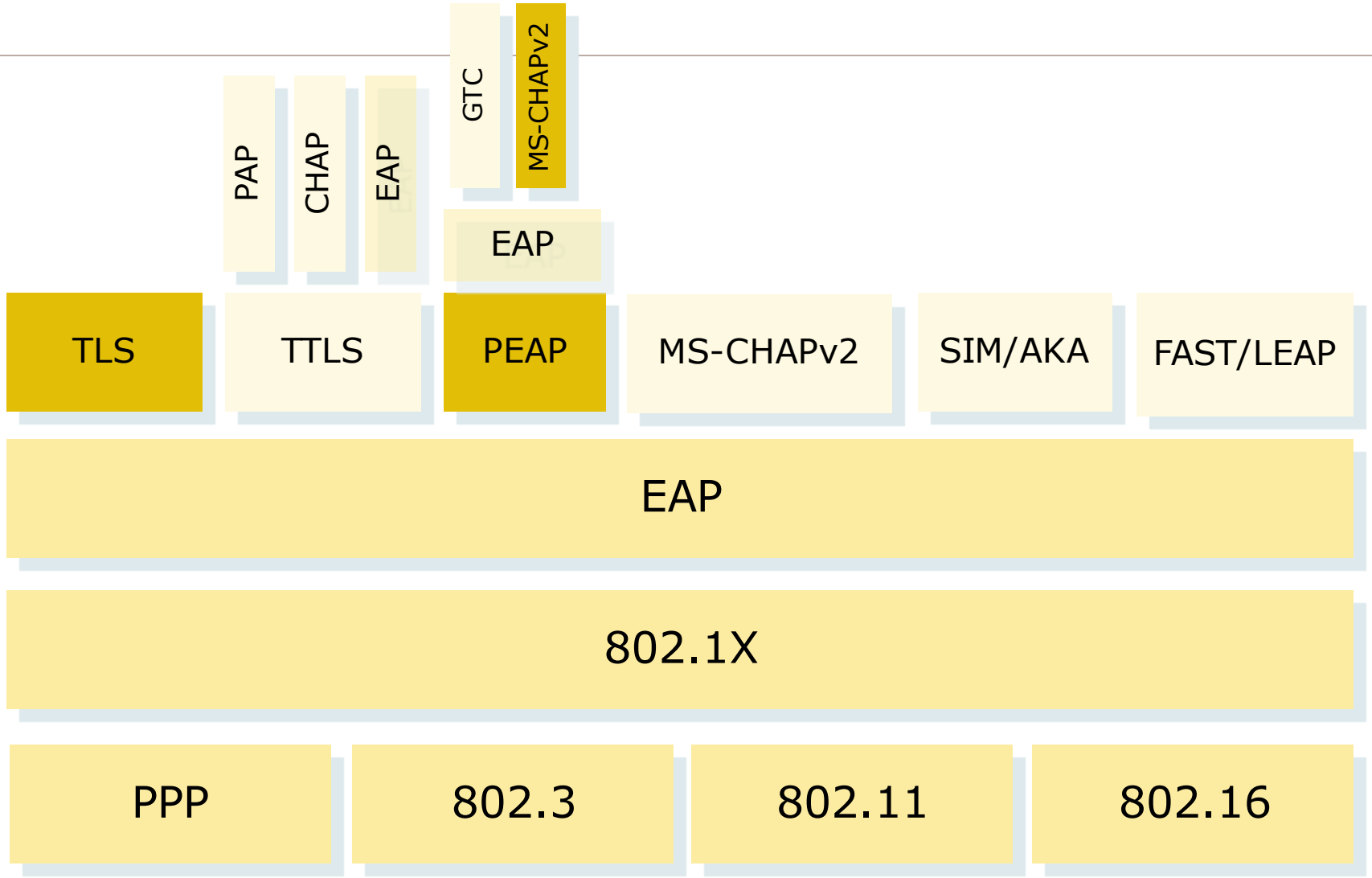


EAP

- EAP byl vyvinut pro autentizaci PPP
- 802.1x rozšířil jeho použití v sítích 802
  - ne pouze 802.11 ale i
  - 802.3
  - 802.16
  - …
- zprávy EAP se zapouzdřují do rámců 802.1x
- EAP sám o sobě autentizaci neřeší
  - definuje obecný formát a syntaxi zpráv
  - konkrétní formy autentizace – EAP metody

Obecný EAP (Extensible Authentication Protocol)

- AP vyšle po asociaci klienta EAP REQUEST-ID
- Klient odpoví EAP RESPONSE-ID, obsahující identifikační údaje uživatele
- AP 'přebalí' tuto zprávu do paketu RADIUS ACCESS_REQUEST a pošle RADIUS serveru
- RADIUS server odpoví RADIUS ACCESS_ACCEPT nebo DENY, což AP 'přebalí' pro klienta jako EAP SUCCESS / FAILURE
- Pokud je autentizace úspěšná, tak port, přes nějž tato komunikace probíhala, je otevřen pro datovou komunikaci klienta


PAP
CHAP
EAP
GTC
MS-CHAPv2
EAP
TLS
TTLS
PEAP
MS-CHAPv2
SIM/AKA
FAST/LEAP
EAP
802.1X
PPP
802.3
802.11
802.16

Metody EAP

Vybrané varianty protokolu EAP

EAP-MD5

- tato varianta EAP umožňuje pouze jednosměrnou autentizaci klienta.
- server odešle náhodné číslo (challenge)
- klient spočte hash: MD-5(challenge,heslo)
- pokud útočník může získat výzvu i odpověď lze použít slovníkový útok
- server se neautentizuje -> spoofing
- EAP-MD5 nelze vyžít k distribuci klíčů
- EAP-MD5 lze použít v LAN ale ne v WLAN

Metody EAP - LEAP (Lightweight EAP)

- vzájemná autentizace klienta a serveru
- proprietární protokol firmy Cisco
- označován také jako EAP-Cisco Wireless
- jsou k dispozici nástroje pro získání hesel
    - slovníkový útok
- modifikovaný MS-CHAPv2
- už. heslo šifrováno pomocí 3x DES (56b)
    - klíče vygenerovány pomocí MD4 (128b = 16B)
        - klíč1: `B1 B2 B3 B4 B5 B6 B7`
        - klíč2: `B8 B9 B10 B11 B12 B13 B14`
        - klíč3: `B15 B16 0 0 0 0 0` (pouze 216 komb.)

Metody EAP

EAP-TLS (Transport Layer Security)

- nejbezpečnější, nejdražší na implementaci
- vzájemná autentizace pomocí certifikátů a protokolu TLS
- server používá TLS k dokázání vlastnictví digitálního certifikátu a to samé požaduje od klienta
- klient používá svůj certifikát k prokázání své identity a k výměně dat pro generování klíčů
- po úspěšné autentizaci je tunel ukončen, ale klíče odvozené během EAP-TLS se používají k šifrování pomocí AES, TKIP nebo WEP.

Metody EAP

EAP-SIM (Subscriber Identity Module)

- vzájemná autentizace na základě SIM karty (nebo obecně nějaké smart-karty)
- požadavky na autentizaci podle 802.1X jsou přenášené protokolem EAP-SIM přes GW operátora do AuC příslušné GSM sítě.
- předpokládané použití při autentizaci smartphonů roamujících mezi WiFi a GSM sítěmi.

EAP-AKA (Authentication and Key Agreement)

- stejné jako EAP-SIM, ale pro sítě UMTS používající USIM (User Service Identity Module)
- používá silnější autentizační prostředky než EAP-SIM

Metody EAP

EAP-FAST (Flexible Authentication via Secure Tunneling)

- vytvořilo Cisco jako náhradu LEAP
- vzájemná autentizace
- použití zabezpečeného tunelu (stejně jako EAP-TTLS nebo PEAP)
- EAP-FAST nevyžaduje, aby se server autentizoval pomocí certifikátu
- pro pomalé klienty typu WiFi telefony, kde by ověřování digitálních certifikátů trvalo dlouho
- v současnosti je použití omezeno pouze na WiFi sítě se zařízeními od firmy Cisco

Metody EAP

EAP-TTLS (Tunneled TLS)

- AP se autentizuje pomocí má certifikátu
- klient nemá certifikát, autentizuje se pomocí protokolu PAP/CHAP(jméno/heslo), který je zapouzdřen v SSL tunelu
- proprietární protokol firem Funk Software a Certicom
- existují dvě verze:
  - EAP-TTLSv0 …RFC5281
  - EAP-TTLSv1 … nyní ve stádiu draftu IETF http://tools.ietf.org/html/draft-funk-eap-ttls-v1-00
- v praxi se neuplatnil
- nahradil ho EAP-PEAPv0/MSCHAP-v2

Metody EAP

PEAP (Protected EAP)

- velmi podobný EAP-TTLS
- pouze server se autentizuje certifikátem
- TLS spojení pro bezpečnou autentizaci klienta
- otevřený standard vyvinutý firmami Microsoft, Cisco a RSA Security

Od 05/2005 je možné používat dvě varianty PEAP k autentizaci podle WPA/WPA2:

1) PEAPv1/EAP-GTC
2) **PEAPv0/EAP-MSCHAPv2**

Metody EAP

PEAPv1/EAP-GTC (Generic Token Card)

- vyvinulo Cisco
- umožňuje používání jiných vnořených autentizačních protokolů než jen MSCHAPv2
- definuje obálku EAP pro přenos jednorázových hesel generovaných zařízeními jako je „RSA Secur ID“
- vhodné pro dvoufaktorovou autentizaci
- MS ho nikdy neimplementoval do Windows
- Cisco má své proprietární protokoly LEAP a EAP-FAST a také moc nepropaguje PEAPv1
- neexistuje nativní podpora v OS → PEAPv1 se nepoužívá

Metody EAP

PEAPv0/EAP-MSCHAPv2

- 2. nejrozšířenější po EAP-TLS, vyvinul ho Microsoft
- MS neuznává PEAPv1, proto označuje protokol PEAPv0 pouze jako PEAP (tzn. neuvádí v0 a v1)
- známe implementace : AEGIS
  - Windows
  - od firmy Meetinghouse xsupplicant
  - všechny POSIX (Linux, BSD, Unix like OS)
  - projekt Open1x.org

Metody EAP

Kromě těchto verzí existují i jiné varianty PEAP:

PEAP-EAP-TLS

- velmi podobný EAP-TLS
- autentizace klienta pomocí certifikátu, přes kanál šifrovaný pomocí TLS
- podporuje ho MS, ale ne Cisco a většina výrobců
- takřka se nepoužívá

PEAPv0-EAP-SIM / PEAPv1-EAP-SIM

- podporuje Cisco, ale ne MS
- vytvořen pro GSM sítě
- autentizace SIM karty v síti
- WiFi aliance se snaží rozšířit podporu EAP i mimo klasické bezdrátové sítě , zatím nepříliš úspěšně
- není nativně podporován v žádném OS

Srovnání EAP metod

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Autentizace Serveru	--	hash hesla	veřejný klíč (certifikát)	veřejný klíč (certifikát)	veřejný klíč (certifikát)
Autentizace klienta	hash hesla	hash hesla	veřejný klíč (certifikát nebo Smart karta)	CHAP, PAP, MS-CHAP(v2)	EAP-MS-CHAPv2 nebo veřejný. klíč
Dynamické Posílání klíčů	ne	ano	ano	ano	ano
Poznámka	Nejjedno-dušší a nejslabší varianta	LEAP = Lightweight EAP	TLS = Transport Layer Security	TTLS = Tunelled TLS	PEAP = Protected EAP

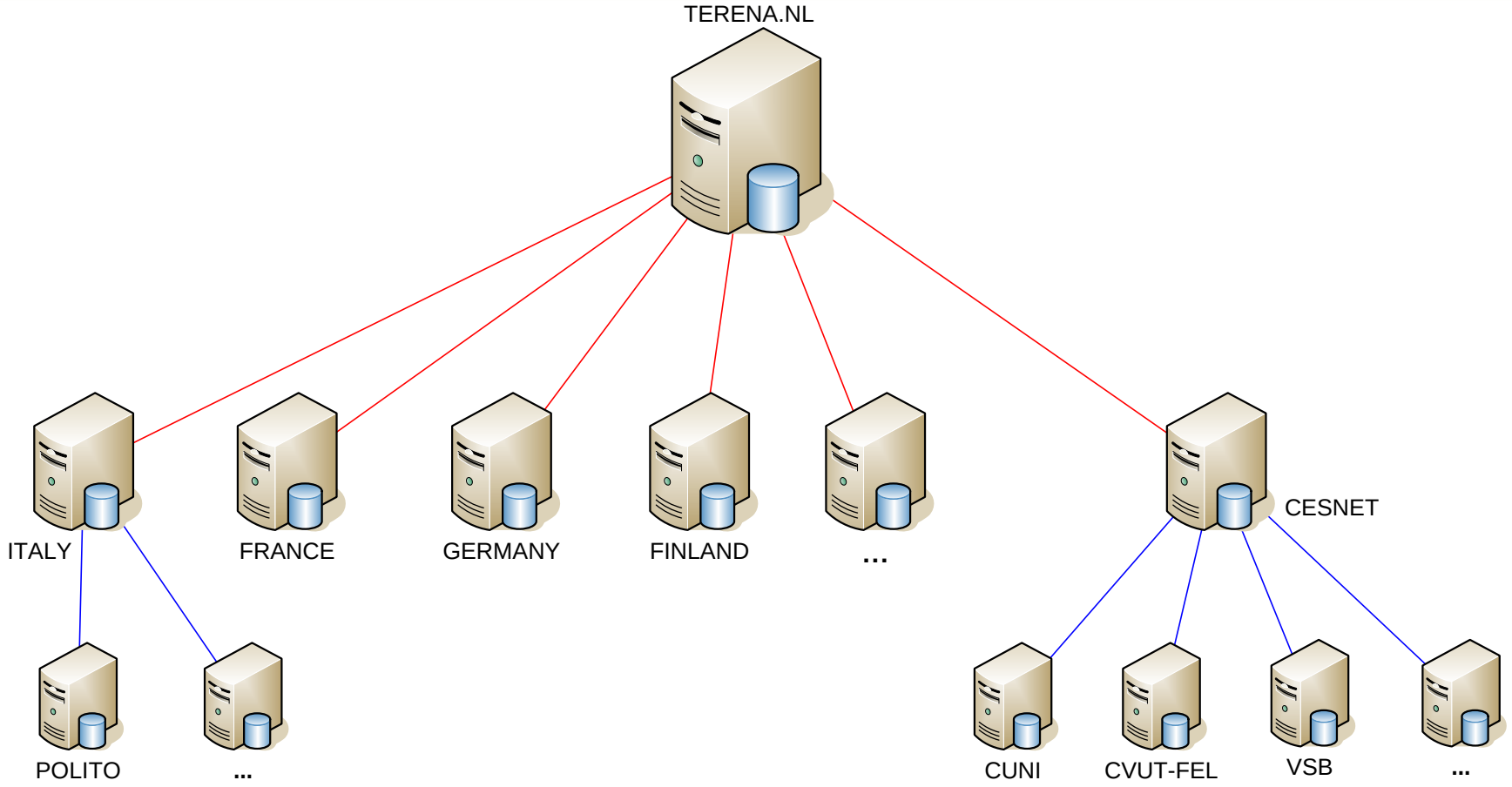
Varianty EAP podporované v rámci 802.11i

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

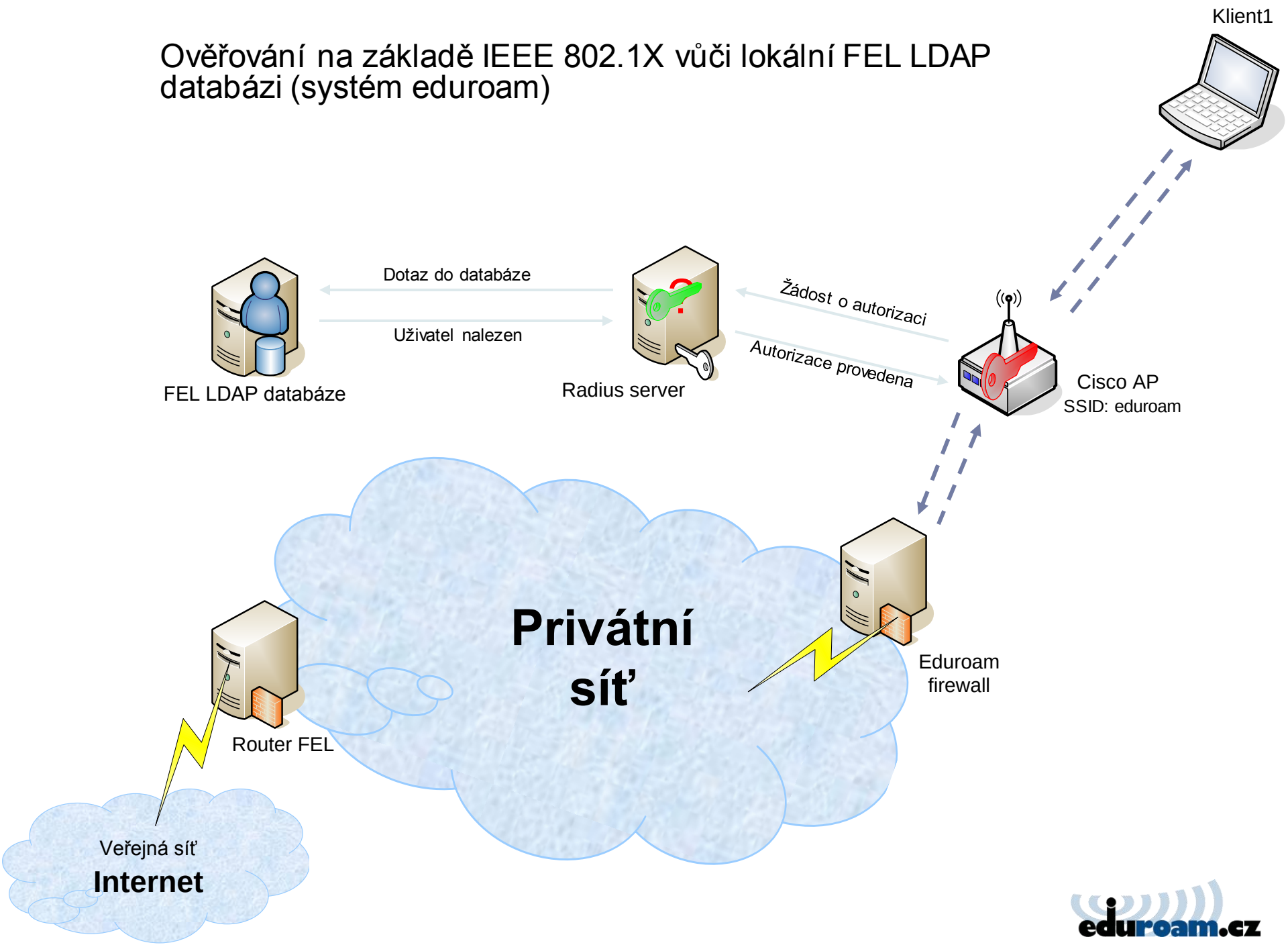
Autentizace pomocí 802.1x v projektu eduroam

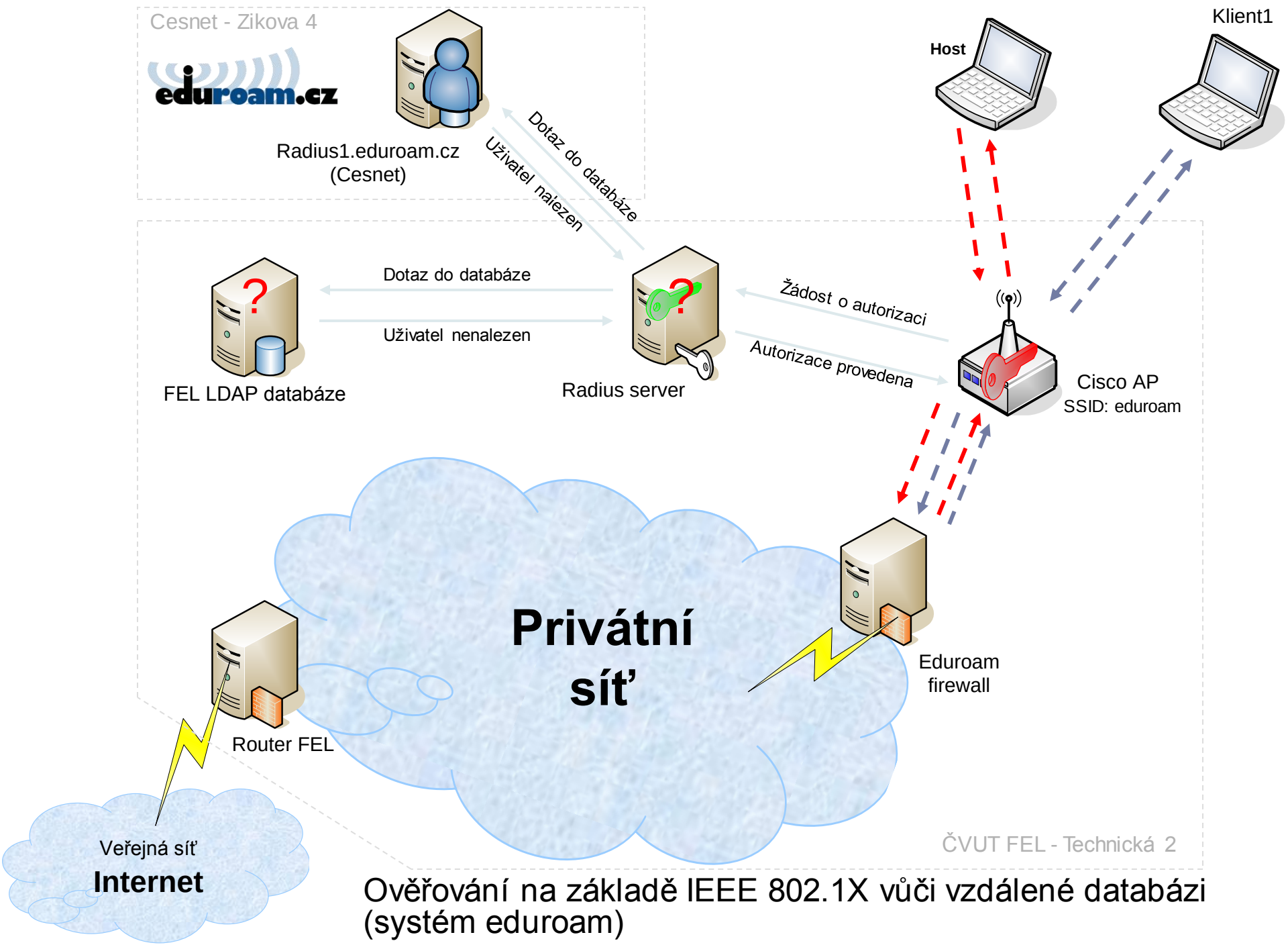
- http://www.eduroam.org/?p=europe
- mezinárodní projekt zabývající se mobilitou a roamingem v počítačových sítích
- praktický příklad IP roamingu mezi organizacemi
- v ČR ho koordinuje CESNET
- uživatel, který má účet pouze u jedné takové organizace (domovské síti) má oprávnění použít kteroukoliv síť organizace zapojené do projektu eduroam.
- ověřování se děje pomocí RADIUS serverů
- hiearchická struktura (podobně jako u DNS)
- směrování autentizačních požadavků na základě tzv. realmů
- uživatelské jméno má tvar username@realm
- realm – libovolný řetězec, v praxi shody s doménovým jménem instituce např. vanekt1@fel.cvut.cz

Struktura RADIUS serverů v rámci projektu eduroam



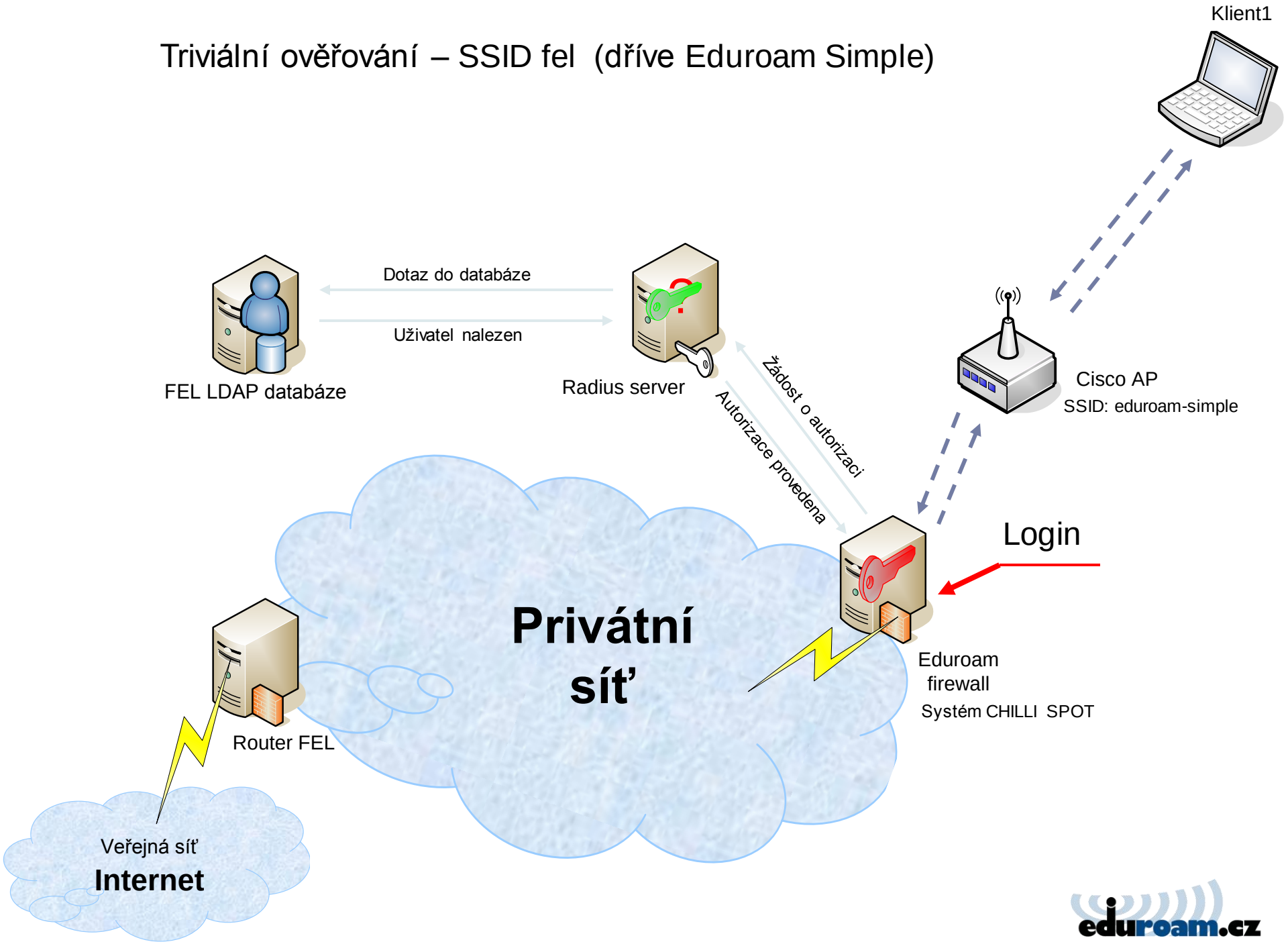
Ověřování na základě IEEE 802.1X vůči lokální FEL LDAP databázi (systém eduroam)





Ověřování na základě IEEE 802.1X vůči vzdálené databázi (systém eduroam)

Triviální ověřování – SSID fel (dříve Eduroam Simple)



Útoky na fyzické a spojové vrstvě sítí 802.11

- **I při použití 802.11i je síť stále zranitelná těmito typy útoků!**
- falšování nechráněných řídících rámců typu Deauthentication/Disassociation
- narušování řízení přístupu k médiu pomocí falšování rámců RTS/CTS
  - RTS flood – účinné v sítích s velkým počtem skrytých uzlů
  - CTS flood
- DoS útoky na zprávy EAP - padělání zpráv EAPOL-Start, EAPOL-Success, EAPOL-Logoff, EAPOL-Failure
- současné poslání více než 255 požadavků na asociaci vedoucí k vyčerpání pole „EAP identifier“ (8 bitů)

Zabezpečení sítí
IEEE 802.3 (Ethernet)

Zabezpečení Ethernetu

- 802.1AE – MACSec
  - 2006 - schváleno
    - 2011 – práce na přidání AES256-GCM do standardu
  - rozšíření eth. rámce o 4B
  - Cisco Nexus 7000,5000 a 2000

- 802.1AF – key management
  - začleněno do 802.1x-2010
- 802.1AR – Secure Device Identity
  - od 10/2009 draft 2.3
  - již existují zařízení s podporu
    - např. Cisco CGS 2520 (Grid Switch)

Dotazy