

# **Text laboratórnej úlohy**

Laboratórna úloha č. 8

## **Autentizácia pomocou EAP a RADIUS**

# Úvod k laboratórnej úlohe

Cieľom laboratórnej úlohy je priblížiť študentom existujúce možnosti centralizovanej autentizácie v porovnaní s mechanizmami pre lokálne overenie identity užívateľov, resp. zariadení, oboznámiť ich s princípmi zabezpečenia prístupu do siete pomocou **autentizačných protokolov EAP (*Extensible Authentication Protocol*) a RADIUS (*Remote Authentication Dial-In User Service*)** a poskytnúť im priestor k získaniu skúseností s implementáciou RADIUS servera ako centrálného prvku pre riadenie prístupu a zabezpečené pripojenie k sieti.

V tejto úlohe získate základné poznatky o priebehu autentizácia klienta vo Wi-Fi sieti s podporou IEEE 802.1X. V teoretickej časti bude vysvetlené akým spôsobom sa konfiguruje FreeRADIUS server a ako prebieha proces overovania identity užívateľa prostredníctvom externého autentizačného mechanizmu. V praktickej časti si najskôr vyskúšate vo vytvorenej virtuálnej sieti pozostávajúcej z troch virtuálnych strojov predstavujúcich klienta, prístupový bod a autentizačný server v prostredí VMware **nasadiť a konfigurovať FreeRADIUS server**, predstavujúci centrálny bod autentizácie jeho prepojenie s prístupovým bodom prostredníctvom protokolu EAP a tiež samotnú autentizáciu klienta. Významnou súčasťou úlohy bude následná analýza priebehu autentizačného procesu pomocou sieťovej analýzy, ktorá študentom umožní lepšie porozumieť fungovaniu úzkej spolupráce medzi jednotlivými vrstvami sieťovej architektúry, predovšetkým medzi linkovou, sieťovou a aplikačnou vrstvou.

## Požiadavky pre vypracovanie úlohy:

- software: VMware Workstation Player pre virtualizáciu staníc,
- virtuálne stroje: tri virtuálne stroje s Kali Linux.

## 1. Teoretický úvod

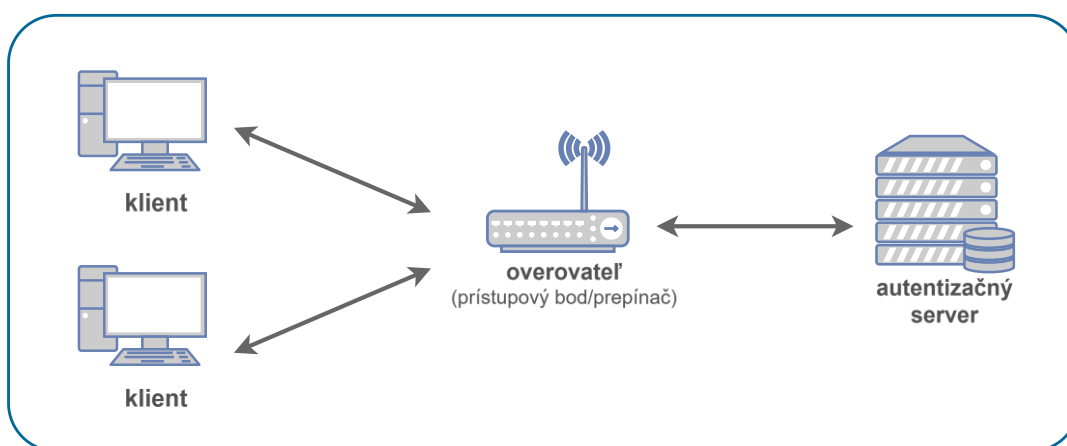
V tejto laboratórnej úlohe venovanej autentizačným protokolom EAP a RADIUS sa zoznámite s možnosťami centralizovaného riadenia prístupu a autentizácie užívateľov v počítačových sieťach. Autentizácia predstavuje jeden z najdôležitejších aspektov nevyhnutných ku dosiahnutiu maximálnej úrovne zabezpečenia.

Kombinácia **autentizačnej metódy EAP (*Extensible Authentication Protocol*) a systému RADIUS (*Remote Authentication Dial-In User Service*)** sa využíva najmä v podnikových Wi-Fi sieťach a VPN pre centralizovanú správu overovania identity overovania používateľov a následného riadenia ich prístupu k zdieľaným sieťovým prostriedkom.

## 1.1. IEEE 802.1X

IEEE 802.1X je sieťový štandard definovaný organizáciou IEEE<sup>1</sup> slúžiaci pre kontrolu prístupu do lokálnych sietí. Je základom pre kontrolu prístupu realizovanej na úrovni fyzických portov (tzv. *port-based network access control* – PNAC), čo v praxi znamená, že zariadenie (resp. klient) nemôže získať plnohodnotný prístup k sieťovým službám, pokiaľ úspešne neprebehne proces jeho autentizácie. Tento proces prebieha na základe spolupráce troch hlavných súčastí:

- **klient** (*supplicant*) – resp. koncové zariadenie (čo môže byť napr. notebook alebo virtuálny stroj), ktoré sa pokúša pripojiť do siete a predkladá svoju identitu;
- **overovateľ** (*authenticator*) – spravidla prístupový bod<sup>2</sup> do bezdrôtovej siete alebo prepínač (switch), ktorý reguluje prístup koncových klientov do siete a sprostredkúva výmenu autentizačných informácií medzi daným klientom a autentizačným serverom;
- **autentizačný server** – overovací server (typicky RADIUS), ktorý na základe stanovených konfiguračných pravidiel a uložených prístupových údajov v procese autentizácie rozhodne, či bude klientovi povolený alebo zamietnutý prístup do siete.



Obrázok 1.1 Základné komponenty 802.1X a ich vzájomné prepojenie<sup>3</sup>.

<sup>1</sup> IEEE (*Institute of Electrical and Electronics Engineers*) je medzinárodná organizácia zameraná na vývoj technických štandardov v oblasti elektrotechniky, elektroniky, výpočtovej techniky a telekomunikácií. Organizácia IEEE je zodpovedná za tvorbu mnohých známych sieťových štandardov, medzi ktoré patria, okrem vyššie uvedeného IEEE 802.1X pre autentizáciu, tiež napr. IEEE 802.3 pre špecifikáciu technológie Ethernet alebo IEEE 802.11 zameraný na bezdrôtové technológie Wi-Fi.

<sup>2</sup> Pre označenie prístupového bodu bezdrôtovej siete je zaužívané použitie skratky „AP“ (z angl. termínu slova *Access Point*).

<sup>3</sup> Prevzaté z [1].

Štandard IEEE 802.1X sa často využíva v kombinácii s protokolom EAP (*Extensible Authentication Protocol*) a v podnikových sieťach predstavuje bežný spôsob riadenia bezpečného prístupu. Podrobné znenie štandardu IEEE 802.1X možno nájsť na oficiálnych stránkach [2], bližšie vysvetlenie problematiky a priebeh procesu autentizácie je vysvetlený napr. v literatúre [3], [4], [5].

## 1.2. Extensible Authentication Protocol (EAP)

**EAP predstavuje flexibilný autentizačný *framework*** navrhnutý za účelom podpory rôznych metód autentizácie pre prístupujúcich užívateľov. Nejedná sa o konkrétne autentizačný mechanizmus, resp. protokol, ale o rámec, ktorý implementuje **niekoľko rôznych autentizačných metód**. Jednotlivé autentizačné metódy sú založené na princípe výmeny správ medzi klientom (napr. používateľským zariadením) a autentizačným serverom (napr. RADIUS serverom). Je široko využívaný v bezdrôtových sieťach a tiež zabezpečených VPN pripojeniach.

EAP definuje rôzne metódy autentizácie, pričom medzi najznámejšie patria:

- **EAP-MD5:** jednoduchá autentizačná metóda založená na princípe výzva-odpoveď, kedy klient žiadajúci o overenie identity obdrží od autentizačného servera náhodne generovanú výzvu (*challenge*), na ktorú odosiela odpoveď (*response*) obsahujúcu hash určený z overovacieho faktoru klienta, typicky hesla, a náhodnej výzvy, ktorú získal od servera. Túto metódu však nemožno považovať za dostatočne bezpečnú, nakoľko sú obe správy (výzva aj odpoveď) prenášané nešifrovane v otvorenej podobe.
- **EAP-TLS:** metóda využíva certifikáty pre autentizáciu klienta a servera. Jedná sa o najbezpečnejšiu alternatívu spomedzi známych a využívaných metód, avšak prináša nutnosť zaistenia mechanizmov pre vydávanie a následnú správu kryptografických certifikátov.
- **EAP-TTLS:** rozširuje metódu EAP-TLS o podporu kombinácie certifikátov a použitia tradičných prihlasovacích (autentizačných) údajov, napr. v podobe prístupového mena a hesla. Certifikát sa používa len pre overenie identity servera, čo zjednodušuje implementáciu autentizačnej metódy.
- **PEAP** (*Protected EAP*): metóda obsahuje mechanizmy pre tunelovanie autentizačných údajov cez šifrované spojenie pomocou TLS. Používateľské meno a heslo sú prenášané vnútri vytvoreného bezpečného tunela, čo zvyšuje mieru zaistenia dôvernosti autentizačných údajov žiadateľa o overenie identity.

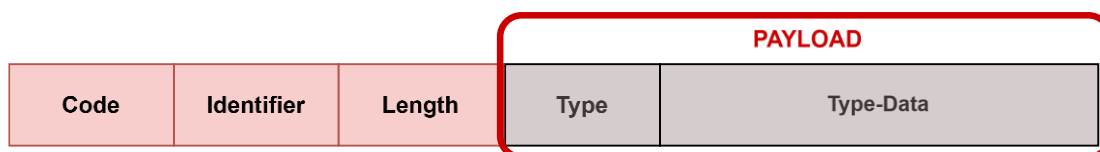
Protokol EAP definuje základný rámec pre autentizačný proces. Každá autentizačná metóda využíva rovnaké typy základných EAP správ, ktoré si medzi sebou vymieňajú klient a autentizačný server (sprostredkované cez AP, resp. prepínač). Rozlišujeme štyri základné typy EAP správ, ich prehľad je uvedený v tab. 1.1.

Tabuľka 1.1 Prehľad typov EAP správ.

Typ správy	Kód	Odosielateľ	Popis
<b>EAP-Request</b> (požiadavka)	1	Server	Výzva klientovi pre zadanie požadovaných údajov (napr. identita, heslo, certifikát)
<b>EAP-Response</b> (odpoveď)	2	Klient	Odpoveď klienta na výzvu servera – obsahuje požadované údaje.
<b>EAP-Success</b>	3	Server	Potvrdenie úspešnej autentizácie – klient má povolený prístup do siete.
<b>EAP-Failure</b>	4	Server	Oznámenie o neúspešnej autentizácii – prístup klienta je zamietnutý.

Každá EAP správa má nasledovný základný formát (viď obr. 1.2 nižšie):

- **Code** – označuje typ správy (1=Request, 2=Response, 3=Success, 4=Failure);
- **Identifier** – slúži pre spárovanie výzvy a odpovede;
- **Length** – dĺžka EAP správy v B;
- **Payload** – pole využívané v procese autentizácie, je obsiahnuté len v správach EAP-Request a EAP-Response a ďalej sa delí na:
  - **Type**<sup>4</sup> – určuje, čo bude obsahom nasledujúcich dát (Type-Data) – napríklad, či ide o výmenu identity klienta, výzvu na zadanie hesla, odoslanie certifikátu apod. Pole definuje konkrétnu EAP metódu alebo príslušný krok, resp. fázu autentizačného procesu.
  - **Type-Data** – obsahuje vlastné dáta podľa konkrétneho typu správy (napr. reťazec s identitou klienta, náhodná výzva, hash hesla, certifikát atď.)



Obrázok 1.2 Schematické znázornenie štruktúry správy protokolu EAP<sup>5</sup>.

<sup>4</sup> Príklady hodnôt podľa Type sú napr.: **1 = Identity**: požiadavka/odpoveď s identitou (napr. používateľské meno); **2 = Notification**: správa slúži pre informovanie klienta, resp. žiadateľa; **3 = NAK**: odmietnutie typu autentizácie zo strany klienta; **4 = MD5-Challenge**: správa slúži pre odoslanie výzvy a odpovede počas autentizácie MD5.

Uvedený zoznam možných hodnôt nie je konečný, uvedený je len prehľad základných typov, s ktorými ste mali možnosť oboznámiť sa aj na prednáškach predmetu MPC-NSB.

<sup>5</sup> Prevzaté z oficiálnych výučbových materiálov k prednáškam predmetu MPC-NSB – vypracoval garant predmetu a prednášajúcim doc. Karel Burda, CSs. (viď tiež E-learning predmetu).

V procese autentizácie si medzi sebou klient (resp. žiadateľ) a autentizačný server vymieňajú EAP správy sprostredkované cez AP. Typicky **server odosiela požiadavky** (*Request*), na ktoré **klient reaguje svojou odpoveďou** (*Response*). V závislosti na konkrétnom type použitej autentizačnej metódy sa potom líši obsah dátovej časti prenášanej v príslušnej EAP správe. Ako príklad možno uviesť rôzne typy správ, ktoré sú odosielané v procese autentizácie MD5<sup>6</sup>:

- **EAP-Request/Identity:**  
Server žiada klienta o jeho meno (identitu). V poli Type sa uvádza **1 (Identity)**, nasleduje reťazec „Who are you?“.
- **EAP-Response/Identity:**  
Klient ako odpoveď odosiela svoju identitu, zvyčajne vo forme používateľského mena. V poli Type sa opäť uvádza **1 (Identity)**, nasleduje reťazec s identitou.
- **EAP-Request/MD5-Challenge:**  
Server posíla výzvu (*challenge*) pre zadanie autentizačných údajov.
- **EAP-Response/MD5-Challenge:**  
Klient reaguje na výzvu servera a odpovedá správou, ktorá obsahuje údaje pre overenie identity. V prípade autentizácie MD5 sa jedná o *hash* reťazca zloženého z ID žiadateľa, hesla a výzvy, ktorú prijal.

### Autentizácia EAP-MD5

EAP-MD5 je jednoduchá autentizačná metóda používaná pre overovanie identity užívateľov v počítačových sieťach. Funguje tak, že server (autentizátor) pošle klientovi výzvu (*challenge*), a klient na základe svojho mena, hesla a prijatej výzvy vypočíta odpoveď (*response*), ktorú odosiela späť. Server následne porovná klientovu odpoveď s očakávaným výsledkom a na základe toho povolí alebo naopak zamietne prístup klienta do siete.

Výhodou metódy je jej rýchlosť a jednoduchosť, ale medzi hlavné nevýhody patrí absencia mechanizmov pre šifrovanie a akúkoľvek formu ochrany samotných údajov – heslo klienta je totiž prakticky možné získať pomocou útoku hrubou silou<sup>7</sup>. EAP-MD5 nepodporuje overenie servera, a preto sa považuje za nevhodnú pre verejné siete, ale výborne sa hodí na výučbové účely pre vysvetlenie základných princípov a jednotlivých krokov autentizačného procesu.

Priebeh autentizácie EAP-MD5 zahŕňa celkom päť základných krokov, ktorých rozbor prináša nasledujúca tabuľka č. 1.2 (schematické znázornenie priebehu komunikácie vid' na obr. 1.3).

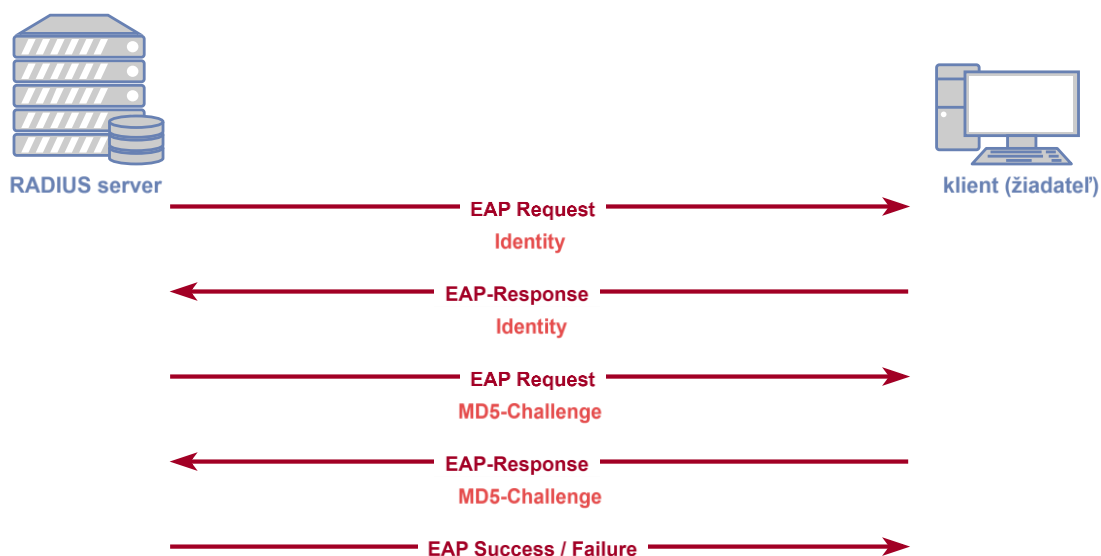
---

<sup>6</sup> Popis autentizácie MD5 bude nasledovať.

<sup>7</sup> Pokiaľ útočník zachytí správu s identitou klienta (ID), výzvu servera a následne odpoveď od klienta obsahujúcu *hash* reťazca (ID || heslo || výzva), mohol by sa teoreticky pokúsiť postupným skúšaním rôznych možných vstupov (resp. hesiel) nájsť výstupný *hash* zhodný s tým od klienta. V prípade úspechu by bolo zrejmé, že našiel odpovedajúce heslo.

Tabuľka 1.2 Správy odosielané v procese autentizácie EAP-MD5.

<b>Krok</b>	<b>Odosielateľ → Prijímateľ</b>	<b>Typ správy</b>	<b>Obsah</b>
1	Autentizátor → Klient	<b>EAP-Request</b> <b>Identity</b>	Výzva na zaslanie identity (napr. „Kto si?“)
2	Klient → Autentizátor	<b>EAP-Response</b> <b>Identity</b>	Klient odošle svoju identitu (napr. „peter“)
3	Autentizátor → Klient	<b>EAP-Request</b> <b>MD5-Challenge</b>	Výzva obsahujúca náhodný reťazec ( <i>challenge</i> ) a ID
4	Klient → Autentizátor	<b>EAP-Response</b> <b>MD5-Challenge</b>	Klient vygeneruje MD5 hash: MD5(ID + heslo + <i>challenge</i> )
5	Autentizátor → Klient	EAP-Success / EAP-Failure	Server porovná vypočítaný hash a pošle odpoveď o výsledku autentizácie (úspech/neúspech)



Obrázok 1.3 Schematické znázornenie výmeny správ medzi klientom a autentizačným serverom pri EAP-MD5 autentizácii<sup>8</sup>.

<sup>8</sup> Prevzaté z oficiálnych výučbových materiálov k prednáškam predmetu MPC-NSB – vypracoval garant predmetu a prednášajúcim doc. Karel Burda, CSs. (viď tiež E-learning predmetu).

## EAPoL (EAP over LAN)

Pri komunikácii prebiehajúcej v sieťach IEEE 802.1X sa EAP správy medzi klientom (*supplicant*) a prístupovým bodom (*authenticator*) prenášajú vo formáte EAP over LAN na spojovej vrstve – tzv. **EAPoL správy**. EAPoL predstavuje rozšírenie protokolu EAP, navrhnuté špecificky pre použitie v sieťach založených na prenosových technológiách Ethernet a Wi-Fi, kde sa autentizačné údaje prenášajú priamo na spojovej vrstve, t. j. na druhej vrstve RM ISO/OSI. EAPoL slúži len na komunikáciu klienta s AP a jeho úlohou je prenášať EAP správy zapuzdrené do ethernetového rámca na spojovej vrstve. Štandard EAPoL definuje päť základných typov správ (viď tab. 1.3).

Tabuľka 1.3 Prehľad typov EAPoL správ.

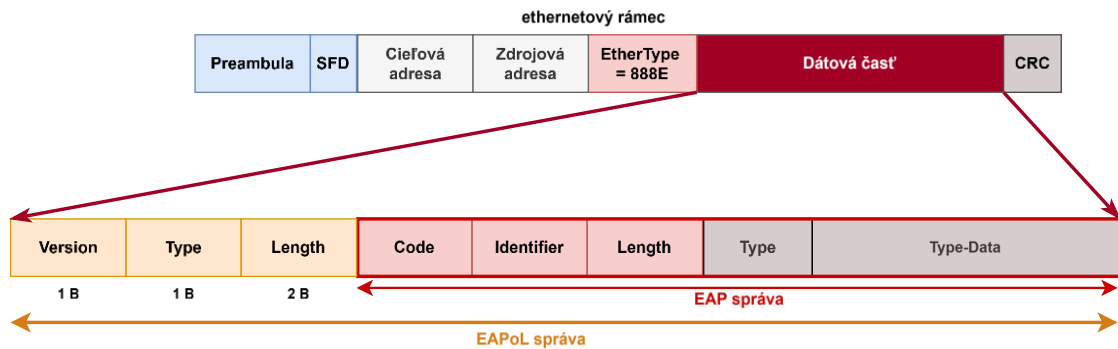
Typ	Názov správy	Účel
0x00	EAP-Packet	Obsahuje samotnú EAP správu
0x01	EAPoL-Start	Iniciuje autentizačný proces
0x02	EAPoL-Logoff	Označuje, že klient sa odhlasuje zo siete, slúži k ukončeniu spojenia
0x03	EAPoL-Key	Používa sa na výmenu šifrovacích kľúčov (napr. v protokole WPA/WPA2)
0x04	EAPoL-Encapsulated-ASF-Alert	Menej bežná, málo používaný typ správy určený pre špecifické bezpečnostné výstrahy

Proces zapuzdrenia EAPoL správy do ethernetového rámca na úrovni spojovej vrstvy je graficky znázornený na obr. 1.4, pohľad na štruktúru samotnej EAPoL správy taktiež. Popis a význam jednotlivých polí nasleduje:

- **Version** – verzia protokolu EAPoL (napr. 0x01 pre IEEE 802.1X);
- **Type** – typ EAPoL správy (napr. 0x00 pre EAP-Packet);
- **Length** – dĺžka dátovej časti správy v B;
- **Body** – samotný obsah, resp. správa EAP protokolu (napr. EAP výzva (*Request*), odpoveď (*Response*), apod.) – pole je prítomné len u správy typu **EAP-Packet**.

Prístupový bod (AP) následne zapuzdruje tieto EAP správy do správ protokolu RADIUS na aplikačnej vrstve a preposiela ich ďalej na autentizačný server (podrobnejší popis bude nasledovať).





Obrázok 1.4 Schematické znázornenie zapuzdrenia EAPoL správy do rámca technológie Ethernet<sup>9</sup>.

Výhodou EAP je jeho modularita a tak isto aj schopnosť prispôbiť sa rôznym scenárom z reálneho sveta. Metódy *frameworku* EAP predstavujú základné piliere zabezpečenia najmä v dnešných Wi-Fi sieťach s WPA-Enterprise, nakoľko umožňujú výber spomedzi širokého spektra rozličných autentizačných metód podľa konkrétnych požiadaviek.

Podrobný popis architektúry, typov a formátov odosielaných správ a používaných autentizačných metód je možné nájsť v oficiálnom štandarde definujúcom EAP, dokumente RFC: *Extensible Authentication Protocol* (EAP), viď [6]. Viac o jednotlivých autentizačných metódach dostupných v rámci *frameworku* EAP, vrátane detailnej analýzy výhod a naopak obmedzení a nedostatkov jednotlivých prístupov sa možno dočítať v literatúre [7].

### 1.3. RADIUS (*Remote Authentication Dial-In User Service*)

RADIUS predstavuje aplikačný protokol založený na architektúre *klient-server*, ktorý poskytuje **služby AAA** (*Authentication, Authorization, Accounting*), teda autentizáciu, autorizáciu a účtovanie. Bol vyvinutý ako mechanizmus centralizovanej autentizácie užívateľov. V kontexte IEEE 802.1X je kľúčovým prvkom autentizačný server RADIUS, kedy v lokálnych sieťach zastupuje jeho úlohu prístupový bod, ktorý vystupuje ako klient protokolu RADIUS a všetky správy prijaté od klient preposiela na autentizačný server.

Medzi hlavné súčasti architektúry RADIUS patrí:

- **klient RADIUS:** zariadenie, ktoré pre prístupujúceho užívateľa sprostredkúva proces autentizácie (napr. Wi-Fi prístupový bod alebo VPN server). Toto zariadenie prijíma požiadavky na pripojenie od používateľov a odosiela ich na autentizačnému RADIUS serveru;

<sup>9</sup> Prevzaté z oficiálnych výučbových materiálov k prednáškam predmetu MPC-NSB – vypracoval garant predmetu a prednášajúcim doc. Karel Burda, CSs. (viď tiež E-learning predmetu). Pozn.: podrobný popis položiek záhlavia Ethernetu nie je uvádzaný, nakoľko sa predpokladá na strane študentov znalosť problematiky (viď E-learning predmetu MPC-NSB, Téma 3).

- **RADIUS server:** spracováva autentizačné požiadavky, overuje zadané autentizačné údaje a na základe výsledku procesu overovania identity tiež rozhoduje o pridelení, resp. zamietnutí prístupu;
- **databáza užívateľov:** jedná sa o úložisko obsahujúce prihlasovacie (autentizačné) údaje užívateľov, prípadne i ďalšie informácie a oprávnenia potrebné pre účely následného riadenia prístupu k zdieľaným prostriedkom. Databázou môže byť napr. súbor, LDAP server alebo iný adresárový systém.

Protokol RADIUS využíva na transportnej vrstve jednoduchý bezstavový protokol UDP a typicky komunikuje na portoch 1812 (pre autentizáciu) a 1813 (účtovanie). Po úspešnej autentizácii môže byť prístupujúcemu užívateľovi povolený prístup do siete alebo k požadovaným prostriedkom.

### Autentizačný server RADIUS v procese autentizácie

V procese autentizácie EAP-MD5 vystupujú tri kľúčové komponenty – klient (žiadateľ), prístupový bod (AP) a autentizačný server RADIUS (viď obr. 1.5). Prístupový bod vystupuje v úlohe sprostredkovateľa, ktorý iba prenáša autentizačné správy medzi klientom a serverom, pričom, komunikácia medzi klientom a AP prebieha vo forme EAP správ zapuzdrených v protokole EAPoL (EAP over LAN), ktorý sa prenáša cez Ethernet.



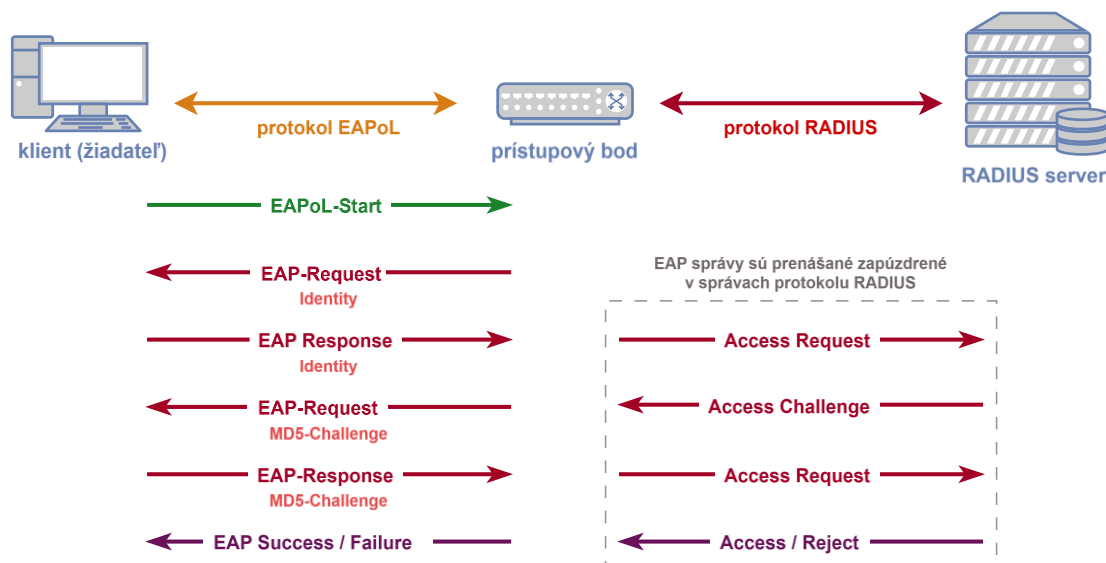
Obrázok 1.5 Komponenty siete s autentizáciou EAP-MD5 a ich vzájomná komunikácia.

Autentizačný server je zodpovedný za samotné overenie identity klienta. Keď AP získa identitu klienta vo forme správy **EAP-Response/Identity**, zapuzdruje túto správu do správy protokolu RADIUS typu **Access-Request** a odosiela ju na server. Server odpovedá výzvou typu **Access-Challenge**, ktorá obsahuje náhodný reťazec, (výzvu, *challenge*), a ten je následne odoslaný klientovi cez AP vo forme **EAP-Request/MD5-Challenge**.

Klient z výzvy, ID výmeny a svojho hesla vypočíta *hash* a ten odosiela ako reakciu (odpoveď, *response*) späť ako **EAP-Response/MD5-Challenge**. Túto odpoveď AP opäť zabalí do správy **Access-Request** a preposiela na RADIUS server. Server overí správnosť výpočtu (porovná ho s vlastnou vypočítanou hodnotou *hash*) a na základe toho rozhodne o úspešnosti autentizácie. V prípade úspechu odošle správu **Access-Accept**,

inak **Access-Reject**. AP následne doručí klientovi výslednú správu **EAP-Success**, resp. **EAP-Failure**.

Takto navrhnutý mechanizmus zabezpečuje, že heslo klienta nie je nikdy prenášané v otvorenej podobe. AP pritom nepozná žiadne autentizačné údaje – jeho úlohou je len zapuzdrenie EAP správ do RADIUS formátu a späť. Protokol RADIUS sa tak používa výlučne medzi AP a autentizačným serverom, zatiaľ čo EAPoL slúži na prenos správ medzi klientom a AP. Podrobne je možné celý priebeh komunikácie vidieť na obr. 1.6.



Obrázok 1.6 Schematické znázornenie autentizácie EAP-MD5 podľa štandardu IEEE 802.1X<sup>10</sup>.

Pre viac informácií a podrobnejšie vysvetlenie a popis vyššie uvedených protokolov a metód autentizácie je možné nahliadnuť do literatúry [8], [9], [10].

## 1.4. Použité nástroje

### Wireshark

Wireshark je sieťový analyzátor, ktorý umožňuje sledovať dátové prenosy. Použitie tohto nástroja ste si prakticky vyskúšali už v rámci niekoľkých predošlých laboratórnych úloh, takže jeho bližší popis nebude už ďalej podrobne uvádzaný.

<sup>10</sup> Prevzaté z oficiálnych výučbových materiálov k prednáškam predmetu MPC-NSB – vypracoval garant predmetu a prednášajúcim doc. Karel Burda, CSs. (viď tiež E-learning predmetu).

## FreeRADIUS

**FreeRADIUS** predstavuje *open-source* možnosť implementácie RADIUS protokolu pre autentizáciu, autorizáciu a účtovanie prístupov v sieťach. Umožňuje implementáciu RADIUS serverov a používa sa v podnikových aj verejných sieťach pre potreby centralizovaného overovania užívateľov. FreeRADIUS podporuje širokú škálu autentizačných protokolov, vrátane EAP-MD5, PEAP, EAP-TTLS, a mnohých ďalších, vďaka čomu je vhodným riešením pre použitie v rôznorodých sieťových prostrediach.

Okrem samotnej autentizácie disponuje FreeRADIUS aj možnosťou monitorovania aktivít užívateľov v sieti a vytvárania záznamov o ich prístupoch k prostriedkom. FreeRADIUS je modulárny a flexibilný, čo umožňuje jeho integráciu s databázami, LDAP servermi a inými externými autentizačnými systémami.

### Inštalácia a konfigurácia RADIUS servera

V rámci praktickej časti budete realizovať vlastnú implementáciu RADIUS servera. Pre tento účel bude využitý nástroj FreeRADIUS<sup>11</sup> dostupný v Kali Linux.

Inštalácia FreeRADIUS na Kali Linux:

```
sudo apt-get install freeradius
```

Konfigurácia autentizačnej politiky v súbore `/etc/freeradius/3.0/users` pre pridanie nového užívateľa:

```
testuser Cleartext-Password := "heslo123"
```

Spustenie vytvoreného RADIUS servera:

```
sudo systemctl start freeradius
```

## Hostapd

**Hostapd** predstavuje softvérové riešenie umožňujúce bežným klientskym zariadeniam (napr. virtuálnemu stroju s Kali Linux) emulovať funkcionality plnohodnotného prístupového bodu (*authenticator*) v zmysle štandardu IEEE 802.1X. Je navrhnutý najmä pre bezdrôtové siete, ale v laboratórnych podmienkach môže byť využitý taktiež aj v simulovanom ethernetovom prostredí. Umožňuje implementáciu autentizačných mechanizmov, správu SSID<sup>12</sup>, zabezpečenie siete a komunikáciu s RADIUS serverom. V rámci laboratórnej úlohy bude nástroj `hostapd` použitý za účelom vytvorenia jednoduchého autentizačného bodu siete, ktorý sprostredkúva výmenu údajov medzi klientom a RADIUS serverom prostredníctvom EAP.

---

<sup>11</sup> Viac informácií o FreeRADIUS je dostupných na oficiálnych stránkach projektu, viď [11].

<sup>12</sup> SSID (*Service Set Identifier*) predstavuje názov bezdrôtovej siete, ktorý sa zobrazuje používateľom pri pripojení ku konkrétnej Wi-Fi.

Základné parametre ako názov siete (SSID), rozhranie sieťovej karty, povolenie mechanizmu autentizácie IEEE 802.1X a údaje o RADIUS serveri sú súčasťou konfiguračného súboru **hostapd.conf**. Príklad konfigurácie:

```
interface=eth0
driver=wired
ssid=EduLab
ieee8021x=1
auth_server_addr=192.168.126.130
auth_server_port=1812
auth_server_shared_secret=heslo1245
```

Vysvetlenie jednotlivých nastavení, ktoré sú obsahom uvedenej konfigurácie:

- **interface=eth0** – určuje sieťové rozhranie, na ktorom bude hostapd počúvať a sprostredkovať autentizačné procesy;
- **driver=wired** – špecifikuje priebeh 802.1X autentizácie cez ethernetové pripojenie;
- **ssid=EduLab** – nastavuje názov siete (SSID), ktorý bude vysielaný AP;
- **ieee8021x=1** – aktivuje podporu autentizačného protokolu IEEE 802.1X;
- **auth\_server\_addr=192.168.126.130** – IP adresa RADIUS servera.
- **auth\_server\_port=1812** – štandardný port pre autentizačné požiadavky použitý na strane RADIUS servera;
- **auth\_server\_shared\_secret=heslo1245** – zdieľané heslo (tajný kľúč) na zabezpečenie komunikácie medzi AP a RADIUS serverom.

Po definícii konfiguračných parametrov a uložení príslušného konfiguračného súboru nasleduje spustenie hostapd pomocou príkazu:

```
sudo hostapd hostapd.conf
```

Uvedený príkaz zabezpečí načítanie konfiguračného súboru a spustenie služby **hostapd** s požadovanými nastaveniami. Je nevyhnutné spustiť ho s oprávneniami administrátora (sudo), pretože práca so službou **hostapd** zahŕňa manipuláciu so sieťovými rozhraniami, ich nastavením a konfiguráciu autentizačných procesov, ktoré vyžadujú vyššie systémové oprávnenia. **Pozn.: správna konfigurácia a spustenie tohto nástroja je nevyhnutná pre úspešné sprostredkovanie autentizácie medzi klientom a RADIUS serverom.**

## Wpa\_supplicant

Jedná sa o softvérový nástroj, ktorý **umožňuje zariadeniu (klientovi) bezpečne sa pripojiť k bezdrôtovej sieti vyžadujúcej autentizáciu pomocou protokolu IEEE 802.1X**. Vytvorená inštancia nástroja wpa\_supplicant funguje ako klientská

aplikácia, ktorá obsluhuje a riadi procese autentizácie klienta a sprostredkúva výmenu autentizačných EAP správ medzi klientskym zariadením a prístupovým bodom<sup>13</sup>. Tento nástroj slúži teda k zaisteniu bezpečnej komunikácie klienta s prístupovým bodom (AP) pomocou protokolov 802.1X a EAP, pričom podporuje rôzne typy EAP autentizačných metód (napr. EAP-MD5, EAP-TLS, EAP-TTLS, PEAP a ďalšie).

---

<sup>13</sup> AP zastávajúci funkciu *authenticator* v procese autentizácie IEEE 802.1X.

## 2. Praktická časť

V rámci praktickej časti úlohy získate komplexný prehľad o možnostiach implementácie autentizačných protokolov EAP a RADIUS a tiež vlastné praktické skúsenosti s nastavením a správnou konfiguráciou vhodných metód autentizácie a pokročilého riadenia prístupu k zdrojom v počítačovej sieti.

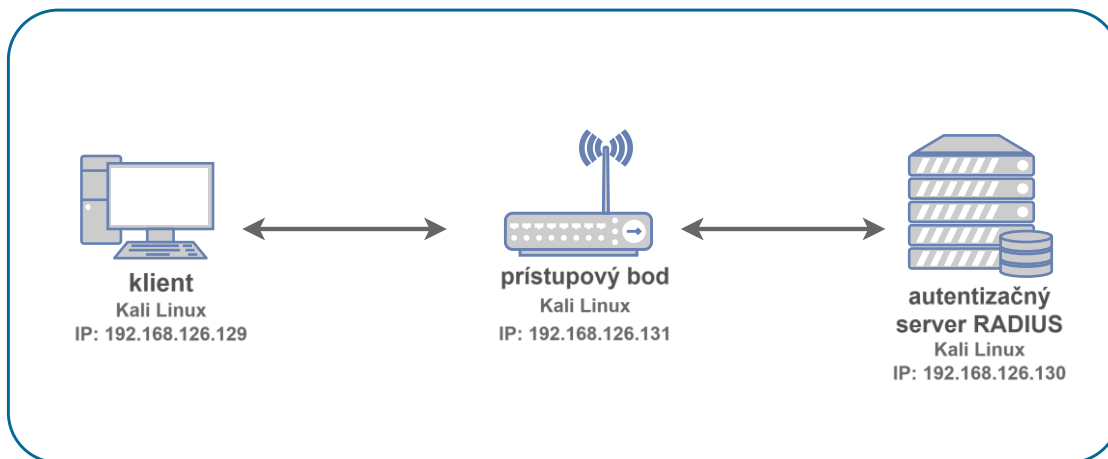
### 2.1. Topológia virtuálnej siete a nastavenie virtuálnych strojov

Vytvorená sieť bude pozostávať z troch virtuálnych strojov:

- **klient:** simulované koncové zariadenie, ktoré sa pripája do siete cez 802.1X
- **Access Point** (*authenticator*) = **prístupový bod:** zariadenie využívajúce `hostapd`, sprostredkovateľ autentizácie, resp. komunikácie klienta s autentizačným RADIUS serverom
- **RADIUS server:** zariadenie s implementovanou inštanciou autentizačného servera pomocou nástroja `freeradius`.

Sieťová konfigurácia:

- klient: 192.168.126.129
- prístupový bod: 192.168.126.131
- RADIUS server: 192.168.126.130



Obrázok 2.1 Topológia siete laboratórnej úlohy.

Všetky virtuálne stroje musia byť prepojené v rovnakej virtuálnej podsieti, doporučené použiť sieťový režim: "**Host-Only**".



### Poznámka k vytvorenej topológii:

Pre emuláciu prístupového bodu (AP) použite virtuálny stroj, ktorý bol v predchádzajúcich laboratórnych úlohách použitý ako zariadenie „útočníka“. Príslušný VM je pripravený pre použitie nástroja `hostapd`, aby mohol funkčne zastúpiť prístupový bod simulovanej siete.

## 2.2. Zoznámenie sa s použitými nástrojmi

Prehľad základných príkazov pre jednotlivé používané nástroje

- **FreeRADIUS**

- inštalácia:

```
sudo apt install freeradius
```

- spustenie:

```
sudo systemctl start freeradius
```

- overenie stavu:

```
sudo systemctl status freeradius
```

- záznamy o udalostiach (logy) sú dostupné v súbore:

```
/var/log/freeradius/radius.log
```

- **Hostapd**

- inštalácia:

```
sudo apt install hostapd
```

- konfiguračný súbor obsahujúci nastavenie SSID, parametrov siete a parametrov súvisiacich s procesom autentizácie:

```
/etc/hostapd/hostapd.conf
```

- **Wpa\_supplicant**

- nastavenie služby `wpa_supplicant` sa uskutočňuje úpravou konfiguračného súboru:

```
/etc/wpa_supplicant/wpa_supplicant.conf
```

- príklad spustenia procesu autentizácie:

```
sudo wpa_supplicant -i eth0 -c  
/etc/wpa_supplicant/wpa_supplicant.conf -D wired
```



## 2.3. Postup pre vypracovanie laboratórnej úlohy

### A) Príprava prostredia

#### Spustenie virtuálnych strojov:


- Otvorte VMware Workstation Pro (umiestnený na ploche).
- Spustite postupne všetky tri virtuálne stroje (klient, AP, RADIUS server).
- Skontrolujte, že všetky VMs sú pripojené do rovnakej virtuálnej siete (napr. NAT alebo Host-Only). Uistite sa tiež v správnosti konfigurácie sieťových parametrov, overte priradenie IP adries.
- Prihláste sa do prostredia Kali Linux postupne na všetky VMs.

VM „klient“ – prihlasovacie údaje: **Username:** klient, **Password:** kali

VM „AP“ – prihlasovacie údaje: **Username:** kali, **Password:** kali

VM „RADIUS“ – prihlasovacie údaje: **Username:** server, **Password:** kali

#### Overenie sieťovej konektivity:

- Otvorte **terminál** (kliknite na ikonu terminálu  v záhlaví horného pracovného panelu alebo stlačte **Ctrl + Alt + T**).
- Na jednotlivých VMs si zobrazte priradené IP adresy (na rozhraní **eth0**) pomocou príkazu:

```
ip a
```

- Skontrolujte sieťovú konektivitu medzi všetkými strojmi pomocou **ping** z klienta na AP a server, a tiež v oboch smeroch medzi AP a RADIUS serverom.


```
ping <ip_adresa_zariadenia>
```

Ak prichádza odpoveď **ping echo reply** zo strany servera, sieťová komunikácia medzi zariadeniami funguje.

### B) Konfigurácia prístupového bodu

Aby mohol prístupový bod vytvorenej siete vystupovať v procese autentizácie klienta ako *authenticator* a sprostredkovať tak komunikáciu medzi klientom a autentizačným RADIUS serverom, je potrebné príslušný VM vhodne nakonfigurovať, pre tento účel bude použitý nástroj **hostapd**, pomocou ktorého je možné na „bežnom zariadení“ emulovať funkcionality plnohodnotného prístupového bodu.

## Použitie nástroja hostapd

- Na VM, ktorý bude plniť úlohu prístupového bodu, otvorte terminál kliknutím na ikonu  umiestnenú v záhlaví hlavného pracovného okna alebo v menu zvolíte **Applications > System Tools > Terminal**. Otvorí sa okno s príkazovým riadkom.
- Nainštalujte hostapd pomocou príkazu:

```
sudo apt install hostapd bridge-utils -y
```

- Aby mohol VM obstarávať funkcie AP v autentizačnom procese, je nutné uskutočniť patričné zmeny v konfigurácii, konkrétne v konfiguračnom súbore **/etc/hostapd/hostapd.conf**. Vytvorte alebo upravte súbor:

```
sudo nano /etc/hostapd/hostapd.conf
```

- Do súboru vložte nasledovnú konfiguráciu:

```
interface=eth0
driver=wired
ssid=EduLab
ieee8021x=1
auth_server_addr=192.168.126.130
auth_server_port=1812
auth_server_shared_secret=radiusheslo
```

- Po úprave konfigurácie stlačte kombináciu kláves **Ctrl + O** (uloženie), potvrdíte názov súboru klávesou **Enter** a následne ukončíte textový editor **nano** pomocou kombinácie **Ctrl + X**.
- Alternatívne môžete úpravu konfigurácie ukončiť stlačením **Ctrl + X**, následne pre potvrdenie uloženia vykonaných zmien stlačte **Y** (ako Yes/áno), a nakoniec potvrdíte stlačením **Enter**. Týmto spôsobom sa zmeny uložia a editor sa zároveň zatvorí.
- Následne spustíte službu hostapd pomocou príkazu:

```
sudo hostapd /etc/hostapd/hostapd.conf
```

V prípade úspešného spustenia služby sa v používanom terminálovom okne zobrazí stav **AP-ENABLED**.

### C) Konfigurácia RADIUS servera

Implementácia a následná konfigurácia vlastného autentizačného RADIUS servera na jednom z používaných VMs bude realizovaná pomocou nástroja FreeRADIUS.

#### Inštalácia nástroja FreeRADIUS

- Na serveri spustíte terminál.
- Po zobrazení okna s príkazovým riadkom najskôr skontrolujte, či je FreeRADIUS na VM nainštalovaný, príp. ho doinštalujte pomocou príkazu:

```
sudo apt update  
sudo apt install freeradius
```

#### Konfigurácia užívateľa

- Po inštalácii je potrebné na autentizačnom RADIUS serveri vytvoriť záznam o autentizačných údajoch klienta (žiadateľa):
  - Pre potreby editovania konfiguračných súborov nástroja FreeRADIUS bude potrebné **použiť privilegovaný režim**. Zadať príkaz:

```
sudo -i
```

ako heslo (*password*) zadajte: **kali**

- Otvorte súbor:

```
sudo nano /etc/freeradius/3.0/users
```

- a do súboru vložte nasledujúci záznam:

```
student Cleartext-Password := "tajneheslo"
```

#### Konfigurácia prístupového bodu (AP)

- V ďalšom kroku je potrebné definovať tiež parametre spojenia medzi RADIUS serverom a prístupovým bodom.
  - Otvorte súbor:

```
sudo nano /etc/freeradius/3.0/clients.conf
```

- a do súboru vložte nasledujúci záznam:

```
client ap {  
    ipaddr = 192.168.126.131  
    secret = radiusheslo  
}
```

## Spustenie služby

- Následne server reštartujte a spustite službu:

```
sudo systemctl start freeradius
```

- Po spustení služby FreeRADIUS sledujte logy (záznamy udalostí) na overenie správnosti použitých nastavení – potrebné logy sa automaticky zobrazia v termináli po zadaní príkazu:

```
sudo journalctl -u freeradius -f
```

Logy obsahujú dôležité informácie o priebehu autentizačného procesu, ako sú úspešné alebo neúspešné autentizačné pokusy, chyby v konfigurácii, odmietnuté žiadosti o prístup alebo problémy so sieťovou komunikáciou. Ak sa v logoch objavia chybové hlásenia (napr. neplatné prihlasovacie údaje, nesprávny kľúč, resp. *shared secret* medzi AP a RADIUS serverom apod.), je potrebné všetky zaznamenané chyby analyzovať a opraviť.

- Príklad ukážkového výstupu logu FreeRADIUS:

```
(0) Received Access-Request Id 45 from 192.168.126.128:54321 to 192.168.126.130:1812 length 150
(0) User-Name = "student"
(0) NAS-IP-Address = 192.168.126.128
(0) Called-Station-Id = "00-11-22-33-44-55:EduLab"
(0) Calling-Station-Id = "66-77-88-99-AA-BB"
(0) EAP-Message = 0x0200000d0173747564656e74
(0) Message-Authenticator = 0x1234567890abcdef1234567890abcdef
(0) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(0) authorize {
(0)     ok
(0) } # authorize = ok
(0) Found Auth-Type EAP
(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(0) authenticate {
(0)     eap: Peer sent EAP Response (code 2) ID 0 length 13
(0)     eap: No EAP Start, assuming it's an on-going EAP conversation
(0) } # authenticate = ok
(0) Sent Access-Accept Id 45 from 192.168.126.130:1812 to 192.168.126.128:54321 length 80
```

## D) Konfigurácia klienta

Pre zaistenie bezpečného pripojenia k bezdrôtovej sieti a zaisteniu autentizácie pomocou protokolu IEEE 802.1X a komunikácie s autentizačným serverom RADIUS bude na strane klienta použitý nástroj `wpa_supplicant`.

### Použitie nástroja `wpa_supplicant`

- Na VM klienta spustite terminál.
- Nainštalujte `wpa_supplicant` a spustite:

```
sudo apt install wpasupplicant -y
```

- Vytvorte alebo upravte konfiguračný súbor služby `wpa_supplicant`:

```
sudo nano /etc/wpa_supplicant/wpa_supplicant.conf
```

- Do súboru vložte nasledovnú konfiguráciu:

```
network={
    ssid="EduLab"
    key_mgmt=IEEE8021X
    eap=MD5
    identity="student"
    password="tajneheslo"
}
```

- Upravený súbor uložte pomocou **Ctrl + O**, potvrdíte stlačením klávesy **Enter** a nakoniec ukončíte pomocou **Ctrl + X**.
- Následne spustíte `wpa_supplicant`:

```
sudo wpa_supplicant -i eth0 -c
/etc/wpa_supplicant/wpa_supplicant.conf -D wired
```

Sledujte okno terminálu, v ktorom by sa mala zobrazíť hláška potvrdzujúca úspešnosť pripojenia.

### Sledovanie a analýza komunikácie vo Wiresharku

- Na klientovi (prípadne na AP) spustíte **Wireshark** pomocou príkazu:

```
sudo wireshark &
```

Prepínač `'sudo'` spustí nástroj Wireshark s oprávneniami administrátora, čo je nevyhnutné pre zachytávanie sieťovej prevádzky v Kali Linux.

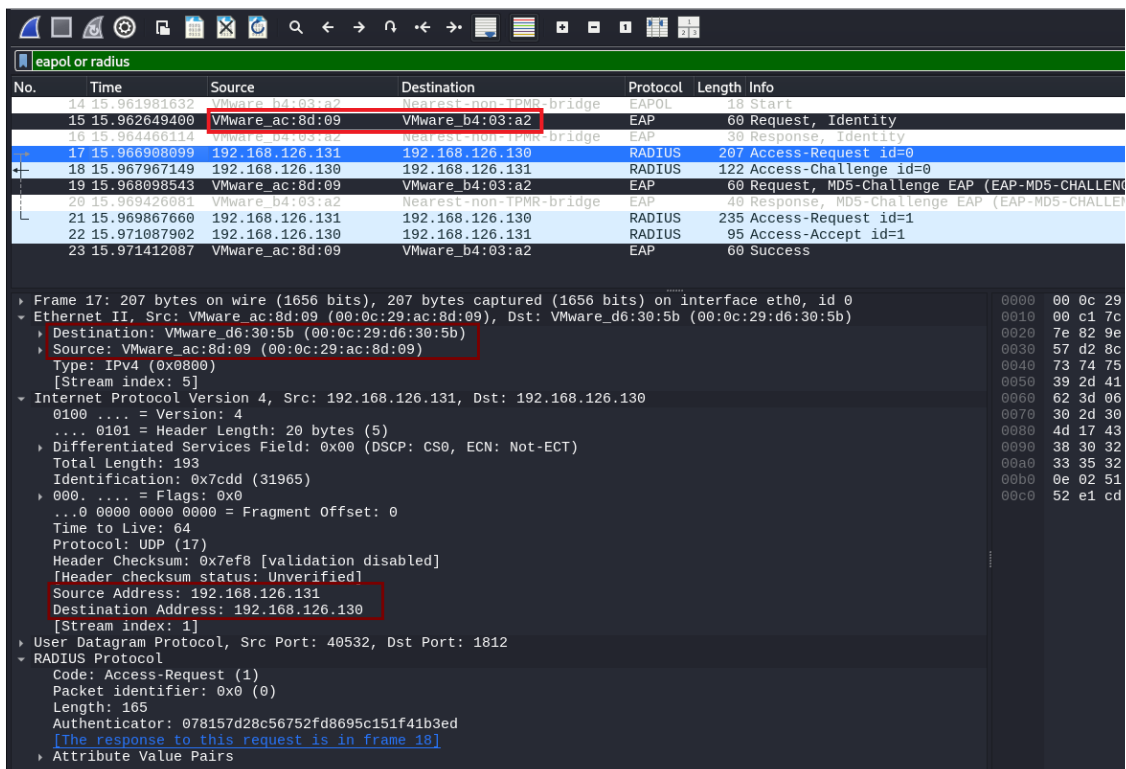
- Zvoľte rozhranie **eth0** a následne spustíte zachytávanie dátovej komunikácie kliknutím na tlačidlo "**Start Capturing**" (ikona modrého žraloka) alebo voľba **Capture > Start**.
- Nastavte filter<sup>14</sup> pre zachytávanie paketov protokolov EAP a RADIUS. Do poľa pre filter v hornej časti Wiresharku zadajte

eap or radius
---------------

- Po spustení zachytávania komunikácie sa pokúste klientom pripojiť k sieti a sledujte prebiehajúci proces autentizácie. Zamerajte sa najmä na:
  - zahájenie komunikácie a výmenu EAP správ pri autentizácii EAP-MD5 (Identity Request/Response, Success/Failure);
  - v zachytenej komunikácii na AP analyzujte požiadavky Access-Request a odpovede Access-Accept/Reject v RADIUS protokole.
- Rozkliknite zachytené pakety a analyzujte ich podrobnosti:
  - v EAP paketoch si všimajte hodnoty ako "Identity", "Request", "Response",
  - hodnoty v poli **Identifier** v príslušných správach Request/Response,
  - v paketoch protokolu RADIUS sledujte poradie odoslaných správ a ich odpovedajúcu hodnotu v poli **Identifier**,
  - ďalej atribúty ako User-Name, NAS-IP-Address, Message-Authenticator,
  - overte zhodu medzi identitou v EAP a RADIUS správach;
  - a nakoniec sledujte, či sa v prípade úspešnej autentifikácie objaví správa "Access-Accept".
- Po dokončení procesu môžete zachytávanie prebiehajúcej komunikácie ukončiť kliknutím na "**Stop Capturing**". Ukážku zachytenej komunikácie môžete vidieť nižšie na obr. 2.2.

---

<sup>14</sup> Na strane klienta bude postačujúci filter **eap**, nakoľko k výmene správ protokolu RADIUS dochádza len v rámci komunikácie medzi AP a serverom.



Obrázok 2.2 Ukážka zachytenej komunikácie – výmena správ v priebehu autentizácie EAP-MD5.

## 2.4. Samostatná úloha

### E) Konfigurácia autentizačnej metódy EAP-TLS

V poslednej časti laboratórnej úlohy si vyskúšate implementáciu autentizačnej metódy EAP-TLS, pričom využijete v procese overenia identity klienta možnosť multifaktorovej autentizácie, a to v kombinácii hesla a certifikátu. Využijete Wireshark pre zachytenie a analýzu výmeny správ. Nakoniec porovnáte rozdiely medzi použitými metódami autentizácie na základe analýzy dátovej komunikácie – venujte pozornosť rozdielom v porovnaní s EAP-MD5.

**Cieľom vašej samostatnej práce bude implementovať autentizačnú metódu založenú na certifikátoch EAP-TLS, namiesto autentizačného mechanizmu EAP-MD5, a následne nakonfigurovať autentizačnú politiku využívajúcu multifaktorovú autentizáciu (heslo + certifikát). Vygenerujte vlastné certifikáty pre server a klienta a analyzujte rozdiely medzi jednotlivými metódami autentizácie na základe zachytených dátových paketov.**

### Užitočné príkazy:

- Pre automatické vytvorenie základnej certifikačnej authority (CA), generovanie certifikátu pre server aj kľúčov je možné použiť:

```
cd /etc/freeradius/3.0/certs/  
sudo ./bootstrap
```

- Vytvorené certifikáty sa nachádzajú v adresári `/etc/freeradius/3.0/certs/` – konkrétne:
  - `ca.pem` – certifikát certifikačnej authority
  - `server.pem` – certifikát servera
  - `server.key` – súkromný kľúč servera
  - `client.pem` – certifikát klienta
  - `client.key` – súkromný kľúč klienta
- úprava konfiguračného súboru `/etc/freeradius/3.0/mods-enabled/eap` na RADIUS serveri:

```
tls {  
    default_eap_type = mschapv2  
    copy_request_to_tunnel = yes  
    use_tunneled_reply = yes  
}
```

```
tls-config tls-common {  
    private_key_file = /etc/freeradius/3.0/certs/server.key  
    certificate_file = /etc/freeradius/3.0/certs/server.pem  
    ca_file = /etc/freeradius/3.0/certs/ca.pem  
}
```

- pre kopírovanie súborov (certifikátov) medzi zariadeniami je možné využiť `scp`
- uloženie certifikátov na strane klienta do adresára:  
`/etc/wpa_supplicant/certs/`
- taktiež bude potrebná vhodná úprava konfiguračného súboru na strane klienta, kedy v súbore `/etc/wpa_supplicant/wpa_supplicant.conf` správne nakonfigurujete použitie certifikátov:



```
network={
    ssid="TESTNET"
    key_mgmt=WPA-EAP
    eap=TTLS
    identity="client"
    password="heslo_klienta"
    ca_cert= <certifikat_cert_autority>
    client_cert= <certifikat_klienta>
    private_key= <sukromny_kluc_klienta>
    phase2="auth=MSCHAPV2"
}
```

### 3. Záver

V tejto laboratórnej úlohe ste sa zoznámili s možnosťami centralizovanej autentizácie klientov s využitím autentizačného servera RADIUS.

V praktickej časti ste vo vytvorenej virtuálnej sieti simulovali pomocou troch VMs **autentizačný proces využívajúci metódu EAP-MD5** a mali možnosť analyzovať priebeh celej komunikácie prístupujúceho klienta so vzdialeným autentizačným RADIUS serverom, ktorej sprostredkovateľom bol prístupový bod. V prostredí nástroja Wireshark ste analyzovali výmenu EAP správ, ktoré sú prenášané v priebehu autentizácie, a to jednak medzi klientom a prístupovým bodom prostredníctvom protokolu EAPoL na spojovej vrstve, a následne aplikačným protokolom RADIUS medzi prístupovým bodom a autentizačným serverom. Vašou samostatnou úlohou bolo následne **implementovať metódu EAP-TLS** využívajúcu pre overenie identity klienta certifikát s verejným kľúčom a uskutočniť jej porovnanie s predošlou použitou autentizačnou metódou.

#### 3.1. Kontrolné otázky

1. Ktoré tvrdenia správne popisujú fungovanie autentizačného mechanizmu podľa IEEE 802.1X?
  - A) Overenie identity prebieha ešte pred pridelením IP adresy klientovi
  - B) IEEE 802.1X je vhodný len pre bezdrôtové siete
  - C) Komunikácia medzi klientom a prístupovým bodom prebieha cez EAPoL
  - D) IEEE 802.1X zabezpečuje šifrovanie prenosu autentizačných údajov
2. Ktoré z nasledujúcich výrokov platia o úlohe prístupového bodu (*authenticator*) v architektúre IEEE 802.1X?
  - A) Posudzuje platnosť prihlasovacích údajov a vydáva rozhodnutie o prístupe
  - B) Vystupuje ako sprostredkovateľ komunikácie medzi klientom a autentizačným RADIUS serverom
  - C) S klientom komunikuje prostredníctvom protokolu EAPoL
  - D) Generuje prístupové heslá pre klientov v lokálnej sieti
3. Vyberte nesprávne tvrdenia o protokole RADIUS:
  - A) Komunikácia medzi klientom a RADIUS serverom prebieha prostredníctvom transportného protokolu UDP na porte 1812
  - B) RADIUS šifruje celé pakety pomocou TLS
  - C) RADIUS umožňuje centralizované overenie identity
  - D) RADIUS prenáša EAPoL správy ako súčasť autentizačných požiadaviek
4. Ktoré typy EAP metód využívajú digitálne certifikáty?
  - A) EAP-TLS
  - B) EAP-MD5
  - C) EAP-PEAP
  - D) EAP-TTLS

5. Ktoré tvrdenia o nástroji FreeRADIUS sú pravdivé?
  - A) Podporuje rôzne autentizačné metódy, vrátane EAP
  - B) podporuje použitie iba jednej autentizačnej metódy v jednom okamihu
  - C) Môže byť konfigurovaný na prácu s TLS
  - D) Nepodporuje použitie autentizačnej metódy EAP-MD5
6. Aké informácie sú prenášané v správe *Access-Request* protokolu RADIUS?
  - A) Užívateľské meno (User-Name)
  - B) Hash hesla alebo autentizačný token
  - C) ID a heslo užívateľa (klienta)
  - D) IP a MAC adresa klienta
7. Aký príkaz v Kali Linux slúži na spustenie služby FreeRADIUS?
  - A) sudo start radiusd
  - B) sudo systemctl start freeradius
  - C) radiusctl enable
  - D) freeradius --run
8. Ktoré EAP správy sú typicky súčasťou autentizačného procesu pri overovaní identity s využitím metódy EAP-MD5?
  - A) Identity Request
  - B) Identity Response
  - C) EAPOL Success/Failure
  - D) Access Request
9. Čo je typické pre komunikáciu medzi klientom a AP počas výmeny EAP správ?
  - A) Komunikácia prebieha pomocou protokolu EAPoL
  - B) Pakety sú prenášané v ethernetovom rámci na spojovej vrstve
  - C) Všetka komunikácia je šifrovaná pomocou TLS
  - D) Klient komunikuje priamo s autentizačným RADIUS serverom
10. Ktoré z nasledujúcich tvrdení o EAP over LAN (EAPoL) sú nepravdivé?
  - A) EAPoL sa používa na prenos EAP správ cez káblové alebo bezdrôtové LAN siete
  - B) EAPoL správy sú zapuzdrené priamo do IP paketov
  - C) EAPoL zaisťuje komunikáciu medzi klientom a AP
  - D) EAPoL šifruje všetky EAP správy pomocou TLS

## 4. Literatúra

- [1] Cloudradius: *Breaking Down the 802.1X Protocol*. [online]. 2024. [cit. 2025-04-20]. Dostupné z: <https://www.cloudradius.com/breaking-down-the-802-1x-protocol/>
- [2] IEEE Standard for Local and metropolitan area networks: *Port-Based Network Access Control* (802.1X). 2010. ISBN 978-0-7381-6204-2. [online]. [cit. 2025-04-20]. Dostupné z: <https://standards.ieee.org/ieee/802.1X/7345/>
- [3] Cisco: *Understanding 802.1X Port-Based Authentication*. [online]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/lan-switching/802-1x/8207-802-1x.html> [cit. 2025-04-20].
- [4] LinuxHint: *What is IEEE 802.1X?* [online]. 2024. [cit. 2025-04-20]. Dostupné z: [https://linuxhint.com/ieee\\_802\\_1x\\_protocol\\_intro/](https://linuxhint.com/ieee_802_1x_protocol_intro/)
- [5] Red Hat: *802.1X Authentication* [online]. 2024. [cit. 2025-04-20]. Dostupné z: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/deployment\\_guide/s1-wificonfig-8021x](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s1-wificonfig-8021x)
- [6] ABOBA, B., BLUNK, L., VOLLBRECHT, J., CARLSON, J., LEVKOWETZ, H. *Extensible Authentication Protocol* (EAP). RFC 3748. [Internet Requests for Comments]. RFC Editor, 2004. [cit. 2025-04-20]. Dostupné z: <https://datatracker.ietf.org/doc/html/rfc3748>
- [7] A Survey of Authentication Protocols in IEEE 802.1X Standard. In: *International Journal of Computer Applications*. [online]. [cit. 2025-04-20]. Dostupné z: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.107.3918>
- [8] FADEL, Michael. *Authentication Protocols: Your Guide to the Basics* [online]. San Francisco: WorkOS, 2022. [cit. 2025-04-20]. Dostupné z: <https://workos.com/blog/authentication-protocols-your-guide-to-the-basics>
- [9] MORTÁGUAA, D. André ZÚQUETEB and Paulo SALVADOR. *Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0*. In: *Computer Networks*. 2024. s.1389–1286. [online]. [cit.2024-12-07]. Dostupné z: <https://doi.org/10.1016/j.comnet.2024.110337>
- [10] NAMAN, D. Mohammad ABDULWAHAB and Abbas IBRAHIM. *RADIUS Authentication on Unifi Enterprise System Controller using Zero-Handoff Roaming in Wireless Communication*. In: *JASTT*, vol.1. 2020. s.118–124. [online]. Dostupné z: [10.38094/jastt1427](https://doi.org/10.38094/jastt1427). [cit.2024-12-07]
- [11] FREERADIUS PROJECT. *FreeRADIUS Documentation*. [online]. 2023 [cit. 2025-04-18]. Dostupné z: <https://wiki.freeradius.org/>