

# **Text laboratorní úlohy**

Laboratorní úloha č. 8

## **Autentizace pomocí EAP a RADIUS**

# Úvod k laboratorní úloze

Cílem této laboratorní úlohy je studentům přiblížit možnosti centralizované autentizace v porovnání s mechanismy lokálního ověřování identity uživatelů, resp. zařízení. Seznámí se s principy zabezpečení přístupu do sítě pomocí **autentizačních protokolů EAP (Extensible Authentication Protocol) a RADIUS (Remote Authentication Dial-In User Service)** a získají praktické zkušenosti s implementací RADIUS serveru jakožto centrálního prvku pro řízení přístupu a zabezpečené připojení do sítě.

V rámci této úlohy získáte základní poznatky o procesu autentizace klienta ve Wi-Fi síti s podporou standardu IEEE 802.1X. V teoretické části bude vysvětlen způsob konfigurace serveru FreeRADIUS a popsán proces ověřování identity uživatele prostřednictvím externího autentizačního mechanismu. V praktické části si v připravené virtuální síti složené ze tří virtuálních strojů ve VMware – klienta, přístupového bodu a autentizačního serveru – vyzkoušíte **nasazení a konfiguraci FreeRADIUS serveru**, jako centrálního autentizačního bodu, jeho propojení s přístupovým bodem pomocí protokolu EAP a samotnou autentizaci klienta. Důležitou součástí úlohy bude analýza průběhu autentizačního procesu pomocí nástrojů síťové analýzy, která studentům umožní lépe porozumět vzájemné spolupráci jednotlivých vrstev síťové architektury, především linkové, síťové a aplikační.

## Požadavky pro vypracování úlohy:

- software: VMware Workstation Player pro virtualizaci stanic,
- virtuální stroje: tři virtuální stroje s Kali Linux.

## 1. Teoretický úvod

V této laboratorní úloze zaměřené na autentizační protokoly EAP a RADIUS se seznámíte s možnostmi centralizovaného řízení přístupu a ověřování uživatelů v počítačových sítích. Autentizace je jedním z klíčových prvků pro dosažení vysoké úrovně zabezpečení.

Kombinace **autentizační metody EAP (Extensible Authentication Protocol)** a **systému RADIUS (Remote Authentication Dial-In User Service)** se běžně využívá především v podnikových Wi-Fi sítích a VPN, kde slouží k centralizované správě ověřování identity uživatelů a řízení jejich přístupu ke sdíleným síťovým prostředkům.

### 1.1. IEEE 802.1X

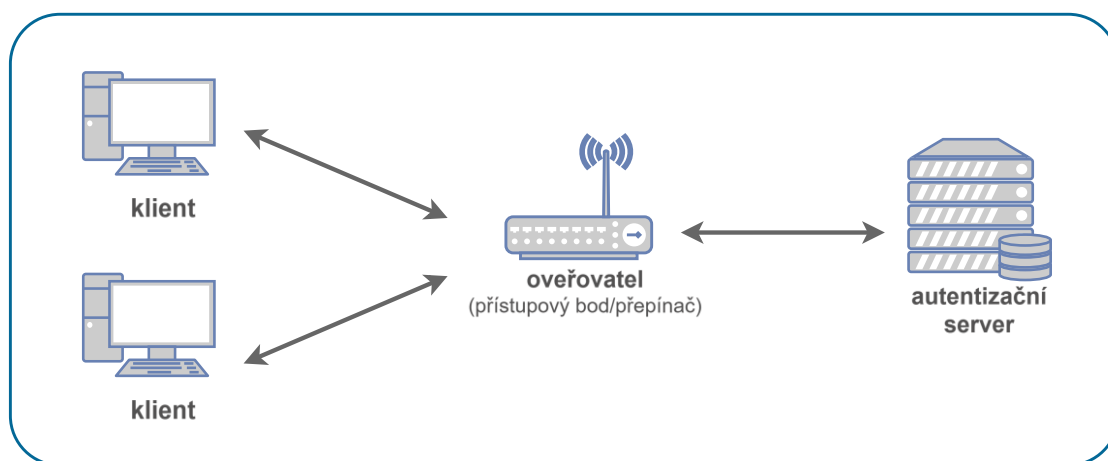
IEEE 802.1X je síťový standard definovaný organizací IEEE<sup>1</sup>, který slouží ke kontrole přístupu do lokálních sítí. Představuje základní technologii pro řízení přístupu na úrovni

---

<sup>1</sup> IEEE (*Institute of Electrical and Electronics Engineers*) je mezinárodní organizace zaměřená na vývoj technických standardů v oblasti elektrotechniky, elektroniky, výpočetní techniky a telekomunikací. Organizace IEEE je zodpovědná za tvorbu mnoha známých síťových standardů, mezi které – kromě výše

fyzických portů (tzv. *port-based network access control* – PNAC). V praxi to znamená, že zařízení (klient) nezíská plný přístup k síťovým službám, dokud neproběhne úspěšně autentizační proces. Tento proces zahrnuje spolupráci tří základních prvků:

- **klient** (*supplicant*) – resp. koncové zařízení (např. notebook nebo virtuální stroj), které se snaží připojit do sítě a předkládá svou identitu;
- **ověřovatel** (*authenticator*) – zpravidla přístupový bod<sup>2</sup> do bezdrátové sítě nebo přepínač (switch), který reguluje přístup koncových klientů do sítě a zprostředkovává výměnu autentizačních informací mezi těmito klienty a autentizačním serverem;
- **autentizační server** – ověřovací server (typicky RADIUS), který na základě definovaných konfiguračních pravidel a uložených přihlašovacích údajů rozhoduje, zda klientovi bude přístup do sítě povolen či zamítnut.



Obrázek 1.1 Základní komponenty 802.1X a jejich vzájemné propojení<sup>3</sup>.

Standard IEEE 802.1X se často používá ve spojení s protokolem EAP (*Extensible Authentication Protocol*) a v podnikových sítích představuje běžný způsob řízení bezpečného přístupu. Detailní znění standardu IEEE 802.1X je dostupné na oficiálních stránkách [2], přičemž bližší vysvětlení principů a průběhu autentizace lze nalézt i v odborné literatuře [3], [4], [5].

---

zmíněného IEEE 802.1X pro autentizaci – patří například také IEEE 802.3 specifikující technologii Ethernet nebo IEEE 802.11 zaměřený na bezdrátové technologie Wi-Fi.

<sup>2</sup> Pro označení přístupového bodu bezdrátové sítě se běžně používá zkratka „AP“ (z angl. termínu slova *Access Point*).

<sup>3</sup> Převzato z [1].

## 1.2. Extensible Authentication Protocol (EAP)

**EAP představuje flexibilní autentizační *framework*** navržený pro podporu různých metod ověřování přístupujících uživatelů. Nejedná se o konkrétní autentizační protokol, ale o rámec, který umožňuje využití **několika různých autentizačních metod**. Jednotlivé metody jsou založeny na výměně zpráv mezi klientem (např. uživatelským zařízením) a autentizačním serverem (např. RADIUS serverem). EAP se široce používá v bezdrátových sítích a v zabezpečených VPN připojeních.

Mezi nejznámější autentizační metody EAP patří:

- **EAP-MD5:** jednoduchá autentizační metoda založená na principu výzva-odpověď, kdy klient žádající o ověření identity obdrží od autentizačního serveru náhodně generovanou výzvu (*challenge*), na kterou odpovídá zprávou (*response*) obsahující hash vytvořený z autentizačního faktoru klienta, typicky hesla, a náhodné výzvy, kterou získal od serveru. Tato metoda však není považována za bezpečnou, protože výměna obou zpráv (výzvy a odpovědi) probíhá nešifrovaně.
- **EAP-TLS:** metoda využívá digitální certifikáty jak na straně klienta, tak serveru. Jde o nejbezpečnější variantu mezi dostupnými metodami, avšak vyžaduje zavedení infrastruktury pro správu certifikátů.
- **EAP-TTLS:** rozšiřuje metodu EAP-TLS o možnost kombinace certifikátu a tradičních přihlašovacích (autentizačních) údajů, např. v podobě přístupového jména a hesla. Certifikát se používá pouze k ověření serveru, což usnadňuje implementaci autentizační metody.
- **PEAP** (*Protected EAP*): metoda obsahuje mechanismy pro tunelování autentizačních údajů přes šifrované TLS spojení. Uživatelské jméno a heslo jsou přenášeny uvnitř tohoto bezpečného kanálu, čímž se zvyšuje míra zajištění důvěrnosti autentizačních údajů žadatele o ověření identity.

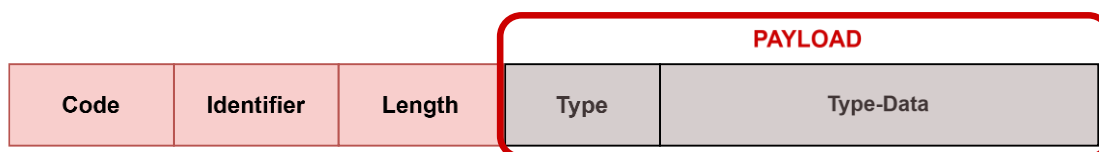
Protokol EAP definuje základní rámec pro autentizační proces, přičemž všechny metody využívají stejné typy základních EAP zpráv, které si klient a autentizační server (zprostředkovaně přes přístupový bod nebo přepínač) vyměňují. Existují čtyři základní typy zpráv, jejich přehled je uveden v tab. 1.1.

Tabulka 1.1 Přehled typů EAP zpráv.

Typ zprávy	Kód	Odesílatel	Popis
<b>EAP-Request</b> (požadavek)	1	Server	Výzva klientovi k zadání požadovaných údajů (např. identita, heslo, certifikát)
<b>EAP-Response</b> (odpověď)	2	Klient	Odpověď klienta na výzvu serveru – obsahuje požadované údaje.
<b>EAP-Success</b>	3	Server	Potvrzení úspěšné autentizace – klient získává přístup do sítě.
<b>EAP-Failure</b>	4	Server	Oznámení o neúspěšné autentizaci – přístup klienta je zamítnut.

Každá EAP zpráva má následovný základní formát (viz obr. 1.2 níže):

- **Code** – označuje typ zprávy (1=Request, 2=Response, 3=Success, 4=Failure);
- **Identifier** – slouží ke spárování výzvy a odpovědi;
- **Length** – délka EAP zprávy v bajtech;
- **Payload** – pole využívané v procesu autentizace, je obsaženo jenom ve zprávách EAP-Request a EAP-Response. Dělí se na:
  - **Type**<sup>4</sup> – určuje, co bude obsahem následujících dat (Type-Data) – například, zda se jedná o výměnu identity klienta, výzvu pro zadání hesla, odeslání certifikátu apod. Pole definuje konkrétní EAP metodu nebo příslušný krok, resp. fázi autentizačního procesu.
  - **Type-Data** – obsahuje vlastní data podle konkrétního typu zprávy (např. řetězec s identitou klienta, náhodná výzva, hash hesla, certifikát atd.)



Obrázek 1.2 Schematické znázornění struktury zprávy protokolu EAP<sup>5</sup>.

<sup>4</sup> Příklady hodnot pole *Type* jsou např.: **1 = Identity**: požadavek/odpověď s identitou (např. uživatelské jméno); **2 = Notification**: zpráva sloužící k informování klienta, resp. žadatele; **3 = NAK**: odmítnutí typu autentizace ze strany klienta; **4 = MD5-Challenge**: zpráva používaná pro odesílání výzvy a odpovědi v průběhu autentizace MD5.

Uvedený seznam možných hodnot není úplný – jedná se pouze o základní typy, se kterými jste se mohli seznámit i na přednáškách předmětu MPC-NSB.

<sup>5</sup> Převzato z oficiálních výukových materiálů k přednáškám předmětu MPC-NSB – vypracoval garant předmětu a přednášející doc. Karel Burda, CSs. (viz též E-learning předmětu).

V procesu autentizace si mezi sebou klient (resp. žadatel) a autentizační server vyměňují EAP zprávy zprostředkovaně přes AP. Typicky **server odesílá požadavky** (*Request*), na které **klient reaguje odpovědí** (*Response*). V závislosti na konkrétním typu použité autentizační metody se liší obsah datové části přenášené v příslušné EAP zprávě. Jako příklad lze uvést různé typy zpráv, které jsou odesílány v průběhu autentizačního procesu pomocí metody MD5<sup>6</sup>:

- **EAP-Request/Identity:**  
Server vyžaduje od klienta jeho jméno (identitu). V poli *Type* je uvedena hodnota **1 (Identity)**, následuje textový řetězec „*Who are you?*“.
- **EAP-Response/Identity:**  
Klient v odpovědi zasílá svou identitu, obvykle ve formě uživatelského jména. V poli *Type* je opět uvedena hodnota **1 (Identity)**, následuje řetězec s identitou.
- **EAP-Request/MD5-Challenge:**  
Server zasílá výzvu (*challenge*) k zadání autentizačních údajů.
- **EAP-Response/MD5-Challenge:**  
Klient reaguje na výzvu serveru a odesílá zprávu, která obsahuje údaje potřebné k ověření identity. V případě autentizace pomocí MD5 jde o *hash* řetězce složeného z ID žadatele, hesla a přijaté výzvy.

### Autentizace EAP-MD5

EAP-MD5 je jednoduchá autentizační metoda používaná k ověřování identity uživatelů v počítačových sítích. Funguje na principu, kdy server (autentizátor) odešle klientovi výzvu (*challenge*) a klient na základě svého uživatelského jména, hesla a obdržené výzvy vypočítá odpověď (*response*), kterou zašle zpět. Server následně tuto odpověď porovná s očekávaným výsledkem a na základě shody klientovi přístup do sítě buď povolí, nebo zamítne.

Výhodou této metody je její rychlost a jednoduchost. Mezi hlavní nevýhody však patří absence jakýchkoli mechanismů pro šifrování či ochranu přenášených dat – klientovo heslo lze totiž poměrně snadno získat pomocí útoku hrubou silou<sup>7</sup>. EAP-MD5 nepodporuje ověření serveru, a proto je považována za nevhodnou pro použití ve veřejných sítích. Výborně se však hodí pro výukové účely, protože umožňuje názorně vysvětlit základní principy a jednotlivé kroky autentizačního procesu.

Průběh autentizace pomocí EAP-MD5 zahrnuje celkem pět základních kroků, jejichž analýzu přináší následující tabulka č. 1.2 (schematické znázornění průběhu komunikace je uvedeno na obr. 1.3).

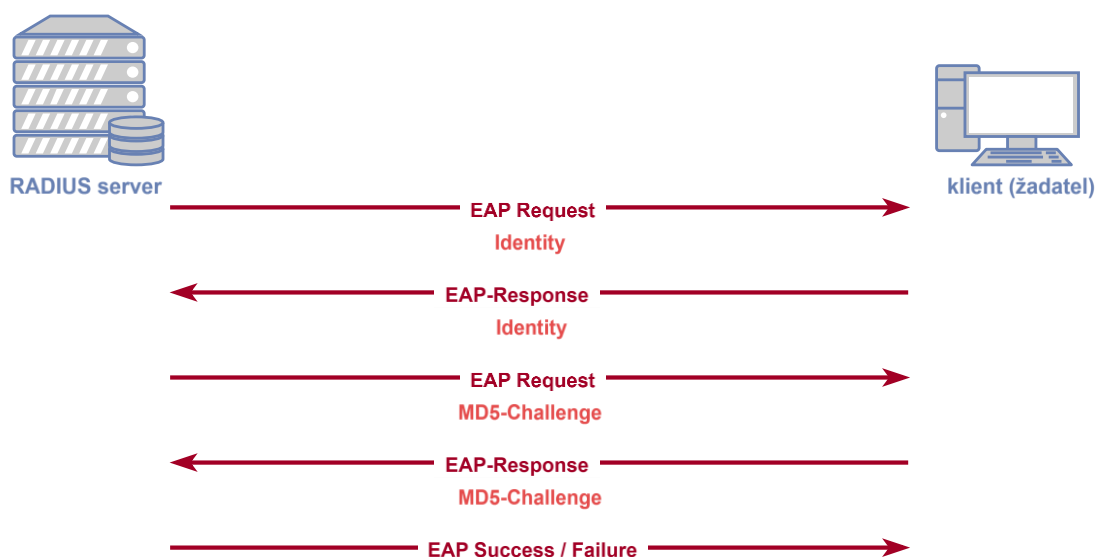
---

<sup>6</sup> Popis autentizace MD5 bude následovat.

<sup>7</sup> Pokud útočník zachytí zprávu s identitou klienta (ID), výzvu serveru a následně odpověď od klienta obsahující *hash* řetězce (ID || heslo || výzva), mohl by se teoreticky pokusit postupným zkoušením různých možných vstupů (resp. hesel) nalézt výstupní *hash*, který se shoduje s tím, který odeslal klient. V případě úspěchu by bylo zřejmé, že našel odpovídající heslo.

Tabulka 1.2 Zprávy odesílané v procesu autentizace EAP-MD5.

<b>Krok</b>	<b>Odesílatel → Příjemce</b>	<b>Typ zprávy</b>	<b>Obsah</b>
1	Autentizátor → Klient	<b>EAP-Request</b> <b>Identity</b>	Výzva k zaslání identity (např. „Kdo jsi?“)
2	Klient → Autentizátor	<b>EAP-Response</b> <b>Identity</b>	Klient odešle svou identitu (např. „peter“)
3	Autentizátor → Klient	<b>EAP-Request</b> <b>MD5-Challenge</b>	Výzva obsahující náhodný řetězec ( <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 vypočtený hash a odešle odpověď o výsledku autentizace (úspěch/neúspěch)



Obrázek 1.3 Schematické znázornění výměny zpráv mezi klientem a autentizačním serverem při EAP-MD5 autentizaci<sup>8</sup>.

<sup>8</sup> Převzato z oficiálních výukových materiálů k přednáškám předmětu MPC-NSB – vypracoval garant předmětu a přednášející doc. Karel Burda, CSs. (viz též E-learning předmětu).

## EAPoL (EAP over LAN)

Při komunikaci probíhající v sítích IEEE 802.1X jsou EAP zprávy mezi klientem (*supplicant*) a přístupovým bodem (*authenticator*) přenášeny ve formátu EAP over LAN na linkové vrstvě – tzv. **EAPoL zprávy**. EAPoL představuje rozšíření protokolu EAP navržené specificky pro použití v sítích založených na přenosových technologiích Ethernet a Wi-Fi, kde se autentizační data přenášejí přímo na druhé (linkové) vrstvě referenčního modelu ISO/OSI. Slouží výhradně ke komunikaci klienta s AP a jeho úkolem je přenášet EAP zprávy zapouzdřené do ethernetového rámce na linkové vrstvě. Standard EAPoL definuje pět základních typů zpráv (viz tab. 1.3).

Tabulka 1.3 Přehled typů EAPoL zpráv.

Typ	Název zprávy	Účel
0x00	EAP-Packet	Obsahuje samotnou EAP zprávu
0x01	EAPoL-Start	Iniciuje autentizační proces
0x02	EAPoL-Logoff	Označuje, že klient se odhlasuje ze sítě, slouží k ukončení spojení
0x03	EAPoL-Key	Používá se pro výměnu šifrovacích klíčů (např. v protokolu WPA/WPA2)
0x04	EAPoL-Encapsulated-ASF-Alert	Méně běžný typ zprávy pro specifická bezpečnostní upozornění

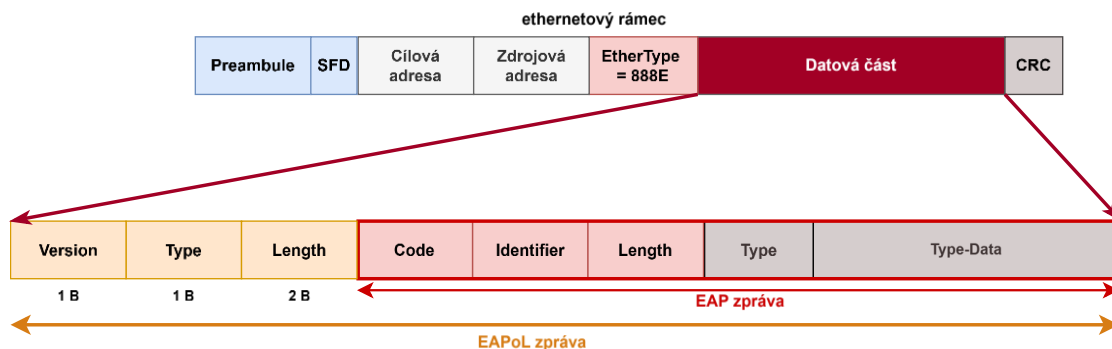
Proces zapouzdření EAPoL zprávy do ethernetového rámce na úrovni linkové vrstvy je znázorněn na obr. 1.4, přičemž struktura samotné EAPoL zprávy je rovněž graficky zobrazena. Význam jednotlivých polí je následující:

- **Version** – verze protokolu EAPoL (např. 0x01 pro IEEE 802.1X);
- **Type** – typ EAPoL zprávy (např. 0x00 pro EAP-Packet);
- **Length** – délka datové části zprávy v bajtech;
- **Body** – samotný obsah, tj. zpráva EAP protokolu (např. EAP výzva (*Request*), odpověď (*Response*), apod.) – pole je přítomné pouze u zpráv typu EAP-Packet.

Přístupový bod (AP) následně tyto EAP zprávy zapouzdřuje do zpráv protokolu RADIUS na aplikační vrstvě a přeposílá je dále na autentizační server (podrobnější popis bude následovat).

Výhodou protokolu EAP je jeho modularita a schopnost přizpůsobit se různým scénářům z praxe. Metody *frameworku* EAP tvoří základní pilíře zabezpečení zejména v dnešních Wi-Fi sítích s WPA-Enterprise, jelikož umožňují výběr z široké škály různých autentizačních metod podle konkrétních požadavků.





Obrázek 1.4 Schematické znázornění zapouzdření EAPoL zprávy do rámce technologie Ethernet<sup>9</sup>.

Podrobný popis architektury, typů a formátů přenášených zpráv i používaných autentizačních metod lze nalézt v oficiálním standardu definujícím EAP, dokumentu RFC: *Extensible Authentication Protocol* (EAP), viz literatura [6]. Více o jednotlivých autentizačních metodách dostupných v rámci EAP frameworku, včetně detailní analýzy výhod, a naopak omezení a nedostatků jednotlivých přístupů, lze najít v literatuře [7].

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

RADIUS je aplikační protokol založený na architektuře *klient–server*, který poskytuje **služby AAA** (*Authentication, Authorization, Accounting*), tedy autentizaci, autorizaci a účtování. Byl vyvinut jako mechanismus centralizované autentizace uživatelů. V kontextu IEEE 802.1X je klíčovým prvkem autentizační server RADIUS. V lokálních sítích plní jeho úlohu přístupový bod, který vystupuje jako klient protokolu RADIUS a veškeré zprávy přijaté od klienta přeposílá na autentizační server.

Mezi hlavní součásti architektury RADIUS patří:

- **klient RADIUS:** zařízení, které pro přistupujícího uživatele zprostředkovává proces autentizace (např. Wi-Fi přístupový bod nebo VPN server). Toto zařízení přijímá požadavky na připojení a odesílá je autentizačnímu RADIUS serveru;
- **RADIUS server:** zpracovává autentizační požadavky, ověřuje zadané autentizační údaje a na základě výsledku procesu ověřování identity rozhoduje o povolení či zamítnutí přístupu;
- **databáze uživatelů:** jedná se úložiště obsahující přihlašovací (autentizační) údaje uživatelů a případně i další informace a oprávnění nezbytná pro řízení

<sup>9</sup> Převzato z oficiálních výukových materiálů k přednáškám předmětu MPC-NSB – vypracoval garant předmětu a přednášející doc. Karel Burda, CSs. (viz též E-learning předmětu). Pozn.: podrobný popis položek záhlaví Ethernetu není uveden, jelikož se předpokládá na straně studentů znalost problematiky (viz E-learning předmětu MPC-NSB, Téma 3).

přístupu ke sdíleným prostředkům. Může jít např. o soubor, LDAP server nebo jiný adresářový systém.

Protokol RADIUS využívá na transportní vrstvě jednoduchý bezstavový protokol UDP a typicky komunikuje na portech 1812 (pro autentizaci) a 1813 (pro účtování). Po úspěšné autentizaci může být přístupujícímu uživateli umožněn přístup do sítě či k požadovaným prostředkům.

### Autentizační server RADIUS v procesu autentizace

V procesu autentizace EAP-MD5 vystupují tři klíčové komponenty – klient (žadatel), přístupový bod (AP) a autentizační server RADIUS (viz obr. 1.5). Přístupový bod slouží jako prostředník, který pouze přenáší autentizační zprávy mezi klientem a serverem. Komunikace mezi klientem a AP probíhá formou EAP zpráv zapouzdřených do EAPoL (EAP over LAN), které jsou přenášeny přes Ethernet.

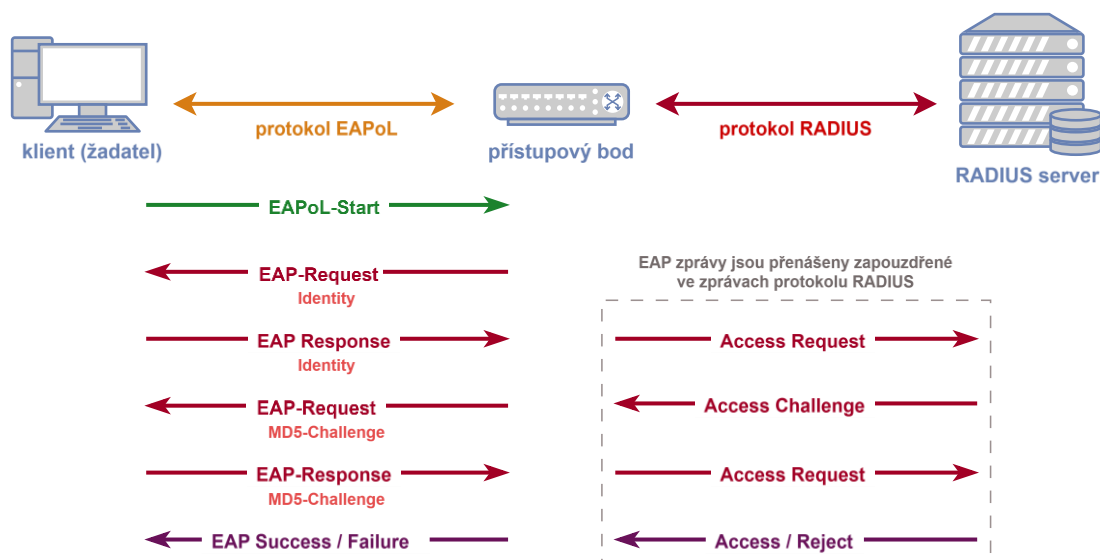


Obrázek 1.5 Komponenty sítě s autentizací EAP-MD5 a jejich vzájemná komunikace.

Autentizační server je zodpovědný za samotné ověření identity klienta. Jakmile AP obdrží od klienta zprávu typu **EAP-Response/Identity** s jeho identitou, zapouzdří ji do RADIUS zprávy typu **Access-Request** a odešle na server. Server odpoví výzvou typu **Access-Challenge**, která obsahuje náhodný řetězec (výzvu, *challenge*), a ten je následně přeposlán klientovi prostřednictvím AP jako zpráva typu **EAP-Request /MD5-Challenge**.

Klient z výzvy, ID výměny a svého hesla spočítá *hash* a odešle jej zpět jako reakci (odpověď, *response*) ve zprávě **EAP-Response/MD5-Challenge**. AP tuto odpověď opět zapouzdří do zprávy **Access-Request** a přepośle ji RADIUS serveru. Server ověří správnost výpočtu (porovná s vlastním výpočtem hodnoty *hash*) a na základě výsledku rozhodne o úspěšnosti autentizace. V případě úspěchu odešle zprávu **Access-Accept**, jinak **Access-Reject**. AP poté informuje klienta výslednou zprávou **EAP-Success**, resp. **EAP-Failure**.

Tento mechanismus zajišťuje, že heslo klienta nikdy není přenášeno v otevřené podobě. AP přitom nezná žádné autentizační údaje – jeho úkolem je pouze zapouzdření EAP zpráv do formátu RADIUS a zpět. Protokol RADIUS se používá výhradně pro komunikaci mezi AP a autentizačním serverem, zatímco EAPoL slouží k přenosu zpráv mezi klientem a AP. Podrobný průběh komunikace je znázorněn na obr. 1.6.



Obrázek 1.6 Schematické znázornění autentizace EAP-MD5 podle standardu IEEE 802.1X<sup>10</sup>.

Pro více informací a podrobnější vysvětlení a popis výše uvedených protokolů a metod autentizace je možné nahlédnout do literatury [8], [9], [10].

## 1.4. Použité nástroje

### Wireshark

Wireshark je síťový analyzátor, který umožňuje sledování datových přenosů. Použití tohoto nástroje jste si prakticky vyzkoušeli již v několika předchozích laboratorních úlohách, a proto zde nebude detailněji popisován.

### FreeRADIUS

**FreeRADIUS** představuje *open-source* řešení pro implementaci protokolu RADIUS určeného k autentizaci, autorizaci a účtování přístupů v sítích. Umožňuje nasazení RADIUS serverů a je využíván jak v podnikových, tak ve veřejných sítích pro potřeby centralizovaného ověřování uživatelů. FreeRADIUS podporuje široké spektrum autentizačních protokolů, včetně EAP-MD5, PEAP, EAP-TTLS a mnoha dalších, což z něj činí vhodné řešení pro různorodá síťová prostředí.

Kromě samotné autentizace nabízí FreeRADIUS také možnosti monitorování činnosti uživatelů v síti a vytváření záznamů o jejich přístupech ke zdrojům. FreeRADIUS je modulární a flexibilní, což umožňuje jeho integraci s databázemi, LDAP servery a dalšími externími autentizačními systémy.

<sup>10</sup> Převzato z oficiálních výukových materiálů k přednáškám předmětu MPC-NSB – vypracoval garant předmětu a přednášející doc. Karel Burda, CSs. (viz též E-learning předmětu).

## Instalace a konfigurace RADIUS serveru

V rámci praktické části úlohy budete realizovat vlastní implementaci RADIUS serveru. Pro tento účel bude využit nástroj FreeRADIUS<sup>11</sup> dostupný v systému Kali Linux.

Instalace FreeRADIUS na Kali Linux:

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

Konfigurace autentizační politiky v souboru `/etc/freeradius/3.0/users` pro přidání nového uživatele:

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

Spuštění vytvořeného RADIUS serveru:

```
sudo systemctl start freeradius
```

## Hostapd

**Hostapd** představuje softwarové řešení, které umožňuje běžným klientským zařízením (např. virtuálnímu stroji s Kali Linux) emulovat funkcionalitu plnohodnotného přístupového bodu (*authenticator*) ve smyslu standardu IEEE 802.1X. Je primárně navržen pro bezdrátové sítě, avšak v laboratorních podmínkách může být využit i v simulovaném ethernetovém prostředí. Umožňuje implementaci autentizačních mechanismů, správu SSID<sup>12</sup>, zabezpečení sítě a komunikaci s RADIUS serverem. V rámci laboratorní úlohy bude nástroj `hostapd` použit k vytvoření jednoduchého autentizačního bodu sítě, který zprostředkovává výměnu údajů mezi klientem a RADIUS serverem prostřednictvím EAP.

Základní parametry jako název sítě (SSID), síťové rozhraní, povolení mechanismu autentizace IEEE 802.1X a údaje o RADIUS serveru jsou součástí konfiguračního souboru **hostapd.conf**. Příklad konfigurace:

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

<sup>11</sup> Více informací o FreeRADIUS je dostupných na oficiálních stránkách projektu, viz [11].

<sup>12</sup> SSID (*Service Set Identifier*) představuje název bezdrátové sítě, který se zobrazuje uživatelům při připojení ke konkrétní Wi-Fi.

Vysvětlení jednotlivých nastavení obsažených v konfiguraci:

- **interface=eth0** – určuje síťové rozhraní, na kterém bude **hostapd** naslouchat a zprostředkovávat autentizační procesy;
- **driver=wired** – specifikuje průběh 802.1X autentizace přes ethernetové připojení;
- **ssid=EduLab** – nastavuje název sítě (SSID), který bude AP vysílat;
- **ieee8021x=1** – aktivuje podporu autentizačního protokolu IEEE 802.1X;
- **auth\_server\_addr=192.168.126.130** – IP adresa RADIUS serveru.
- **auth\_server\_port=1812** – standardní port pro autentizační požadavky používaný na straně RADIUS serveru;
- **auth\_server\_shared\_secret=heslo1245** – sdílené heslo (tajný klíč) pro zabezpečení komunikace mezi přístupovým bodem a RADIUS serverem.

Po definování konfiguračních parametrů a uložení příslušného konfiguračního souboru se služba **hostapd** spouští příkazem:

```
sudo hostapd hostapd.conf
```

Uvedený příkaz zajistí načtení konfiguračního souboru a spuštění služby **hostapd** s požadovanými nastaveními. Je nezbytné jej spouštět s administrátorskými oprávněními (**sudo**), protože práce se službou **hostapd** zahrnuje manipulaci se síťovými rozhraními, jejich konfiguraci a správu autentizačních procesů, které vyžadují vyšší úroveň systémových oprávnění. **Pozn.: správná konfigurace a spuštění tohoto nástroje je nezbytné pro úspěšné zprostředkování autentizace mezi klientem a RADIUS serverem.**

### **wpa\_supplicant**

Jedná se o softvérový nástroj, který **umožňuje zařízení (klientovi) bezpečně se připojit k bezdrátové síti vyžadující autentizaci pomocí protokolu IEEE 802.1X**. Spuštěná instance nástroje **wpa\_supplicant** funguje jako klientská aplikace, která obsluhuje a řídí proces autentizace klienta a zajišťuje výměnu autentizačních EAP zpráv mezi klientským zařízením a přístupovým bodem<sup>13</sup>. Tento nástroj tedy slouží k zajištění bezpečné komunikace klienta s přístupovým bodem (AP) prostřednictvím protokolů 802.1X a EAP, přičemž podporuje různé typy EAP autentizačních metod (např. EAP-MD5, EAP-TLS, EAP-TTLS, PEAP a další).

---

<sup>13</sup> AP zastávající funkci **authenticator** v procesu autentizace IEEE 802.1X.

## 2. Praktická část

V rámci praktické části úlohy získáte komplexní přehled o možnostech implementace autentizačních protokolů EAP a RADIUS a také vlastní praktické zkušenosti s nastavením a správnou konfigurací vhodných metod autentizace a pokročilého řízení přístupu ke zdrojům v počítačové síti.

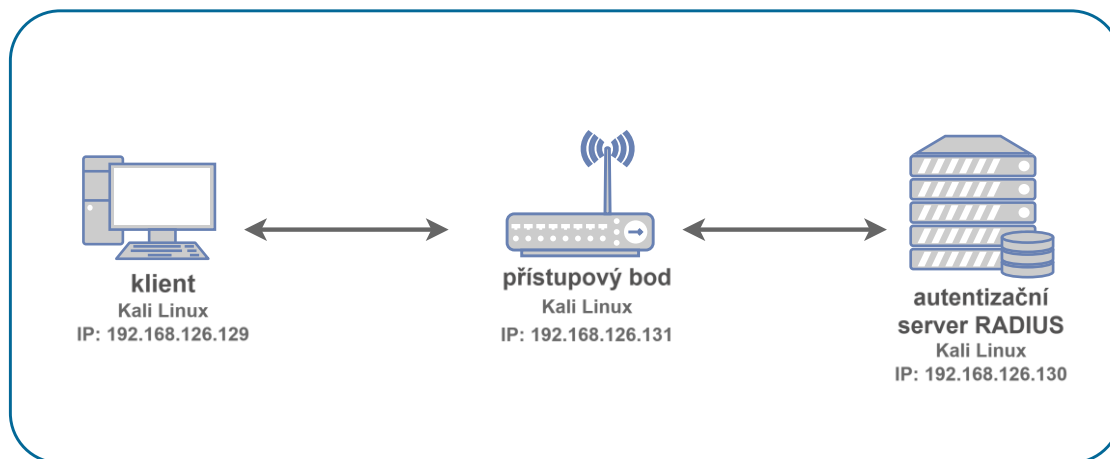
### 2.1. Topologie virtuální sítě a nastavení virtuálních strojů

Vytvořená síť bude sestávat ze tří virtuálních strojů:

- **klient:** simulované koncové zařízení, které se připojuje do sítě přes 802.1X
- **Access Point** (*authenticator*) = **přístupový bod:** zařízení využívající `hostapd`, zprostředkovatel autentizace, resp. komunikace klienta s autentizačním RADIUS serverem
- **RADIUS server:** zařízení s implementovanou instancí autentizačního serveru pomocí nástroje `FreeRADIUS`

**Síťová konfigurace:**

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



Obrázek 2.1 Topologie sítě laboratorní úlohy.

Všechny virtuální stroje musí být propojeny ve stejné virtuální podsíti, doporučuje se použít síťový režim: "**Host-Only**".



### Poznámka k vytvořené topologii:

Pro emulaci přístupového bodu (AP) použijte virtuální stroj, který byl v předchozích laboratorních úlohách použit jako zařízení „útočníka“. Příslušný VM je připraven k použití nástroje *hostapd*, aby mohl funkčně zastoupit přístupový bod simulované sítě.

## 2.2. Seznámení se s použitými nástroji

Přehled základních příkazů pro jednotlivé používané nástroje

- **FreeRADIUS**

- instalace:

```
sudo apt install freeradius
```

- spuštění:

```
sudo systemctl start freeradius
```

- ověření stavu:

```
sudo systemctl status freeradius
```

- záznamy o událostech (logy) jsou dostupné v souboru:

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

- **Hostapd**

- instalace:

```
sudo apt install hostapd
```

- konfigurační soubor obsahující nastavení SSID, síťových parametrů a parametrů souvisejících s autentizačním procesem:

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

- **Wpa\_supplicant**

- nastavení služby *wpa\_supplicant* se provádí úpravou konfiguračního souboru:

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

- příklad spuštění autentizačního procesu:

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

## 2.3. Postup pro vypracování laboratorní úlohy


### A) Příprava prostředí

#### Spuštění virtuálních strojů:

- Otevřete VMware Workstation Pro (zástupce na ploše).
- Postupně spusťte všechny tři virtuální stroje (klient, AP, RADIUS server).
- Zkontrolujte, že všechny VMs jsou připojeny ke stejné virtuální síti (nastavení např. NAT nebo Host-Only). Ověřte také správnost síťové konfigurace a přidělení IP adres.
- Přihlaste se do prostředí Kali Linux na všech VMs.

VM „klient“	– přihlašovací údaje: <b>Username:</b> klient, <b>Password:</b> kali
VM „AP“	– přihlašovací údaje: <b>Username:</b> kali, <b>Password:</b> kali
VM „RADIUS“	– přihlašovací údaje: <b>Username:</b> server, <b>Password:</b> kali

#### Ověření síťové konektivity:

- Otevřete **terminál** (kliknutím na ikonu terminálu  na horní liště nebo stlačte **Ctrl + Alt + T**).
- Na jednotlivých VMs si zobrazte přidělené IP adresy (na rozhraní `eth0`) příkazem:

```
ip a
```

- Zkontrolujte konektivitu mezi stroji pomocí ping z klienta na AP a server, a obousměrně mezi AP a RADIUS serverem:

```
ping <ip_adresa_zařízení>
```


Pokud přichází odpověď **ping echo reply** ze strany serveru, síťová komunikace mezi zařízeními funguje.

### B) Konfigurace přístupového bodu

Aby mohl přístupový bod vytvořené sítě v procesu autentizace klienta vystupovat jako *authenticator* a zprostředkovávat komunikaci mezi klientem a autentizačním RADIUS serverem, je třeba příslušný VM náležitě nakonfigurovat. Pro tento účel bude použit nástroj `hostapd`, který umožňuje plnohodnotně emulovat funkčnost přístupového bodu na „běžném zařízení“.



## Použití nástroje hostapd

- Na VM, který bude zastávat roli přístupového bodu, otevřete terminál (ikona  v horním panelu nebo v menu: **Applications > System Tools > Terminal**). Otevře se okno s příkazovou řádkou.

- Nainstalujte hostapd pomocí příkazu:

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

- Aby mohl VM obstarávat funkce AP v autentizačním procesu, je nutné vhodně upravit konfiguraci v konfiguračním souboru **/etc/hostapd/hostapd.conf**. Vytvořte nebo upravte soubor:

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

- Do souboru vložte požadovanou konfiguraci:

```
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 úpravě konfigurace stiskněte kombinaci kláves **Ctrl + O** (uložení), potvrďte název souboru klávesou **Enter** a nakonec ukončete textový editor **nano** kombinací **Ctrl + X**.
- Alternativně můžete úpravu konfigurace ukončit stlačením **Ctrl + X**, poté pro potvrzení vykonaných změn stlačte **Y** (Yes/ano), a nakonec potvrďte stlačením **Enter**. Tímto způsobem se změny uloží a editor se ukončí.
- Následně spusťte službu hostapd:

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

V případě úspěšného spuštění služby se v používaném terminálovém okně zobrazí stav **AP-ENABLED**.

### C) Konfigurace RADIUS serveru

Implementace a následná konfigurace vlastního autentizačního RADIUS serveru na jednom z používaných VMs bude provedena pomocí nástroje FreeRADIUS.

#### Instalace nástroje FreeRADIUS

- Na serveru otevřete terminál.
- Po zobrazení okna s příkazovou řádkou nejdříve zkontrolujte, jestli je FreeRADIUS na VM nainstalován, případně nainstalujte příkazem:

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

#### Konfigurace uživatele

- Po instalaci je nutné na autentizačním RADIUS serveru vytvořit záznam o autentizačních údajích klienta (žadatele):
  - Pro úpravu konfiguračních souborů nástroje FreeRADIUS bude třeba **použít privilegovaný režim**. Zadejte příkaz:

```
sudo -i
```

jako heslo (*password*) zadejte: **kali**

- Otevřete soubor:

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

- a do souboru vložte následující záznam:

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

#### Konfigurace přístupového bodu (AP)

- V dalším kroku je třeba definovat také parametry spojení mezi RADIUS serverem a přístupovým bodem.
  - Otevřete soubor:

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

- a do souboru vložte následující záznam:

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

## Spuštění služby

- Následně server restartujte a spusťte službu:

```
sudo systemctl start freeradius
```

- Po spuštění služby FreeRADIUS sledujte logy (záznamy událostí) pro ověření správnosti použitých nastavení – potřebné logy se automaticky zobrazí v terminálu po zadání příkazu:

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

Logy obsahují důležité informace o průběhu autentizačního procesu, jako jsou úspěšné nebo neúspěšné pokusy o autentizaci, chyby v konfiguraci, zamítnuté požadavky na přístup nebo problémy se sítovou komunikací. Pokud se v logech objeví chybová hlášení (např. neplatné přihlašovací údaje, nesprávný klíč, resp. *shared secret* mezi AP a RADIUS serverem apod.), je třeba všechny zaznamenané chyby analyzovat a opravit.

- Příklad ukázkového 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) Konfigurace klienta

Pro zajištění bezpečného připojení k bezdrátové síti a autentizace pomocí protokolu IEEE 802.1X a komunikace s autentizačním serverem RADIUS bude na straně klienta použit nástroj `wpa_supplicant`.

### Použití nástroje `wpa_supplicant`

- Na VM klienta otevřete terminál.
- Nainstalujte `wpa_supplicant` a spusťte:

```
sudo apt install wpa_supplicant -y
```

- Vytvořte nebo upravte konfigurační soubor služby `wpa_supplicant`:

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

- Do souboru vložte následující konfiguraci:

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

- Upravený soubor uložte pomocí kombinace kláves **Ctrl + O**, potvrďte stiskem klávesy **Enter** a následně ukončete pomocí **Ctrl + X**.
- Poté spusťte `wpa_supplicant`:

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

Sledujte výstup v terminálu, ve kterém by se mělo zobrazit hlášení potvrzující úspěšné připojení.

### Sledování a analýza komunikace ve Wiresharku

- Na klientovi (případně na AP) spusťte **Wireshark** pomocí příkazu:

```
sudo wireshark &
```

Přepínač **'sudo'** spustí nástroj Wireshark s oprávněními administrátora, což je nezbytné pro zachytávání síťového provozu v Kali Linux.

- Vyberte rozhraní **eth0** a spusťte zachytávání datové komunikace kliknutím na tlačítko "**Start Capturing**" (ikona modrého žraloka) nebo volbou **Capture > Start**.
- Nastavte filtr<sup>14</sup> pro zachytávání paketů protokolů EAP a RADIUS. Do pole pro filtr v horní části Wiresharku zadejte:

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

- Po spuštění zachytávání komunikace se pokuste připojit klienta k síti a sledujte průběh autentizačního procesu. Zaměřte se zejména na:
  - zahájení komunikace a výměnu EAP zpráv při autentizaci EAP-MD5 (Identity Request/Response, Success/Failure);
  - v zachycené komunikaci na AP analyzujte požadavky Access-Request a odpovědi Access-Accept/Reject v protokolu RADIUS.
- Rozklikněte zachycené pakety a analyzujte jejich podrobnosti:
  - v EAP paketech si všimněte hodnoty "Identity", "Request", "Response",
  - hodnoty v poli **Identifier** v příslušných zprávách Request/Response,
  - v paketech protokolu RADIUS sledujte pořadí odeslaných zpráv a odpovídající hodnotu v poli **Identifier**,
  - dále atributy jako User-Name, NAS-IP-Address, Message-Authenticator,
  - ověřte shodu mezi identitou v EAP a RADIUS zprávách;
  - a nakonec sledujte, zda se v případě úspěšné autentizace objeví zpráva "Access-Accept".
- Po dokončení procesu můžete zachytávání probíhající komunikace ukončit kliknutím na "**Stop Capturing**". Ukázku zachycené komunikace můžete vidět níže obr. 2.2.

<sup>14</sup> Na straně klienta bude postačující filtr **eap**, jelikož k výměně zpráv protokolu RADIUS dochází pouze v rámci komunikace mezi AP a serverem.

No.	Time	Source	Destination	Protocol	Length	Info
14	15.961991632	VMware_ac:8d:09	Nearest-non-IPMR-bridge	EAPOL	18	Start
15	15.962649400	VMware_ac:8d:09	VMware_b4:03:a2	EAP	60	Request, Identity
16	15.964466114	VMware_b4:03:a2	Nearest-non-IPMR-bridge	EAP	30	Response, Identity
17	15.966908099	192.168.126.131	192.168.126.130	RADIUS	207	Access-Request id=0
18	15.967967149	192.168.126.130	192.168.126.131	RADIUS	122	Access-Challenge id=0
19	15.968098543	VMware_ac:8d:09	VMware_b4:03:a2	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
20	15.969426081	VMware_b4:03:a2	Nearest-non-IPMR-bridge	EAP	40	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
21	15.969867660	192.168.126.131	192.168.126.130	RADIUS	235	Access-Request id=1
22	15.971087902	192.168.126.130	192.168.126.131	RADIUS	95	Access-Accept id=1
23	15.971412087	VMware_ac:8d:09	VMware_b4:03:a2	EAP	60	Success

Frame 17: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface eth0, id 0  
 Ethernet II, Src: VMWare\_ac:8d:09 (00:0c:29:ac:8d:09), Dst: VMWare\_d6:30:5b (00:0c:29:d6:30:5b)  
 Destination: VMWare\_d6:30:5b (00:0c:29:d6:30:5b)  
 Source: VMWare\_ac:8d:09 (00:0c:29:ac:8d:09)  
 Type: IPv4 (0x0800)  
 [Stream index: 5]  
 Internet Protocol Version 4, Src: 192.168.126.131, Dst: 192.168.126.130  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 193  
 Identification: 0x7cdd (31965)  
 0000 .... = Flags: 0x0  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 64  
 Protocol: UDP (17)  
 Header Checksum: 0x7ef8 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 192.168.126.131  
 Destination Address: 192.168.126.130  
 [Stream index: 1]  
 User Datagram Protocol, Src Port: 40532, Dst Port: 1812  
 RADIUS Protocol  
 Code: Access-Request (1)  
 Packet identifier: 0x0 (0)  
 Length: 165  
 Authenticator: 078157d28c56752fd8695c151f41b3ed  
 [The response to this request is in frame 18]  
 Attribute Value Pairs

Obrázek 2.2 Ukázka zachycené komunikace – výměna zpráv v průběhu autentizace EAP-MD5.

## 2.4. Samostatný úkol

### E) Konfigurace autentizační metody EAP-TLS

V poslední části laboratorního cvičení si vyzkoušíte **implementaci autentizační metody EAP-TLS**, přičemž v procesu ověření identity klienta využijete možnost multifaktorové autentizace, a to v kombinaci hesla a certifikátu. Pro zachycení a analýzu výměny zpráv použijete nástroj Wireshark. Na závěr porovnáte rozdíly mezi použitými metodami autentizace na základě analýzy datové komunikace – věnujte pozornost rozdílům oproti EAP-MD5.

**Cílem vaší samostatné práce bude implementovat autentizační metodu založenou na certifikátech EAP-TLS, namísto autentizačního mechanismu EAP-MD5, a následně nakonfigurovat autentizační politiku využívající vícefaktorovou autentizaci (heslo + certifikát). Vygenerujte vlastní certifikáty pro server a klienta a analyzujte rozdíly mezi jednotlivými metodami autentizace na základě zachycených datových paketů.**

### Užitečné příkazy:

- Pro automatické vytvoření základní certifikační autority (CA), generování certifikátu pro server i klíčů je možné použít:

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

- Vytvořené certifikáty se nacházejí ve složce `/etc/freeradius/3.0/certs/` – konkrétně:
  - `ca.pem` – certifikát certifikační autority
  - `server.pem` – certifikát serveru
  - `server.key` – soukromý klíč serveru
  - `client.pem` – certifikát klienta
  - `client.key` – soukromý klíč klienta
- úprava konfiguračního souboru `/etc/freeradius/3.0/mods-enabled/eap` na RADIUS serveru:

```
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  
}
```

- pro kopírování souborů (certifikátů) mezi zařízeními je možné využít `scp`
- uložení certifikátů na straně klienta do složky:  
`/etc/wpa_supplicant/certs/`
- rovněž bude nutná vhodná úprava konfiguračního souboru na straně klienta – v souboru `/etc/wpa_supplicant/wpa_supplicant.conf` správně nakonfigurujte použití certifikátů:

```
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= <soukromy_klic_klienta>
    phase2="auth=MSCHAPV2"
}
```



### 3. Závěr

V tomto laboratorním cvičení jste se seznámili s možnostmi centralizované autentizace klientů s využitím autentizačního serveru RADIUS.

V praktické části jste ve vytvořené virtuální síti simulovali pomocí tří virtuálních strojů **autentizační proces využívající metodu EAP-MD5** a měli jste možnost analyzovat průběh celé komunikace přistupujícího klienta se vzdáleným autentizačním RADIUS serverem, jehož zprostředkovatelem byl přístupový bod. V prostředí nástroje Wireshark jste analyzovali výměnu EAP zpráv, které jsou přenášeny v průběhu autentizace, a to jednak mezi klientem a přístupovým bodem prostřednictvím protokolu EAPoL na linkové vrstvě, a následně aplikačním protokolem RADIUS mezi přístupovým bodem a autentizačním serverem. Vaším samostatným úkolem bylo následně **implementovat metodu EAP-TLS** využívající pro ověření identity klienta certifikát s veřejným klíčem a provést její porovnání s předchozí použitou autentizační metodou.

#### 3.1. Kontrolní otázky

1. Která tvrzení správně popisují fungování autentizačního mechanismu podle IEEE 802.1X?
  - A) Ověření identity probíhá ještě před přidělením IP adresy klientovi
  - B) IEEE 802.1X je vhodný pouze pro bezdrátové sítě
  - C) Komunikace mezi klientem a přístupovým bodem probíhá přes EAPoL
  - D) IEEE 802.1X zajišťuje šifrování přenosu autentizačních údajů
2. Která z následujících výroků platí o úloze přístupového bodu (*authenticator*) v architektuře IEEE 802.1X?
  - A) Posuzuje platnost přihlašovacích údajů a vydává rozhodnutí o přístupu
  - B) Vystupuje jako zprostředkovatel komunikace mezi klientem a autentizačním RADIUS serverem
  - C) S klientem komunikuje prostřednictvím protokolu EAPoL
  - D) Generuje přístupová hesla pro klienty v lokální síti
3. Vyberte nesprávná tvrzení o protokolu RADIUS:
  - A) Komunikace mezi klientem a RADIUS serverem probíhá prostřednictvím transportního protokolu UDP na portu 1812
  - B) RADIUS šifruje celé pakety pomocí TLS
  - C) RADIUS umožňuje centralizované ověření identity
  - D) RADIUS přenáší EAPoL zprávy jako součást autentizačních požadavků
4. Které typy EAP metod využívají digitální certifikáty?
  - A) EAP-TLS
  - B) EAP-MD5
  - C) EAP-PEAP

- D) EAP-TTLS
5. Která tvrzení o nástroji FreeRADIUS jsou pravdivá?
- A) Podporuje různé autentizační metody, včetně EAP
  - B) Podporuje použití pouze jedné autentizační metody v jednom okamžiku
  - C) Může být konfigurován pro práci s TLS
  - D) Nepodporuje použití autentizační metody EAP-MD5
6. Jaké informace jsou přenášeny ve zprávě *Access-Request* protokolu RADIUS?
- A) Uživatelské jméno (User-Name)
  - B) Hash hesla nebo autentizační token
  - C) ID a heslo uživatele (klienta)
  - D) IP a MAC adresa klienta
7. Jaký příkaz v Kali Linux slouží ke spuštění služby FreeRADIUS?
- A) `sudo start radiusd`
  - B) `sudo systemctl start freeradius`
  - C) `radiusctl enable`
  - D) `freeradius --run`
8. Které EAP zprávy jsou typicky součástí autentizačního procesu při ověřování identity pomocí metody EAP-MD5?
- A) Identity Request
  - B) Identity Response
  - C) EAPOL Success/Failure
  - D) Access Request
9. Co je typické pro komunikaci mezi klientem a AP během výměny EAP zpráv?
- A) Komunikace probíhá pomocí protokolu EAPoL
  - B) Pakety jsou přenášeny v ethernetovém rámci na linkové vrstvě
  - C) Veškerá komunikace je šifrována pomocí TLS
  - D) Klient komunikuje přímo s autentizačním RADIUS serverem
10. Která z následujících tvrzení o EAP over LAN (EAPoL) jsou nepravdivá?
- A) EAPoL se používá pro přenos EAP zpráv přes kabelové nebo bezdrátové LAN sítě
  - B) EAPoL zprávy jsou zapouzdřeny přímo do IP paketů
  - C) EAPoL zajišťuje komunikaci mezi klientem a AP
  - D) EAPoL šifruje všechny EAP zprávy pomocí TLS

## 4. Literatura

- [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/>