VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Radim Čuhel

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ŘÍZENÍ PŘÍSTUPU K LOKÁLNÍ SÍTI POMOCÍ PROTOKOLU IEEE 802.1X
IEEE 802.1X FOR LAN NETWORK ADMISSION CONTROL

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Radim Čuhel**
AUTHOR

VEDOUCÍ PRÁCE — **Mgr. Karel Slavíček, Ph.D.**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Radim Čuhel ***ID:*** 203201
Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Řízení přístupu k lokální síti pomocí protokolu IEEE 802.1x

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je analyzovat možnosti využití protokolu IEEE 802.1x pro řízení přístupu k soudobým lokálním sítím. Věcným výstupem je implementace autentizačního serveru v podobě virtuálního serveru v laboratoři a vytvoření vzorové konfigurace sítě a laboratorní úlohy, na které se budou moci s protokolem IEEE 802.1x seznámit další studenti.

DOPORUČENÁ LITERATURA:

[1] 802.1X-2010-IEEE Standard for Local nad metropolitan networks - Port-Based Network Access Control - IEEE Standard. 301 Moved Permanently [online]. Copyright (c) Copyright 2019 ITTT [cit. 15.09.2019]. Dostupné z: https://ieeexplore.ieee.org/document/5409813

[2] GEIER, James T. Implementing 802.1X security solutions for wired and wireless networks. Hoboken, J.J.: Wiley. c2008. ISBN 9780470168608.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Mgr. Karel Slavíček, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Tato semestrální práce se zaobírá řízením přístupu k soudobým lokálním sítím pomocí protokolu IEEE 802.1X. V úvodu práce se vyskytují základní pojmy v řízení přístupu do sítě a možné standardy a protokoly, které se v dnešní době používají. Věcným výstupem je implementace autentizačního serveru v podobě virtuálního serveru v laboratoři, vytvoření vzorové konfigurace sítě a laboratorní úlohy, ve které se budou moci s protokolem IEEE 802.1X seznámit i další studenti.

KLÍČOVÁ SLOVA

AAA, Protokol, RADIUS, Zabezpečení sítě, 802.1X.

ABSTRACT

This semestral work deals with the control of access to current local networks using IEEE 802.1X protocol. At the beginning of the thesis are the basic concepts of network access control and possible standards and protocols that are used today. The practical output is the implementation of an authentication server in the form of a virtual server in the laboratory, creating a sample network configuration and a laboratory task in which other students will be able to learn the IEEE 802.1X protocol.

KEYWORDS

AAA, Protocol, Network security, RADIUS, 802.1X.

ČUHEL, Radim. Řízení přístupu k lokální síti pomocí protokolu IEEE 802.1X. Brno, 2019. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/123061. Semestrální práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Karel Slavíček.

PROHLÁŠENÍ

Prohlašuji, že svůj semestrální projekt na téma Řízení přístupu k lokální síti pomocí protokolu IEEE 802.1X jsem vypracoval samostatně pod vedením vedoucího semestrálního projektu a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedeného semestrálního projektu dále prohlašuji, že v souvislosti s vytvořením tohoto semestrálního projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval mému vedoucímu práce Mgr. Karlovi Slavíčkovi, Ph.D. za odbornou pomoc při vytváření této práce.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době je téma zabezpečení metalických (drátových), ale i bezdrátových sítí velice diskutované a každý by měl o této problematice vědět. Jelikož špatné zabezpečení od domácích až po podnikové sítě, kde figurují uživatelské informace, data k účtům a spousta soukromých informací. Hlavně se bavíme o bezdrátových sítích, kde se může případný útočník připojit na delší vzdálenosti. U metalických sítí je to poněkud složitější, aby útočník dostal přístup ke kabelu a mohlo dojít k jeho připojení do zařízení. Když je zabezpečení nedostatečné, případní útočníci mohou použít několik typů útoků, které vedou k prolomení zabezpečení a poté a odcizení dat. U domácích sítí to není až takový problém, ale nikdo nechce, aby se cizí uživatel připojoval k jeho síti, popřípadě získal soukromé informace. Standard, který se stará o autentizaci a zabezpečení přístupu klienta do počítačové sítě se nazývá 802.1X. Používá pro tuto práci mnoho protokolů, které jsou implementovány a rozdělují se podle účinnosti zabezpečení. Ideální zabezpečovací protokol by měl být bezpečný a snadno implementovatelný.

V době, kdy metalické a bezdrátové sítě vznikaly, bylo zabezpečení dostačující. Avšak v tomto oboru jsou nové věci objevovány každý den. S vývojem nových standardů a typů přenosů informací je potřeba i vyvíjet metody, kterými budou tyto přenosy dat zabezpečeny. Jelikož to co je považováno v tuto chvíli za bezpečné, zítra nemusí být.

Cílem této práce je seznámit čtenáře se standardy a protokoly používaných v autentizaci a zabezpečení přístupu klienta do počítačové sítě. Praktickým výstupem je sestavení a nakonfigurování autentizačního serveru v podobě virtuálního serveru RADIUS pro laboratorní užití.

1 ŘÍZENÍ PŘÍSTUPU K SÍTI

Základním tématem v řízení přístupu do sítě, ať už bezdrátové nebo metalické je přístup pouze oprávněným osobám nebo zařízením. K dispozici máme několik přístupů. V této kapitole si o nich řekneme základní informace.

1.1 Certifikát a přístupové údaje

Tato možnost zabezpečení je primárně využívána ve firemních počítačových sítích s protokolem 802.1x. Každý uživatel, který by měl mít přístup má svoje přístupové údaje (ve formě ID a hesla) nebo certifikát. Tyto údaje pro přihlášení jsou dostupné v počítačové databázi (MySQL, LDAP, Active direktory, apod.), každému uživateli je vytvořeno nové ID a heslo nebo certifikát, který může později používat. Významnou výhodou tohoto přístupu je udržení uživatelů jen v sektorech, které sami mohou používat (např. v podnikových systémech jsou přístupy pro sekretářku, správce systému, ředitele atd.). Přístupu může administrátor jednoduše zablokovat, tím ztratí uživatel přístup do sítě [1].

1.2 Sdílený klíč

Pro přístup k síti, kde je použit sdílený klíč je potřeba znát klíč (heslo), které je předem nastaveno na AP, a uživatelé se přes něj připojují. Přístup k síti je umožněn pomocí šifrovacích algoritmů WEP, WPA nebo WPA2. Výhodou je jednoduchost nastavení klíče, avšak při jeho změně je potřeba sdělit nový klíč uživatelům k opětovnému přihlášení. Tato metoda představuje pouze základní zabezpečení, jelikož uživatel (i nepovolený) se může připojit kdykoliv, když je v dosahu AP a zná klíč [1].

1.3 MAC adresa

MAC adresa (Media Access Control) je jedinečný celosvětový identifikátor pro každé síťové zařízení, který je získán už při výrobě. Přístup k síti je řízený pomocí jednotlivých přístupových bodů. MAC adresa zařízení je při přístupu kontrolována s adresami, které jsou uloženy v daném přístupovém bodě na přístupovém seznamu ACL (Access Control List). MAC adresa je číslo, má 48bitů, které se zapisuje jako šestice dvojciferných hexadecimálních čísel oddělených dvojtečkou nebo pomlčkou. Výhodou je jednoduchost. Nevýhodou je velké množství uložených adres na přístupovém bodě a snadná změna MAC adresy. [2].

2 ZABEZPEČENÍ PŘÍSTUPU K DATOVÉ SÍTI S VYUŽITÍM IEEE

S vývojem a rozvojem teleinformačních sítí se musel ošetřit přístup pro nepovolané osoby do bezdrátových nebo metalických sítí. U těchto sítí nelze směrovat jen do určitého prostoru, proto je důležité používat zabezpečovací prvky, aby se k sítím mohli připojit pouze osoby, které mají toto právo. Původní standart z roku 1997 pro bezdrátové sítě WLAN 802.11 již obsahoval prvky zabezpečení WEP (Wired Equivalent Privacy). Netrvalo příliš dlouho a tento typ zabezpečení byl prolomen. Kalifornskou univerzitní skupinou byl v roce 2001 představen dokument o nedostatcích tohoto algoritmu s použitím šifrovací sady RC4. Poté byl oznámen první útok na algoritmus WEP. Organizace IEEE, která byla zodpovědná za standard 802.11, v roce 2002 představila nový typ zabezpečení pro připravovaný standard 802.11i. Jelikož tato mezera v bezpečnosti WEP nemohla zůstat dlouho prázdná. Touto dobou vznikal nový algoritmus využívající současný hardware pro bezdrátový přenos. Netrvalo dlouho a byl uveden nový typ zabezpečovacího algoritmu zvaný WPA (Wi-Fi Protected Access) používající algoritmus TKIP (Temporal Key Integrity Protocol). Schválení standardu 802.11i bylo v roce 2004 s bezpečnostním protokolem WPA2. Tento algoritmus používá oproti původnímu protokolu WPA jiný algoritmus AES (Advanced Encryption Standart). AES je stále dnes považován za bezpečný a doporučuje se pro zabezpečení v menších sítí WLAN bez infrastruktury pro použití 802.1x. Pro zabezpečení 802.1x je v kombinaci s RADIUS autentizačním serverem jedinou bezpečnou autentizační metodou [3].

2.1 IEEE 802.11

Standard 802.11 a 802.11x odkazují na specifikace a vývoj skupinou IEEE (Institute of Electrical and Electronics Engineers) pro bezdrátovou technologie přenosu signálu LAN (WLAN). Standard 802.11 specifikuje bezdrátový přenos mezi klientem a základní stanicí nebo mezi dvěma klienty. V roce 1997 byla definována první verze standardu v přenosovém pásmu 2,4 GHz s rozprostřeným spektrem a maximální rychlostí 2Mbit/s. Tento standard je považován jako základní stavební jednotka pro vznik a vývoj nových navazujících standardů, které se označují x1X (X označuje písmeno z abecedy pro označení dalších standardů). IEEE 802.11 řeší základní problém v bezdrátovém přístupu ke sdílenému médiu protokolem CSMA/CA, který je nástupcem protokolu ALOHA, respektive Slotted ALOHA. Zatímco v metalických (drátových) sítích se využívá protokol CSMA/CD. Kvůli nízkým kapacitám byl v roce 1999 uvolněn standard 802.11b, který umožňoval přenosové rychlosti až 11Mbit/s v přenosovém pásmu 2,4GHz. Ve stejném roce byl povolen standard 802.11a, který umožňoval přenos v pásmu 5GHz s rychlostí až 54Mbit/s. Výhodou 5GHz pásma bylo větší množství nepřekrývajících se kanálů (8 oproti 3 v pásmu 2,4GHz). V roce 2003 přišel očekávaný nástupce standardu 802.11b standard 802.11g s přenosovou rychlostí 54Mbit/s, který byl v Evropě ve velkém zastoupení a zpětně kompatibilní s 802.11b. V roce 2009 byl uvolněn standard 802.11n, který se aktuálně nejvíce používá, zavádí novou technologii MIMO (Multiple-Input, Multiple-Output). Dokáže zvýšit přenosovou kapacitu až na

600Mbit/s díky kombinaci více antén v rámci jednoho přístupového bodu. Maximální počet antén dle normy je 8, avšak v praxi je využívá zatím 3-4. Standard 802.11n je možné používat v kombinaci ve využití obou pásem, 2,4 GHz i 5GHz. V roce 2013 byl vypuštěn standard 802.11ac, vychází z 802.11n, změny spočívají v možnosti nastavení širších kanálů (80 nebo 160 MHz oproti 40MHz) v pásmu 5GHz, více prostorových toků (až osm oproti čtyřem), modulace vyššího řádu (až 256-QAM oproti 64-QAM) a jeho maximální rychlost je až 1800Mbit/s v kanálech v pásmu 5GHz. Nejnovějším standardem, který se vytvořil v roce 2019 je standard 802.11ax, označován jako

Wi-Fi 6. Je udáváno, že tento standard by měl být 4x rychlejší než předchozí (802.11ac). Dokáže operovat ve všech pásmech od 1 do 6GHz, avšak používá se především pásmo 2,4 a 5GHz. Dokáže používat modulace vyššího řádu až 1024-QAM. Mezi největší klady patří přítomnost OFDMA (Orthogonal frequency-division multiple access) metody kódování signálu na různé frekvence s využitím paralelního přenosu od/k více uživatelům [3],[4],[7]. Přehled jednotlivých standardů je vidět v tabulce 1.

Základní přehled standardů pro bezdrátové sítě

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
IEEE 802.11 původní	1997	2,4	2	DSSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	OFDM, MIMO
IEEE 802.11ac	2013	2,4 a 5	1800	OFDM, MIMO
IEEE 802.11ax	2019	2,4 a 5	3500	OFDMA, MU-MIMO

Tabulka 1: Přehled jednotlivých standardů IEEE 802.1X [5][6]

2.1.1 Ethernet standard 802.3

Ethernet je souhrn technologií pro počítačové sítě (LAN a WAN) standardizovaných jako 802.3. Jeho vývoj začal v sedmdesátých letech a v osmdesátých letech vývojáři usoudili, že je možná jeho standardizace u společnosti IEEE. V minulosti se stal velice populární díky své jednoduchosti, rychlosti, přímočarosti, nízké implementaci, ale i dnes si najde své místo např. v sítích WAN a větších sítích. Jeho rychlost postupem času vzrostla z 1Mbit/s až na 100Gbit/s. Mezi vedení po kterém byl provozován, patří kroucená dvoulinka, koaxiální kabely a optické kabely. Ve starších sítích můžeme potkat koaxiální kabely. Modernizací sítí se snažíme o předělání na optické kabely, které mají v dnešní domě bezkonkurenční vlastnosti, ať už se bavíme o přenášených rychlostech, vzdálenosti, malé ztrátovosti nebo imunitě vůči elektromagnetickému rušení. K připojení kabelu do routeru se používá především patice typu RJ-45. Když bychom chtěli zařadit Ethernet do sedmivrstvého modelu ISO/OSI,

našli bychom ho na fyzické a linkové vrstvě, jelikož se zabývá přeposíláním rámců mezi uzly, které spolu sousedí a má představy jak přenášet jednotlivé bity. V modelu TCP/IP bychom ho zařadili do vrstvy síťového rozhraní. Díky tomu, že je reprezentován na fyzické a linkové vrstvě, můžeme po něm provozovat jeden či více protokolů síťové vrstvy, jako je Apple Talk, DECnet, IPX/SPX, ale především IPv4 a IPv6 pro služby internetu. Komunikaci u Ethernetu nelze předem odhadnout, použití náhody (nedeterminismu). To znamená, že žádný uzel nemá jistotu, že přijde na řadu a bude moct posílat svoje rámce. Čím menší je provoz v daném segmentu, tím se pravděpodobnost odeslání rámců zvyšuje. Proto je Ethernet špatně aplikovatelný především tam, kde je potřeba garance komunikace (např. v řízené výrobě). Tím pádem je jeho využití především v kancelářských, školských a domácích podmínkách, kde je jeho použitelnost plně dostačující [8].

2.1.2 Rozdíl mezi Wi-Fi a Ethernetem

Hlavním rozdílem mezi Wi-Fi a Ethernetem je jeho distribuce. Zatímco u Wi-Fi je jeho připojení řešeno prostorem a uživatel si sám řídí přiřazení do SSID nebo VLAN. Záleží k jakému SSID se uživatel hlásí a podle toho se autentizační server rozhoduje, zda k tomuto připojení má oprávnění, jeho žádost potvrdí nebo zamítne.

U metalického (kabelového) vedení (Ethernetu) je přítomen switch, který řídí, do jakého portu se uživatel může připojit. Ethernetový switch může přiřadit stejný port k různým VLAN připojením. RADIUS server posílá switch informace, které použije při autentizaci uživatele.

V tabulce 2 je vidět stručné porovnání mezi Wi-Fi a Ethernetem.

Vlastnosti Wi-Fi vs. Ethernet

	Wi-Fi	**Ethernet**
Rychlost	Pomalé přenášení dat	Rychlé přenášení dat
Spolehlivost	Rychlost závisí na mnoha faktorech	Konstantní rychlost
Zabezpečení	Datový tok potřebuje být šifrovaný	Data nepožadují šifrování
Zpoždění	Vysoké	Nízké
Rozšiřitelnost	Snadná instalace a rozšíření	Vyžaduje přítomnost kabelů

Tabulka 2: Přehled vlastností Wi-Fi vs. Ethernet [9]

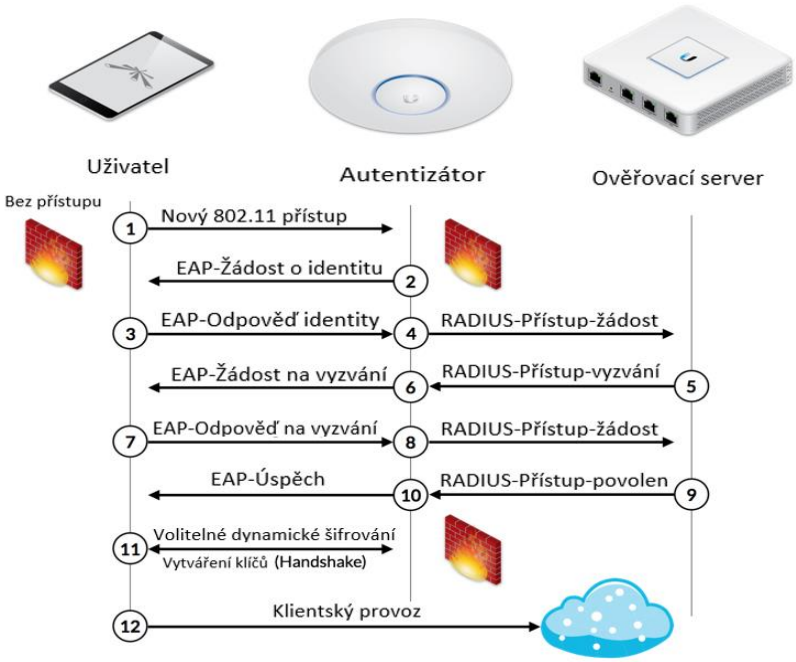
2.2 AAA

Standard AAA (Autentizace**,** Autorizace a Accounting) je skupina určitých požadavků pro povolení připojení uživatele či nikoli. Server RADIUS je autentizační autorita, která ověří identitu uživatele s použitím protokolu EAP. Uživatel, který úspěšně prošel procesem autentizace je přiděleno přístupové právo, tím je myšlena

autorizace. Accountingem rozumíme sběr informací o uživateli, který se autorizoval. Jsou to především informace o přeneseném množství dat, trvání připojení a zařízení, ze kterého se k síti připojil [10],[11].

2.3 IEEE 802.1X

IEEE 802.1X je protokol, který slouží pro autentizaci a zabezpečení přístupu klienta do počítačové sítě. Při připojení klienta k přípojnému bodu (u metalických vedení pomocí UTP kabelu do portu switche nebo k bezdrátovému bodu u Wi-Fi), je po klientovi požadován pomocí protokolu IEEE 802.1X proces autentizace (např. ID a heslo). Dokud se klient nepřihlásí pomocí správného přístupu do sítě, přípojný bod blokuje veškerý datový provoz s výjimkou autentizačního provozu. Protokol najdeme na druhé vrstvě modelu ISO/OSI a jedná se o řízení přístupu na úrovni switche, nebo virtuálního portu přístupového bodu WLAN. Hlavním úkolem 802.1X je zapouzdření zpráv EAP tak, aby nebylo nutné používat pro předávání zpráv třetí vrstvu (síťová vrstva) modelu ISO/OSI. EAP definuje formát pro zprávy zasílané mezi třemi částmi. Supplicant, neboli klient, který žádá přístup do sítě, authenticator, který zpracovává požadavek switch/access point a autentizační server (např. RADIUS server) ověřující uživatele, s kterým komunikuje switch/access point [10],[11]. Podrobný popis připojení uživatele k bezdrátové síti je znázorněn na obrázku 1.



Obrázek 1: Princip autentizace v protokolu 802.1X pro bezdrátové vedení [11]

2.4 WEP

Pod názvem WEP (Wired Equivalent Privacy) si můžeme představit názvy různých zabezpečení pro bezdrátové i drátové sítě podle původního standardu 802.11 z roku 1997, které už jsou dnes zastaralé. Hlavním cílem bylo utajit přenášené data. Výrobci ho nemuseli implementovat ve svých zařízeních, jelikož ve standardu byl označen jako nepovinný. K šifrování se používá algoritmus RC4 (Rivest Cipher 4), které bychom našli na druhé vrstvé síťového modelu ISO/OSI . Jedná se o šifrovací algoritmus založený na klíči o 10 nebo 26 hexadecimálních znacích (40 nebo 104 bitů). Obsahuje také CRC (Cyclic Redundancy Check) ke kontrole integrity jednotlivých paketů. Jelikož tento protokol zabezpečení byl snadno prolomitelný, byl nahrazen protokolem WPA2 [12],[13].

2.4.1 WEPplus

WEPplus je označení vylepšení protokolu WEP, které mělo odstranit tzv. slabé inicializační vektory, kterými může útočník velice jednoduše dopočítat použitý šifrovací klíč použitý v proudové šifry RC4. Když dojde k prolomení zabezpečení, může útočník odposlouchávat provoz a poté se i do bezdrátové sítě připojit. Toto zabezpečení však nemá žádný význam, není-li implementováno na všech zařízeních, poté je toto zabezpečení stejné jako při použití WEP [13].

2.4.2 WEP2

Toto vylepšení odstraňuje nedostatky, které mělo původní WEP. Zesiluje šifrování na 128 bitů oproti původním 64 bitům ve WEP a rozšiřuje inicializační vektory, ale i přes to je snadno prolomitelné, jen to zabere více času. Bylo používané na zařízeních, na kterých se nemohlo používat zabezpečení WPA a WPA2 [14].

2.4.3 Dynamic WEP

Dynamické WEP odkazuje na kombinaci protokolu 802.1X a EAP (Extensible Authentication Protocol), kde jsou WEP klíče měněny dynamicky. Prvním krokem k tomu, aby bylo WEP bezpečnější bylo nutné obnovování klíčů dynamicky. Všechny stanice v síti sdílí klíč k zašifrování dat, které jsou přenášeny a každá stanice má svoje mapovací klíče pro unicast přenos dat. WEP nespecifikuje přenos rámců s klíči. Klíče jsou generovány a posílány napříč systémem. Dynamické WEP používá vylepšený přenos rámců s klíči, používá silný kryptografický protokol ke generování a potom

k jejich posílání v zašifrované formě přes nedůvěryhodnou sít. Generování WEP klíče závisí na použitém kryptografickém autentizačním protokolu. Dynamické WEP zachází s rámci stejně jako WEP, jedinou změnou je pouze generování a distribuce v periodických intervalech. Dynamické WEP je mnohem bezpečnější než statické WEP jelikož život klíče je mnohem kratší. Každý útok musí počítat s odlišnou délkou života klíčů [15].

2.5 WPA

WPA (Wi-Fi Protected Access) je označení bezpečnostního standardu pro ochranu sítí zařízeních s možností bezdrátového připojení k internetu. WPA bylo vyvinuto společností Wi-Fi Allience k poskytnutí více sofistikovaného šifrování dat a lepší autentizace uživatelů než toho bylo u dosavadního standardu WEP. Tento standart se začal používat od roku 2003, kde byl představen pro draft 802.11i. Snažením šifrovacího mechanismu WPA bylo odstranit nedostatky jeho předchůdce WEP, avšak mají stále implementované stejné základní bloky mechanismu. Jednou z největších změn oproti WEP je použití WPA-PSK (Pre-Shared Key). Klíče, které používá WPA mají 256 bitů. Další významnou změnou v implementaci standardu WPA jsou zprávy kontroly integrity (kontrola, jestli útočník změnil pakety mezi přístupovým bodem a klientem) a protokol TKIP (Temporaly Key integrity Protocol).

TKIP protokol využívá s každým zařízením sadu klíčů, které jsou v rámci komunikace dynamicky měněny. Inicializace spojení probíhá se sdíleným klíčem, který je použitý jenom jednou, a tudíž se neopakuje znovu. Protokol TKIP pro šifrování dat byl později nahrazen AES (Advanced Encryption Standard). AES (Advanced Encryption Standard) je šifrovací standard schválený NSA (National Security Agency). Používá algoritmus Rijndael, který se skládá z blokové šifry používající 256, 192 nebo 128 bitový klíč a je považován za výrazně silnější než RC4. Aby bylo možné podporovat AES, musí být hardware bezdrátové sítě a podporující výpočetní zařízení schopna podporovat AES namísto tradičního šifrování WEP. Protokol MIC (Message Integrity Check) je implementován pro kontrolu integrity dat, který generuje 64 bitový kontrolní součet. Jestliže MIC detekuje dva chybné rámce v jedné minutě, je znovu klientské zařízení vráceno k bodu, kdy je potřeba povolit jeho přístup, vytváří se nové klíče. Když útočník zachytí šifrovanou zprávu, poté ji změní a vysílá datový paket. MIC pomáhá zabránit tomuto typu datového útoku přidáním pole MIC do příslušného rámce bezdrátové sítě. Tato funkce poskytuje kontrolu integrity. Pokud jsou rámce bezdrátovým přístupovým bodem přijaty mimo pořadí, jsou následně vyřazeny.

Předem byla zajištěná společná kompatibilita, aby mohly zabezpečení fungovat na stejném hardware a musel se pouze přehrát jejich firmware. WPA využívá stejnou proudovou šifru, která má 128 bitový klíč a inicializační vektor o velikosti 48 bitů [4],[12].

2.5.1 WPA2

WPA2 je bezpečnostní standard k ochraně počítačů, které jsou připojeny do bezdrátové sítě. Jeho účelem je dosáhnout úplného souladu se standarde 802.11i, které bylo jenom částečně dosaženo s WPA. Od roku 2006 byla WPA oficiálně nahrazena WPA2. Jednou z nejvýznamnějších změn mezi WPA a WPA2 je povinné používání algoritmů AES a zavedení protokolu CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) jako náhradou za TKIP. TKIP je však ve WPA2 stále zachován jako záložní systém a pro interoperabilitu s WPA.

V současné době je primární bezpečnostní zranitelnost systému WPA2 nejasná (a vyžaduje, aby útočník již měl přístup k zabezpečené síti Wi-Fi, aby získal přístup k určitým klíčům a poté udržoval útok proti jiným zařízením v síti), proto jsou bezpečnostní důsledky známých zranitelností WPA2 téměř zcela omezeny na podnikové sítě a zaslouží si jen malou či žádnou praktickou úvahu, pokud jde o zabezpečení domácí sítě.

Bohužel stejná zranitelnost, která je největší dírou v bezpečnosti WPA - vektor útoku prostřednictvím nastavení Wi-Fi Protected Setup (WPS) - zůstává v moderních přístupových bodech, podporujících WPA2 [4],[12].

2.5.2 WPA3

WPA3 je dosud nejnovější verzí bezpečnostního protokolu. Bylo vydáno v roce 2018. Nejvýznamnější rozšíření nového bezpečnostního protokolu je větší ochrana jednoduchých hesel, individualizované šifrování pro osobní a otevřené sítě a bezpečnější šifrování pro podnikové sítě. Spuštěním certifikačního programu Wi-Fi Alliance pro WPA3-Personal, který poskytuje individualizovanější šifrování a WPA3-Enterprise, který zvyšuje kryptografickou sílu pro sítě přenášející citlivá data. Spolu s těmito dvěma režimy nasazení představila aliance Wi-Fi také připojení Wi-Fi Easy Connected, což je funkce, která má zjednodušit proces spárování zařízení Wi-Fi bez displejů, jako např. IoT. Je to funkce, která se s velkou možností objeví u mnoha zařízení WPA3-Personal, která může nahradit nebo může být použita místo WPS. Volitelná funkce Wi-Fi Enhanced Open, která umožňuje bezproblémové šifrování v otevřených hotspotových sítích Wi-Fi. WPA3 poskytuje vylepšení v obecném šifrování Wi-Fi díky SAE (Simultaneous Authentication of Equals), která nahrazuje protokol PSK používanou v předchozích verzích WPA [16].

2.6 EAP

Extensible Authentication Protocol (EAP) je autentizační rámec, nikoli specifický autentizační mechanismus, který se často používá v bezdrátových sítích a point-to-point připojení. Protokol EAP je označován jako základ ve standardu 802.1X. Nejstarším typem dokumentu tohoto protokolu bylo RFC 2284, ze kterého vychází dokument s označením RFC 3748. V dnešní době je aktualizovaný dokument s označením RFC 5247. Poskytuje některé běžné funkce a vyjednávání metod autentizace nazývaných metody EAP. EAP je obecný protokol pro autentizaci, který také podporuje více metod autentizace, jako jsou tokenové karty, Kerberos, jednorázová hesla, certifikáty, autentizace pomocí veřejného klíče a smart karty. IEEE 802.1X určuje, jak by měl být protokol EAP zapouzdřen do rámců LAN. Protokol používaný mezi uživatelskou stanicí a autentizátorem nebo ověřovacím serverem. V současné době je definováno asi 40 různých metod.

V bezdrátové komunikaci používající protokol EAP si uživatel vyžádá připojení k síti WLAN prostřednictvím přístupového bodu, který poté vyžádá identitu uživatele a odešle tuto identitu na ověřovací server, jako je RADIUS. Server požádá AP o důkaz totožnosti, který AP získá od uživatele, a poté odešle zpět na server, aby dokončil ověření. Ověřování EAP je iniciováno serverem (autentizátorem), zatímco mnoho dalších ověřovacích protokolů je iniciováno klientem (peer).

Výměna ověřování EAP probíhá následovně:

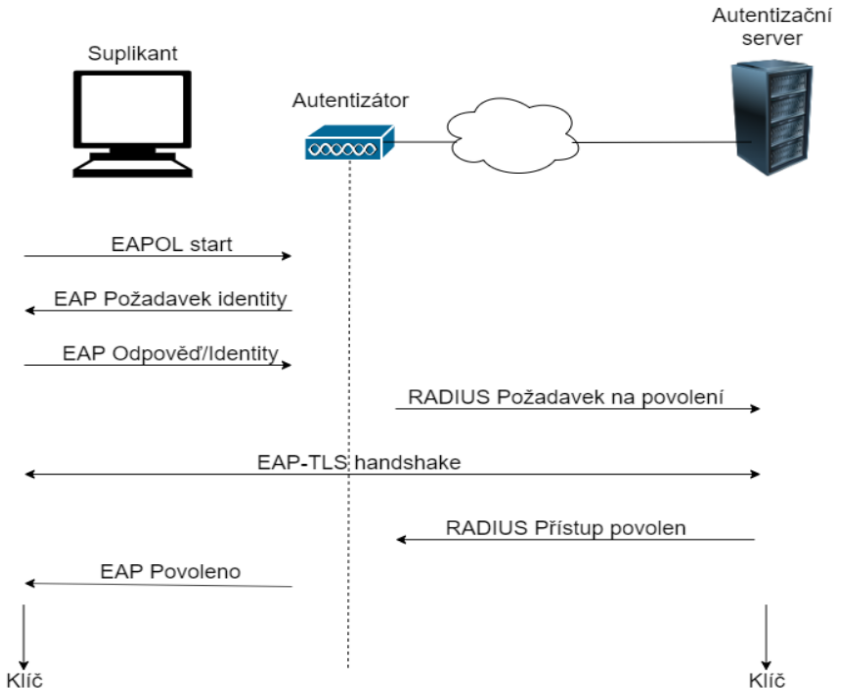
1) Ověřovatel (server) odešle požadavek na ověření peer (klienta).

2) Peer pošle paket Response jako odpověď na platnou žádost.

3) Ověřovatel odešle další paket požadavku a partner odpoví odpovědí. Pořadí žádostí a odpovědí pokračuje tak dlouho, jak je potřeba. Protokol EAP je protokolem „lock step“, takže nový požadavek nemůže být odeslán, než je původní požadavek, dříve, než obdrží platnou odpověď.

4) Konverzace pokračuje, dokud autentizátor nemůže autentizovat partnera (nepřijatelné odpovědi na jednu nebo více požadavků). V tomto případě musí implementace autentizátoru vyslat selhání EAP. Alternativně může ověřovací konverzace pokračovat, dokud autentizátor nezjistí, že došlo k úspěšné autentizaci. V tomto případě musí autentizátor vyslat úspěch EAP [17],[18].

Princip zasílání zpráv u EAP je znázorněn na obrázku 2.



Obrázek 2: Komunikace u EAP pomocí zasílání zpráv [19]

Struktura paketu EAP

- **Kód** (8 bitů) identifikuje typ paketu EAP, používá se k interpretaci datového pole paketu. Když má paket neplatnou hodnotu, je zahozen.
  Mohou se zde objevit tyto hodnoty – *Request, Response, Success, Failure.*
- **Identifikátor** (8 bitů) obsahuje celé číslo bez znaménka, které se používá k porovnávání požadavků s odpověďmi.
- **Délka** (16 bitů) definuje délku paketu EAP
- **Data** s proměnnou délkou pole. V závislosti na typu paketu může být datové pole dlouhé i 0 bajtů. Interpretace datového pole je založena na hodnotě pole Code [18],[20].

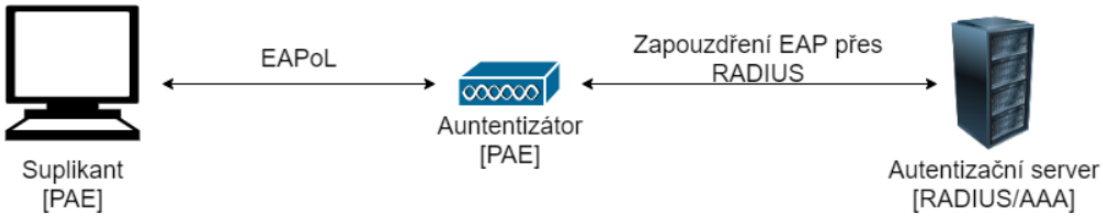
2.6.1 EAPoL

EAPoL (Extensible Authentication Protocol over LAN) je síťový port ověřovací protokol používaný v IEEE 802.1X vyvinutý pro poskytování obecného síťového přihlášení pro přístup k síťovým prostředkům.

EAPoL, podobně jako EAP, je jednoduché zapouzdření, které může běžet přes jakoukoli LAN. Stejné tři hlavní komponenty jsou definovány v EAP a EAPoL k provedení ověřovací konverzace. Obrázek ukazuje, jak jsou tyto komponenty LAN připojeny v kabelovém prostředí [21].

Hlavní komponenty:

- **Supplicant**: zařízení, které hledá přístup k síťovým prostředkům (PAE)
- **Authenticator**: řídí přístup k síti (PAE)
- **Authentication Server**: RADIUS server/AAA



Obrázek 3: Architektura EAPoL [22]

Z obrázku 3 je patrné, že komunikace pomocí EAPoL je pouze mezi zařízením, které se chce připojit do sítě a autentizátorem.

Bylo zde přidáno několik užitečných zpráv. Ne všechny typy rámců EAPoL jsou k přenášení zpráv EAP, ale některé jsou i pro provádění administrativních úkolů. Je definováno 5 typů EAPoL zpráv:

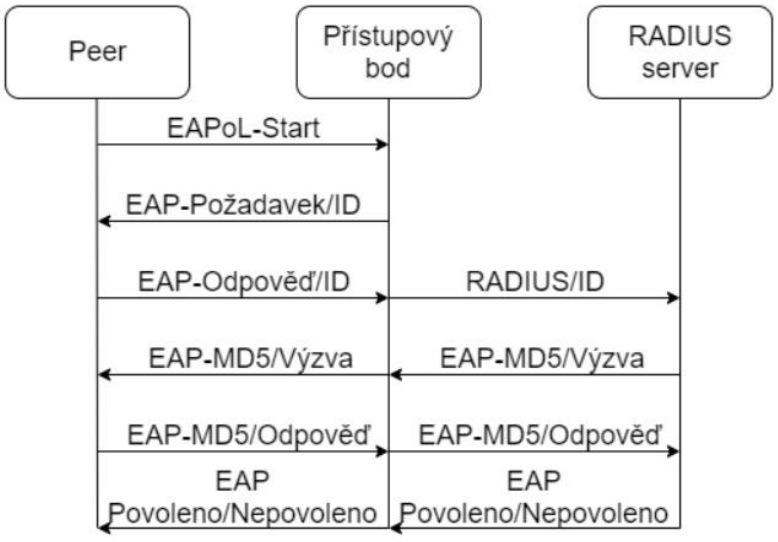
- **EAPoL-Start** slouží k ověření pro žadatele, zda je přítomen ověřoval a oznamuje, že je žadatel připraven.
- **EAPoP-Key** slouží k odeslání šifrovacích klíčů od ověřovatele (autentizátor) k žadateli (klient), jakmile je rozhodnuto o přijetí do sítě.
- **EAPoL-Packet** se používá pro odesílání zpráv EAP přes LAN.
- **EAPoL-Logoff** slouží k informování autentizátoru, že klient chce být odpojený od sítě. Poté se autentizátor opět nastaví do stavu, kdy je připravený na připojení dalšího klienta.
- **EAPoL-Encapsulated-ASF-Alert** slouží pro posílání upozornění prostřednictvím paketu [20].

2.6.2 EAP-MD5

EAP-MD5 je základní bezpečnostní metoda ve standardu EAP a jako přihlašovací údaje používá pouze uživatelské jméno a heslo. Heslo je zde přenášeno formou MD5 hashe (Mesage-Digesn algorithm). Definována je v RFC 3748. EAP-MD5 chrání výměnu zpráv vytvořením jedinečného „otisku prstu“, který digitálně podepíše každý paket, aby se zajistilo, že zprávy EAP jsou autentické. U metody EAP-MD5 se používá pro ověření klienta protokol CHAP (Challenge-Handshake Authentication Protocol). EAP-MD5 je velmi nízké zabezpečení a provádí své operace velmi rychle, což usnadňuje implementaci a konfiguraci.

EAP-MD5 nepoužívá žádné certifikáty PKI (Public Key Infrastructure) k ověření klienta ani k zajištění silného šifrování k ochraně ověřovacích zpráv mezi klientem a ověřovacím serverem a nepodporuje vytváření klíčů, které jsou nutné pro využití dynamického WEP, WPA nebo WPA2 pro zvýšení bezpečnosti. Také nepodporuje vzájemné ověřování mezi klientem a serverem. (PKI je systém procesů, technologií a zásad, který umožňuje šifrování a podepisování dat. Můžete vydávat digitální certifikáty, které ověřují totožnost uživatelů, zařízení nebo služeb. Tyto certifikáty vytvářejí zabezpečené připojení pro veřejné webové stránky i soukromé systémy). Díky tomu je ověřovací protokol EAP-MD5 citlivý na útoky hrubou silou, slovními útoky, odposlechem relací a útoky typu Man-in-the-Middle. EAP-MD5 je nejvhodnější pro výměnu zpráv EAP ve drátových sítích, kde je klient EAP přímo připojen k ověřovateli a šance na odposlech nebo zachycení zprávy jsou velmi nízké. Na obrázku 4 je popsán princip autentizace s EAP-MD5 [23].

Proces autentizace s použitím EAP-MD5

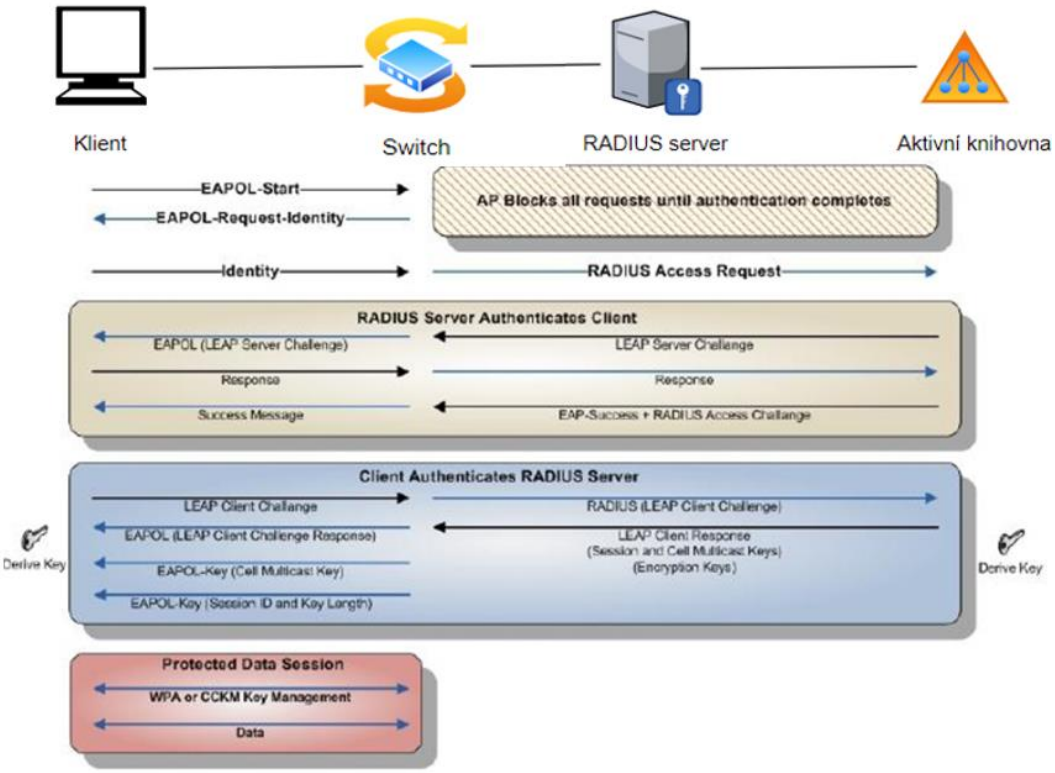


Obrázek 4: Proces autentizace s použitím EAP-MD5 [23]

2.6.3 EAP-LEAP

Koncem roku 2000 vytvořila společnost Cisco pro svou řadu přístupových bodů bezdrátové sítě LAN protokol EAP s názvem LEAP (Lightweight Extensible Authentication Protocol) jako způsob řešení bezpečnostních nedostatků ve WEP. LEAP umožňuje klientům častou autentizaci. Po každé úspěšné autentizaci získají klienti nový klíč WEP. Jedinou společnou vlastnost, kterou má s metodou MD5 zůstává autentizace použitím pouze uživatelského jména a hesla. Teoretickou slabostí LEAP byla už dobře známa od začátku, jelikož se v podstatě jedná o vylepšenou verzi EAP-MD5 s přidáním dynamického vytváření klíčů WEP a vzájemným ověřováním mezi bezdrátovým klientem a serverem RADIUS. LEAP může být nakonfigurován tak, aby používal TKIP místo dynamického WEP. Cisco LEAP, podobně jako WEP, má od roku 2003 známé bezpečnostní slabiny, které se týkají prolomení hesla offline. U metody EAP-MD5, kde se používal pro ověření klienta protokol CHAP (Challenge-Handshake Authentication Protocol).LEAP používá upravenou verzi MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) ověřovacího protokolu, který byl vydán společností Microsoft v roce 1998 v normě RFC 2433. U této verze bylo pouze podporováno ověření klienta oproti serveru, ale nepodporovala obousměrnou autentizaci. Tato možnost byla později doimplementována pro metodu LEAP společností Cisco. Tímto bylo prakticky docíleno odolnosti proti typu útoku Man-in-the-Middle.

LEAP je zásadně slabý, protože poskytuje nulovou odolnost proti offline slovníkovým útokům. Důvodem je to, že ochrana osobních údajů používaných pro ověřování bezdrátové sítě LAN závisí pouze na MS-CHAPv2. Výsledkem je, že tyto informace lze snadno kompromitovat pomocí nástroje s názvem ASLEAP, který byl publikován v roce 2004. Odpovědí společností Cisco na offline slovníkové útoky bylo vždy používat dostatečně silná a složitá hesla, avšak dnešní uživatelé používají průměrná nebo až podprůměrná hesla kvůli zapamatovatelnosti. Velkou slabinou je metoda posílání hesla pro proces ověření stejně jako u EAP-MD5. Nešifrované heslo je odesíláno prostřednictvím challenge a challenge-response řetězce. Když útočník zjistí generování řetězců, může pomocí slovníkového útoku toto heslo odhalit.[24] Na obrázku 5 je vidět posílání zpráv v EAP-LEAP [24].



Obrázek 5: Proces autentizace s použitím EAP-LEAP [25]

2.6.4 EAP-FAST

S cílem poskytnout průmyslu vhodnou náhradu k překonání nedostatků zjištěných u LEAP bylo společností Cisco vyvinuto EAP-FAST (Flexible Authentication via Secure Tunneling), také známý jako flexibilní autentizace pomocí zabezpečeného tunelování. Metoda byla ratifikována organizací IETF v roce 2007 s rámci RFC 4851. Používá se v bezdrátových sítích a point-to-point připojení k provádění autentizace relace. Protokol byl vytvořen, aby pomohl udržet snadnou implementaci, díky kterému se stal LEAP populárním a zároveň se zaměřil na slabiny zabezpečení spojené s LEAP, zejména při používání „slabých“ hesel. EAP-FAST, který se stal nástupcem LEAP umožňuje volitelné použití slabých stránek zabezpečení a také využívá PAC (Protected Access Credential) k vytvoření tunelu TLS (Transport Layer Security). Tunel se následně používá k ověření pověření klienta, kde není nutné použití certifikátu. Protokol lze nainstalovat do počítače se systémem Windows instalací modulu EAP-FAST poskytovaného společností Cisco a má nativní podporu v OS X počínaje verzí OS 10.4.8 a novější [24].

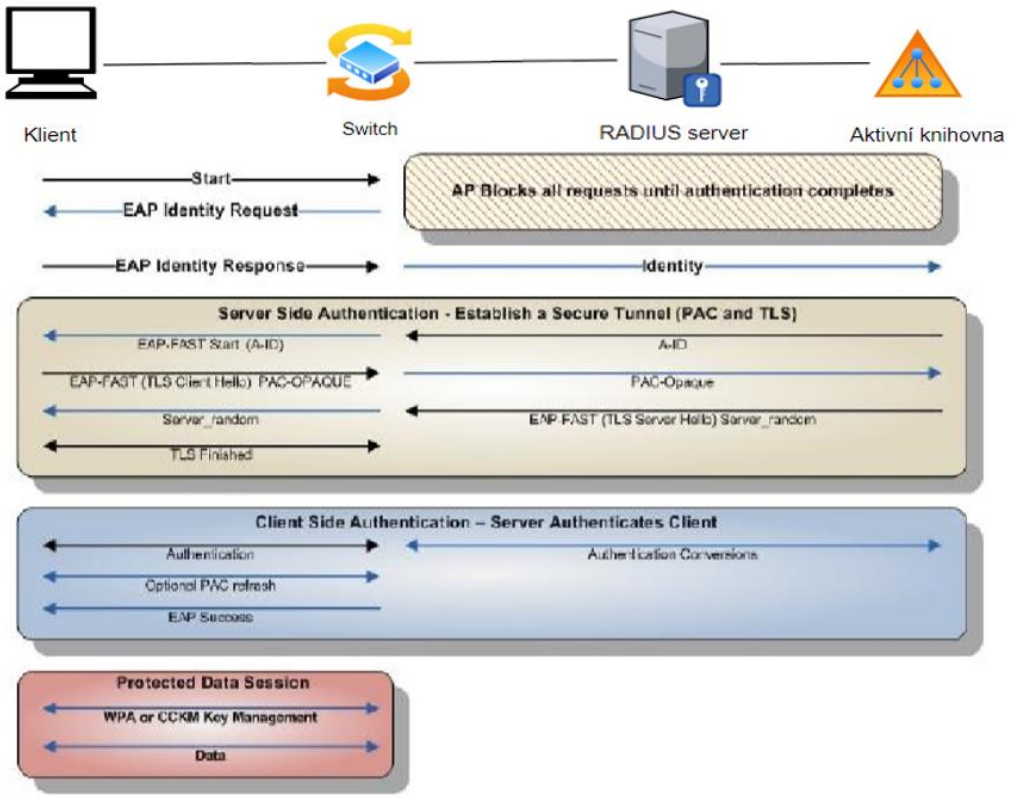
Protokol EAP-FAST pracuje ve třech fázích:

Fáze 0: (Přenos PAC klíče) Ve fázi 0 protokol používá ADHP (Authenticated Diffie-Hellman Protocol) ke sdílení klíče, které bude použito během zabezpečené komunikace fáze 1. Tento aspekt protokolu eliminuje potřebu zřídit primární nebo hlavní klíč pokaždé, když si klient přeje připojení k síti. Tato fáze je také označována PAC provisioning. Fáze nemusí být implementována a může být přeskočena, jestliže je klíč poslán manuálně.

Fáze 1: (Vytvoření tunelu) Během fáze 1 se protokol ověřuje pomocí PAC (Protected Access Credentials). Mezi klientem a serverem RADIUS dojde k vytvoření přímého Point-to-Point spojení s absencí autentizátoru (např. pomocí AP). Každému uživateli je při vytvoření tunelu vytvořen i unikátní klíč (PAC), který je vytvořen právě na serveru RADIUS. Tím je zajištěno, že během fáze 2 bude zachována integrita připojení i důvěrnost.

Fáze 2: (Ověřování). V této fázi protokol oboustranně autentizuje peer výměnou přihlašovacích údajů přes TLS tunel, který se vytvořil v 1. fázi s použitím metody MS-CHAPv2. Protokol lze implementovat bez použití souborů PAC a poté jednoduše použít TLS (Transport Layer Security) [3].

Díky TLS tunelu je metoda EAP-FAST odolná proti Man-in-the-Middle útokům. Metoda také odolává slovníkovým útokům, jelikož je přenos hesel zabezpečen. Proces zasílání zpráv u EAP-FAST je na obrázku 6.



Obrázek 6: Proces autentizace s použitím EAP-FAST [25]

2.6.5 EAP-PEAP

PEAP (Protected Extensible Authentication Protocol) je verze EAP, ověřovacího protokolu používaného v bezdrátových sítích a Point-to-Point připojení. Byla vyvinuta společnostmi Microsoft, Cisco Systems a RSA Security v roce 2002. Jejím hlavním úkolem bylo odstranění dosavadních trhlin v zabezpečovacích protokolech, které doposud byly požívány. U této metody je také kladen velký důraz na jednoduchost implementace a rozšiřitelnost. Protokol PEAP je navržen tak, aby poskytoval bezpečnější autentizaci pro sítě WLAN 802.11, které podporují řízení přístupu k portům 802.1X.

Tento protokol zapouzdřuje protokol EAP do TLS (Transport Layer Security) šifrovaného a ověřovacího tunelu. PEAP ověřuje server pomocí certifikátu veřejného klíče a provádí ověřování v zabezpečené relaci TLS (Transport Layer Security), přes kterou se mohou uživatelé WLAN, WLAN stanice a ověřovací server autentizovat sami. Pro vytvoření TLS tunelu stačí pouze certifikát, který je na straně serveru. Každá stanice má samostatný šifrovací klíč. Při použití ve spojení s protokolem TKIP má každý klíč omezenou životnost. PEAP je produkt, který byl dodáván s hlavními operačními systémy, jako je Microsoft Windows XP.

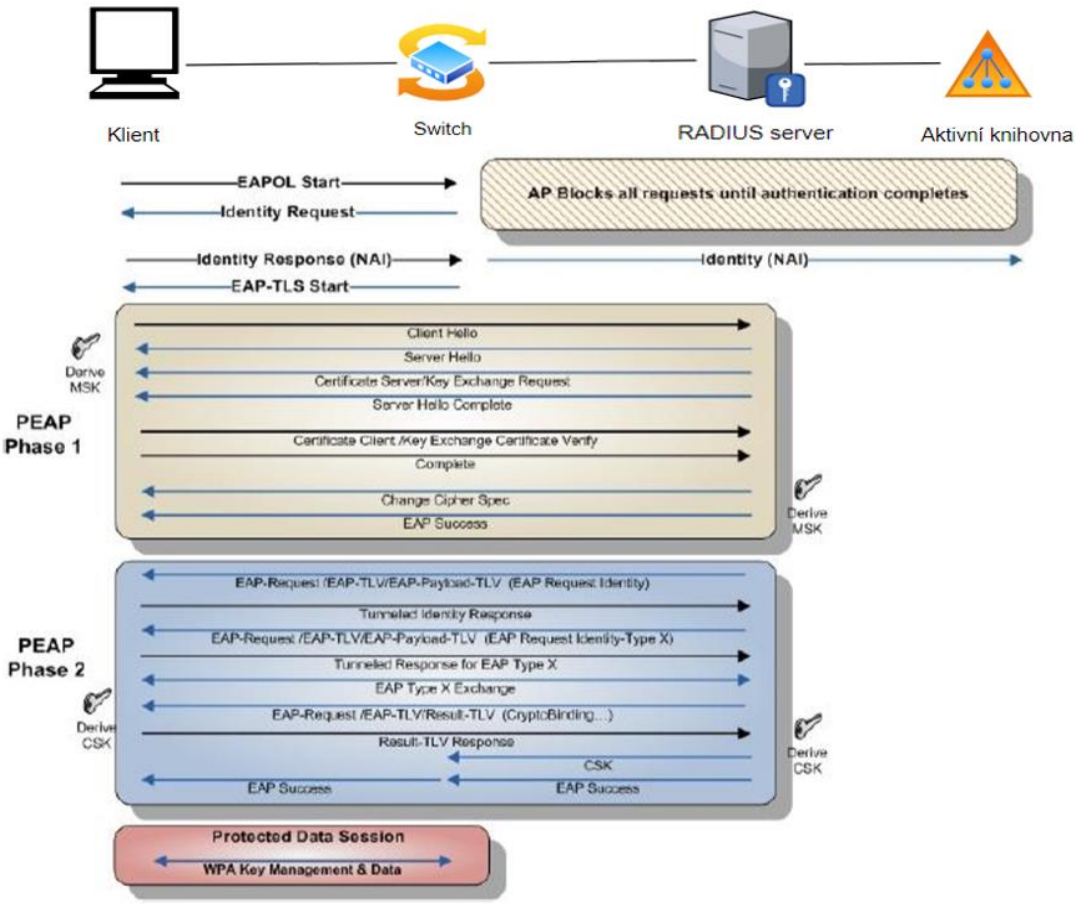
EAP-PEAP nespecifikuje žádné metody pro proces autentizace, tudíž řeší pouze vnější zabezpečení a vnitřní závisí na mechanismech, které jsou implementovány [3],[24],[26].

Nejvíce používanými autentizačními mechanismy jsou metody:

EAP-PEAPv0 (EAP-MSCHAPv2)

EAP-PEAPv1 (EAP-GTC)

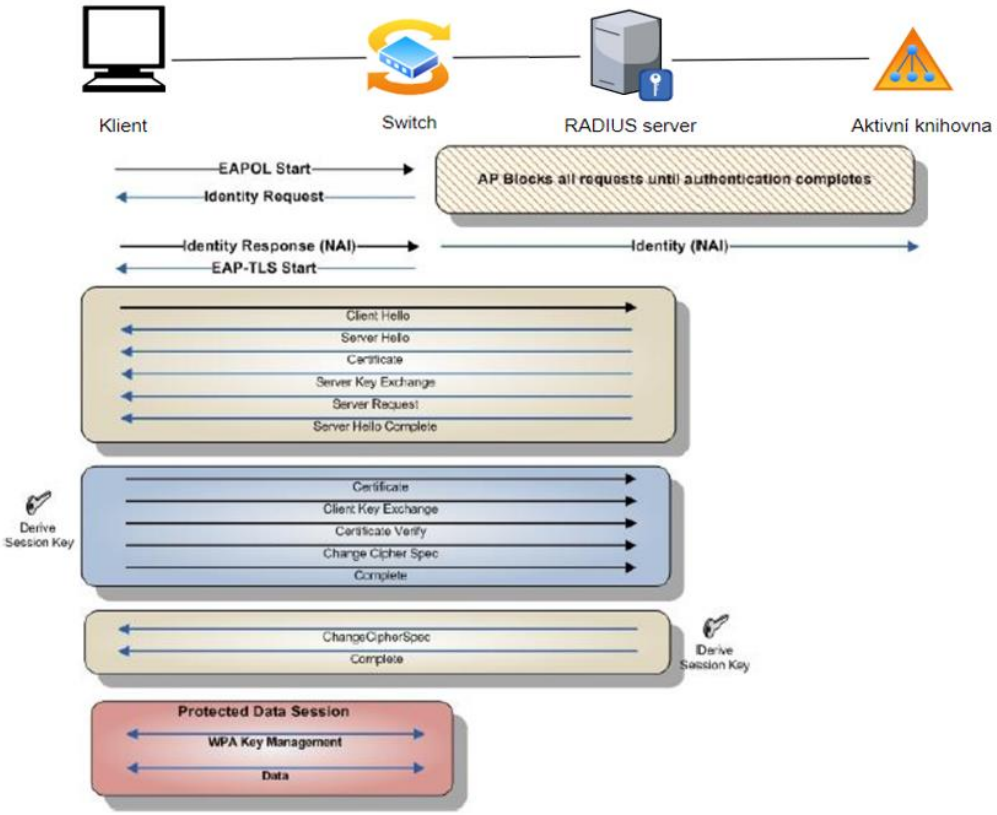
Proces zasílání zpráv u EAP-PEAP je uvedený na obrázku 7.



Obrázek 7: Proces autentizace s použitím EAP-PEAP [25]

2.6.6 EAP-TLS

Tato metoda EAP-TLS (EAP-Transport Layer Security) je popsána v RFC 5216. EAP-TLS je stále považován za jeden z nejbezpečnějších dostupných standardů EAP pro bezdrátové sítě, které používají kódování TLS mezi klientem a serverem RADIUS. Tím je vysoce podporována všemi výrobci hardwaru a softwaru pro bezdrátové LAN. Při implementaci EAP-TLS se zakládá na společné autentizaci klienta a serveru RADIUS pomocí certifikátu X.509. Použití certifikátu je v tomto případě povinné, jelikož nahrazuje ověření pomocí uživatelského jména a hesla. Tímto jsou ovlivněny vyšší náklady na vytvoření infrastruktury. Na autentizačním serveru je uložen serverový certifikát, na klientské straně může být certifikát uložen na čipové kartě, v registru nebo v souborovém systému. Metoda je odolná proti útoku typu Man-in-the-Middle a dynamického obnovení šifrovacích klíčů. Metoda EAP-TLS a EAP-PEAP jsou nejvíce používané pro ověřovací procesy, jelikož jsou podporovány na všech operačních systémech [3],[24],[27]. Proces zasílání zpráv EAP-TLS je uveden na obrázku 8.

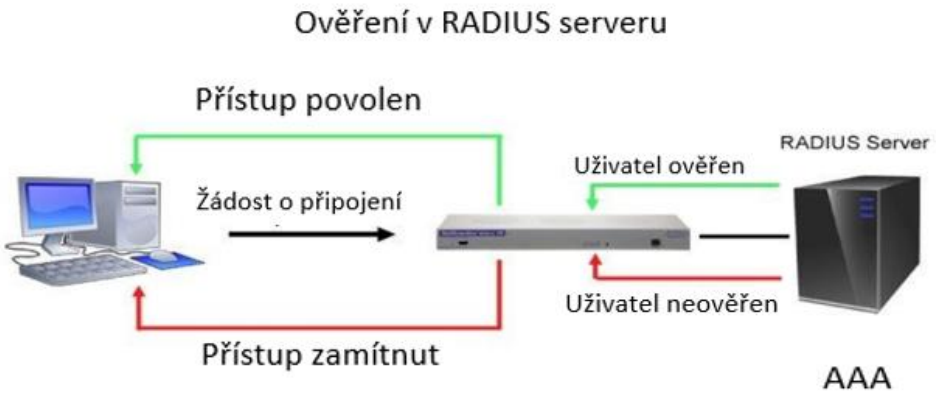


Obrázek 8: Proces autentizace pomocí EAP-TLS [25]

3 RADIUS SERVER

RADIUS (Remote Authentication Dial-In User Service) je protokol, který byl původně navržen tak, aby autentizoval vzdálené uživatele k serveru pro telefonický přístup. RADIUS, vytvořený společností Livingston, je průmyslovým standardem používaným mnoha společnostmi, které vyrábí síťové produkty a je navrhovaným standardem IETF (Internet Engineering Task Force). Standard IEEE, pod kterým je RADIUS uznán z pohledu specifikace je RFC 2865 a z pohledu účtování v RFC 2866. RADIUS se nyní používá v celé řadě procesů autentizace. Je to protokol klient-server a software, který umožňuje serverům vzdáleného přístupu komunikovat s centrálním serverem, aby mohl ověřovat uživatele dial-in a autorizoval jejich přístup k požadovanému systému nebo službě. RADIUS také dokáže udržovat uživatelské profily v centrální databázi, kterou mohou sdílet všechny vzdálené servery. Když se uživatel pokusí ověřit, zařízení odešle zprávu serveru RADIUS. Pokud je server RADIUS správně nakonfigurován tak, aby měl zařízení jako klienta, RADIUS odešle zprávu o přijetí nebo odmítnutí zpět do zařízení (server síťového přístupu), jak je znázorněno na obrázku 9. Při vydání požadavku uživatelem na autentizaci je klientem vytvořen požadavek na přístup, který obsahuje jméno, heslo a číslo portu, na kterém probíhá připojení. Požadavek je odeslán na server. Jestliže odpověď nepřijde do určeného času, je požadavek opakován.

Jeho nejzásadnější vlastností je velmi vysoké síťové zabezpečení, protože komunikační transakce mezi uživatelem a RADIUS serverem jsou zprostředkována pomocí sdíleného tajemství. Sdílené tajemství není posíláno po síti, po síti jsou pouze posílána uživatelská hesla v zašifrované podobě [28],[29],[30],[31].



Obrázek 9: Povolení nebo odmítnutí ze strany serveru síťového přístupu [28]

3.1 Switch

Switch (přepínač) je zařízení, které funguje jako přepínač propojující více zařízení ve stejné síti. Umožňuje sdílet informace mezi propojenými zařízeními, které spolu hovoří. Dají se rozdělit na dvě skupiny, na nespravované a spravované switche. Nespravovaný switch pracuje tak, abychom se mohli jednoduše připojit bez nutnosti konfigurace. Bývají obvykle implementována pro základní připojení. Často se používají v domácnostech, laboratořích nebo v konferenčních místnostech. Spravovaný switch poskytuje lepší zabezpečení, více funkcí a flexibility, jelikož jsou konfigurovatelné, tak jak potřebujeme v naší síti. Ethernetový switch, používaný ve spojení s kompatibilním ověřovacím serverem RADIUS, ve své roli autentizátoru umožní přístup k jeho portům (a následně k síti), jakmile zařízení (žadatel) je úspěšně autentizováno pomocí RADIUS server [32].

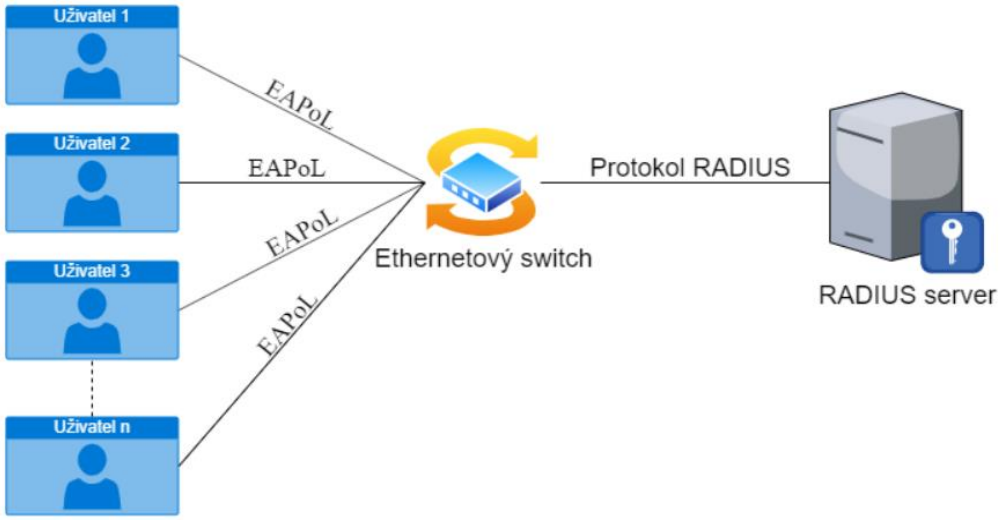
3.2 Autentizace 802.1X s využitím Ethernetového switche

802.1X je standard IEEE pro řízení přístupu k síti pomocí portu PNAC (Port based Network Access Control). Poskytuje mechanismus ověřování pro zařízení, která se snaží o přístup k síti LAN. Funkce ověřování 802.1X na přepínači je založena na standardu IEEE 802.1X standardního řízení přístupu na základě portů.

Komunikačním protokolem mezi koncovým zařízením a přepínačem je Extensible Authentication Protocol over LAN (EAPoL). EAPoL je verze EAP navržená pro práci se sítěmi Ethernet. Komunikačním protokolem mezi ověřovacím serverem a

přepínačem je RADIUS. Zapojení je na obrázku 10.

Během procesu ověřování přepínač dokončí několik výměn zpráv mezi koncovým zařízením a ověřovacím serverem. Zatímco probíhá ověřování 802.1X, může síť přenášet pouze přenos 802.1X a řízení provozu na síti. Ve vrstvě datového propojení je blokován další provoz, například provoz DHCP a HTTP.



Obrázek 10: Princip autentizace 802.1X s Ethernetovým switchem [33]

Supplicant (také nazýván koncové zařízení/uživatel) požaduje připojení k síti. Koncové zařízení je podporováno standardem 802.1X a poskytuje ověřovací údaje pomocí protokolu EAP. Požadovaná pověření závisí na použité verzi EAP - konkrétně na uživatelském jménu a hesle pro EAP-MD5 nebo uživatelském jménu a klientských certifikátech pro zabezpečení autentizace pomocí protokolu Transport Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP- TTLS) a Chráněné EAP (PEAP). Server VLAN můžeme nakonfigurovat pro odmítnutí serveru tak, aby poskytoval omezený přístup k LAN pro koncová zařízení, která odeslala nesprávné ověření. Poté server LAN může těmto koncovým zařízením poskytnou pouze připojení k internetu.

Authenticator port access entity (Subjekt pro přístup k portu autentizátoru) je termín pro ověřovatele. Přepínač je autentizátor a řídí přístup blokováním veškerého provozu do koncových zařízení, dokud nedojde k jejich autentizaci.

Authentication server (Autentizační server) obsahuje databázi, podle které provádí autentizační rozhodnutí. Pro každé koncové zařízení obsahuje informace o pověření, kam se daný klient může připojit. Ověřovatel předá přihlašovací údaje od koncového zařízení autentizačnímu serveru. Jestliže jsou informace shodné s informacemi, které jsou v databázi autentizačního serveru, přístup je povolen. V případě neshody je přístup odepřen [33].

Princip autentizace:

1. Koncové zařízení inicializuje autentizační přístup do Ethernetového switche.
2. Ethernetový switch pošle výzvu koncovému zařízení o přihlašovací ID a heslo.
3. Koncové zařízení odešle odpověď.
4. RADIUS klient odešle přihlašovací ID a zašifrovaní heslo na RADIUS server.
5. RADIUS server odpoví Accept, Reject, nebo Challenge.

[34]

3.3 Virtuální servery

RADIUS server pracuje s centrální databází klientů k jejich autentizaci do sítě. RADIUS server pracuje jako protokol typu klient-server, v případě přístupu ověřuje každého uživatele, který se chce připojit k síti pomocí jedinečného šifrovacího klíče. Mezi největší schopnosti RADIUS serveru patří schopnost AAA- ověřování, autentizace a účetnictví. AAA server oplývá zvýšenou bezpečností a efektivitou. RADIUS servery jsou používány v každé firmě na rozdělení jednotlivých uživatelů, podle toho k čemu jsou pověření (síť pro účetnictví, správu systému, ředitele, atd.) [34].

3.3.1 TekRADIUS pro systém Windows

TekRADIUS je sada serverů určena pro zařízení s windows a jedná se o bezplatnou verzi, avšak dají se i dokoupit různá rozšíření. TekRADIUS je určen v RFC 2865 a RFC 2866. což uživatelům umožňuje protokolovat podrobnosti relace do souboru protokolu a omezit počet současných relací. TekRADIUS podporuje RFC 2868 pro podporu tunelových protokolů a také RFC 3079 pro odvozování klíčů s Microsoft point-to-point šifrováním. Uživatelé mohou ověřovat a autorizovat připojení PPTP(Point-to-Point Tunneling Protocol) nebo L2TP(Layer 2 Tunnel Protocol) [35].

3.3.2 FreeRADIUS

FreeRADIUS byl založen v červnu roku 1999 Miquelem van Smoorenburgerem a Alanem DeKokem. První veřejné vydání kódu bylo v srpnu roku 1999, další verze v květnu 2001. Od tohoto roku jsou vydávány nové verze v rámci několika měsíců. Jedná se o jeden s největších serverů, který používá každý den přes 100 milionů lidí po celém světě pro připojení k internetu. Je používán přes 50 tisíci weby. Jeho hrubý odhad je, že FreeRADIUS používá více než 1/3 uživatelů na internetu. Od svého vzniku se rozšířili o několik další produktů např. freeradius-client A BSD licensed RADIUS client library nebo mod_auth_radius A RADIUS module pro Apache [36].

3.3.3 RADL RADIUS

Tento RADIUS server je bezplatný a používá se pro testování a vyhodnocování. Umožňuje propojení přístupových zařízení se serverem RADIUS ke kontrole přístupu uživatelů. Protokol RADIUS používá zprávy typu UDP (User Datagram Protocol) na portu 1812 pro ověřovací zprávy RADIUS a port 1813 pro účetní zprávy RADIUS [37].

3.3.4 BSDRADIUS

Tento server je určený především k použití ve VOIP (voice over IP). Měl by být schopný využít požadavky AAA v periodicky krátkých časových intervalech. Je celý napsán v Pythonu. BDSRADIUS využívá knihovnu pyrad pro operace, jako je analýza slovníkových atributů, vytváření autorizačních a účetních paketů. Primárně je použitelný na Linuxu [38].

3.3.5 JRADIUS

Jedná se o server Java s názvem modulu rlm_jradius, který je zabudovaný do serveru FreeRADIUS. Modul pomocí sdružených připojení k serveru JRADIUS předává požadavky RADIUS a pakety odpovědí JRADIUS pro kterýkoli ze vstupních bodů modulu FreeRADIUS. To znamená, že obsahuje žádosti o ověření, účtování nebo proxy server JRADIUS [39].

3.3.6 Zaniklé virtuální servery

V dnešní době už zaniklé virtuální servery RADIUS.

Cistron RADIUS
IC-RADIUS
GNU RADIUS
Lucent RADIUS
OpenRADIUS
XtRADIUS
[40]

3.3.7 Výběr virtuálního serveru

Virtuálního serveru byl vybrán podle obtížnosti implementace a možnosti rozšíření. Jedním z nejrozšířenějších virtuálních serverů je FreeRADIUS, který byl také použit ve zkušební verzi implementace s pomocí nástroje VMware workstation player, kde běží Ubuntu 19.10 mimo laboratoř v domácích podmínkách.

3.4 Praktická část bakalářské práce

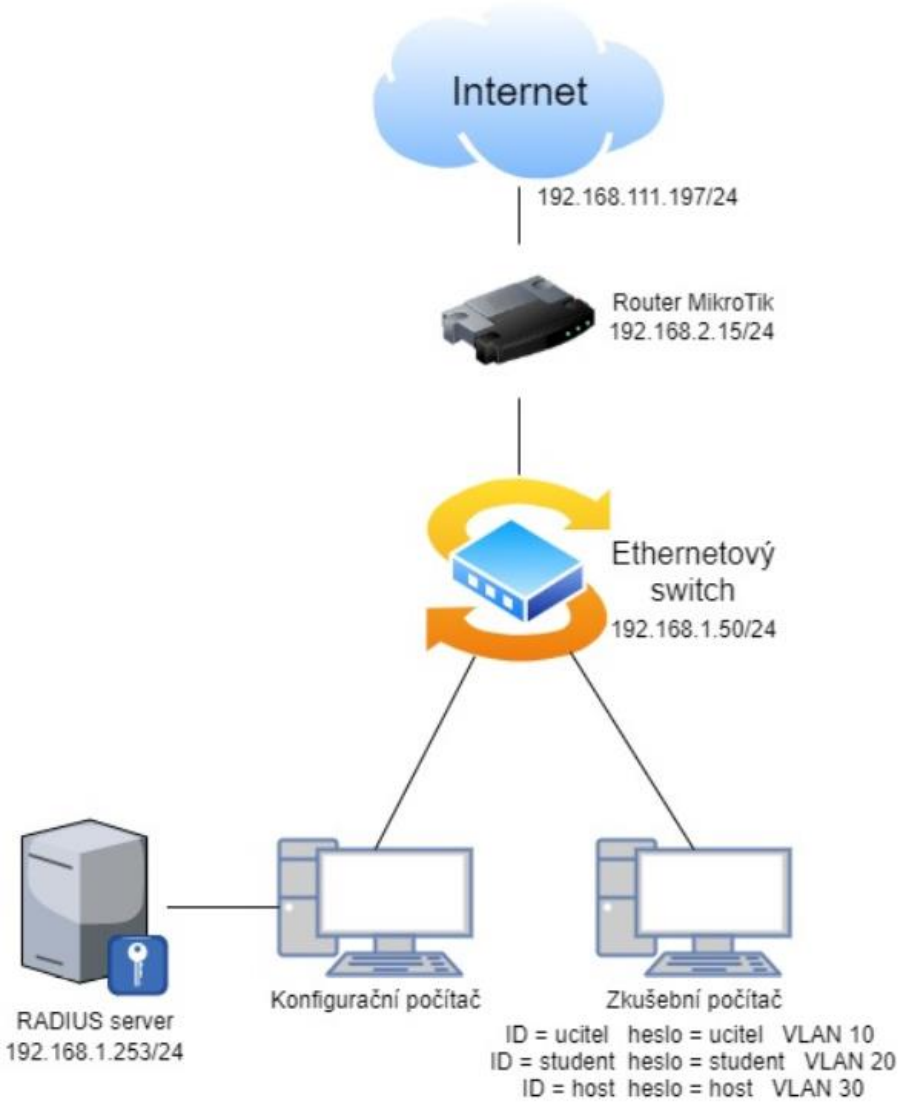
Tato část bakalářské práce se bude zaobírat zapojením, konfigurováním a odzkoušením praktické části a následně vytvoření vzorové laboratorní úlohy.

3.4.1 Princip fungování zkušebního stanoviště

Zapojení je sestaveno ze dvou počítačů, ethernetového switche a routeru MikroTik. Konkrétní zapojení je zobrazeno na obrázku č.11. Po konfiguraci se připojí zkušební počítač do switche (v tomto případě na port 3). Na zkušebním počítači vyskočí okno pro zadání přihlašovacích údajů. Přihlašovací údaje jsou jiné do každé konkrétní VLANy. Při správném zadání přihlašovacích údajů je uživatel autentizován a je připojen do VLANy, do které chtěl. Ověření, že je ve správné VLANě si může ověřit v cmd pomocí příkazu `ipconfig`. Přidělování IP adres do VLAN je voleno tak, aby bylo připojení na první pohled zřejmé. Úspěšná nebo neúspěšná autentizace je ověřena v programu WireShark a logu FreeRADIUSu.

3.4.2 Zapojení topologie sítě

Topologie sítě pro zkušební účely na obrázku 11. Na konfigurační počítači běží virtuální prostředí Ubuntu verze 19.10, kde je implementovaný RADIUS server. Počítač je současně zapojený do ethernetového switche pro jeho konfiguraci. Zkušební počítač, kterým je ověřena funkčnost celé topologie, je zapojen do ethernetového switche. Popis jednotlivých portů je popsaný níže v kapitole konfigurace CISCO switche.



Obrázek 11: Topologie testované sítě

3.5 Konfigurace FreeRADIUS serveru

Prostředí, kde běží FreeRADIUS server je Ubuntu 19.10.

3.5.1 Nastavení clienta

Client je zařízení, které slouží pro připojení uživatele do sítě. Například client může být konfigurovatelný switch nebo AP. V tomto případě máme zapojený konfigurovatelný ethernetový switch, který zasílá požadavky o autentizaci uživatele na RADIUS server, ten mu následně odpovídá, zda došlo ke shodě s ID a heslem, které jsou uloženy v konfiguračním souboru users. Nastavení clienta [41]:

```
client cisco-switch {
      ipv4addr   = 192.168.1.50/24
      secret     = cisco
      nastype    = cisco
}
```

Vysvětlení atributů

- cisco-switch – název klienta
- ipv4addr – IP adresa klienta
- secret – sdílené heslo pro komunikaci mezi RADIUS serverem a klientem/NAS
- nastype - používá ke sdělování skriptu checkrad.pl

3.5.2 Nastavení users

Uživatelé, které chceme, aby se mohli autentizovat do sítě, vytvoříme v konfiguračním souboru users. Princip spočívá v tom, že po zadání ID a hesla pošle switch zprávu na RADIUS server, tam je konfigurační soubor users projetý od shora dolů, v případě shody je poslána zpráva zpět na switch a dochází k autentizaci uživatele.

Pro zkušební účely byly vytvořeni tři uživatelé, kteří se připojují do různých VLAN podle jejich přihlašovacích údajů. Nastavení users [41]:

```
ucitel   Cleartext-Password := „ucitel“
         Tunnel-Type                = VLAN,
         Tunnel-Medium-Type         = IEEE-802,
         Tunnel-Private-Group-ID    = 10


student  Cleartext-Password := „student“
         Tunnel-Type                = VLAN,
         Tunnel-Medium-Type         = IEEE-802,
         Tunnel-Private-Group-ID    = 20


  host   Cleartext-Password := „host“
         Tunnel-Type                = VLAN,
         Tunnel-Medium-Type         = IEEE-802,
         Tunnel-Private-Group-ID    = 30
```

Vysvětlení atributů

- -ucitel – ID uživatele
- „ucitel“ – heslo uživatele (bez uvozovek)
- Tunnel-Type (VLAN) – tento atribut označuje tunelové protokoly, které mají být použity
- Tunnel-Medium-Type (IEEE-802) - označuje, které transportní médium
- použít při vytváření tunelu
- Tunnel-Private-Group-ID (10) – označuje ID VLANy, do které má být uživatel připojen

3.5.3 Nastavení peap a ttls zpráv

V konfiguračním souboru eap.conf je potřeba nastavit use_tunneled_reply na „yes“ u zpráv typu PEAP aTTLS. Při spuštění motod tunelu EAP chybí AVP odpověď. Pokud nastavíte u EAP „use_tunnelled_reply = yes“, znamená to, že v odpovědi by mělo být použito uživatelské jméno z tunelové odpovědi. Tím budou použity atributy pro konečný přístup Access-Accept. Tunelovaná relace EAP potřebuje výchozí typ EAP, který je oddělený od typu pro netunulovaný modul EAP. V tunelu PEAP je doporučeno používat MS-CHAPv2, protože jde o výchozí typ podporovaný klienty Windows.

Atributy odpovědi odeslané do NAS jsou obvykle založeny na jménu uživatele „mimo“ tunelu (obvykle „anonymní“). Pokud chcete poslat atributy odpovědi na základě uživatelského jména uvnitř tunelu, nastavte TTLS konfigurační záznam use_tunneled_reply = yes a odpověď do NAS bude převzata z odpovědi na tunelovaný požadavek. Tím budou použity atributy pro konečný přístup Access-Accept [41]:

```
ttls {
      tls = tls-common
      default_eap_type = md5
      copy_request_to_tunnel = no
      use_tunneled_reply = yes
      virtual_server = "inner-tunnel"
}

peap{
      tls = tls-common
      default_eap_type = mschapv2
      copy_request_to_tunnel = no
      use_tunneled_reply = yes
      virtual_server = "inner-tunnel"
}
```

3.5.4 Nastavení Logování zpráv (accept a reject)

Pro logování zpráv je potřeba nastavit v souboru radiusd.conf tyto hodnoty. Cesta do tohoto souboru vede přes etc/freeradius/3.0/radius.conf. Logování se ukládá do složky var/log/freeradius/radius.log [41]:.

```
Log {
      destination = files
      colourise = yes
      file = ${logdir}/radius.log
      syslog_facility = deamon
      stripped_names = no
      auth = yes
      auth_accept = yes
      auth_reject = yes
}
```

3.6 Konfigurace CISCO switche

Ethernetový switch je značky CISCO. V tomto případě je ethernetový switch použit ke komunikaci s nakonfigurovaným routerem MikroTik a RADIUS serverem. Do eth. switche jsou také připojováni uživatelé, kteří se chtějí připojit do vytvořených VLANek. Switch je nakonfigurován do základního nastavení a povolení služby RADIUS. Základní konfigurace tohoto switche spočívá v nastavení IP adresy na VLAN 1 (defaultní VLAN) a defaultní brány, která je potřeba, abychom se mohli připojit a mohli konfigurovat switch. Připojení je zprostředkováno programem Putty s komunikací typu Telnet nebo SSH. Jestliže se chceme ke switchi přihlásit, musí být ve stejném IP rozsahu, jako je konfigurační počítat (v tomto případě 192.168.1.x/24).

Na switchi jsou nastavené přihlašovací údaje, aby nedocházelo k úpravám od neoprávněných osob. Dále jsou na switchi nastaveny VLANy, do kterých se autentizuje uživatel, při zadání správného ID a hesla. Pro komunikaci mezi switchem a routerem MikroTik je nastaven trunk. Trunk je využívám k propojení switche s dalšími switchi nebo v tomto případě k propojení s aktivním prvkem (routrem).

Poslední část konfigurace je komunikace s RADIUS serverem.

Nastavené VLANy

```
interface Vlan1
 ip address 192.168.1.50 255.255.255.0
 ip default-gateway 192.168.1.15
 ip route 0.0.0.0 0.0.0.0 192.168.1.254

vlan 10
 name ucitel
!
vlan 20
 name student
!
vlan 30
 name host
```

Nastavení ID a hesla pro přístup do switche

```
Username admin privilege 15 secret 5 $1$j28O$UVfcbZDo0WKLFF/FX7P0D.
```

Povolení služby RADIUS

```
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Nastavení komunikace s RADIUS serverem

```
radius-server host 192.168.1.253 auth-port 1812 acct-port 1813 key cisco
```

Nastavení portů

Port 3 – port pro připojení zkušebního počítače

```
interface FastEthernet0/3
 switchport mode access
dot1x pae authenticator
 dot1x port-control auto
dot1x host-mode multi-host
dot1x violation-mode protect
 dot1x reauthentication
```

Samozřejmě lze takto nastavit více portů, kromě komunikačního portu s routerem a konfiguračního portu.

Port 23 – port pro komunikaci s konfiguračním počítačem (port je pouze nastaven jako access)

```
interface FastEthernet0/23
 switchport mode access
```

Port 24 – port nakonfigurovaný jako trunk

```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
```

3.7 Konfigurace routeru MikroTik

Pro tuto laboratorní úlohu byl vybrán MikroTik hAP lite, který je snadno dostupný a pro tuto laboratorní úlohu je naprosto dostačující. MikroTik je nastavený v základní konfiguraci, kde jsou nastaveny jednotlivé VLANy, jejich IP adresy, DHCP servery a NAT pro přístup k internetu. Na portu 1 je připojení do domácí sítě a na portu 2 je všechna komunikace se switchem (trunk). Pro snadnější konfiguraci mezi Routerem MikroTik, switchem CISCO a konfiguračním počítačem, je na portu 3 a 4 nastaven Bridge. Na routeru MikroTik hAP lite, na kterém je tato laboratorní úloha připravena,

vypadá konkrétní nastavení takto:

Nastavení VLAN

```
/interface vlan
add interface=ether2 name="Host(vlan30)" vlan-id=30
add interface=ether2 name="Student(vlan20)" vlan-id=20
add interface=ether2 name="Ucitel(vlan10)" vlan-id=10
```

Nastavení IP adres

```
/ip address
add address=192.168.2.15/24 interface=ether2 network=192.168.2.0
add address=10.10.10.1/24 interface="Ucitel(vlan10)" network=10.10.10.0
add address=10.10.20.1/24 interface="Student(vlan20)" network=10.10.20.0
add address=10.10.30.1/24 interface="Host(vlan30)" network=10.10.30.0
add address=192.168.1.14/24 interface="bridge(3+4)" network=192.168.1.0
```

Nastavení DHCP serveru

```
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface="Ucitel(vlan10)" name=dhcp1
add address-pool=dhcp_pool1 disabled=no interface="Student(vlan20)" name=dhcp2
add address-pool=dhcp_pool2 disabled=no interface="Host(vlan30)" name=dhcp3
add address-pool=dhcp_pool4 disabled=no interface="bridge(3+4)" name=dhcp4
/ip dhcp-server network
add address=10.10.10.0/24 gateway=10.10.10.1
add address=10.10.20.0/24 gateway=10.10.20.1
add address=10.10.30.0/24 gateway=10.10.30.1
add address=192.168.1.0/24 gateway=192.168.1.15
/ip pool
add name=dhcp_pool0 ranges=10.10.10.2-10.10.10.254
add name=dhcp_pool1 ranges=10.10.20.2-10.10.20.254
add name=dhcp_pool2 ranges=10.10.30.2-10.10.30.254
add name=dhcp_pool4 ranges=192.168.1.16-192.168.1.254
```

Nastavení DHCP klienta na ethernet 1

Nastavení Bridge

```
/interface bridge
add name="bridge(3+4)"
/interface bridge port
add bridge="bridge(3+4)" interface=ether3
add bridge="bridge(3+4)" interface=ether4
```

Nastavení NAT

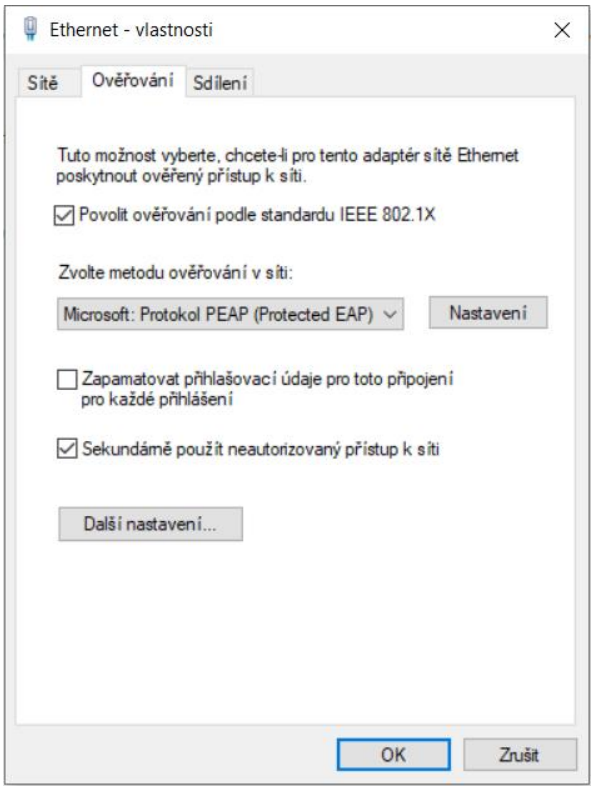
```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
```

DNS je nestavena na IP adresu 8.8.8.8

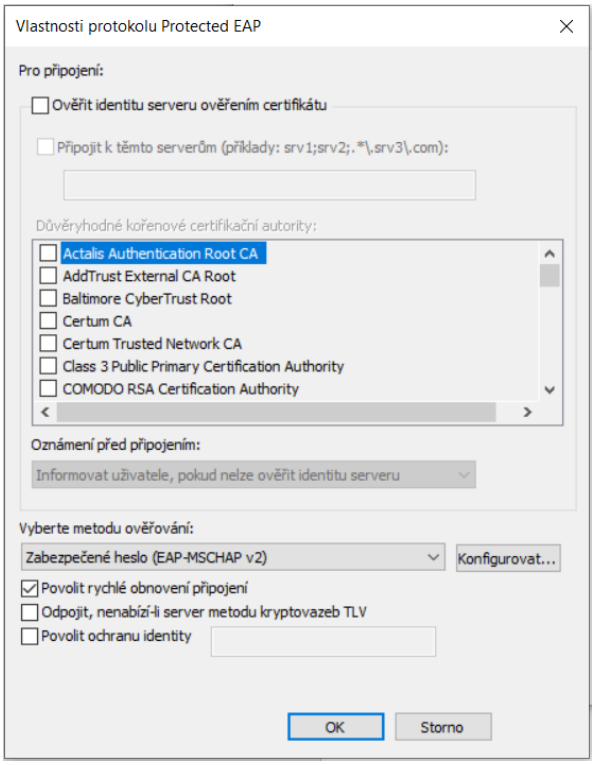
3.8 Povolení protokolu 802.1X na počítači s Windows

Aby bylo možné používat ověření pomocí protokolu 802.1X na počítači, musíme ho nejprve povolit.

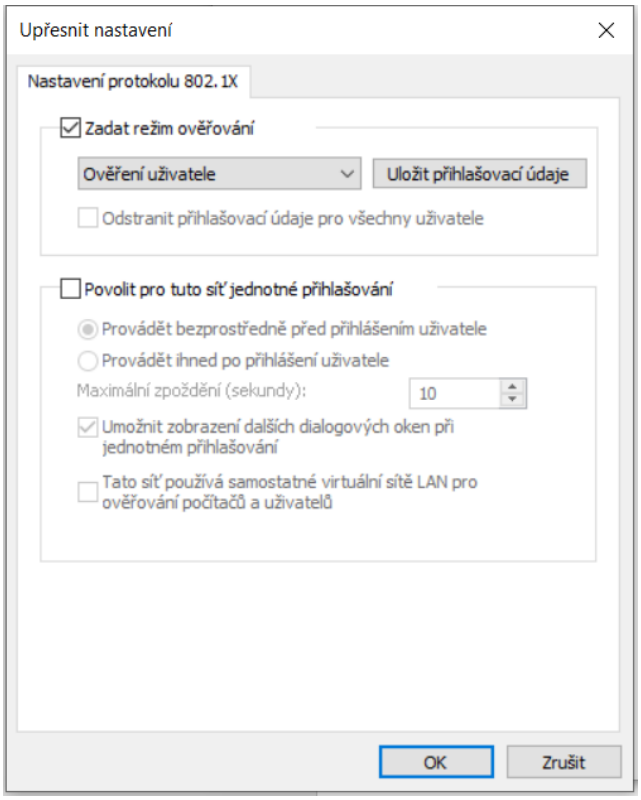
V záložce „tento počítač“ klikneme na Spravovat. Zvolíme Služky a Aplikace a dále klikneme na tlačítko Služby, zde najdeme službu Wired AutoConfig Service, kterou povolíme. Dále je potřeba konkrétněji nastavit možnosti ověření na adaptéru. V záložce Ovládací panely – Síť a internet – Síťová připojení rozklikneme vlastnosti síťového adaptéru Ethernet – Ověřování.



Obrázek 12a: Povolení protokolu 802.1X na počítači s Windows



Obrázek 12b: Povolení protokolu 802.1X na počítači s Windows



Obrázek 12c: Povolení protokolu 802.1X na počítači s Windows

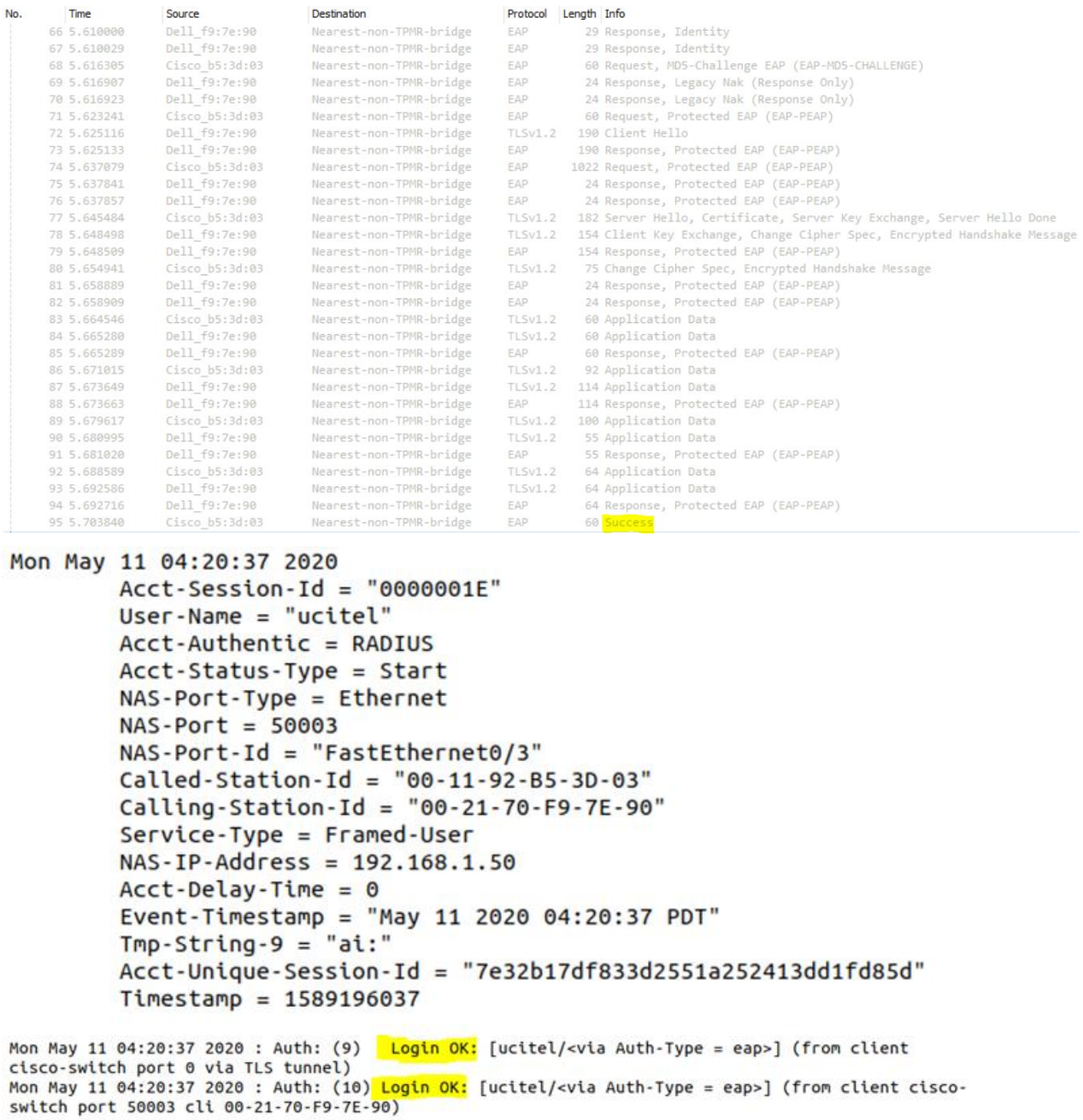
3.9 Odzkoušení zapojení a zachycení komunikace

Před zkouškou celé konfigurace není přístup k internetu, jak je vidět na obrázku č. 13, zkoušky byla provedena nástrojem ping na adresu 8.8.8.8. Po úspěšné autentizaci bylo připojení k internetu zase obnoveno. Přiřazení uživatele do jednotlivých VLAN můžeme upravovat možnosti a pravomoci uživatele.

```
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
Reply from 8.8.8.8: bytes=32 time=8ms TTL=54
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
Reply from 8.8.8.8: bytes=32 time=8ms TTL=54
Reply from 8.8.8.8: bytes=32 time=8ms TTL=54
Reply from 8.8.8.8: bytes=32 time=7ms TTL=54
```

Obrázek 13: Ping pro ověření přístupu k internetu

Na obrázku č. 14 je vidět úspěšná autentizace uživatele „učitel“.



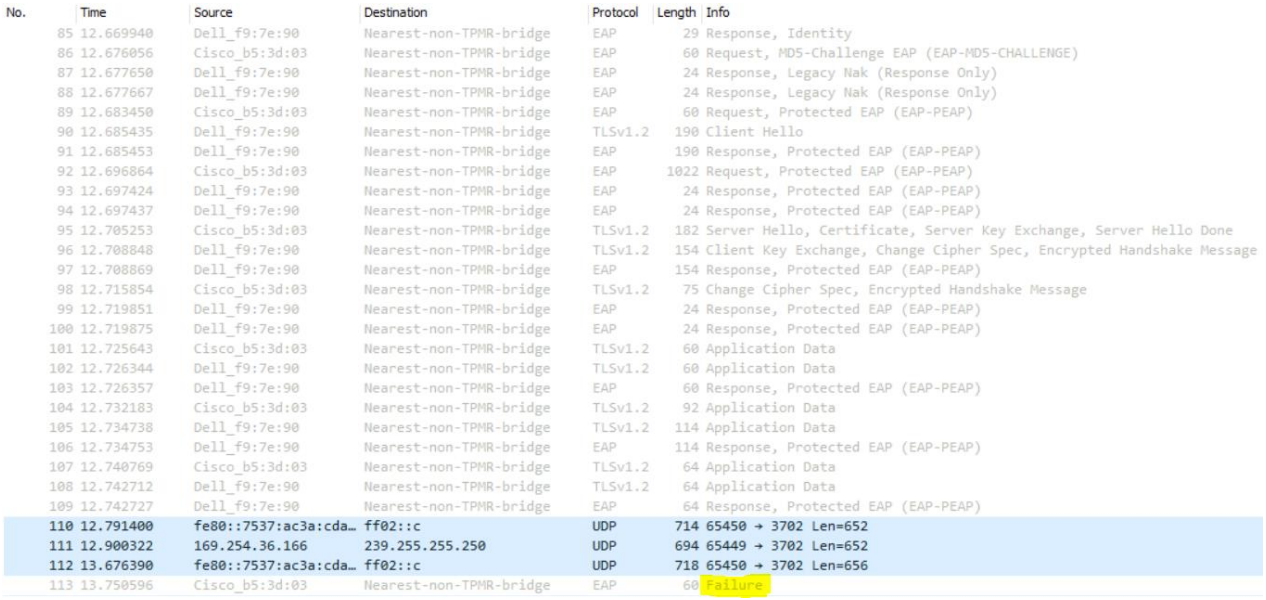
No.	Time	Source	Destination	Protocol	Length	Info
66	5.610000	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	29	Response, Identity
67	5.610029	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	29	Response, Identity
68	5.616305	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
69	5.616907	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
70	5.616923	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
71	5.623241	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, Protected EAP (EAP-PEAP)
72	5.625116	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	190	Client Hello
73	5.625133	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	190	Response, Protected EAP (EAP-PEAP)
74	5.637079	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	1022	Request, Protected EAP (EAP-PEAP)
75	5.637841	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
76	5.637857	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
77	5.645484	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	182	Server Hello, Certificate, Server Key Exchange, Server Hello Done
78	5.648498	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	154	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
79	5.648509	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	154	Response, Protected EAP (EAP-PEAP)
80	5.654941	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	75	Change Cipher Spec, Encrypted Handshake Message
81	5.658889	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
82	5.658909	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
83	5.664546	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
84	5.665280	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
85	5.665289	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	60	Response, Protected EAP (EAP-PEAP)
86	5.671015	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	92	Application Data
87	5.673649	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	114	Application Data
88	5.673663	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	114	Response, Protected EAP (EAP-PEAP)
89	5.679617	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	100	Application Data
90	5.680995	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	55	Application Data
91	5.681020	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	55	Response, Protected EAP (EAP-PEAP)
92	5.688589	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
93	5.692586	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
94	5.692716	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	64	Response, Protected EAP (EAP-PEAP)
95	5.703840	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Success

```
Mon May 11 04:20:37 2020
        Acct-Session-Id = "0000001E"
        User-Name = "ucitel"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Ethernet
        NAS-Port = 50003
        NAS-Port-Id = "FastEthernet0/3"
        Called-Station-Id = "00-11-92-B5-3D-03"
        Calling-Station-Id = "00-21-70-F9-7E-90"
        Service-Type = Framed-User
        NAS-IP-Address = 192.168.1.50
        Acct-Delay-Time = 0
        Event-Timestamp = "May 11 2020 04:20:37 PDT"
        Tmp-String-9 = "ai:"
        Acct-Unique-Session-Id = "7e32b17df833d2551a252413dd1fd85d"
        Timestamp = 1589196037

Mon May 11 04:20:37 2020 : Auth: (9)  Login OK: [ucitel/<via Auth-Type = eap>] (from client
cisco-switch port 0 via TLS tunnel)
Mon May 11 04:20:37 2020 : Auth: (10) Login OK: [ucitel/<via Auth-Type = eap>] (from client cisco-
switch port 50003 cli 00-21-70-F9-7E-90)
```

Obrázek 14: Úspěšná autentizace uživatele

Na obrázku 15 je vidět neúspěšná autentizace uživatele „učitel“ po zadání nesprávného hesla.



No.	Time	Source	Destination	Protocol	Length	Info
85	12.669940	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	29	Response, Identity
86	12.676056	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
87	12.677650	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
88	12.677667	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
89	12.683450	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, Protected EAP (EAP-PEAP)
90	12.685435	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	190	Client Hello
91	12.685453	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	190	Response, Protected EAP (EAP-PEAP)
92	12.696864	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	1022	Request, Protected EAP (EAP-PEAP)
93	12.697424	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
94	12.697437	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
95	12.705253	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	182	Server Hello, Certificate, Server Key Exchange, Server Hello Done
96	12.708848	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	154	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
97	12.708869	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	154	Response, Protected EAP (EAP-PEAP)
98	12.715854	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	75	Change Cipher Spec, Encrypted Handshake Message
99	12.719851	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
100	12.719875	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
101	12.725643	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
102	12.726344	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
103	12.726357	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	60	Response, Protected EAP (EAP-PEAP)
104	12.732183	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	92	Application Data
105	12.734738	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	114	Application Data
106	12.734753	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	114	Response, Protected EAP (EAP-PEAP)
107	12.740769	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
108	12.742712	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
109	12.742727	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	64	Response, Protected EAP (EAP-PEAP)
110	12.791400	fe80::7537:ac3a:cda…	ff02::c	UDP	714	65450 → 3702 Len=652
111	12.900322	169.254.36.166	239.255.255.250	UDP	694	65449 → 3702 Len=652
112	13.676390	fe80::7537:ac3a:cda…	ff02::c	UDP	718	65450 → 3702 Len=656
113	13.750596	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Failure

```
Mon May 11 04:21:53 2020
        Acct-Session-Id = "0000001E"
        User-Name = "ucitel"
        Acct-Authentic = RADIUS
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Session-Time = 76
        Acct-Input-Octets = 66579
        Acct-Output-Octets = 41344
        Acct-Input-Packets = 249
        Acct-Output-Packets = 110
        Acct-Status-Type = Stop
        NAS-Port-Type = Ethernet
        NAS-Port = 50003
        NAS-Port-Id = "FastEthernet0/3"
        Called-Station-Id = "00-11-92-B5-3D-03"
        Calling-Station-Id = "00-21-70-F9-7E-90"
        Service-Type = Framed-User
        NAS-IP-Address = 192.168.1.50
        Acct-Delay-Time = 0
        Event-Timestamp = "May 11 2020 04:21:53 PDT"
        Tmp-String-9 = "ai:"
        Acct-Unique-Session-Id = "7e32b17df833d2551a252413dd1fd85d"
        Timestamp = 1589196113

Mon May 11 04:21:59 2020 : Auth: (20)  Login incorrect (mschap: MS-CHAP2-Response is incorrect):
[ucitel/<via Auth-Type = eap>] (from client cisco-switch port 0 via TLS tunnel)
Mon May 11 04:21:59 2020 : Auth: (21) Login incorrect (eap_peap: The users session was previously
rejected: returning reject (again.)): [ucitel/<via Auth-Type = eap>] (from client cisco-switch
port 50003 cli 00-21-70-F9-7E-90)
```

Obrázek 15: Neúspěšná autentizace uživatele

ZÁVĚR

Cílem této práce bylo prostudování tématiky řízení k lokální síti s využitím protokolu se standardem IEEE 802.1X a zaměřením se na autentizaci pomocí serveru RADIUS k lokální síti. Poté navrhnout a implementovat pracoviště pro vybudování virtuálního serveru pro laboratorní účely.

V teoretické části této práce jsou popsány jednotlivé standardy a protokoly, které je možné využívat k účelům spojeným s autentizací uživatele přes server RADIUS. Dále jsou zde popsány protokoly k zabezpečení posílání autentizačních zpráv mezi koncovým zařízením a serverem RADIUS. Jsou zde popsány jednotlivé zařízení, které byly potřeba k realizaci praktické části, jako je například switch a server RADIUS.

Praktická část se zaobírá využitím zařízeních k autentizaci uživatele a následně jeho povolení nebo odmítnutí přístupu do sítě. Zařízení bude zpočátku implementováno v domácích podmínkách a poté v laboratorním prostředí na Ústavu telekomunikací. S pomocí nástroje VMware workstation player bylo implementováno linuxové prostředí Ubuntu verze 19.10, kde je nainstalován FreeRADIUS. Dále byl použit pro zkušební verzi router MikroTik hAP lite, který lze konfigurovat v programu winbox. V práci bylo popsáno nastavení jednotlivých zařízení a vysvětlení funkcí, které byly potřeba k implementaci této laboratorní úlohy se zaměřením na protokol IEEE 802.1X.

LITERATURA

[1] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce [online]. 3. aktualizované vydání. Brno: Computer Press, 2006 [cit. 2019-11-28]. ISBN 80-251-0892-9. Dostupné z: http://media0.wgz.cz/files/media0:510108fed47d9.pdf.upl/Po%C4%8D%C3%ADta%C4%8Dov%C3%A9+s%C3%ADt%C4%9B.pdf

[2] Guo F., Chiueh T. (2006) Sequence Number-Based MAC Address Spoof Detection. In: Valdes A., Zamboni D. (eds) Recent Advances in Intrusion Detection. RAID 2005. Lecture Notes in Computer Science, vol 3858. Springer, Berlin, Heidelberg [cit. 2019-11-28]

[3] BUBENÍK, Martin. Analýza zabezpečení podnikových sítí s protokolem IEEE 802.1X [online].2018[cit.2019-11-29].Dostupné z: https://dk.upce.cz/bitstream/handle/10195/70557/BubenikM_AnalyzaZabezpeceni_TB_2018.pdf?sequence=1&isAllowed=y. Diplomová práce. Univerzita Pardubice Fakulta elektrotechniky a informatiky.

[4] ŽÁKAVCOVÁ, Monika. Tvorba bezdrátové domácí sítě Wi-fi a možnost sdílení pomocí technologie Bluetooth [online]. Praha, 2009 [cit. 2019-11-28]. Dostupné z: http://info.sks.cz/www/zavprace/soubory/68700.pdf. Bakalářská práce. Vysoká škola ekonomická v Praze Fakulta informatiky a statistiky Vyšší odborná škola informačních služeb v Praze.

[5] IEEE 802.11. Ww.wi-fi.unas.cz [online]. [cit. 2019-11-28]. Dostupné z: http://wi-fi.unas.cz/ieee-802-11.php

[6] What is 802.11ax Wi-Fi, and will it really deliver 10Gbps? (updated). Www.extremetech.com [online]. [cit. 2019-11-28]. Dostupné z: https://www.extremetech.com/computing/184685-what-is-802-11ax-wifi-and-do-you-really-need-a-10gbps-connection-to-your-laptop

[7] Nové technologie - OFDMA, BSS coloring, ... Https://www.alternetivo.cz/ [online]. [cit. 2019-11-28]. Dostupné z: https://www.alternetivo.cz/default.asp?inc=inc/info/80211ax.htm

[8] Část XX.: Příběh Ethernetu. Https://www.earchiv.cz/ [online]. 2006 [cit. 2019-11-28]. Dostupné z: https://www.earchiv.cz/b06/b1200001.php3

[9] *Wi-Fi vs. Ethernet: Which Connection to Use?* [online]. 25.7.2018 [cit. 2019-12-04]. Dostupné z: https://ubidots.com/blog/wi-fi-vs-ethernet-which-connection-to-use/

[10] STANKUŠ, Martin. Autentizace, autorizace a accounting v prostředí IEEE 802.1X / RADIUS [online]. 2007 [cit. 2019-11-28]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/projekty0607/RADIUS-Stankus.pdf

[11] *Intro to Networking - AAA, 802.1X, EAP & RADIUS* [online]. [cit. 2019-11-29]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/115007253447-Intro-to-Networking-AAA-802-1X-EAP-RADIUS

[12] FITZPATRICK, JASON. The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords [online]. , 1 [cit. 2019-11-28]. Dostupné z: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

[13] Wired Equivalent Privacy [online]. [cit. 2019-11-29]. Dostupné z: https://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy

[14] *Wired Equivalent Privacy 2 (WEP2)* [online]. [cit. 2019-11-29]. Dostupné z: https://www.techopedia.com/definition/10962/wired-equivalent-privacy-2-wep2

[15] Dynamic WEP. *Https://www.cisco.com/* [online]. [cit. 2019-11-28]. Dostupné z: https://www.cisco.com/assets/sol/sb/WAP321_Emulators/WAP321_Emulator_v1.0.0.3/help/Wireless11.html

[16] GEIER, Eric. What is WPA3? And some gotchas to watch out for in this Wi-Fi security upgrade [online]. 2018, , 1 [cit. 2019-11-28]. Dostupné z: https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html

[17] 802.1X Overview and EAP Types [online]. 2019 [cit. 2019-11-28]. Dostupné z: https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-io/wireless-networking.html

[18] EAP, Extensible Authentication Protocol. Http://www.networksorcery.com/ [online]. [cit. 2019-11-28]. Dostupné z: http://www.networksorcery.com/enp/protocol/eap.htm

[19] *Extensible Authentication Protocol* [online]. [cit. 2019-12-06]. Dostupné z: https://www.revolvy.com/page/Extensible-Authentication-Protocol

[20] The Extensible Authentication Protocol. Https://flylib.com/ [online]. [cit. 2019-11-28]. Dostupné z: https://flylib.com/books/en/2.519.1/the_extensible_authentication_protocol.html

[21] EAPOL. Http://etutorials.org/ [online]. [cit. 2019-11-28]. Dostupné z: http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+8.+Access+Control+IEEE+802.1X+EAP+and+RADIUS/EAPOL/

[22] *EAPoL – Extensible Authentication Protocol over LAN* [online]. [cit. 2019-12-06]. Dostupné z: https://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/

[23] LIU, Fanbao a Tao XIE. How to Break EAP-MD5 [online]. 2012 [cit. 2019-11-28]. Dostupné z: https://hal.inria.fr/hal-01534313/document

[24] 802.1X Overview and EAP Types [online]. 2019 [cit. 2019-11-28]. Dostupné z: https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-io/wireless-networking.html

[25] Church, C.: EAP Authentication Protocols, [online]. 2009 [cit. 2019-12-04]. URL https://layer3.wordpress.com/2009/08/16/eap-authentication-protocols

[26] Protected Extensible Authentication Protocol [online]. 2017 [cit. 2019-11-28]. Dostupné z: https://ldapwiki.com/wiki/Protected%20Extensible%20Authentication%20Protocol#ref-Protected%20Extensible%20Authentication%20Protocol-1

[27] KERNER, Sean Michael. EAP-TLS Detailed as WiFi Security Best Practice at SecTor [online]. 14.11.2017, , 1 [cit. 2019-11-28]. Dostupné z: https://www.eweek.com/security/eap-tls-detailed-as-wifi-security-best-practice-at-sector

[28] The NetGuardian Voice 16 G2 With RADIUS. Https://www.dpstele.com/ [online]. [cit. 2019-11-28]. Dostupné z: https://www.dpstele.com/rtu/snmp/voice-16-radius.php

[29] How RADIUS Server Authentication Works. Https://www.watchguard.com/ [online]. [cit. 2019-11-28]. Dostupné z: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/authentication/radius_how_works_c.html

[30] ROUSE, Margaret. RADIUS (Remote Authentication Dial-In User Service) [online]. 2007, , 1 [cit. 2019-11-28]. Dostupné z: https://searchsecurity.techtarget.com/definition/RADIUS

[31] *CO JE TO RADIUS?* [online]. [cit. 2019-12-04]. Dostupné z: https://best-hosting.cz/cs/napoveda/co-je-to-radius

[32] *How does a network switch work?* [online]. [cit. 2019-12-06]. Dostupné z: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-how.html#~introduction

[33] *Access Control and Authentication on Switching Devices* [online]. 9.7.2019 [cit. 2019-12-06]. Dostupné z: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/access-control-authentication-for-switching-device.html#jd0e51

[34] *HOW A RADIUS SERVER WORKS* [online]. [cit. 2019-12-06]. Dostupné z: https://networkradius.com/how-a-radius-server-works/

[35] *Download TekRADIUS 5.5.2.1 for Windows* [online]. 26.8.2019 [cit. 2019-12-06]. Dostupné z: https://downloads.tomsguide.com/TekRADIUS,0301-38298.html

[36] *The FreeRADIUS Server Project* [online]. [cit. 2019-12-06]. Dostupné z: https://freeradius.org/about/

[37] *Radl - Free Radius Server* [online]. [cit. 2019-12-06]. Dostupné z: https://www.loriotpro.com/Products/RadiusServer/FreeRadiusServer_EN.php

[38] *Open Source RADIUS Server for VoIP* [online]. 2017 [cit. 2019-12-06]. Dostupné z: http://www.bsdradius.org/

[39] *JRadius with FreeRADIUS* [online]. [cit. 2019-12-06]. Dostupné z: https://coova.github.io/JRadius/FreeRADIUS/

[40] *Glossary/Other RADIUS Servers* [online]. [cit. 2019-12-06]. Dostupné z: https://wiki.freeradius.org/glossary/Other-RADIUS-Servers

[41] Configuring RADIUS. Cisco - Global Home Page [online]. Copyright © 2017, Cisco Systems, Inc. All rights reserved. [cit. 03.05.2020]. Dostupné z: https://www.cisco.com/c/dam/en/us/td/docs/routers/asr920/configuration/guide/sec-usr-rad/16-6-1/b-sec-usr-rad-xe-16-6-asr920.html#GUID-13A5765B-5676-4756-A0EF-10B4E60B1E39

SEZNAM POUŽITÝCH ZKRATEK

AAA - Authentication, Authorization and Accounting protocol

ACL – Access Control List

ADHP - Authenticated Diffie-Hellman Protocol

AES - Advanced Encryption Standard

AP – Access Point

ASLEAP -

CCMP - Counter Cipher Mode with Block Chaining Message Authentication Code Protocol

CRC - Cyclic redundancy check

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

DECnet - Digital Equipment Corporation

DHCP - Dynamic Host Configuration Protocol

DSSS - Direct Sequence Spread Spectrum

Dynamic WEP – Dynamic Wired Equivalent Privacy

EAP - Extensible Authentication Protocol

EAP-MD5 - message-digest algorithm 5

EAPoL - Extensible Authentication Protocol over LAN

FAST - Flexible Authentication via Secure Tunneling

HTTP - Hypertext Transfer Protocol

CHAP - Challenge-Handshake Authentication Protocol

CHAPv2 - Challenge-Handshake Authentication Protocol

ID - Identity Document

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IP - IP address

IPv4 - Internet Protocol version 4

IPv6 - Internet Protocol version 6

IPX/SPX - Internetwork Packet Exchange/Sequenced Packet Exchange

ISO/OSI - International Organization for Standardization/Open Systems Interconnection

L2TP - Layer 2 Tunnel Protocol

LAN - Local Area Network

LDAP - Lightweight Directory Access Protocol

LEAP - Lightweight Extensible Authentication Protocol

MAC – Media Access Control

MIC - Message Integrity Check

MIMO - Multiple-input multiple-output

MS-CHAP - Microsoft Challenge Handshake Authentication Protocol

MU-MIMO - Multiple-User Multiple-Input Multiple-Output

NSA - National Security Agency

OFDM - Orthogonal Frequency Division Multiplexing

OFDMA - Orthogonal frequency-division multiple access

OS - Operating system

PAC - Protected Access Credential

PAE - Physical Address Extension

PEAP - Protected Extensible Authentication Protocol

PKI - Public Key Infrastructure

PNAC - Port based Network Access Control

PPTP - Point-to-Point Tunneling Protocol

PSK - Pre-shared key

QAM - Quadrature amplitude modulation

RADIUS - Remote Authentication Dial-In User Service

RC4 - Rivest Cipher 4

RFC - Request For Comments

RSA - Rivest, Shamir, Adleman

SAE - Simultaneous Authentication of Equals

SSID - Service Set Identifier

TCP/IP - Transmission Control Protocol/Internet Protocol

TKIP - Temporaly Key integrity Protocol

TLS - Transport Layer Security

TTLS - Tunneled Transport Layer Security

UDP - User Datagram Protocol

UTP - Unshielded Twisted Pair

VOIP - voice over IP

WAN - Wide Area Network

WEP - Wired Equivalent Privacy

WEP2 - Wired Equivalent Privacy 2

WEPplus - Wired Equivalent Privacy plus

Wi-Fi - Wireless Fidelity

WLAN - Wireless LAN

WPA - Wi-Fi Protected Access

WPA2 - Wi-Fi Protected Access 2

WPA3 - Wi-Fi Protected Access 3

WPS - Wi-Fi Protected Setup

PŘÍLOHA 1 – VZOROVÉ ZADÁNÍ LABORATORNÍ ÚLOHY

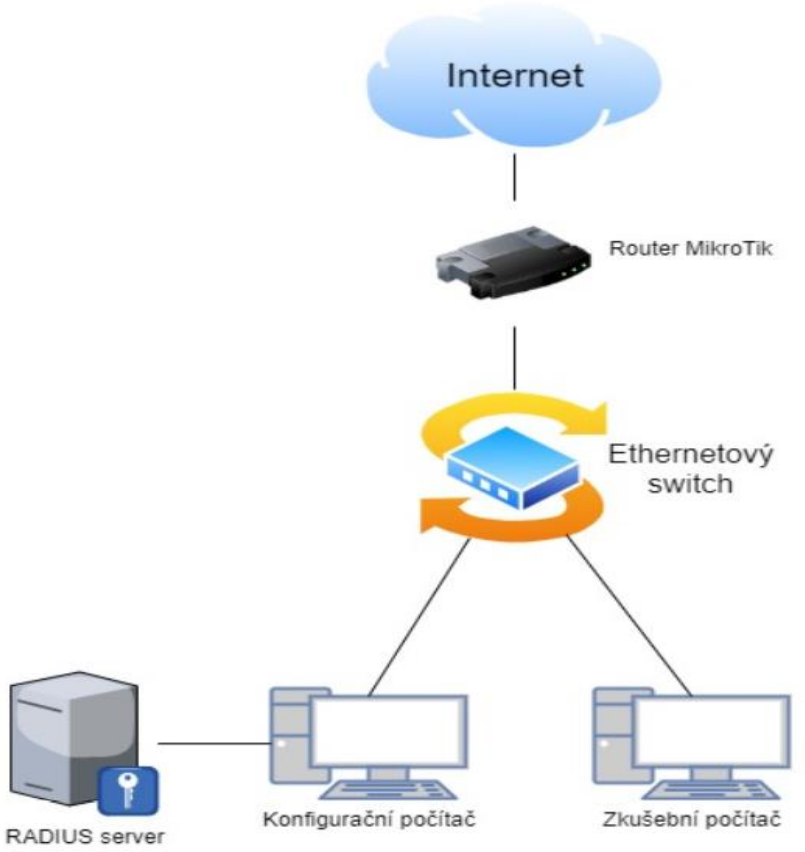
CÍL LABORATORNÍ ÚLOHY

Cílem této úlohy je seznámit studenta s možností zabezpečení lokálního připojení pomocí protokolu IEEE 802.1X. Student absolvováním této úlohy bude schopen porozumět RADIUS serveru a jeho konfigurace a také základní konfiguraci v rámci switche CISCO společně s routerem MikroTik.

TEORETICKÝ ÚVOD

RADIUS (Remote Authentication Dial-In User Service) je protokol, který byl původně navržen tak, aby autentizoval vzdálené uživatele k serveru pro telefonický přístup. RADIUS, vytvořený společností Livingston, je průmyslovým standardem používaným mnoha společnostmi, které vyrábí síťové produkty a je navrhovaným standardem IETF (Internet Engineering Task Force). Standard IEEE, pod kterým je RADIUS uznán z pohledu specifikace je RFC 2865 a z pohledu účtování v RFC 2866. RADIUS se nyní používá v celé řadě procesů autentizace. Je to protokol klient-server a software, který umožňuje serverům vzdáleného přístupu komunikovat s centrálním serverem, aby mohl ověřovat uživatele dial-in a autorizoval jejich přístup k požadovanému systému nebo službě. RADIUS také dokáže udržovat uživatelské profily v centrální databázi, kterou mohou sdílet všechny vzdálené servery. Když se uživatel pokusí ověřit, zařízení odešle zprávu serveru RADIUS. Pokud je server RADIUS správně nakonfigurován tak, aby měl zařízení jako klienta, RADIUS odešle zprávu o přijetí nebo odmítnutí zpět do zařízení (server síťového přístupu), jak je znázorněno na obrázku 9. Při vydání požadavku uživatelem na autentizaci je klientem vytvořen požadavek na přístup, který obsahuje jméno, heslo a číslo portu, na kterém probíhá připojení. Požadavek je odeslán na server. Jestliže odpověď nepřijde do určeného času, je požadavek opakován.

Jeho nejzásadnější vlastností je velmi vysoké síťové zabezpečení, protože komunikační transakce mezi uživatelem a RADIUS serverem jsou zprostředkována pomocí sdíleného tajemství. Sdílené tajemství není posíláno po síti, po síti jsou pouze posílána uživatelská hesla v zašifrované podobě.



Obrázek 1: Topologie zapojení stanoviště

Zadání a postup měření

1. Spusťte virtuální počítat Ubuntu.

2. Zapněte terminál, zde budeme konfigurovat celý Radius server. Stáhněte FreeRadius příkazem *apt-get update*, následně napište příkaz *apt-get install freeradius*. Tímto se do virtuálního počítače nainstaloval radius server.

3. Zkontrolujte, jestli jste ve stejném adresovém rozsahu (pc, switch, virtuální pc), jestliže ne, změňte nastavení adresního rozsahu.

4. Teď se zaměříme na konfiguraci FreeRadiusu. Budeme nastavovat klienta (switch), se kterým bude radius komunikovat. Client je zařízení, které slouží pro připojení uživatele do sítě. Například client může být konfigurovatelný switch nebo AP. V tomto případě máme zapojený konfigurovatelný ethernetový switch, který zasílá požadavky o autentizaci uživatele na RADIUS server, ten mu následně odpovídá, zda došlo ke shodě s ID a heslem, které jsou uloženy v konfiguračním souboru users. V okně terminálu zadejte příkaz *sudo nano /etc/freeradius/3.0/clients.conf*.

Tímto se vám zobrazí konfigurace klienta. Projděte si ji. Pro komunikaci klienta a freeradiusu stačí do konfigurace zapsat:

```
client „název klienta“ {
      ipv4addr = „ip adresa klienta“
      secret = „heslo“
      nastype = cisco
      }
```

Vysvětlení atributů

- cisco-switch – název klienta
- ipv4addr – IP adresa klienta
- secret – sdílené heslo pro komunikaci mezi RADIUS serverem a klientem/NAS
- nastype - používá ke sdělování skriptu checkrad.pl

5. Nastavení uživatelů, kteří se budou moci autentizovat, se konfiguruje v souboru users. Uživatelé, které chceme, aby se mohli autentizovat do sítě, vytvoříme v konfiguračním souboru users. Princip spočívá v tom, že po zadání ID a hesla pošle switch zprávu na RADIUS server, tam je konfigurační soubor users projetý od shora dolů, v případě shody je poslána zpráva zpět na switch a dochází k autentizaci uživatele. Pro zkušební účely vytvořte alespoň 2 uživatele, kteří se připojují do různých VLAN podle jejich přihlašovacích údajů. Otevření souboru users je obdobné jako u klienta. Příkaz v terminálu je *sudo nano /etc/freeradius/3.0/users*.

```
„název uživatele“ Cleartext-Password := „heslo“
        Tunnel-Type                    = VLAN,
        Tunnel-Medium-Type             = IEEE-802,
        Tunnel-Private-Group-ID        = 10
```

Vysvětlení atributů

- -„název uživatele“ – ID uživatele (bez uvozovek)
- „heslo“ – heslo uživatele (bez uvozovek)
- Tunnel-Type (VLAN) – tento atribut označuje tunelové protokoly, které mají být použity
- Tunnel-Medium-Type (IEEE-802) - označuje, které transportní médium bude použito při vytváření tunelu

- Tunnel-Private-Group-ID (10) – označuje ID VLANy, do které má být uživatel připojen

6. Jako poslední věc je potřeba nastavení peap a ttls zpráv. Do souboru se dostanete příkazem *sudo nano /etc/freeradius/3.0/mods-enabled/eap.* V konfiguračním souboru eap.conf je potřeba nastavit use_tunneled_reply na „yes“ u zpráv typu PEAP aTTLS. Při spuštění metod tunelu EAP chybí AVP odpověď. Pokud nastavíte u EAP „use_tunnelled_reply = yes“, znamená to, že v odpovědi by mělo být použito uživatelské jméno z tunelové odpovědi. Tím budou použity atributy pro konečný přístup Access-Accept.

```
ttls {
tls = tls-common
      default_eap_type = md5
      copy_request_to_tunnel = no
      use_tunneled_reply = yes
      virtual_server = "inner-tunnel"
     }
peap{
      tls = tls-common
      default_eap_type = mschapv2
      copy_request_to_tunnel = no
      use_tunneled_reply = yes
      virtual_server = "inner-tunnel"
      }
```

Pro logování zpráv je potřeba nastavit v souboru radiusd.conf tyto hodnoty. Cesta do tohoto souboru vede přes etc/freeradius/3.0/radius.conf. Logování se ukládá do složky var/log/freeradius/radius.log.

```
Log {
     destination = files
     colourise = yes
     file = ${logdir}/radius.log
     syslog_facility = deamon
     stripped_names = no
     auth = yes
     auth_accept = yes
     auth_reject = yes
     }
```

Restartujte FreeRadius příkazem *sudo /etc/init.d/freeradius restart* a podívejte se, jestli je FreeRadius aktivní příkazem *systemctl status freeradius.service.*

7. Připojte se k routeru MikroTik a proveďte jeho základní konfiguraci pro přístup k internetu. Vytvořte konfiguraci pro VLANy, jejich IP adresy, DHCP servery a NAT pro přístup k internetu. Pro snadnější práci vytvořte mezi dvěma porty na routeru Bridge pro současnou konfiguraci routeru a switche. Dále nastavte firewall, aby bylo možné po připojení na konkrétní VLAN dostat se jenom na určité webové stránky. První VLAN se dostane všude, druhá VLAN se dostane pouze na *www.vutbr.cz* a třetí VLAN se dostane pouze na *apollo.vutbr.cz*. Je potřeba si vytvořit Address lists pro *vutbr.cz* a *apollo.vutbr.cz*. Ve Filter rules vytvořte pravidla pro omezení (stačí 4 pravidla – tři accept a jeden drop). V záložce Filter Rules zmáčkněte +, tím vytvoříte nové pravidlo - chain = forward, Src.Address = adresa sítě VLANy, Action = accept. Obdobně proveďte pro ostatní VLANy. Pro drop filter nastavte chain = forward, Protocol = tcp, Dst. Port = 80,443 (http,https), Action= drop.

8. V tomto případě je použit ethernetový switch ke komunikaci s nakonfigurovaným routerem MikroTik a RADIUS serverem. Do eth. switche jsou také připojováni uživatelé, kteří se chtějí připojit do vytvořených VLANek. Switch nakonfigurujte do základního nastavení a povolte služby RADIUS. Základní konfigurace tohoto switche spočívá v nastavení IP adresy na VLAN 1 (defaultní VLAN) a defaultní brány, která je potřeba, abychom se mohli připojit a mohli konfigurovat switch. Připojení je zprostředkováno programem Putty s komunikací typu Telnet nebo SSH. Jestliže se chceme ke switchi přihlásit, musí být ve stejném IP rozsahu, jako je konfigurační počítat. Pro komunikaci mezi switchem a routerem MikroTik nastavte trunk.

Povolení služky RADIUS

```
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Nastavení komunikace s RADIUS serverem

```
   radius-server host „IP adresa Radius serveru“ auth-port
1812 acct-port 1813 key „heslo“
```

Nastavení portů

Port 1 – port pro připojení zkušebního počítače

```
interface FastEthernet0/1
 switchport mode access
dot1x pae authenticator
 dot1x port-control auto
dot1x host-mode multi-host
dot1x violation-mode protect
dot1x reauthentication
```

Samozřejmě lze takto nastavit více portů, kromě komunikačního portu s routerem a konfiguračního portu.

Port 23 – port pro komunikaci s konfiguračním počítačem (port je pouze nastaven jako access)

```
interface FastEthernet0/23
 switchport mode access
```

Port 24 – port nakonfigurovaný jako trunk

```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan „vytvořené vlany“
 switchport mode trunk
```

9. Aby zkušební počítač věděl, že má při přihlášení požadovat autentizaci uživatele, je zapotřebí tuto možnost zvolit v nastavení služeb. V záložce „tento počítač“ klikneme na Spravovat. Zvolíme Služky a Aplikace a dále klikneme na tlačítko Služby, zde najdeme službu Wired AutoConfig Service, kterou povolíme. Dále je potřeba konkrétněji nastavit možnosti ověření na adaptéru. V záložce Ovládací panely – Síť a internet – Síťová připojení rozklikneme vlastnosti síťového adaptéru Ethernet – Ověřování a povolíme možnost ověření podle standardu IEEE 802.1X. V nastavení protokolu 802.1X zvolíme možnost ověření uživatele.

10. Zapněte program WireShark a podívejte se na zprávy, které jsou přeposílány mezi Radiusem a testovacím pc.

Otázky:
1. Jaké IP adresy vám přidělil DHCP server u jednotlivých VLAN ?
2. Jaké síťové přístupy byly umožněny u jednotlivých uživatelů ?
3. Proč můžeme použít ping na zakázané stránky v pravidlech ?

Závěr

V závěru student uvede svoje poznatky z konfigurace úlohy.

PŘÍLOHA 2 – VYPRACOVANÝ PROTOKOL

FEKT	Předmět		
	Jméno	Radim Čuhel	
	Ročník 3	Studijní skupina	BPC3-TLI
	Spolupracoval	Měřeno dne	
Kontroloval	Hodnocení	Dne	
Číslo úlohy	Název úlohy **KONFIGURACE RADIUS SERVERU**		

CÍL LABORATORNÍ ÚLOHY

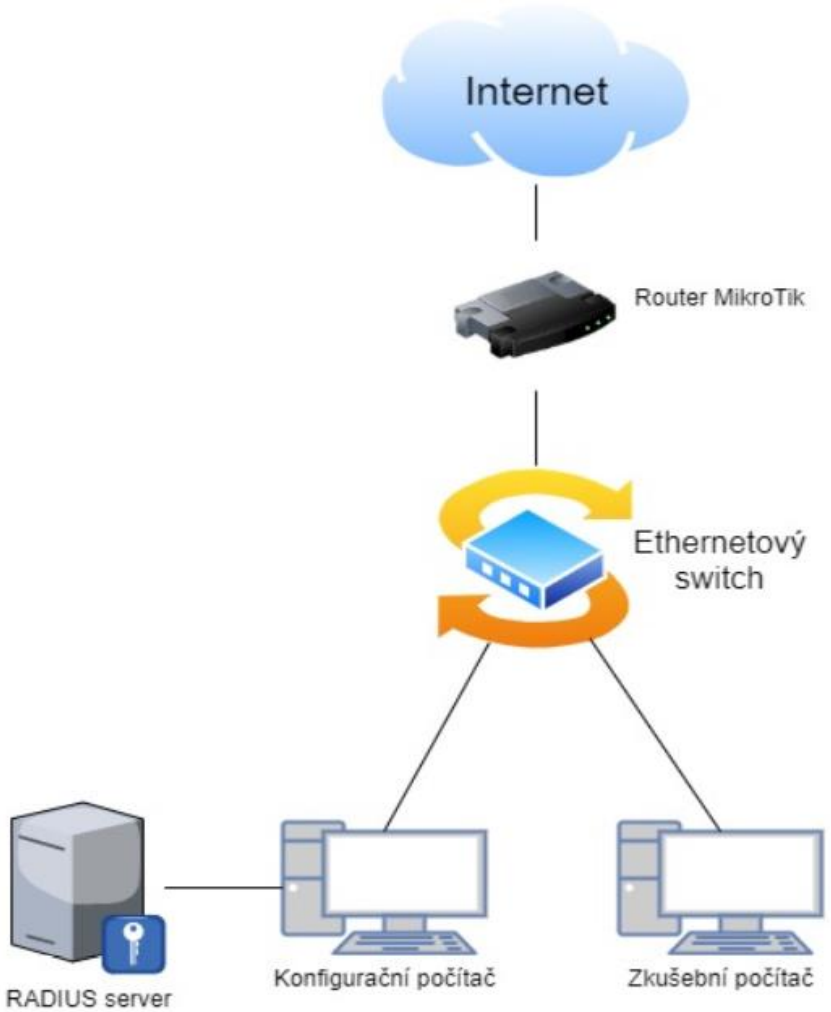
Cílem této úlohy je seznámit studenta s možností zabezpečení lokálního připojení pomocí protokolu IEEE 802.1X. Student absolvováním této úlohy bude schopen porozumět RADIUS serveru a jeho konfigurace a také základní konfiguraci v rámci switche CISCO společně s routerem MikroTik.

TEORETICKÝ ÚVOD

RADIUS (Remote Authentication Dial-In User Service) je protokol, který byl původně navržen tak, aby autentizoval vzdálené uživatele k serveru pro telefonický přístup. RADIUS, vytvořený společností Livingston, je průmyslovým standardem používaným mnoha společnostmi, které vyrábí síťové produkty a je navrhovaným standardem IETF (Internet Engineering Task Force). Standard IEEE, pod kterým je RADIUS uznán z pohledu specifikace je RFC 2865 a z pohledu účtování v RFC 2866. RADIUS se nyní používá v celé řadě procesů autentizace. Je to protokol klient-server a software, který umožňuje serverům vzdáleného přístupu komunikovat s centrálním

serverem, aby mohl ověřovat uživatele dial-in a autorizoval jejich přístup k požadovanému systému nebo službě. RADIUS také dokáže udržovat uživatelské profily v centrální databázi, kterou mohou sdílet všechny vzdálené servery. Když se uživatel pokusí ověřit, zařízení odešle zprávu serveru RADIUS. Pokud je server RADIUS správně nakonfigurován tak, aby měl zařízení jako klienta, RADIUS odešle zprávu o přijetí nebo odmítnutí zpět do zařízení (server síťového přístupu), jak je znázorněno na obrázku 9. Při vydání požadavku uživatelem na autentizaci je klientem vytvořen požadavek na přístup, který obsahuje jméno, heslo a číslo portu, na kterém probíhá připojení. Požadavek je odeslán na server. Jestliže odpověď nepřijde do určeného času, je požadavek opakován.

Jeho nejzásadnější vlastností je velmi vysoké síťové zabezpečení, protože komunikační transakce mezi uživatelem a RADIUS serverem jsou zprostředkována pomocí sdíleného tajemství. Sdílené tajemství není posíláno po síti, po síti jsou pouze posílána uživatelská hesla v zašifrované podobě.



Obrázek 1: Topologie zapojení stanoviště

Zadání a postup měření

1. Spusťte virtuální počítat Ubuntu.

2. Zapněte terminál, zde budeme konfigurovat celý Radius server. Stáhněte FreeRadius příkazem *apt-get update*, následně napište příkaz *apt-get install freeradius*. Tímto se do virtuálního počítače nainstaloval radius server.

3. Zkontrolujte, jestli jste ve stejném adresovém rozsahu (pc, switch, virtuální pc), jestliže ne, změňte nastavení adresního rozsahu.

4. Teď se zaměříme na konfiguraci FreeRadiusu. Budeme nastavovat klienta (switch), se kterým bude radius komunikovat. Client je zařízení, které slouží pro připojení uživatele do sítě. Například client může být konfigurovatelný switch nebo AP. V tomto případě máme zapojený konfigurovatelný ethernetový switch, který zasílá požadavky o autentizaci uživatele na RADIUS server, ten mu následně odpovídá, zda došlo ke shodě s ID a heslem, které jsou uloženy v konfiguračním souboru users. V okně terminálu zadejte příkaz *sudo nano /etc/freeradius/3.0/clients.conf*. Tímto se vám zobrazí konfigurace klienta. Projděte si ji. Pro komunikaci klienta a freeradiusu stačí do konfigurace zapsat:

```
client cisco-switch {
   ipv4addr = 192.168.1.50/24
   secret = cisco
   nastype = cisco
   }
```

   Vysvětlení atributů

   - cisco-switch – název klienta
   - ipv4addr – IP adresa klienta
   - secret – sdílené heslo pro komunikaci mezi RADIUS serverem a klientem/NAS
   - nastype - používá ke sdělování skriptu checkrad.pl

5. Nastavení uživatelů, kteří se budou moci autentizovat, se konfiguruje v souboru users. Uživatelé, které chceme, aby se mohli autentizovat do sítě, vytvoříme v konfiguračním souboru users. Princip spočívá v tom, že po zadání ID a hesla pošle switch zprávu na RADIUS server, tam je konfigurační soubor users projetý od shora dolů, v případě shody je poslána zpráva zpět na switch a dochází k autentizaci uživatele. Pro zkušební účely vytvořte alespoň 2 uživatele, kteří se připojují do různých VLAN podle

jejich přihlašovacích údajů. Otevření souboru users je obdobné jako u klienta. Příkaz v terminálu je *sudo nano /etc/freeradius/3.0/users*.

```
ucitel Cleartext-Password :      = „ucitel“
            Tunnel-Type                 = VLAN,
            Tunnel-Medium-Type          = IEEE-802,
            Tunnel-Private-Group-ID     = 10


student Cleartext-Password :     = „student“
            Tunnel-Type                 = VLAN,
            Tunnel-Medium-Type          = IEEE-802,
            Tunnel-Private-Group-ID     = 20


host  Cleartext-Password : = „host“
            Tunnel-Type                 = VLAN,
            Tunnel-Medium-Type          = IEEE-802,
            Tunnel-Private-Group-ID     = 30
```

Vysvětlení atributů

- -„název uživatele“ – ID uživatele (bez uvozovek)
- „heslo“ – heslo uživatele (bez uvozovek)
- Tunnel-Type (VLAN) – tento atribut označuje tunelové protokoly, které mají být použity
- Tunnel-Medium-Type (IEEE-802) - označuje, které transportní médium

  použít při vytváření tunelu
- Tunnel-Private-Group-ID (10) – označuje ID VLANy, do které má být uživatel připojen

6. Jako poslední věc je potřeba nastavení peap a ttls zpráv. Do souboru se dostanete příkazem *sudo nano /etc/freeradius/3.0/mods-enabled/eap.*
   V konfiguračním souboru eap.conf je potřeba nastavit use_tunneled_reply na „yes“ u zpráv typu PEAP aTTLS. Při spuštění metod tunelu EAP chybí AVP odpověď. Pokud nastavíte u EAP „use_tunnelled_reply = yes“,

znamená to, že v odpovědi by mělo být použito uživatelské jméno z tunelové odpovědi. Tím budou použity atributy pro konečný přístup Access-Accept.

```
ttls {
tls = tls-common
    default_eap_type = md5
    copy_request_to_tunnel = no
    use_tunneled_reply = yes
    virtual_server = "inner-tunnel"
    }
peap{
    tls = tls-common
    default_eap_type = mschapv2
    copy_request_to_tunnel = no
    use_tunneled_reply = yes
    virtual_server = "inner-tunnel"
    }
```

Pro logování zpráv je potřeba nastavit v souboru radiusd.conf tyto hodnoty. Cesta do tohoto souboru vede přes etc/freeradius/3.0/radius.conf. Logování se ukládá do složky var/log/freeradius/radius.log.

```
Log {
      destination = files
      colourise = yes
      file = ${logdir}/radius.log
      syslog_facility = deamon
      stripped_names = no
      auth = yes
      auth_accept = yes
      auth_reject = yes
      }
```

Restartujte FreeRadius příkazem *sudo /etc/init.d/freeradius restart* a podívejte se, jestli je FreeRadius aktivní příkazem *systemctl status freeradius.service.*

7. Připojte se k routeru MikroTik a proveďte jeho základní konfiguraci pro přístup k internetu. Vytvořte konfiguraci pro VLANy, jejich IP adresy, DHCP servery a NAT pro přístup k internetu. Pro snadnější práci vytvořte mezi dvěma portami na routeru Bridge pro současnou konfiguraci routeru a switche. Dále nastavte firewall, aby bylo možné po připojení na konkrétní VLAN dostat se jenom na určité webové stránky. První VLAN se dostane všude, druhá VLAN se dostane pouze na *www.vutbr.cz* a třetí VLAN se dostane pouze na *apollo.vutbr.cz*. Je potřeba si vytvořit Address lists pro *vutbr.cz* a *apollo.vutbr.cz*. Ve Filter rules vytvořte pravidla pro omezení (stačí 4 pravidla – tři accept a jeden drop). V záložce Filter Rules zmáčkněte +, tím vytvoříte nové pravidlo - chain = forward, Src.Address = adresa sítě VLANy, Action = accept. Obdobně proveďte pro ostatní VLANy. Pro drop filter nastavte chain = forward, Protocol = tcp, Dst. Port = 80,443 (http,https), Action= drop.

Výpis konfigurace MikroTiku:

```
/interface bridge
add name="bridge(3+4)"
/interface wireless
set [ find default-name=wlan1 ] ssid=MikroTik
/interface vlan
add interface=ether2 name="Host(vlan30)" vlan-id=30
add interface=ether2 name="Student(vlan20)" vlan-id=20
add interface=ether2 name="Ucitel(vlan10)" vlan-id=10
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=10.10.10.2-10.10.10.254
add name=dhcp_pool1 ranges=10.10.20.2-10.10.20.254
add name=dhcp_pool2 ranges=10.10.30.2-10.10.30.254
add name=dhcp_pool4 ranges=192.168.1.16-192.168.1.254
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface="Ucitel(vlan10)" name=dhcp1
add address-pool=dhcp_pool1 disabled=no interface="Student(vlan20)" name=dhcp2
add address-pool=dhcp_pool2 disabled=no interface="Host(vlan30)" name=dhcp3
```

```
add address-pool=dhcp_pool4 disabled=no interface="bridge(3+4)" name=dhcp4
/interface bridge port
add bridge="bridge(3+4)" interface=ether3
add bridge="bridge(3+4)" interface=ether4
/ip address
add address=192.168.2.15/24 interface=ether2 network=192.168.2.0
add address=10.10.10.1/24 interface="Ucitel(vlan10)" network=10.10.10.0
add address=10.10.20.1/24 interface="Student(vlan20)" network=10.10.20.0
add address=10.10.30.1/24 interface="Host(vlan30)" network=10.10.30.0
add address=192.168.1.14/24 interface="bridge(3+4)" network=192.168.1.0
/ip dhcp-client
add disabled=no interface=ether1
/ip dhcp-server network
add address=10.10.10.0/24 gateway=10.10.10.1
add address=10.10.20.0/24 gateway=10.10.20.1
add address=10.10.30.0/24 gateway=10.10.30.1
add address=192.168.1.0/24 gateway=192.168.1.15
/ip dns
set servers=8.8.8.8
/ip firewall address-list
add address=www.vutbr.cz list=VUT
add address=apollo.vutbr.cz list=Apollo
/ip firewall filter
add action=accept chain=forward src-address=10.10.10.0/24
add action=accept chain=forward dst-address-list=VUT src-address=10.10.20.0/24
add action=accept chain=forward dst-address-list=Apollo src-address=10.10.30.0/24
add action=drop chain=forward dst-port=443,80 protocol=tcp
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/system clock
set time-zone-name=Europe/Prague
```

8. V tomto případě je použit ethernetový switch ke komunikaci s nakonfigurovaným routerem MikroTik a RADIUS serverem. Do eth. switche jsou také připojováni uživatelé, kteří se chtějí připojit do vytvořených VLANek. Switch nakonfigurujte do základního nastavení a povolte služby RADIUS. Základní konfigurace tohoto switche spočívá v nastavení IP adresy na VLAN 1 (defaultní VLAN) a defaultní brány, která je potřeba, abychom se mohli připojit a mohli konfigurovat switch. Připojení je zprostředkováno programem Putty s komunikací typu Telnet nebo SSH. Jestliže se chceme ke switchi přihlásit, musí být ve stejném IP rozsahu, jako je konfigurační počítat. Pro komunikaci mezi switchem a routerem MikroTik nastavte trunk.

Povolení služky RADIUS

```
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Nastavení komunikace s RADIUS serverem

```
radius-server host 192.168.1.253 auth-port 1812 acct-port
1813 key cisco
```

Nastavení portů

Port 1 – port pro připojení zkušebního počítače

```
interface FastEthernet0/1
 switchport mode access
dot1x pae authenticator
 dot1x port-control auto
dot1x host-mode multi-host
dot1x violation-mode protect
dot1x reauthentication
```

Samozřejmě lze takto nastavit více portů, kromě komunikačního portu s routerem a konfiguračního portu.

Port 23 – port pro komunikaci s konfiguračním počítačem (port je pouze nastaven jako access)

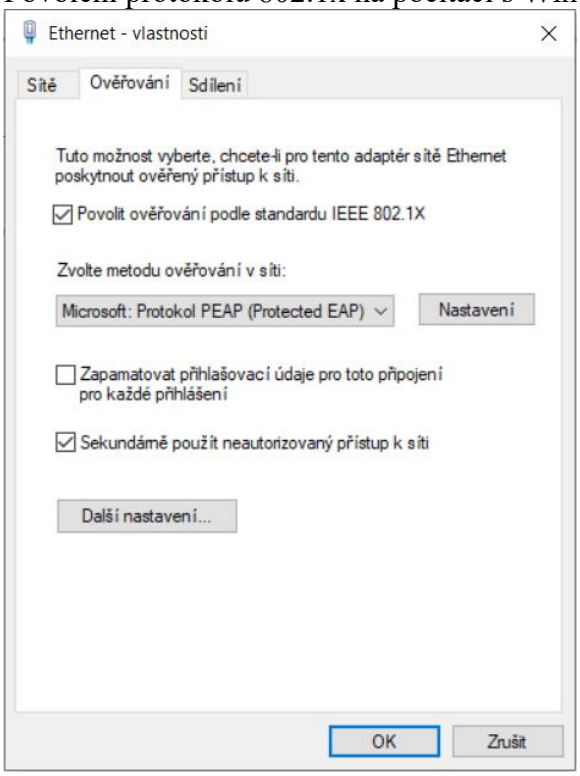
```
interface FastEthernet0/23
 switchport mode access
```

Port 24 – port nakonfigurovaný jako trunk

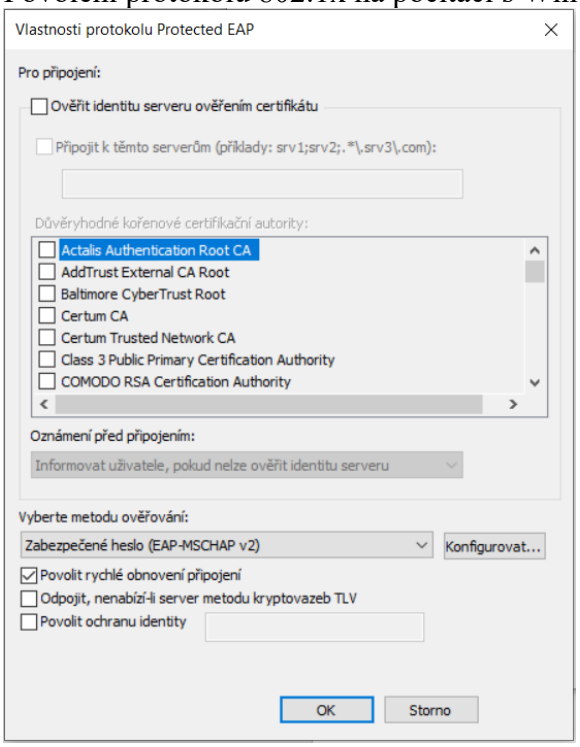
```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
```

9. Aby zkušební počítač věděl, že má při přihlášení požadovat autentizaci uživatele, je zapotřebí tuto možnost zvolit v nastavení služeb. V záložce „tento počítač“ klikneme na Spravovat. Zvolíme Služky a Aplikace a dále klikneme na tlačítko Služby, zde najdeme službu Wired AutoConfig Service, kterou povolíme. Dále je potřeba konkrétněji nastavit možnosti ověření na adaptéru. V záložce Ovládací panely – Síť a internet – Síťová připojení rozklikneme vlastnosti síťového adaptéru Ethernet – Ověřování a povolíme možnost ověření podle standardu IEEE 802.1X. V nastavení protokolu 802.1X zvolíme možnost ověření uživatele.

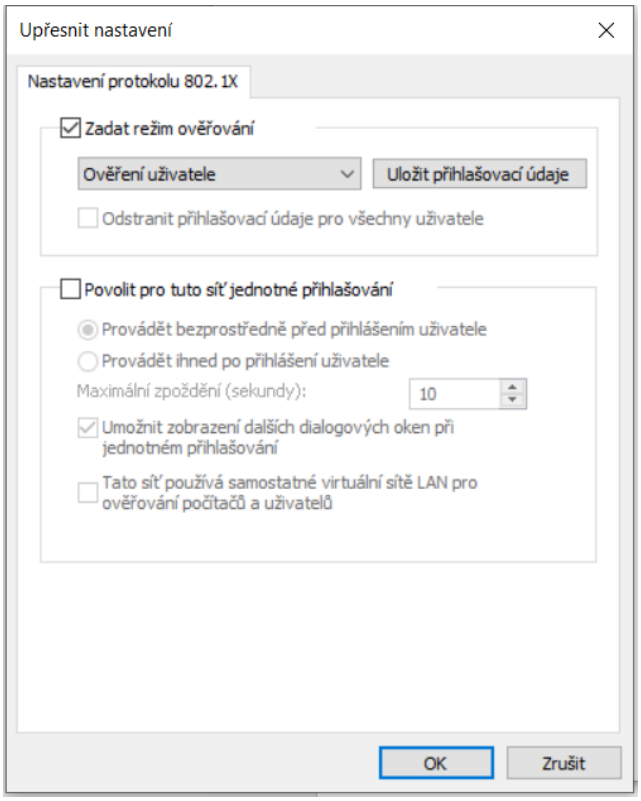
Povolení protokolu 802.1x na počítači s Windows



Povolení protokolu 802.1x na počítači s Windows



Povolení protokolu 802.1x na počítači s Windows



10. Zapněte program WireShark a podívejte se na zprávy, které jsou přeposílány mezi RADIUSem a testovacím pc.

Na obrázku č. 2 je vidět úspěšná autentizace uživatele „učitel“.

No.	Time	Source	Destination	Protocol	Length	Info
66	5.610000	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	29	Response, Identity
67	5.610029	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	29	Response, Identity
68	5.616305	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
69	5.616907	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
70	5.616923	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
71	5.623241	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, Protected EAP (EAP-PEAP)
72	5.625116	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	190	Client Hello
73	5.625133	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	190	Response, Protected EAP (EAP-PEAP)
74	5.637079	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	1022	Request, Protected EAP (EAP-PEAP)
75	5.637841	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
76	5.637857	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
77	5.645484	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	182	Server Hello, Certificate, Server Key Exchange, Server Hello Done
78	5.648498	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	154	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
79	5.648509	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	154	Response, Protected EAP (EAP-PEAP)
80	5.654941	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	75	Change Cipher Spec, Encrypted Handshake Message
81	5.658889	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
82	5.658909	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
83	5.664546	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
84	5.665280	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
85	5.665289	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	60	Response, Protected EAP (EAP-PEAP)
86	5.671015	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	92	Application Data
87	5.673649	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	114	Application Data
88	5.673663	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	114	Response, Protected EAP (EAP-PEAP)
89	5.679617	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	100	Application Data
90	5.680995	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	55	Application Data
91	5.681020	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	55	Response, Protected EAP (EAP-PEAP)
92	5.688589	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
93	5.692586	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
94	5.692716	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	64	Response, Protected EAP (EAP-PEAP)
95	5.703840	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Success

```
Mon May 11 04:20:37 2020
        Acct-Session-Id = "0000001E"
        User-Name = "ucitel"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Ethernet
        NAS-Port = 50003
        NAS-Port-Id = "FastEthernet0/3"
        Called-Station-Id = "00-11-92-B5-3D-03"
        Calling-Station-Id = "00-21-70-F9-7E-90"
        Service-Type = Framed-User
        NAS-IP-Address = 192.168.1.50
        Acct-Delay-Time = 0
        Event-Timestamp = "May 11 2020 04:20:37 PDT"
        Tmp-String-9 = "ai:"
        Acct-Unique-Session-Id = "7e32b17df833d2551a252413dd1fd85d"
        Timestamp = 1589196037

Mon May 11 04:20:37 2020 : Auth: (9)  Login OK: [ucitel/<via Auth-Type = eap>] (from client
cisco-switch port 0 via TLS tunnel)
Mon May 11 04:20:37 2020 : Auth: (10) Login OK: [ucitel/<via Auth-Type = eap>] (from client cisco-
switch port 50003 cli 00-21-70-F9-7E-90)
```

Obrázek 2: Úspěšná autentizace uživatele

Na obrázku je vidět neúspěšná autentizace uživatele „učitel“ po zadání nesprávného hesla.

No.	Time	Source	Destination	Protocol	Length	Info
85	12.669940	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	29	Response, Identity
86	12.676056	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
87	12.677650	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
88	12.677667	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Legacy Nak (Response Only)
89	12.683450	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Request, Protected EAP (EAP-PEAP)
90	12.685435	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	190	Client Hello
91	12.685453	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	190	Response, Protected EAP (EAP-PEAP)
92	12.696864	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	1022	Request, Protected EAP (EAP-PEAP)
93	12.697424	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
94	12.697437	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
95	12.705253	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	182	Server Hello, Certificate, Server Key Exchange, Server Hello Done
96	12.708848	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	154	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
97	12.708869	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	154	Response, Protected EAP (EAP-PEAP)
98	12.715854	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	75	Change Cipher Spec, Encrypted Handshake Message
99	12.719851	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
100	12.719875	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	24	Response, Protected EAP (EAP-PEAP)
101	12.725643	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
102	12.726344	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	60	Application Data
103	12.726357	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	60	Response, Protected EAP (EAP-PEAP)
104	12.732183	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	92	Application Data
105	12.734738	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	114	Application Data
106	12.734753	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	114	Response, Protected EAP (EAP-PEAP)
107	12.740769	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
108	12.742712	Dell_f9:7e:90	Nearest-non-TPMR-bridge	TLSv1.2	64	Application Data
109	12.742727	Dell_f9:7e:90	Nearest-non-TPMR-bridge	EAP	64	Response, Protected EAP (EAP-PEAP)
110	12.791400	fe80::7537:ac3a:cda…	ff02::c	UDP	714	65450 → 3702 Len=652
111	12.900322	169.254.36.166	239.255.255.250	UDP	694	65449 → 3702 Len=652
112	13.676390	fe80::7537:ac3a:cda…	ff02::c	UDP	718	65450 → 3702 Len=656
113	13.750596	Cisco_b5:3d:03	Nearest-non-TPMR-bridge	EAP	60	Failure

Obrázek 3: Neúspěšná autentizace uživatele

Otázky:
1. Jaké IP adresy vám přidělil DHCP server u jednotlivých VLAN ?
2. Jaké síťové přístupy byly umožněny u jednotlivých uživatelů ?
3. Proč můžeme použít nástroj ping na zakázané stránky v pravidlech ?

Závěr

Tato úloha byla zaměřená na konfiguraci RADIUS serveru, kde jsme si zkusili možnosti autentizace uživatele a poté omezení přístupu na webové stránky. IP adresy, které byly DHCP serverem přiděleny jsou pro VLAN 1 : 10.10.10.2, VLAN 2 : 10.10.20.2, VLAN 3 : 10.10.30.2 (tyto IP adresy byly přiděleny ve zkušebním zapojení). VLAN 1 se dostala všude, VLAN2 se dostala pouze na stránku *www.vutbr.cz*, VLAN3 se dostala pouze na stránku *apollo.vutbr.cz*. Nástroj ping funguje i na zakázané stránky, protože v nastavení firewallu není zakázaný protokol ICMP na tyto stránky.