Fakulta elektrotechnická
Katedra telekomunikační techniky

Bakalářská Práce

Autentizace v lokálních sítích pomocí IEEE 802.1x

květen 2019

Bakalant:
Vladimír Lešek

Vedoucí:
Ing. Tomáš Vaněk, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a konzultanta a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

Datum:

.....

podpis bakalanta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Lešek** Jméno: **Vladimír** Osobní číslo: **457101**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Síťové a informační technologie**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Autentizace v lokálních sítích pomocí IEEE 802.1x

Název bakalářské práce anglicky:

Authentication in Local Area Network using IEEE 802.1x

Pokyny pro vypracování:

Seznamte se s pokročilými metodami autentizace stanic v lokálních sítích využívajících technologie IEEE 802.1x a protokoly Radius a LDAP. Navrhněte a v rámci možností zrealizujte, nakonfigurujte a ověřte funkčnost ověřování koncových stanic v LAN komunikujících protokoly Ethernet a WiFi pomocí protokolu Radius. Vlastní ověřování provádějte vůči databázi LDAP. V rámci řešení zvažte i variantu nasazení infrastruktury veřejných klíčů (PKI) a použití tzv. machine certifikátů.

Seznam doporučené literatury:

[1] 802.1X - Port Based Network Access Control, http://www.ieee802.org/1/pages/802.1x.html [on-line]
[2] Remote Authentication Dial In User Service (RADIUS), https://tools.ietf.org/html/rfc2865 [on-line]
[3] Lightweight Directory Access Protocol (LDAP): The Protocol, https://tools.ietf.org/html/rfc4511 [on-line]

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Tomáš Vaněk, Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **11.09.2018** Termín odevzdání bakalářské práce: **24.05.2019**

Platnost zadání bakalářské práce: **16.02.2020**

Ing. Tomáš Vaněk, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

. | Datum převzetí zadání

Podpis studenta

Anotace

Bakalářská práce se zabývá zabezpečením přístupu do lokální sítě pomocí IEEE 8O2.1X. Obsahuje základní popis AAA architektury, protokolů RADIUS, DIAMETER, TACACS, TACACS+, KERBEROS a problematiky PKI. Další částí je implementace tohoto zabezpečení ve firemní sítí. Práce obsahuje konfiguraci prvků v sítě a dalších součást a následné ověření funkčnosti.

Klíčová slova

AAA architektura, IEEE 802.1X, RADIUS, DIAMETER, TACACS, TACACS+, LDAP, Windows server

Summary

The bachelor thesis deals with the security of access to the local network using IEEE 8O2.1X. It contains a basic description of AAA architecture, RADIUS, DIAMETER, TACACS, TACACS+, KERBEROS and PKI issues. Another part is the implementation of this security in the corporate network. The thesis includes configuration of elements in the network and other components and subsequent verification of functionality.

Index Terms

AAA architecture, IEEE 802.1X, RADIUS, DIAMETER, TACACS, TACACS+, LDAP, Windows server

Obsah

1. Úvod

V práci se zabývám autentizací přístupu do lokální sítě pomocí IEEE 802.1X a dalšími součástmi, které souvisí s použitím tohoto standardu.

V teoretické části se budu věnovat AAA architektuře a stručnému popisu a srovnaní protokolů využívajících tuto architekturu, jako jsou protokoly RADIUS, DIAMETER, TACACS, TACACS+ a KERBEROS. Dále popíši komunikaci IEEE 802.1X a protokolu RADIUS od koncové entity až po autentizační server. Stručně také rozeberu protokol LDAP, který je využíván na autentizačním serveru k správě autentizačních dat. Dále se budu věnovat popisu Infrastruktury veřejných klíčů, kterou budu využívat pro ověřovaní koncových stanic.

V praktické části budu využívat nabyté znalosti z teoretické části pro zprovoznění autentizace v existující firemní síti pomocí IEEE 802.1X, RADIUS protokolu a Windows serveru. To bude zahrnovat konfiguraci RADIUS serveru, síťových prvků (switche, routery) koncových stanic a také konfiguraci Certifikační autority na Windows serveru. Posledním krokem bude ověření, zda implementace tohoto řešení bude fungovat podle očekávání.

2. AAA architektura

AAA je zkratka pro Authentication, Authorization, Accounting neboli Autentizace, Autorizace a Účtování. Používá se pro zajištění zabezpečení síťové infrastruktury. Zabývá se identifikací koncové entity v síti (autentizace), právy pro přístup k funkcím sítě (autorizace) a sledováním využití funkcí sítě (účtování). [17] [9]

2.1 Autentizace

Autentizace znamená ověření předkládané identity, že se jedná právě o ni, a ne o nějakou jinou a jestli má právo využívat službu.

Existují tři druhy autentizace:

1. Autentizace klienta

   Entita poskytne autentizační údaje (heslo, token, biometrické údaje) podle kterých ji poskytovatel služby ověří.

2. Autentizace informací

   Informace, které entita posílá, mohou být napadeny nebo poškozeny během doručování autentizačnímu serveru. Aby se tomuto zamezilo, entita ke zprávě přiloží údaje, pomocí kterých je možné ověřit, zda byly informace napadeny a tedy ověřit, jestli je zpráva pravdivá.

3. Vzájemná autentizace

   Zde se neověřuje pouze koncová entita, ale také služba, kterou chce entita využívat. Jde o ověření, zda se entita připojuje ke službě, kterou chce používat. Tedy jestli se nejedná o podvrhnutou/napadenou službu. Tohoto se využívá například u Wi-Fi, kde síť posílá jedinečnou identifikaci a až po ověření sítě pošle entita své identifikační údaje.

Postupy autentizace

1. Two-party (se dvěma účastníky)

   Ověřovací autorita přímo ověří koncovou entitu, která žádá přístup ke službě.

2. Three-party (se třemi účastníky)

   Ověřovací autorita se zeptá výše postavené autority, která má právo rozhodnout, jestli jsou identifikační údaje koncové entity platné a až pak entitu ověří. Tento model

je použit i v protokolu AAA. U tohoto postupu může být koncová entita ověřena i bez toho, aby výše pověřenou autoritu. Například pokud se uživatel hlásí k firemní Wi-Fi ve dvou různých lokalitách. Identifikační údaje jsou v obou lokalitách stejné. Místní ověřovací autority se dotážou nadřazené autority, která rozhoduje o autentizaci.

2.2 Autorizace

Zajišťuje přidělení oprávnění pro danou službu. Tento krok následuje po autentizaci, kdy už je uživatel ověřen. Příklad: do firemní sítě se připojí zákazník účastnící se školení. Zákazník projde autentizací a AAA server mu přidělí práva jen pro přístup na internet a do vnitřní sítě nikoliv. Pokud se připojí zaměstnanec firmy, tak AAA přidělí práva, jak pro přistup na internet, tak i pro přístup do interní sítě. Autorizace často probíhá současně s autentizací a nelze ji oddělit. Například pokud má zaměstnanec ve firmě přístup jen do určených pater, tak se u výtahu čipem zároveň autentizuje a autorizuje. Autentizace: výtah se otevře; Autorizace: bude moc jet jen do konkrétních pater.

Komunikace v procesu autorizace

1. Agent sequence

   Komunikace probíhá přes AAA server jako prostředníka. Uživatel pošle dotaz na danou službu AAA serveru. Pokud má uživatel práva na tuto službu AAA server pošle informaci službě a zároveň informuje uživatele, že byl přístup povolen. (RADIUS, TACACS, TACACS+)

2. Pull sequence

   Uživatel komunikuje přímo se službou, tak dotazy autorizuje u AAA serveru. Pokud autorizace bude úspěšná, služba informuje uživatele. (DIAMETER)

3. Push sequence

   Uživatel se proti službě prokáže tiketem nebo certifikátem, který obdržel od AAA serveru při procesu autentifikace. V podstatě zde uživatel funguje podobně jako prostředník (AAA server) v prvním případě. (KERBEROS)

2.3 Účtování

Mechanismus pro sběr informací a dat o uživateli, který využívá služby (vše co uživatel v dané síti dělal a k jakým službám přistupoval). Data sbírá přímo využívaná služba a posílá je na AAA server. Data se následně dají využít pro audit, dokazování přístupu nebo pro stanovaní poplatku za služby.

Způsoby sběru dat

1. Polling

   AAA server se dotazuje zařízení, které poskytuje služby uživateli.

2. Event-Driven

   Zařízení poskytující službu poskytuje AAA serveru data v určitou dobu. V tuto dobu si je AAA server stáhne. Nestažená data jsou uložena v paměti zařízení, kde se uchovávají po nějakou dobu.

2.4 Protokoly architektury AAA

V architektuře AAA se využívají nejvíce protokoly: RADIUS, TACACS, TACACS+, KERBEROS a DIAMETER.

2.5 RADIUS protokol

Remote Authentication Dial In User Service je AAA protokol, který poskytuje služby centralizované autentizace, účtování a správy IP používaný pro přístup k síti skrze síťové prvky (RADIUS klient). Komunikace pomocí RADIUS protokolu probíhá mezi RADIUS klientem a RADIUS serverem (autentizační server). RADIUS server zajišťuje autentizaci a autorizaci na portu UDP 1812 a accounting na portu UDP 1813. RADIUS server zpracovává informace od RADIUS klienta ve 2 fázích. Ověřením zkontroluje identitu uživatele porovnáním údajů ve své databázi se zaslanými údaji. Po úspěšné autentizaci dojde k druhé fázi a tou je autorizaci, která uděluje, k jakým službám má uživateli přístup (například připojení do konkrétní VLAN). Druhy komunikace mezi klientem a serverem jsou uvedeny v tabulce 2.1 [18] [5]

Typ zprávy	**Význam**
Access-Request	Žádost o autentifikaci
Access-Challenge	Žádost o další informace od koncové entity
Accounting-Request	Statistická data pro účtování
Accounting-Response	Potvrzení příjmu statistických dat
Access-Accept	Koncová entita je ověřena
Access-Reject	Koncová entita nebyla ověřena

Tabulka 2.1: RADIUS zprávy

2.5.1 Podrobnější popis autentizace a autorizace

1. Koncová entita posílá požadavek o přístup k síti na RADIUS klienta. RADIUS klient, pak získá autentizační informace koncové entity. Těmito informacemi naplní zprávu Access-Request a odešle ji na RADIUS server

2. RADIUS server ověří informace ze zprávy Access-Request v databázi vůči, které se ověřuje

3. Jestliže se autentizační údaje neshodují s údaji v databázi, koncová entita nemá přístup do sítě. RADIUS server odešle na RADIUS klienta zprávu Access-Reject. Tím má koncová entita blokovaný přístup do sítě

4. Může nastat situace, že koncová entita neposkytla veškeré autentizační údaje, které RADIUS server požaduje. V takovém případe RADIUS Server odešle na RADIUS klienta zprávu Access-Challenge a ten ji přepošle koncové entitě. Entita odpovídá opět zprávou Access-Request s doplněnými informacemi

5. V případě, že RADIUS server má již všechny požadované autentizační informace od koncové entity a shodují se se záznamy v databázi, RADIUS server pošle zprávu Access-Accept RADIUS klientovi a povolí přístup do sítě

6. Po autentizaci koncové entity následuje autorizace. Ta může proběhnout zároveň s autorizací nebo muže být ovlivněna atributy AVP o kterých se zmiňují v části 2.5.2

2.5.2 Formát paketu

Code – Délka 8 bitů – identifikuje typ RADIUS paketu. Pokud je hodnota neplatná, je paket zahozen. Může obsahovat hodnoty z tabulky 2.1

Identifier – Délka 8 bitů – pomáhá správnému párování odpovídajících požadavků a odpovědí.

Length – Délka 16 bitů – určuje celkovou velikost RADIUS paketu v oktetech. Když by velikost paketu byla menší, něž je hodnota uvedená v poli Délka, může dojít k zahození paketu. Minimální délka je 20 B, maximální délka je 4096 B.

Authenticator – Délka 128 bitů – jeho hodnota je použita při authentizaci odpovědi z RADIUS serveru a dále je použita při šifrování posílaného hesla.

Attribute – Délka se liší podle parametrů AVP (je proměnná) – nesou specifické autentizační, autorizační, informační a konfigurační detaily pro požadavky a odpovědi. Konec seznamu atributů je určen délkou RADIUS paketu.

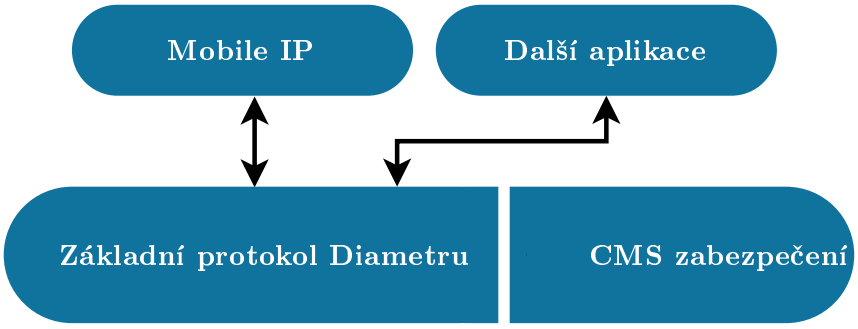
Atributy AVP – Attribute Value Pairs dále ovlivňují autorizaci v síti. Jedná se vždy o dvojici například: „username“ a „Novák“ nebo připojení MAC adresy klienta na konkrétní port authentikátora/připojení do konkrétní VLANy.

U komunikace mezi uživatelem (suplicantem) a switchem (authenticator) se protokol EAP zabaloval standardem 802.1x. Switch tyto informace zpracuje, přeloží a zabalí je do protokolu RADIUS pro komunikaci s RADIUS serverem. (Obrázek se schématem komunikace celé sítě)

2.6 DIAMETER

V roce 2000 byla vytvořena skupina, která se zabývala hledáním nástupce protokolu RADIUS, který se považoval za dokončený. Výsledkem byl protokol Diameter, který splňoval rostoucí nároky a požadavky AAA architektury. Diameter využívá spolehlivého protokolu TCP nebo SCTP a podporuje End-to-End komunikaci, to je hlavní výhoda oproti RADIUS protokolu. Diameter je založen na základním protokolu diametru, který určuje základní procesy (přenos, formát zprávy) a na aplikacích (služby). Příkladem aplikace je CMS zabezpečení (Cryptographic Message Syntax). CMS poskytuje zabezpečení všem dalším aplikacím a protokolu Diameter. Další aplikací může být „Mobile IP“. Tato aplikace umožnuje koncové entitě zachovat si stejnou IP adresu i když se pohybuje mezi různými sítěmi.

End-to-End komunikace – cílový Diameter server komunikuje s koncou entitou přímo, poté co mu požadavek předal jiný server. Předchozí server nemá přístup k informacím o koncové entitě. [2] [4]



Obrázek 2.1: Struktura protokolu Diametr

2.7 TACACS

Terminal Access Controller Access–Control Systém je vzdálený autentizační protokol, který byl původně vyvíjen pro armádu Spojených státu amerických, později vývoj převzala firma Cisco Systems. Používá se pro komunikaci a autentizačním severem. Komunikace standardně probíhá přes UDP na portu 49. Protokol komunikuje se vzdálením autentizačním serverem (někdy také TACACS démon nebo TACACSD), vůči kterému se koncová entita autentizuje. Protokol odesílá na autentizační server jméno a heslo koncové entity. Autentizační proces a algoritmus je otevřený a záleží jaký si provozovatel TACACSD zvolí.

2.8 TACACS+

Navazuje na protokol TACACS, ale není s ním zpětně kompatibilní. Pro komunikaci používá protokol TCP na portu 49. Části standardu AAA, tedy autentizaci, autorizaci a účtování, dělí do nezávislých částí. Oproti tomu RADIUS spojuje části autentizace a autorizace do jedné. Další vylepšení tohoto protokolu je, že šifruje všechny zprávy, které proběhnou v rámci komunikace mezi koncovou entitou a TACACS+ serverem. Zjednodušuje také správu sítě centralizací správy koncových entit a nabití možnost nastavení politik, skupin, času nebo typu koncové entity. Má také rozšířený logovací systém a zaznamenává v něm každé přihlášení koncové entity, a také všechny příkazy, které byly použity entitou. [16]

2.9 KERBEROS

Tento protokol byl vyvinut na MIT (tato verze není volně šiřitelná). Volně šiřitelná verze je vyvíjena Royal Institute of Technology ve Švédsku.

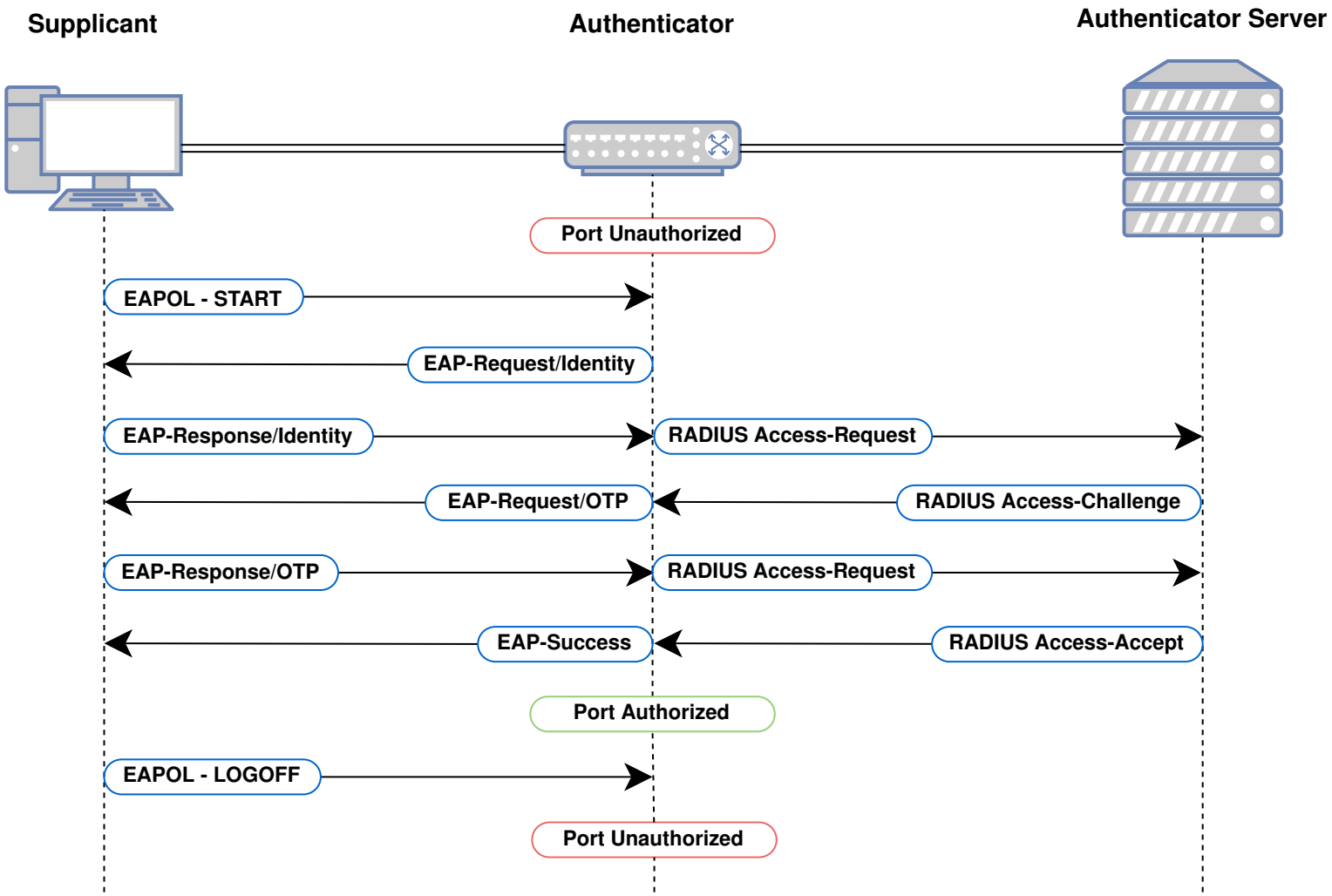
Je to protokol, který vychází z předpokladu takového, že síť, přes kterou se přenášejí informace není důvěryhodná. Proto je kladen maximální důraz na bezpečnost protokolu. Princip autentizace funguje tak, že se koncová entita autentizuje vůči prostředníkovi KDC (Key Distribution Center – centrální autentizační prvek), nikoliv proti službě, kterou požaduje. Zároveň prokazuje svou identitu také KDC. KDC zvyšuje bezpečnost a poskytuje služby více aplikacím. Infrastruktura protokolu je tedy centralizovaná a musí se zajistit dobré zabezpečení tohoto prvku, protože zná všechny šifrovací klíče. Pro přenos hesel v síti se využívají zmíněné časově limitované kryptografické tickety (klíče). Kerberos nezajišťuje dvě vlastnosti AAA architektury, což je autorizace a účtování. [13]

3. Standard IEEE 802.1x

Standard sloužící k zabezpečení přístupu do sítě využívající Port-based Network Access Control. Což znamená kontrolu řízení přístupu založenou na portu. Nejvíce se používá v LAN sítích. U metalických sítí se jedna o fyzické zabezpečení na spojové vrstvě (2. vrstva ISO/OSI).

3.1 Popis komunikace IEEE 802.1x

Standard je založen na EAP protokolu (Extensible Authentication Protocol) RFC 3748. Jedná se tedy zapouzdření neboli „zabalení“ zpráv EAP tak, aby tyto zprávy bylo možné předávat bez zapojení 3. vrstvy modelu OSI/OSI. Ve spojení se klient žádající o přístup do sítě nazývá „supplicant“ a síťový prvek zpracovávající požadavek je nazýván „authenticator“. Tento protokol se používá na síťových prvcích vyšší třídy (např. managovatelné switche). Když se klient připojí do sítě je port ve stavu „unauthorized“. To znamená, že je blokována veškerá komunikace kromě provozu standardu 802.1X. Dalším krokem je autentizace, ta má několik fází: Authenticator předá informace autentizačnímu serveru. V případě protokolu RADIUS Authenticator překládá EAP zprávy do formátu RADIUS „EAP-Message“ (význam zpráv je popsán v kapitole 2.5). Když má klient správné údaje, dojde k úspěšné autentizaci, o které je informován authenticator a povolí další síťovou komunikaci (port se přepne stavu „authorized“). Pokud se klient odpojí, port se přepne do stavu „unauthorized“. Průběh komunikace je vidět na obrázku 3.1. [19]



Obrázek 3.1: Komunikace IEEE 802.1x a RADIUS protokolu

Typ zprávy	Význam
EAPOL - START	Začátek komunikace EAP
EAP-Request/Identity	Žádost o autentizaci
EAP-Response/Identity	Odpověď na žádost (např. síť, do které chce suplicant přístup)
EAP-Request/OTP	Žádost o autentizační údaje (OTP - One Time Password)
EAP-Response/OTP	Odpoveď s autentizačními údaji
EAP-Success	Povolení přístupu do sítě
EAPOL - LOGOFF	Ukončení komunikace se sítí

Tabulka 3.1: EAP zprávy

O autentizaci se v tomto standardu tedy stará EAP. Tento protokol zajišťuje rámec pro různé metody ověřování. Například:

EAP-TLS – Zde se pro autentizaci koncové entity a serveru využívá klientských certifikátů. Je to jedna z nejbezpečnějších metod autentizace EAP. Bohužel ale není tak často používána zřejmě z důvodu distribuce a obnovování klientských certifikátů.

EAP-PEAP – u této metody se také používá certifikát, ale tentokrát na straně serveru. Klient ověří certifikát autentizačního serveru. Pak se vytvoří šifrovaný tunel pomocí TLS, ve kterém probíhá další komunikace protokolu EAP. Například zde dojde k ověření klienta díky metodám MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2), SIM (Subscriber Identity Module) nebo GTC (Generic Token Card) Napravuje nedostatky samotného EAP, který předpokládá zabezpečené fyzické i komunikační kanály. Tato metoda se nedá narušit man-in-the-middle útokem.

Modifikací protokolu EAP je daleko více, ale používá se pouze omezený počet. [1]

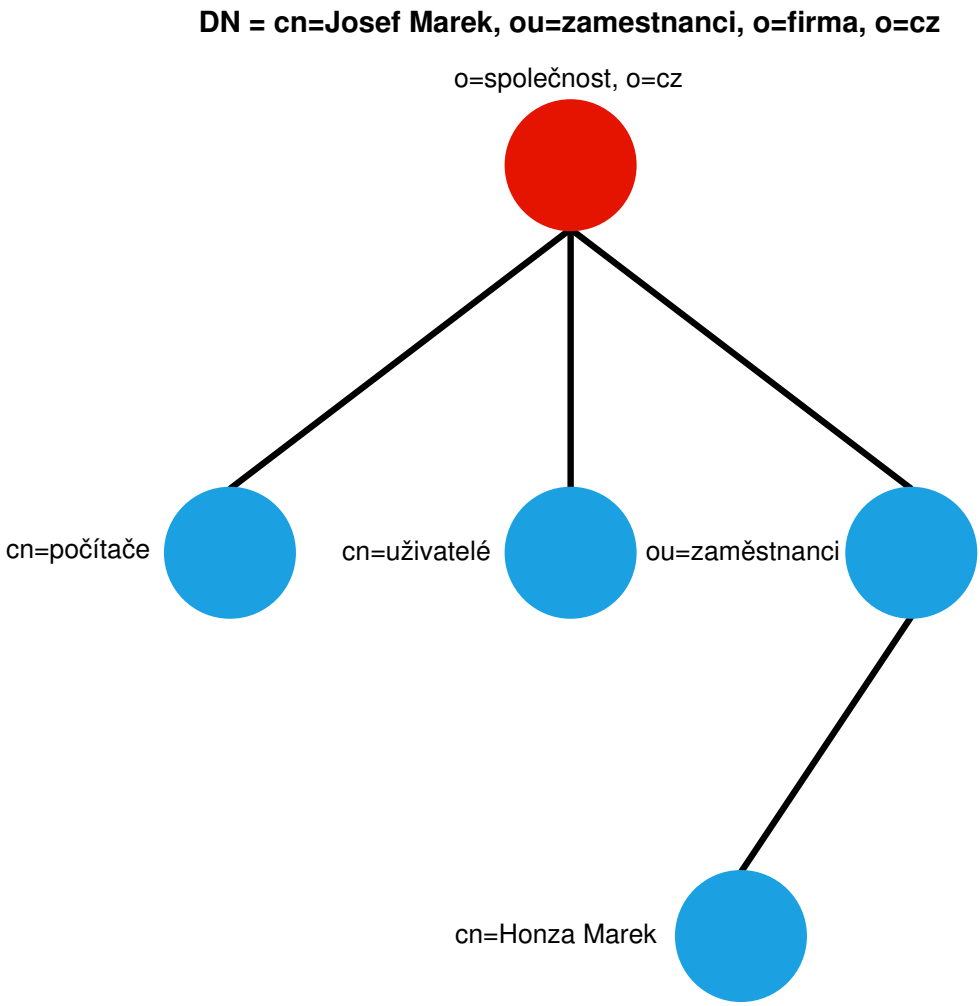
4. LDAP protokol

LDAP (Lightweight Directory Access Protocol) je protokol pro ukládání a přístup k datům na adresářovém serveru, ve stromové struktuře. Jak je patrné z názvu LDAP je zjednodušený (odlehčený) protokol (vynechání složitějších operací →redukce komunikace) založen na standardu X.500 (DAP - Directory Access Protocol, DSP - Directory Service Protocol, DISP - Directory Information Shadowing Protocol, DOP - Directory Operational Bindings Management Protocol), který v 80. letech pokrýval adresářové služby – jsou specializované aplikace, které slouží k ukládání dat, k jejich organizaci a přístupu k nim. V praxi to například znamená seznam lidí firmy, jejich přihlašovací jména, domovské adresáře, osobní informace, jména jejich e-mailů nebo čísla telefonů, ale nemusí to být omezeno pouze na informace o lidech nebo firmách, jsou i jiné aplikace. Pojem LDAP, lze vnímat jako samotný komunikační protokol, ale i adresářový server.

Komunikace je založena na systému klient-server. Pro výměnu dat LDAP používá LDAP Data Interchange Format (LDIF) – standardizovaný textový formát, kde jsou data při přenosu kódována Lightweight Basic Encoding Rules (LBER), to však není z důvodu bezpečnosti, ale nehomogenity prostředí, proto je velmi jednoduchá data dekódovat. [8]

Jak jsem zmínil jedná se o ukládání dat ve stromové struktuře pomocí záznamů. Záznamy se definují pomocí tří základních prvků [11]:

1. Distinguished name (DN)
    - Jednoznačný identifikátor, který se používá pro identifikaci objektů a obsahuje celou cestu k záznamu
    - Existuje ještě Relative Distinguished Name (RDN). Používá se, když nepotřebujeme znát celou cestu k objektu. Tato hodnota je jednoznačná v celé databázi
2. Object class
    - Kategorie, do kterých můžou být objekty zařazeny
    - Může nabývat více hodnot
3. Atributy
    - Nesou informace o stavu záznamu a definují se pomocí objektů, které se definují na serveru. V základu jsou nadefinovány například objekty person nebo organization
    - Základní atributy jsou „o“ – Organization, „ou“ – OrganizationUnit, „uid“ – UserID, „cn“ – CommonName, „c“- Country



Obrázek 4.1: LDAP - Stromová struktura

4.1 Autentizace klienta proti LDAP

Autentizace využívá 3 operací, které pracují s autentizačními informacemi.

1. Bind – inicializuje spojení, vyjednává o metodě autentizace, autentizuje
2. Unbind – ukončí spojení
3. Abandon – klient žádá o ukončení posílání výsledků na poslední dotaz

U LDAP protokolu je 6 druhů autentizace

1. Anonymní autentizace – využívá se operace bind, ale ta nezasílá žádné identifikační údaje o klientovi.

2. Jednoduchá autentizace – tentokrát operace bind zasílá identifikace údaje uživatele pomocí jeho DN a hesla.

3. Jednoduchá autentizace přes TLS/SSL – nejdříve si klient a server vymění certifikáty, které se ověří a poté se otevře zabezpečený kanál TLS/SSL a proběhne autentizace stejně jako v předešlém případě.

4. Proxy autentizace – využívá existence definovaného uživatele, který má právo nahlížet na hesla ostatních uživatelů. Autentizace požadovaného uživatele tedy probíhá přes proxy uživatele, který může například pomocí operace compare porovnat platnost zadaných údajů a pak se připojit k serveru pomocí operace bind.

5. PKI autentizace – založena na principu PKI certifikátů, které jsou uloženy v atributu userCertificate. Klient při připojení zadává heslo k certifikátu a server následně ověří, zdali jsou oba certifikáty na straně uživatele a na straně serveru shodné. Nevýhoda této metody je v tom, že se certifikáty musí aktualizovat na obou stranách.

6. SASL mechanizmus – Simplex Authentication and Security Layer - umožnuje použití množství zásuvných modulů (např. PLAIN - autentizační informace jsou kódování pomocí base64) pro autentizaci uživatele.

4.1.1 Příklad jednoduché autentizace

1. Uživatel posílá žádost o připojení, jehož součásti je uživatelské jméno a heslo klienta LDAP

2. Klient LDAP vytvoří TCP spojení s LDAP serverem

3. Klient LDAP použije správcovské údaje pro příkaz Bind, aby mohl vyhledávat

4. Server LDAP potvrdí klienta LDAP

5. Klient LDAP odešle žádost na vyhledání uživatele na LDAP serveru

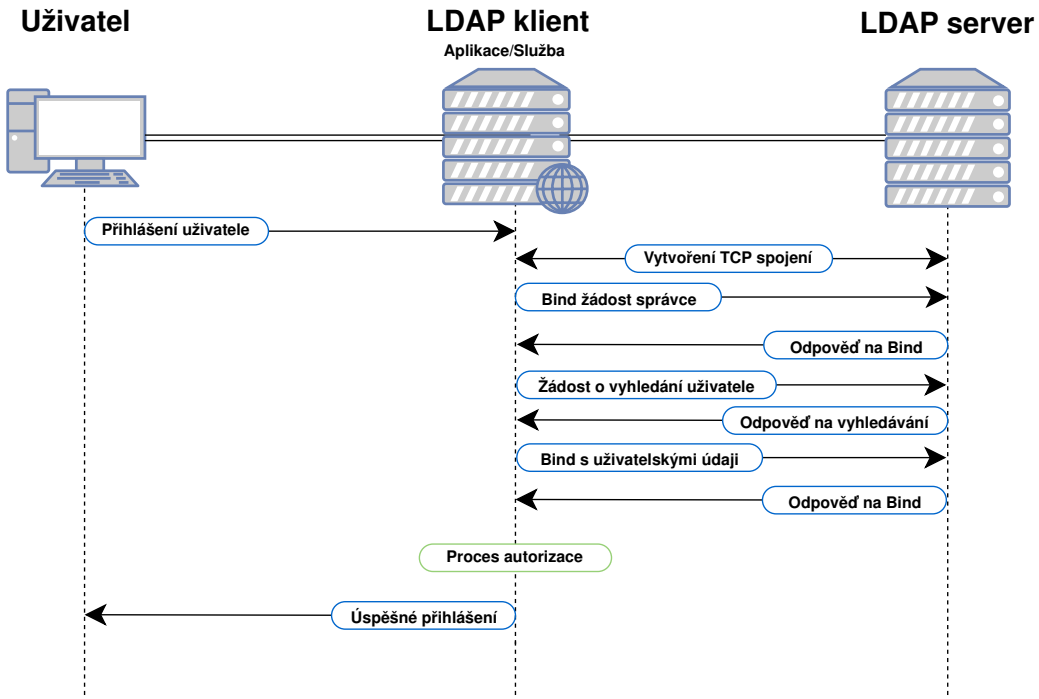
6. Pokud LDAP server našel uživatele odešle odpověď o úspěchu hledání (může být více výsledků)

7. Klient LDAP použije uživatelské jméno a heslo pro příkaz Bind

8. Server LDAP odešle výsledek operace Bind. Pokud by nebyla úspěšná, pošle uživateli zprávu o zamítnutí přístupu

9. Klient LDAP uloží jméno uživatele a začne proces autorizace

10. Klient LDAP odpoví uživateli, že byl úspěšně přihlášen [6]



Obrázek 4.2: LDAP autentizace

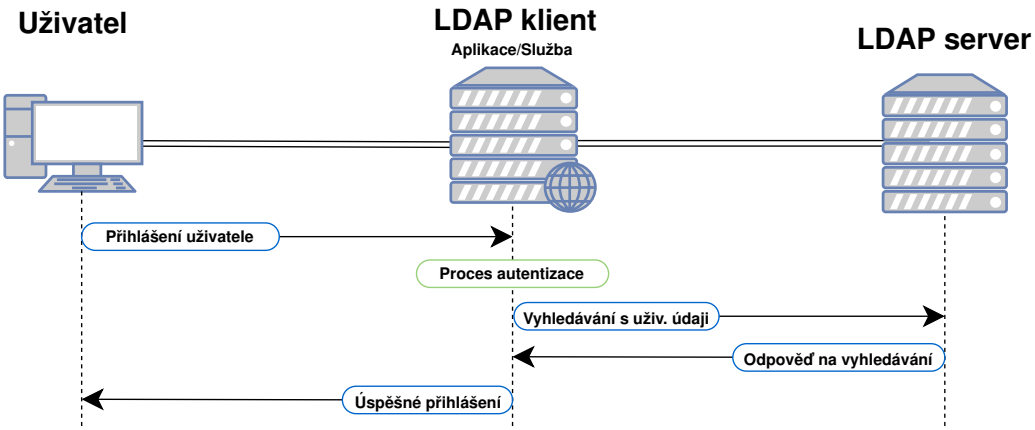
4.2 Autorizace

K autorizaci dochází po skončení autentizace. Vlastně se jedná o nastavení přístupových práv k záznamům a atributům. Když se jedná o uživatelská data může se použít například toto nastavení: Uživatel má právo „write“ na všechny své atributy. U ostatních uživatelů má právo „read“, kromě atributu userPassword, kde je nastaveno právo „none“ (nemůže provádět žádné operace).

4.2.1 Příklad jednoduché autorizace

Uživatel je již úspěšně autentizován

1. Klient LDAP pošle žádost o hledání s uživatelskými údaji
2. Server LDAP vyhledá informace o uživateli podle DN, rozsahu vyhledávání, podmínek filtrování a atributů LDAP, pokud je nalezena shoda upozorní LDAP klienta
3. Klient LDAP odpoví uživateli, že byl úspěšně přihlášen [6]



Obrázek 4.3: LDAP autorizace

5. INFRASTRUKTURA VEŘEJNÝCH KLÍČŮ

Neboli Public Key Infrastructure (PKI) je systém založený na technických postupech, speciálním hardware a software, organizačních principech, aplikacích, standardech, legislativě, dohodách a znalostech se kterými má zajistit autentizaci, důvěrnost, integritu, řízení přístupu a nepopiratelnost. K tomuto se také využívá například technologie elektronického podpisu nebo digitální certifikátu jehož forma je popsána v normě ITU X.509.

PKI využívá asymetrické kryptografie, kdy šifruje data pomocí kryptografických algoritmů a veřejného a privátního klíče. Privátní klíč nelze získat ze znalosti veřejného klíče. Těchto postupů se využívá u elektronických podpisů. [7] [14]

5.1 Základní části PKI

1. 1. Certifikační autorita (CA)
    - Vydává a podepisuje certifikáty
2. Registrační autorita (RA)
    - Vyřizuje žádosti o certifikát
    - Komunikuje se zákazníkem
    - Ověřuje totožnost
3. Validační autorita (VA)
    - Udržuje adresář vydaných certifikátů
    - Zajišťuje dostupnost certifikátu přes Internet (LDAP)
4. Certificate Revocation List (CRL)
    - Seznam zneplatněných certifikátů – mohlo dojít ke kompromitaci certifikátů, a proto byl zneplatněn
5. Online Certificate Status Protocol (OCSP)
    - Protokol pro získání stavu certifikátu
    - Alternativa k CRL – je úspornější, je stále aktuální →CRL se aktualizuje za časový interval

6. Certifikační politiky a prováděcí směrnice (CP a CPS)
    - Množina pravidel určující účel, podmínky, algoritmy při vydávání certifikátu

5.2 Certifikační autorita (CA)

Důležitá část PKI, která vydává digitální certifikáty a tím potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči. Díky tomu stačí důvěřovat CA, která daný digitální certifikát vydala a víme, že údaje v něm jsou správné. Z toho vyplývá, že nejdůležitější u CA je její důvěryhodnost. Ta se dá posoudit například podle toho, jakým způsobem ověřuje údaje žadatele o certifikát. Tyto informace jsou dostupné v dokumentech CP/CPS. Tím, že si žadatel nechá vytvořit certifikát, získá CA mimo jiné peníze na to, aby mohla zaplatit za distribuci svých kořenových certifikátů vydavatelům software jako jsou například Microsoft Windows, Mozilla Firefox. Kořenový certifikát je podepsán samotnou CA, jedná se tedy o „self-signed“ certifikát (1), kde pole vydavatel a držitel je totožné. Hierarchie Certifikační autority je většinou strukturovaná. Je jedna kořenová CA, která má pod sebou další podřízené CA. Když důvěřuji kořenové CA, můžu důvěřovat i podřízeným CA. Podřízené CA se využívají pro různé oblasti činností: komerční certifikáty, kvalifikované certifikáty, časová razítka.

5.2.1 Kvalifikovaní poskytovatelé certifikačních služeb

Jsou definovaní v rámci České republiky v zákonu č. 297/2016 Sb. Plným jménem „Zákon o službách vytvářejících důvěru pro elektronické transakce“, tento zákon se řídí unijním nařízení eIDAS (elektronická identifikace a služby vytvářejících důvěru) Seznam kvalifikovaných certifikačních autorit, které mohou vydávat kvalifikované certifikáty zveřejňuje Ministerstvo vnitra České republiky. V současné době jsou čtyři kvalifikovaní poskytovatelé: `První certifikační autorita, a. s.`, `Česká pošta, s. p.`, `eIdentity a. s.`, `Software602 a.s.` [10] [3]

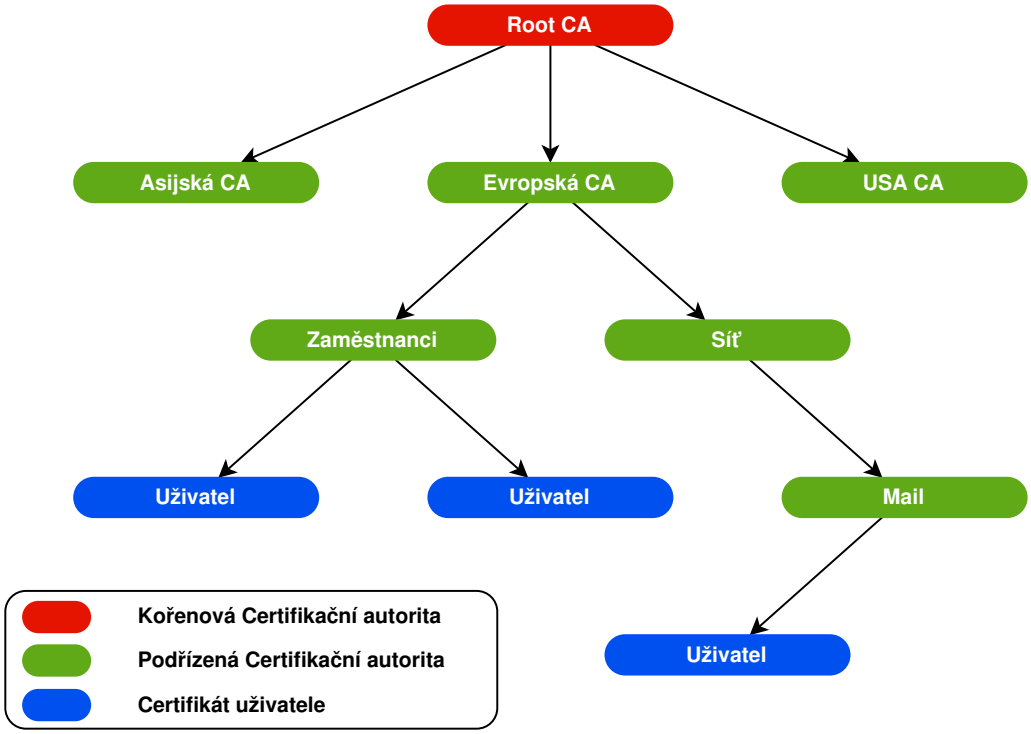
5.2.2 Třídy certifikátů definované CA

Class 0 - Demo certifikáty pro testování. Žádné ověření žadatele není požadováno. Platnost do 30 dnů.

Class 1 (DV – Domain validated) **-** CA kontroluje, zda daná emailová adresa existuje a zda má k ní majitel příslušného veřejného klíče přístup. Kontrola identity na nízké úrovni.

Class 2 (OV – Organization validated) **-** Určen pro firmy, není nutná osobní identifikace (stačí doložit existenci/sídlo firmy).

Class 3 (EV – Extedend validation) **-** Kromě ověření e-mailové adresy je třeba také osobní identifikace osoby na základě průkazu totožnosti nebo pasu. Pro firmy je vyžadována osobní přítomnost oprávněné osoby.



Obrázek 5.1: Příklad hierarchie CA

Class 4 Identifikační proces musí proběhnout na místě oficiálního úřadu pro registraci (státního nebo obecního úřadu).

5.3 Digitální certifikát

Datová struktura sloužící k ověření, že daný veřejný klíč jednoznačně patří entitě (osoba, server, proces), která vlastní odpovídající soukromý klíč. Digitální certifikát vydává důvěryhodná třetí strana, kterou je zde certifikační autorita. Tohoto důvěryhodného ověření se využívá pro ověření různých transakcí (digitální podpis, zabezpečení e-mailu, bezdrátové sítě Wi-Fi (WPA2), síťová autentizace, šifrování zpráv). Ekvivalentem k digitálnímu certifikátu je fyzický certifikát. To může být například řidičský nebo občanský průkaz. Jak jsem zmínil výše struktura certifikátu je popsána v normě ITU X.509. Obsah certifikátu je napsán v jazyce ASN.1 (Abstract Syntax Notation One) – jazyk pro popisování objektů, je nezávislí na počítačové platformě, relativně dobře čitelný pro člověka. Pomocí DER (Distinguished Encoding Rules) se jazyk ASN.1 kóduje pro binární přenos. Existuje ještě formát PEM (Privacy Enhanced Mail), které se používá, když certifikát obsahuje ASCII (Base64) data s předponou „---BEGIN CERTIFICATE---“. Další formáty jsou PKCS#7 a PKCS#12

5.3.1 Obsah digitálního certifikátu

- Identifikace držitele certifikátu
- Veřejný klíč držitele
- Identifikace vydavatele certifikátu
- Platnost certifikátu – od-do
- Pořadové číslo
- Informace, jak má být certifikát používán
- Digitální podpis vydavatele
- Další údaje

5.3.2 Přípony digitálních certifikátů

- .der, .cer, .crt – certifikát zakódovaný pomocí DER
- .pem – Certifikát zakodovaný pomocí PEM
- .p7b, .p7c – PKCS#7 – Struktura SignedData (podepsaná data) bez dat, obsahuje jen certifikáty nebo CRL
- .p12 – PKCS#12 – používá se pro výměnu veřejných i soukromých dat v jednom souboru
- .pfx – Personal inFormation eXchange (výměna osobních informací), předchůdce .p12

5.3.3 Druhy digitálních certifikátů

Digitální certifikáty se liší v tom, jakou mají úroveň důvěryhodnosti, způsobu jejich použití, druhu vlastníka. Ovšem způsob fungovaní je u všech stejný.

1. Self-signed digitální certifikát
    - Certifikát podepsaný „sám sebou“. Veřejný klíč podepsaný odpovídajícím privátním klíčem z páru. Takové certifikáty jsou využívaný například v rámci firem (uzavřené prostředí)
2. Kvalifikovaný digitální certifikát
    - Takový certifikát vydává kvalifikovaná certifikační autorita a při vydávání se v České republice řídí Zákonem o elektronickém podpisu. Tento certifikát nahrazuje klasický ověřený podpis. Používá se například při elektronické komunikaci se státními orgány.

3. Digitální certifikát osoby

    - Obsahuje jméno osoby a povolené úkony s certifikátem. Slouží k ověření digitálních podpisů, povolení přístupu k šifrovaným datům, v internetových prohlížečích místo jména a hesla při autentizaci vůči vzdálenému serveru. Používají se také v poštovních klientech, které podporují standard S/MIME (Secure Multipurpose Internet Mail Extensions).
    - Identifikuje jednu konkrétní fyzickou osobu.

4. Digitální systémový certifikát

    - Lze použít využívat i jako právnická osoba nebo státní orgán. Používá se například při automatizovaném zpracování dokumentů.

5. Digitální certifikát serveru

    - Potvrzuje důvěryhodnost serveru. Uskutečňuje zabezpečenou komunikaci mezi koncovou entitou a serverem.

6. Lze také vydat certifikát osoby, který je určen jen na šifrování nebo jen pro digitální podpis dokumentů. Použitím různých digitálních certifikátů pro různé činnosti se zvyšuje bezpečnost.

Pokud někdo používá digitální certifikát, musíme vyjádřit důvěru v tento certifikát. To můžeme provést v uložišti certifikátů například v Operačním systému nebo v konkrétním programu (internetové prohlížeče, Adobe Reader). Status certifikátu v úložišti může být: důvěryhodný, nedůvěryhodný, nejde rozhodnout. Pokud certifikát není uložen v úložišti, tak nemůžeme posoudit jeho důvěryhodnost.

5.3.4 Životní cyklus digitálního certifikátu

1. Vytvoření žádosti o certifikát

    - Generování párových dat – může nastat před i po žádosti o certifikát
    - Identifikační údaje žadatele, důkaz vlastnictví soukromého klíče, heslo pro komunikaci s CA

2. Vydání certifikátu

3. Platný certifikát

    - Certifikát začíná platit od doby, která je uvedené v certifikátu v poli „od“ (nemusí být platný ihned po vydání)

4. Vypršení platnosti certifikátu

    - Datum platnosti je uveden v obsahu certifikátu v poli „do“ dokumentů.

5. Odvolání certifikátu

    - Zneplatnění certifikátu před dobou, která je uvedené v poli „do“
    - Odvolaný certifikát se uvádí v seznamu CRL/OCSP do doby jeho původní platnosti
    - CA odvolává certifikát:
        - Sama→někdo jiný požádal o certifikaci stejného veřejného klíče
        - Certifikační údaje v certifikátu již nejsou platné
    - Na žádost držitele certifikátu
        - Soukromý klič byl kompromitován
        - Z osobních důvodů
        - Zničení soukromého klíče

6. Obnovení certifikátu

    - Musí k němu dojít dřív, než vyprší platnost certifikátu
    - Posílá se žádost o obnovení Certifikační autoritě

6. Topologie sítě

V této časti práce popíši oblast (nutnou pro realizaci zabezpečení) firemní topologie a prvky sítě, v níž budu realizovat autentizaci stanic pomocí technologie IEEE 802.1X a protokoly RADIUS a LDAP. Koncové stanice budou komunikovat v LAN protokoly WiFi a Ethernet. Ověřování bude probíhat pomocí protokolu RADIUS a vlastní ověřování se provádí vůči databázi Active Directory (řešení od Microsoftu založeno na LDAP databázi).

Ve firmě jsou již zavedeny některé komponenty sloužící k zabezpečení sítě. Implementace nového řešení zlepší zabezpečení vzhledem k připojení cizích zařízení do vnitřní sítě firmy. Příkladem využití může být konání školení externích pracovníků, kterým nebude umožněn přístup do vnitřní sítě, ale jen na internet.

Již jsou implementovány VLANy, které umožňují přístup do vnitřní sítě a na internet nebo jen na internet. Ethernetové zásuvky ve školící místností jsou tedy připojené do školící VLAN – umožňuje přístup jen na internet. Pokud by se ale externí pracovník připojil do ethernetové zásuvky v jiné kanceláři, dostal by se do vnitřní sítě, to představuje určité bezpečnostní riziko. Pro stejný případ jsou nakonfigurována dvě SSID WiFi připojení. Po implementaci zabezpečení pomocí AAA modelu se neoprávněná osoba nedostane do interní sítě, z žádné ethernetové zásuvky a bude stačit jedno SSID WiFi připojení.

6.1 Prvky sítě

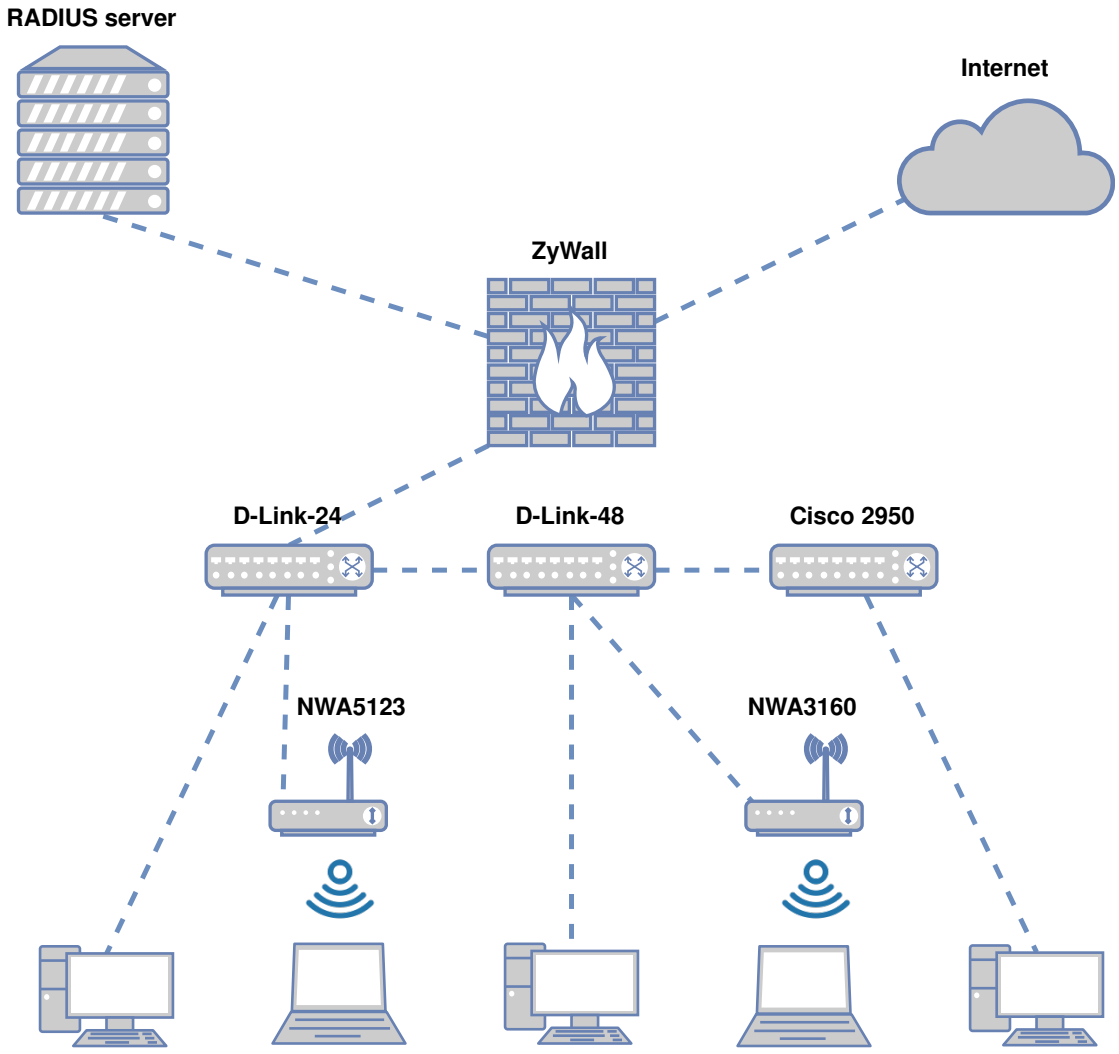
Ve firemní infrastruktuře jsou použity access pointy ZyXel NWA5123-AC a NWA3160-N pro pokrytí WiFi signálem. Pak je zde 48 portový switch D-Link DGS-3100-48 ST a 24 portový D-Link DGS-3100-24 ST. Z důvodu nezasahování do fungující infrastruktury a testovaní byl přidán switch Cisco Catalyst 2950. Jedná se o starší switch, který neumožnuje některé pokročilejší konfigurace – jako je například MAB (MAC Authentication Bypass). Tu bych využil u zařízení, která nepodporují standard IEEE 802.1X (např. starší tiskárny) nebo některé pokročilejší nastavení portů, které by zvýšilo bezpečnost.

Typ	Systém	Processor	RAM
Virtual Machine	Windows Server 2016 Essentials	Intel Xeon E5-2620 v2	16 GB

Tabulka 6.1: HW parametry RADIUS serveru

	Výrobce	Model	Verze firmware
Swiche	D-Link	DGS-3100-24 ST	3.60.28
	D-Link	DGS-3100-48 ST	3.60.28
	Cisco	WS-C2950-24	12.1(22)EA10a
Routery	ZyXEL	NWA5123-AC	V4.22 (AAZY.1)
	ZyXEL	NWA3160-N	V2.23 (UJA.8)
Firewall	ZyXEL	ZyWALL USG 300	3.30 (AQE.7)

Tabulka 6.2: Prvky sítě



Obrázek 6.1: Topologie sítě

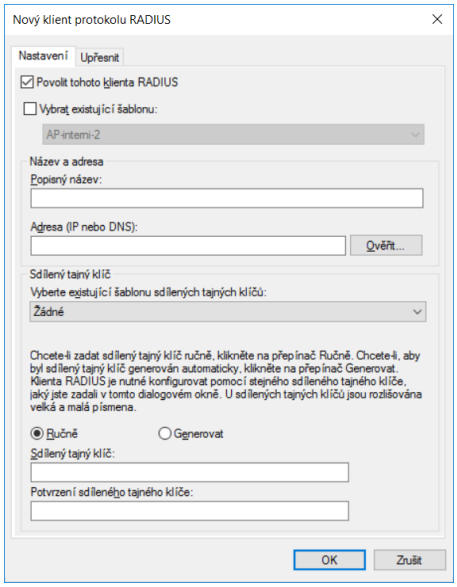
7. Konfigurace jednotlivých částí

Pro nasazení RADIUS serveru byl použit Windows server 2016 Essentials. Nejprve je nutné nakonfigurovat na Windows serveru Network Policy Server, kde se nastavují parametry pro RADIUS server. Dále se musí přidat koncové stanice/uživatele do Active Directory.

Ověřovaní budu realizovat dvěma způsoby: pomocí MAC a uživatelského jména a hesla nebo pomocí MAC a machine certifikátů. Postup je uveden v následujících kapitolách.

7.1 RADIUS Server

Prvním krokem je přidání role serveru „Služba Síťové zásady a přístup“ na Windows serveru. To se provede přes `Správce serveru` →`Správa` →`Přidat role a funkce`. Po této instalaci se v `Nástrojích pro správu` přidá položka `Server NPS (Network Policy Server)` který umožňuje vytvářet a vynucovat zásady přístupu k síti pro ověření požadavku a autorizaci požadavku na připojení v organizaci. Pod touto položkou se přidají Klienti RADIUS: `Klienti a servery RADIUS` →`Klienti RADIUS` →na této položce kliknout pravým tlačítka a vybrat položku `Nová`. Otevře se dialogové okno (obrázek 7.1), kde se nastavuje název, adresa a sdílený tajný klíč klienta RADIUS. Klienty RADIUS se rozumí Switche a Access Pointy, ke kterým se budou připojovat koncová zařízení v síti.



Obrázek 7.1: Konfigurace RADIUS klienta

7.1.1 Ověření pomocí MAC

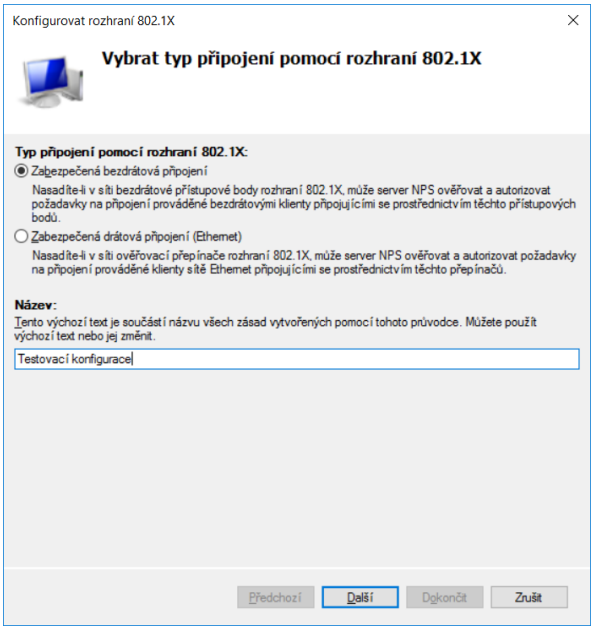
- Připojení skrze Access Pointy

  V Serveru NPS v okně `Standardní konfigurace` se vybere `Server RADIUS pro drátová a bezdrátová připojení pomocí rozhraní 802.1X` a dále pak `Konfigurovat rozhraní 802.1X` (obrázek 7.2). V novém okně `Zabezpečená bezdrátová připojení` a vyplnit název zásady. Na další obrazovce se vybere nakonfigurovaný Klient RADIUS (v tomto případě Access Point). Dále je nezbytné zvolit typ EAP protokolu, v tomto případě je zvolen `Protokol PEAP`. Poté přiřadit požadovanou skupinu uživatelů z AD, kterou chceme přiřadit k této politice. Dokončit konfiguraci.

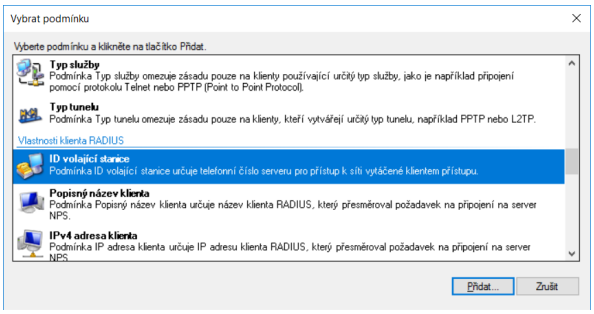
  Vytvořily se zásady pro nové připojení a pro sítě. V tomto stavu se koncové stanice ověřují pouze na základě uživatelského jména a hesla, jejichž databáze je v AD. Pro ověřovaní MAC adresy je třeba přidat v místě `Zásady →Zásady sítě →Název politiky` podmínku `ID volající stanice` (obrázek 7.3) v sekci `Vlastnosti klienta RADIUS`, která přidá RADIUS atribut `calling-station-ID`. Do tohoto atributu lze zadat MAC adresa koncové stanice ve formátu XX-XX-XX-XX-XX-XX. Pomocí oddělovače „|“ lze zadat více MAC adres. Další atributy, které byly použity slouží pro přirazení uživatele do konkrétní VLANy. Jsou to tři atributy: Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-ID. Kde první z nich určuje typ protokolu pro tunelování. Může být obsažen v paketech Access-Request, Access-Accept a Accounting-Request. Pokud je tento atribut v paketu Access-Request, RADIUS server může tento typ tunelu použít, ale nemusí se tím řídit. Když je atribut v paketu Access-Accept, od RADIUS serveru ke koncové entitě, musí komunikace probíhat v určeném tunelu. Jinak koncová entita obdrží Access-Reject. Zvolený parametr je tedy `VLAN`. Druhý atribut označuje, které transportní médium se má použít při vytváření tunelu. Může být obsažen ve stejných paketech jako předchozí atribut a řídí se také stejnými podmínkami. Zvolený parametr je zde `802`. Třetí atribut označuje ID skupiny pro konkrétní tunelovou relaci. V tomto případě atribut určuje ID VLANy do které má být skupina zařazena. Například pokud chceme skupinu „Programátoři“ v AD zařadit do VLAN 25, tak parametr atributu bude `25`. Může být obsažen v paketu Access-Request, Access-Accept. [12]

- Připojení skrze switch

  Zde se konfigurace zásad liší ve dvou místech. Místo `Zabezpečená bezdrátová připojení` se zvolí `Zabezpečená drátová připojení (Ethernet)` a při výběru RADIUS klienta vybrat tentokrát switch.



Obrázek 7.2: Konfigurace rozhraní 802.1X na NPS



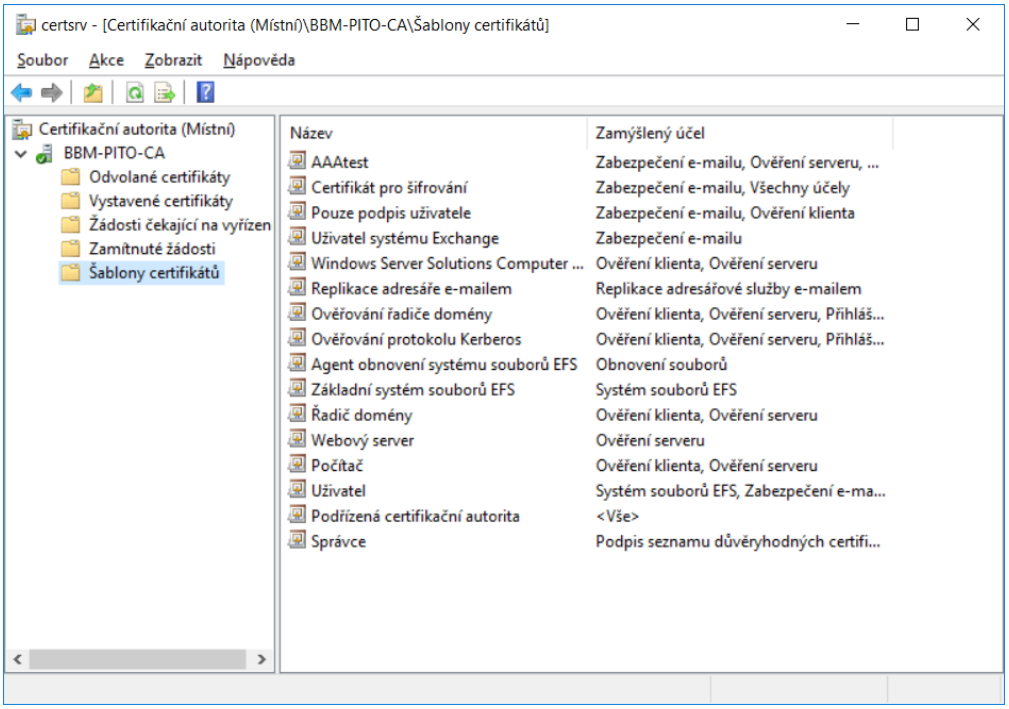
Obrázek 7.3: Podmínka - ID volající stanice

7.1.2 Ověření pomocí machine certifikátů

- Konfigurace Certifikační autority a zásad skupiny

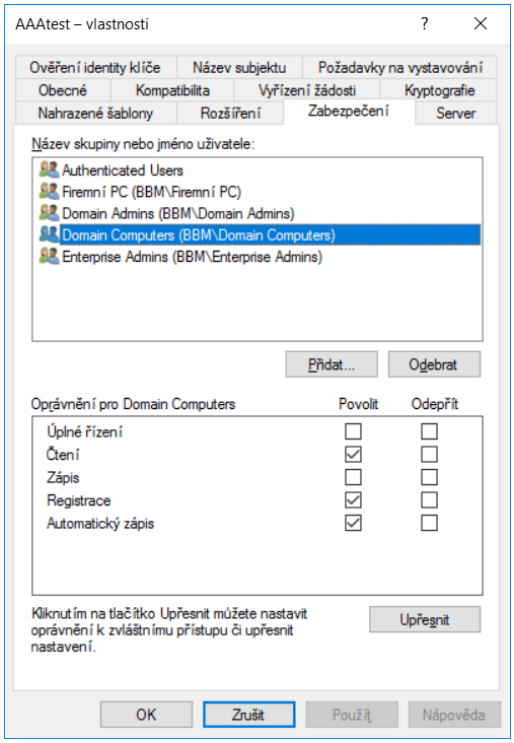
  Pokud má ověřování probíhat pomocí certifikátů, je třeba přidat další roli serveru podobně jako se přidávala služba pro RADIUS server, a to `Služba AC DS (Active Directory Certificate Services)`. Tato služba slouží k vytváření certifikačních autorit a souvisejících služeb rolí, které umožňují vydávat a spravovat certifikáty. Po této instalaci se v `Nástrojích pro správu` přidá položka `Certification Authority`. Zde se nachází seznamy vystavených a odvolaných certifikátů, žádosti čekající na vyřízení, zamítnuté žádosti a šablony certifikátů. Po kliknutí na šablony se zobrazí předdefinované šablony (obrázek 7.4). Pro ověření počítače se využije šablona `Počítač`. Pravým kliknutím mimo šablony se zobrazí

nabídka→vybrat Spravovat →otevře se nové okno se všemi šablonami. Aby šlo šablonu upravovat, například dobu platnosti certifikátu, vytvořím duplikát. Dvojím poklepáním jdou upravovat zmíněné vlastnosti certifikátu. Důležitě je, aby tento certifikát měl na kartě Rozšíření v Použití rozšířeného klíče Ověření klienta a aby na kartě Zabezpečení byla přidána skupina, které chceme certifikát distribuovat, a měla zaškrtnuto Čtení, Registrace, Automatický zápis (obrázek 7.5a). Poté vytvořenou šablonu přidáme do Šablon certifikátu v CA. Pravé kliknutí →Nová položka →Vystavovaná šablona certifikátu a vybrat šablonu.

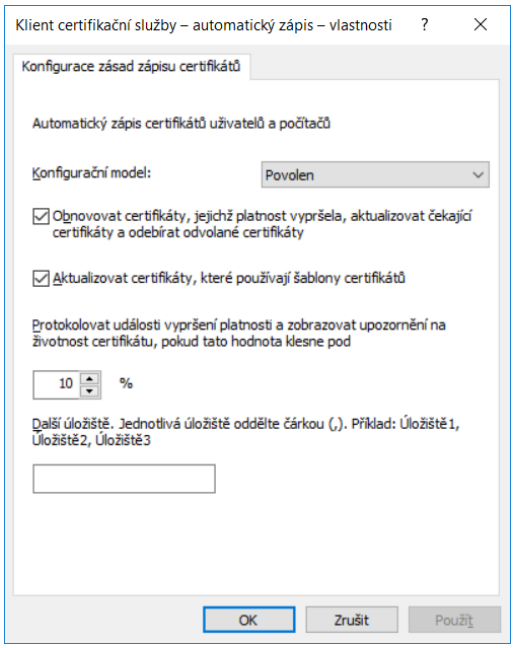


Obrázek 7.4: Šablony certifikátů

Dalším krokem je nastavení Správy zásad skupiny. Zde upravit politiku v Konfigurace počítače →Zásady →Nastavení systému Windows →Nastavení zabezpečení →Zásady veřejných klíčů →Klient certifikační služby - automatický zápis. Povolit konfigurační model a zaškrtnout Obnovovat certifikáty, jejichž platnost vypršela, aktualizovat čekající certifikáty a odebírat odvolané certifikáty, a také druhou položku Aktualizovat certifikáty, které používají šablony certifikátů (obrázek 7.5b). Tímto nastavením se docílí toho, že se vystavený certifikát bude publikován na koncovou stanici automaticky a bude se i automatický obnovovat platnost. Dále do Důvěryhodných kořenových CA přidat CA serveru. [15]



(a) Vlastnosti šablony certifikáru



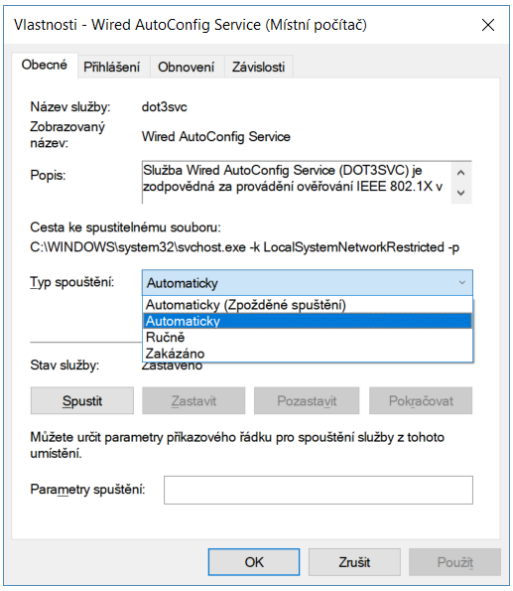
(b) Automatický zápis certifikátu

Obrázek 7.5: Konfigurace automatického publikovaní certifikátů

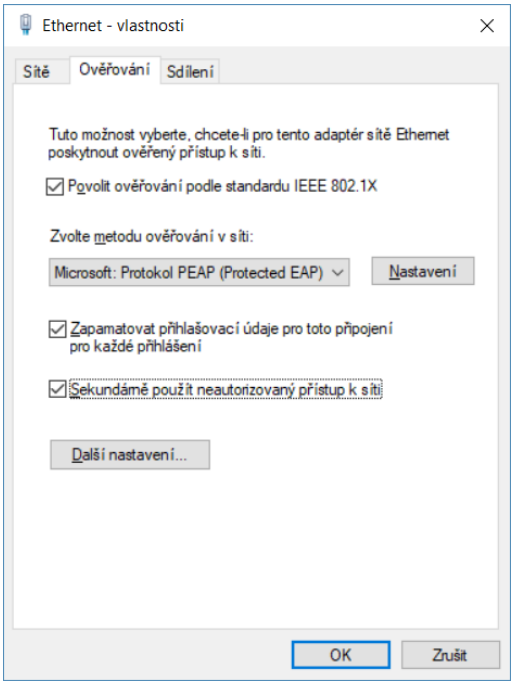
7.2 Koncové stanice

7.2.1 Konfigurace 802.1X

Ve firmě jsou výhradně používané koncové stanice s operačním systémem Windows. Pro komunikaci pomocí 802.1X je nutné spustit službu `Wired AutoConfig Service` a zvolit Typ spouštění: `automaticky`. Po jejím spuštění se ve vlastnostech adaptéru Ethernet zobrazí záložka `ověřování`. Zde je nutné zaškrtnout `Povolit ověřovaní podle standardu IEEE 802.1X` a nastavit parametry připojení. Pro ověření pomocí MAC adresy je nastavení vidět na obrázku 7.6b a ověření pomocí certifikátu na obrázcích 7.7 a 7.8. Pro konfiguraci lze také využít Windows server pomocí konfigurace `zásad skupiny` a `konfigurace počítače`. Po připojení ethernetového kabelu bude uživatel vyzván, aby zadal uživatelské jméno a heslo a provede se autentizace a autorizace. Při připojení na Wi-Fi není třeba nic povolovat v konfiguraci adaptéru a stačí vybrat konkrétní SSID, připojit se a zadat uživatelské jméno a heslo, popřípadě vybrat certifikát pro ověření.



(a) Spuštění služby Wired AutoConfig



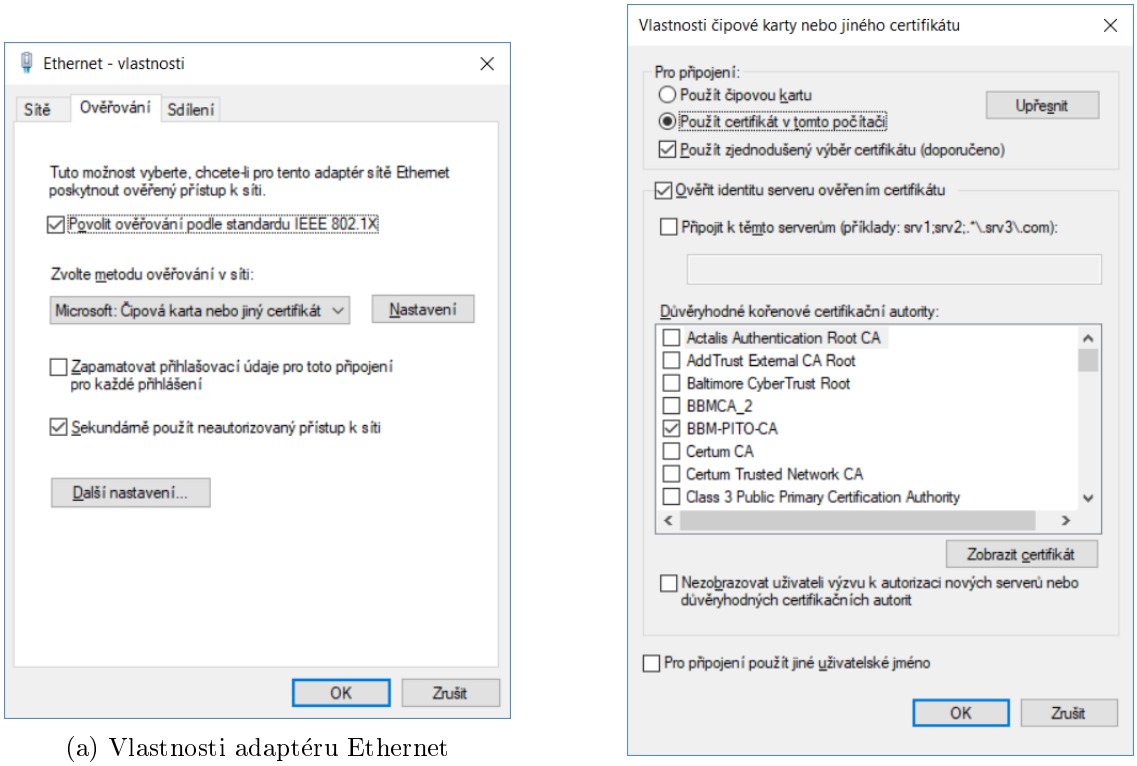
(b) Vlastnosti adaptéru Ethernet

Obrázek 7.6: Konfigurace ověřovaní pomocí protokolu IEEE 802.1X

Pokud je nastavené ověřování pomocí certifikátu koncové stanice, je nutné si o certifikát zažádat. To se provede ve `Správě certifikátů počítačů`. Na složce `Osobní pravým kliknutím →Všechny úkoly →Požádat o nový certifikát`. Otevře se průvodce `Zápis certifikátu`. Vybere se zásada konfigurovaná správcem na AD. Dále se zobrazí seznam dostupných šablon, vybrat požadovanou šablonu a zvolit `zapsat`. Po aktualizaci zásad bude ve složce `Osobní` certifikát vystavený pro danou koncovou stanici.

7.2.2 Zařízení nepodporující Standard 802.1X

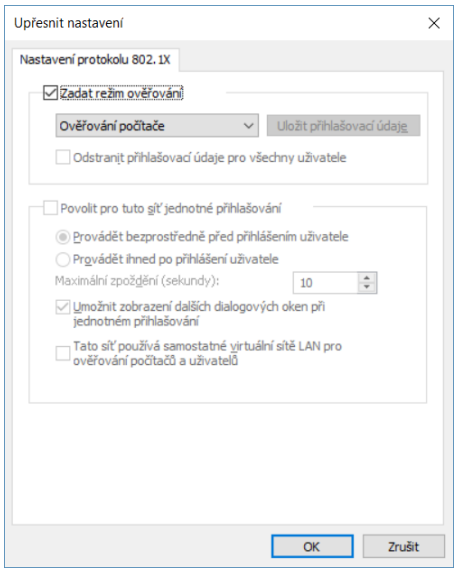
Jedná se například o tiskárny, které nepodporují standard 802.1X. Pro tento případ bude na konkrétních portech switche nastavený filtr MAC adres, které se přiřadí do konkrétní VLANy.



(a) Vlastnosti adaptéru Ethernet

(b) Vlastnosti certifikátu

Obrázek 7.7: Konfigurace ověření pomocí certifikátů



Obrázek 7.8: Další nastavení - režim ověřování

7.3 Switche

7.3.1 Cisco Catalyst 2950

Konfigurace tohoto switche probíhá skrze příkazový řádek pomocí CLI (Command-Line Interface) příkazů. Switch má také webové prostředí, ale to slouží spíše pro jednoduchý přehled stavu, ve kterém se nachází.

Aby bylo možné spustit autentizaci a autorizaci, je nutné spustit AAA access control model pomocí příkazu `AAA new-model` v konfiguračním režimu. Dále je nutné specifikovat RADIUS server, vůči kterému má switch ověřovat, a to pomocí příkazu `radius-server host 192.168.1.1`. Příkaz může být doplněn o parametry `acct-port` - nastavení portu pro účtování (výchozí je port 1813), `auth-port` – nastavení portu pro autentizaci (výchozí je 1812). Pomocí příkazu `radius-server key 1234asdf` bude zadán sdílený tajný klíč, který byl vytvořen při konfiguraci RADIUS klienta na Windows serveru v NPS. K modelu AAA příkaz `aaa authentication dot1x default group radius` přiřadí standart 802.1X a také povolí seznamy všech přidaných RADIUS serverů pro ověření. K Povolení 802.1X na všech portech switche, které jsou nakonfigurovány slouží příkaz `dot1x system-auth-control`. Všechny porty, které mají být použity pro standart 802.1X musí být v modu `access`. Toho se docílí příkazem `switchport mode access`. Pokud by bylo třeba povolit standard jen na konkrétním portu, přejdeme do konfigurace portu a použijeme příkaz `dot1x port-control auto`.

Další možnost konfigurace 802.1X umožňuje přiřadit uživatele, který neprošel autentizací (např. návštěva) do konkrétní VLANy (např. aby měl přístup na internet). To se provede příkazem `dot1x auth-fail vlan 77`. Pokud by zařízení uživatele nepodporovalo standard 802.1X, lze příkazem `dot1x guest-vlan 88` nastavit VLAN, do které switch umožní přístup. Poslední dva příkazy se musí nastavovat na konkrétním interface. Pro urychlení práce se dá použít příkaz `range`, díky kterému je možné konfigurovat více interface najednou – příklad `interface range fastEthernet 0/12 - 24`. Tím lze konfigurovat port 12–24 najednou. Dále lze na portu konfigurovat například po jaké době se koncová entita musí znovu ověřit; maximální počet žádostí o autentizaci, který switch posílá koncové entitě i RADIUS serveru; čas po špatné autentizaci klienta, který switch čeká a maximální počet špatných přihlášení. Poslední příkaz pro AAA model umožní delegovat přiřazení portu do VLAN na RADIUS server `aaa authorization network default group radius`. Příkaz `show dot1x all` v privilegovaném módu zobrazí konfiguraci standardu 802.1X.

Některé porty switche byly nakonfigurovány pro tiskárny, jak jsem se zmínil v sekci 7.2.2. Příkazem `switchport port-security` se zapne zabezpečení na portu. Pak se nastaví pevná MAC adresa `switchport port-security mac-address EC56.C1JA.3425`. Díky parametru u port-security `violation shutdown` se port přepne do stavu shutdown, pokud je MAC adresa koncové entity jiná, než je povolená. Pro znovu zapnutí portu je třeba nastavit časový limit obnovy a to příkazy `errdisable recovery cause psecure-violation` a `errdisable recovery interval 60` v konfiguračním módu. Příkaz `show port-security address` v privilegovaném módu zobrazí jaké MAC ad-

resy jsou přirazeny k portům na switchi. Příkaz `show port-security interface fastEthernet 0/2` zobrazí podrobnější konfiguraci port-security na interface. Příkaz `show running-config` zobrazí aktuálně běžící konfiguraci switche.

```
SWITCH(config)#aaa new-model
SWITCH(config)#radius-server host 192.168.1.1 auth-port 1812
SWITCH(config)#radius-server key 1234asdf
SWITCH(config)#aaa authentication dot1x default group radius
SWITCH(config)#dot1x system-auth-control
SWITCH(config)#interface range fastEthernet 0/4 - 24
SWITCH(config-if-range)#switchport mode access
SWITCH(config-if-range)#dot1x auth-fail vlan 77
SWITCH(config-if-range)#dot1x guest-vlan 88
SWITCH(config-if-range)#exit
SWITCH(config)#aaa authorization network default group radius
SWITCH(config)#interface fastEthernet 0/2
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security mac-address EC56.C1JA.3425
SWITCH(config-if)#switchport port-security violation shutdown
SWITCH(config-if)#exit
SWITCH(config)#errdisable recovery cause psecure-violation
SWITCH(config)#errdisable recovery interval 60
```

```
radius-server host 192.168.1.1 auth-port 1812 acct-port 1813 key 1234asdf
```

Obrázek 7.9: Přehled konfigurace RADIUS severu

```
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
 dot1x port-control auto
 dot1x guest-vlan 30
 dot1x auth-fail vlan 30
 spanning-tree portfast
```

(a) Konfigurace FastEthernet0/5

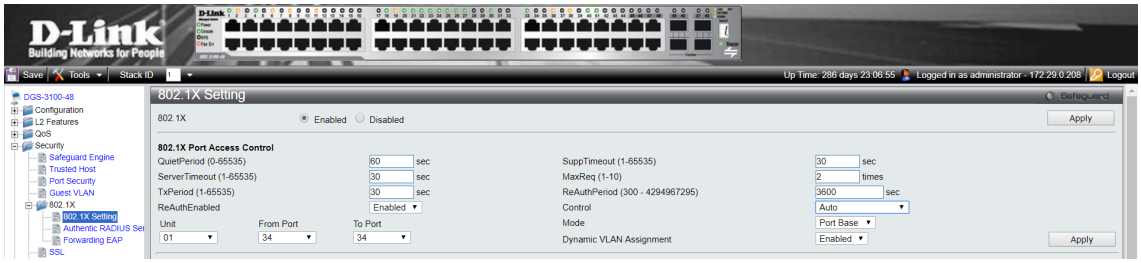
```
Dot1x Info for interface FastEthernet0/4

----------------------------------------------------
Supplicant MAC <Not Applicable>
AuthSM State          = N/A
BendSM State          = N/A
Posture               = N/A
PortStatus            = N/A
MaxReq                = 2
MaxAuthReq            = 2
HostMode              = Single
Port Control          = Auto
ControlDirection      = Both
QuietPeriod           = 60 Seconds
Re-authentication     = Disabled
ReAuthPeriod          = 3600 Seconds
ServerTimeout         = 30 Seconds
SuppTimeout           = 30 Seconds
TxPeriod              = 30 Seconds
Guest-Vlan            = 30
AuthFail-Vlan         = 30
AuthFail-Max-Attempts = 3
```

(b) Konfigurace 802.1X na FastEthernet0/4

Obrázek 7.10: Přehled konfigurace portů

7.3.2 D-Link DSG-3100

Konfiguraci tohoto switche byla provedena přes webové rozhraní. V levém sloupci se nachází položka `Security →802.1X →802.1X Setting`. Zde se provádí nastavení jednotlivých portů. Nejprve je nutné povolit 802.1X volbou `Enable`. Pak se zpřístupní parametry pro nastavení portů. Je zde možnost nastavení stejných timeoutů jako na Cisco switchi a také například maximální počet žádostí o autentizaci. Položka `Control` musí být nastavena na `Auto`. Pokud je používané dynamické přiřazovaní do VLAN, tak musí být povolena položka `Dynamic VLAN Assignment`. Switch také umožňuje autentizaci pomocí MAC adres (podobné MAB u Cisco). Tento parametr se nastavuje v položce `Mode`. Zvolit druhou možnost, kterou je `Port Base`. Dále na položce `Authentic RADIUS Server` přidat RADIUS server, vůči kterému se bude ověřovat. Požadovaná je IP adresa, port pro autentizaci účtování a sdílený tajný klíč. V části `Monitoring →RADIUS Authentication` jsou zobrazeny statistiky o autentizaci.



Obrázek 7.11: Přehled parametrů 802.1X

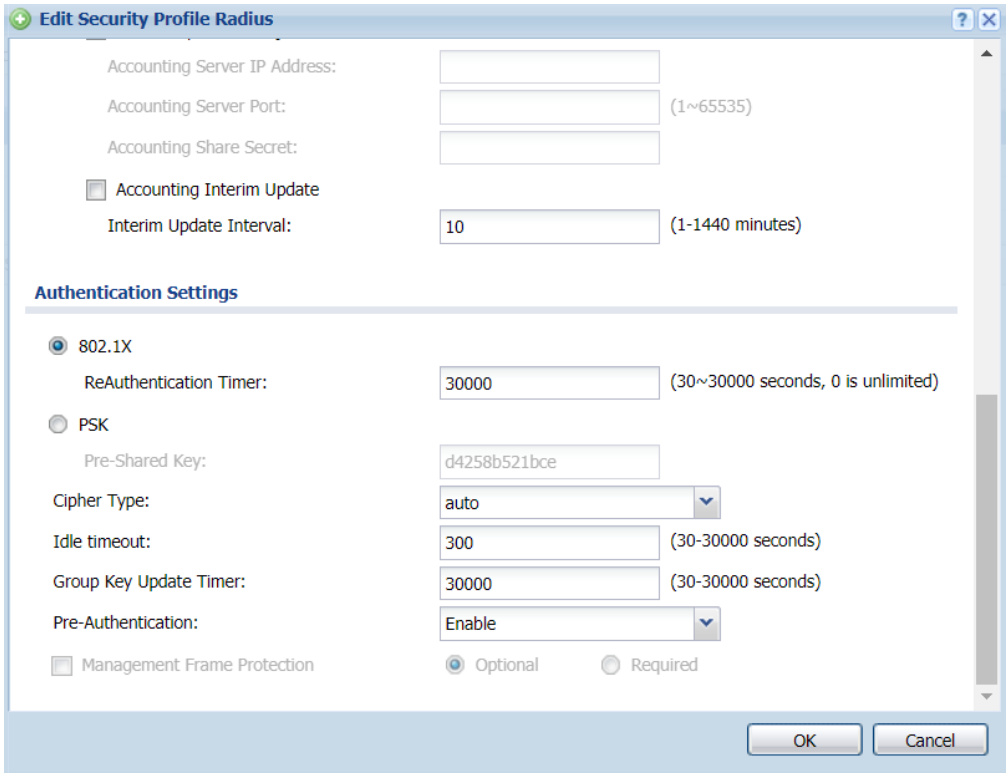
Unit	Port	Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled	Mode	Dynamic VLAN Assignment
1	1:34	Auto	30	60	30	30	2	3600	Enabled	Port Base	Enabled

Obrázek 7.12: Konfigurace 802.1X na portu 34

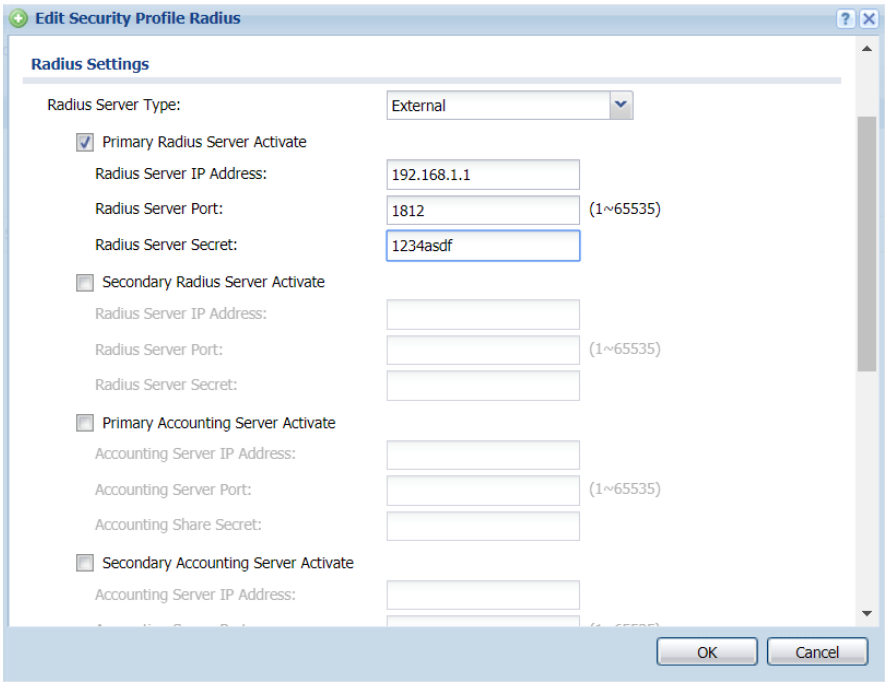
7.4 Access Pointy

U Access Pointů ZyXel NWA5123-AC a NWA3160-N je potřeba nastavit RADIUS server pro ověřovaní podobně jako u switchů. Konfigurace těchto zařízení ZyXel se provádí pomocí webového prostředí.

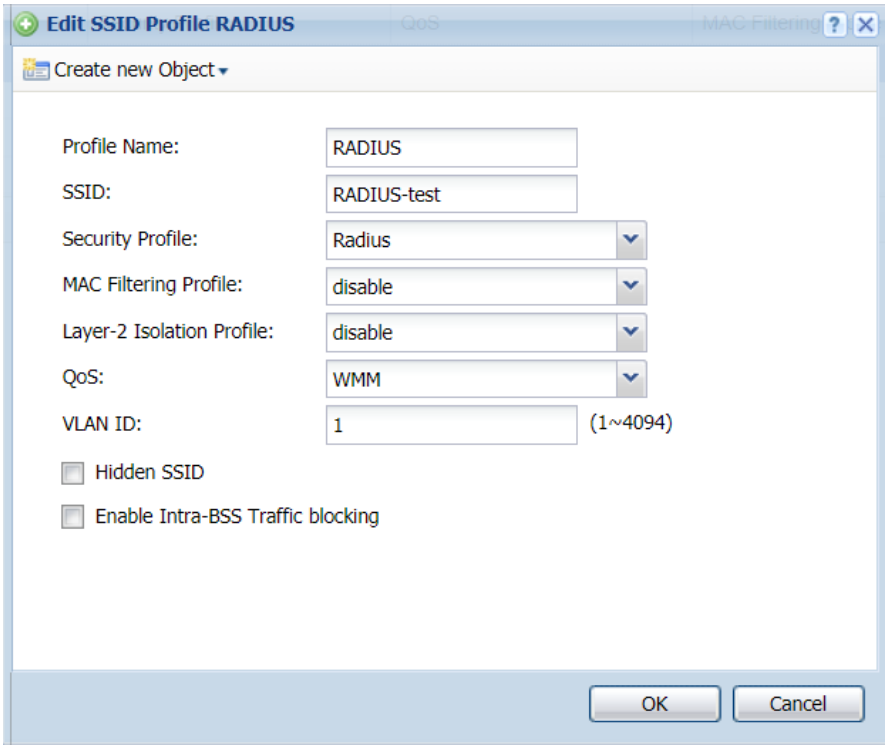
V konfiguraci pod položkou `Object →AP profile →SSID` se vytvoří nový Security profile `Radius`. Security Mode zvolit `wpa2-mix`. Dále je nutné zaškrtnout autentizační metodu `802.1X`, poté se v části `RADIUS settings` zpřístupní pole pro nastavení RADIUS serveru. Nastavení je vidět na obrázcích 7.13 a 7.14. Lze zde také nastavit sekundární RADIUS server. Dalším krokem je vytvoření SSID profilu v `SSID List`. Zadá se název profilu, SSID, vybere vytvořený Security profile `Radiu` a zadá se defaultní VLAN ID. Nastavení je vidět na obrázku 7.15



Obrázek 7.13: Povolení 802.1X



Obrázek 7.14: Konfigurace RADIUS serveru



Obrázek 7.15: Konfigurace SSID profilu

8. Ověření funkčnosti

Pro ověření, že autentizace a autorizace fungují správně, jsem použil program WireShark, díky kterému jsem odchytil komunikaci mezi koncovou stanicí a Authenticatorem. Odchycená komunikace protokolu EAP probíhala, tak jak je uvedeno na obrázku 3.1 Dále jsem provedl kontrolu na RADIUS serveru v konzole `Prohlížeč událostí`. Také jsem ověřil, jestli stanice dostala správnou IP adresu z VLANy, do které měla být připojena podle úspěšného či neúspěšného ověření.

8.1 Úspěšná autentizace a autorizace

Ověřování pomocí MAC adresy a uživatelského jména a hesla je vidět na obrázku 11.1. Z odchycené komunikace je vidět, že probíhá skrze EAP-PEAP. A je také vidět, jakým uživatelským jménem se koncový uživatel ověřuje. Komunikace končí zprávou `EAP-Success`. Na obrázku 11.2 je úspěšné ověření na NPS serveru podle vyhovující politiky (ověření MAC adresy a uživatelského jména a hesla).

Při ověřovaní pomocí certifikátu je opět vidět způsob komunikace na obrázku 11.3. Tentokrát EAP-TLS a jak probíhá vytvoření šifrované komunikace a ověření certifikátů. Poslední EAP zprávou je `EAP-Success`, takže ověření bylo úspěšné. Ověření na NPS serveru se v prohlížeči událostí liší jen v politice, která se na ověření aplikovala.

8.2 Neúspěšná autentizace a autorizace

Pokud při ověřování MAC adresy a uživatelského jména a hesla, je nepovolená MAC adresa nebo jméno a heslo, výsledek obou případů je stejný. Koncová stanice odpoví na `EAP-Request/Identity` zprávou `EAP-Response/Identity` na obrázku 11.4. Ale na RADIUS serveru neprojde ověření přes nastavenou politiku (obrázek 11.5), takže Authenticator odpoví zprávou `EAP-Failure`.

Pokud certifikát, kterým se má koncová stanice ověřovat, vůbec na stanici není, začne probíhat komunikace EAP, ale koncová stanice neodpoví na `EAP-Request/Identity` a komunikace skončí zprávou `EAP-Failure` – jak je vidět na obrázku 11.6. Na Radius server se žádost o ověření nedostane, protože není co ověřovat.

Když certifikát na koncové stanici je, ale nevyhovuje politice nastavené na serveru (nesprávný certifikát, odvolaný certifikát), tak situace dopadne stejně jako např. při nepovolené MAC adrese (obrázek 11.7).

Pokud je na switchy nastavena Quest VLAN, tak se zařízení, která nemají zapnuté nebo

nepodporují ověřovaní IEEE 802.1X připojí právě do této VLANy. Když je nastavený parametr `auth-fail`, tak i když se uživatel neověří, udělí se mu přístup do této VLANy (obrázek kofigurace na portu 7.10b).

9. Závěr

Bakalářská práce se zabývá autentizací v lokálních sítích pomocí IEEE 802.1X. Práce má dvě hlavní části. Je to teoretická a praktická část. V teoretické části jsem popsal vlastnosti AAA architektury a protokoly, které z ní vycházejí (RADIUS, DIAMETER, TACACS, TACACS+ a KERBEROS) 2) . Dalším tématem byl standard IEEE 802.1X 3) , zde jsem se podrobněji věnoval tomu, jakým způsobem protokol komunikuje. Toho jsem využil v praktické části v kapitole 8) Ověření funkčnosti, kde byla tato komunikace zachycena. Také jsem popsal funkci protokolu LDAP, na kterém je založen Active Directory. Poslední kapitola teoretické části byla věnována Infrastruktuře veřejných klíčů.

V praktické části jsem realizoval autentizaci v reálné firemní síti. Nejdříve jsem popsal síť ve firmě (topologie, síťové prvky), následně jsem nakonfiguroval RADIUS server na Windows serveru, koncové stanice a síťové prvky. V kapitole 8) jsem pomocí programu WireShark a Prohlížeče událostí na Windows serveru ověřil funkčnost řešení. To je nyní funkční, jak při připojení ethernetovým kabelem, tak přes Wi-Fi. U obou způsobů funguje autentizace za použití MAC adresy a uživatelského jména, hesla a také pomocí certifikátu koncové stanice. Zatím bylo ve firmě nasazeno řešení pouze pro testovaní, aby se odhalily případné chyby v autentizačním procesu koncových zařízení. Po doladění konfigurace sítě se bude moci přejít na ostrý provoz.

Reference

[1] *802.1X Overview and EAP Types*. en. URL: https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html (cit. 04. 01. 2019).

[2] Jari Arkko et al. *Diameter Base Protocol*. en. URL: https://tools.ietf.org/html/rfc3588 (cit. 04. 01. 2019).

[3] *eSignature*. URL: https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITAL/eSignature (cit. 02. 01. 2019).

[4] Interlink Networks, Inc. *Introduction to Diameter*. URL: https://www.interlinknetworks.com/whitepapers/Introduction_to_Diameter.pdf. 2002.

[5] Alena Kabelová a Libor Dostálek. *Velký průvodce protokoly TCP/IP a systémem DNS*. cs. Computer Press, Albatros Media a.s., březen 2016. ISBN: 978-80-251-3886-1.

[6] *LDAP*. en. 2015. URL: http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485047945.htm (cit. 04. 12. 2018).

[7] Libor Dostálek a Marta Vohnoutová. *Velký průvodce infrastrukturou PKI*. cs. Computer Press, Albatros Media a.s., ún. 2017. ISBN: 978-80-251-4513-5.

[8] Lukáš Zapletal. *Lehký úvod do LDAP*. cs. URL: https://www.root.cz/clanky/lehky-uvod-do-ldap/ (cit. 04. 12. 2018).

[9] Madjid Nakhjiri a Mahsa Nakhjiri. *AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility*. en. John Wiley & Sons, říj. 2005. ISBN: 978-0-470-01194-2.

[10] Jiří Peterka. *Po 16 letech existence přestává platit zákon o elektronickém podpisu*. cs. URL: https://www.lupa.cz/clanky/po-16-letech-existence-prestava-platit-zakon-o-elektronickem-podpisu/ (cit. 02. 01. 2019).

[11] Petr Bouška-Samuraj; e-mail: bouskap@samuraj-cz.com. *Adresářové služby a LDAP, SAMURAJ-cz.com*. cs. URL: https://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/ (cit. 04. 12. 2018).

[12] Petr Bouška-Samuraj; e-mail: bouskap@samuraj-cz.com. *Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce*. cs. URL: https://www.samuraj-cz.com/clanek/cisco-ios-12-ieee-802-1x-a-pokrocilejsi-funkce/ (cit. 26. 04. 2019).

[13] Petr Bouška-Samuraj; e-mail: bouskap@samuraj-cz.com. *Kerberos protokol a Single sign-on, SAMURAJ-cz.com*. cs. URL: https://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/ (cit. 04. 12. 2018).

[14] Petr Hanáček a Jan Staudek. *Certifikační infrastruktury veřejných klíčů, PKI*. URL: https://www.fi.muni.cz/usr/staudek/vyuka/security/stud_lit/D01_C.pdf.

[15] shortpatti. *Manage Network Policy Server (NPS)*. en-us. URL: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-top (cit. 26. 04. 2019).

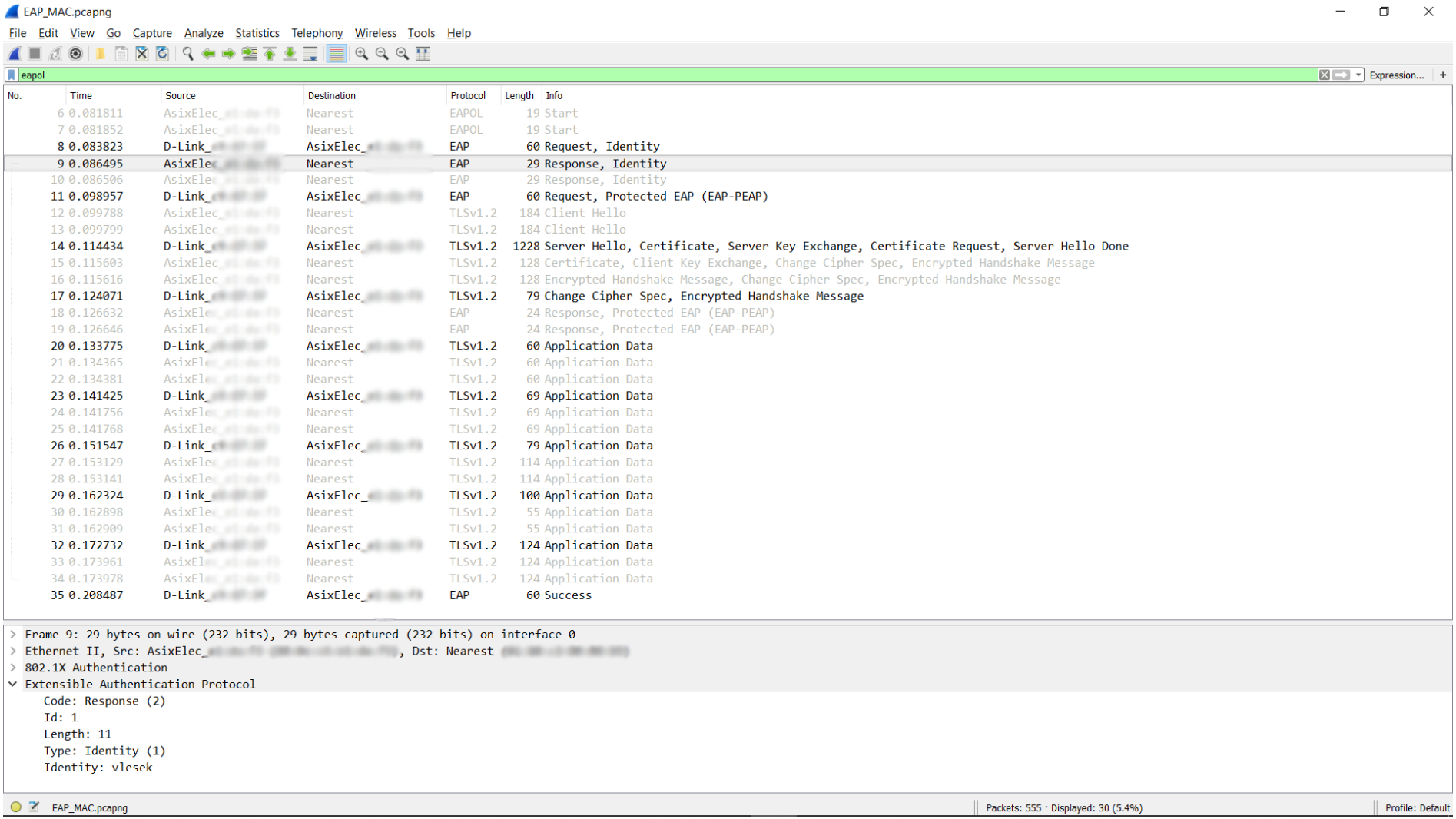
[16] *The Advantages of TACACS+ for Administrator Authentication*. URL: http://www.tacacs.net/docs/TACACS_Advantages.pdf (cit. 04. 01. 2019).

[17] John R. Vollbrecht et al. *Generic AAA Architecture*. en. URL: https://tools.ietf.org/html/rfc2903 (cit. 02. 01. 2019).

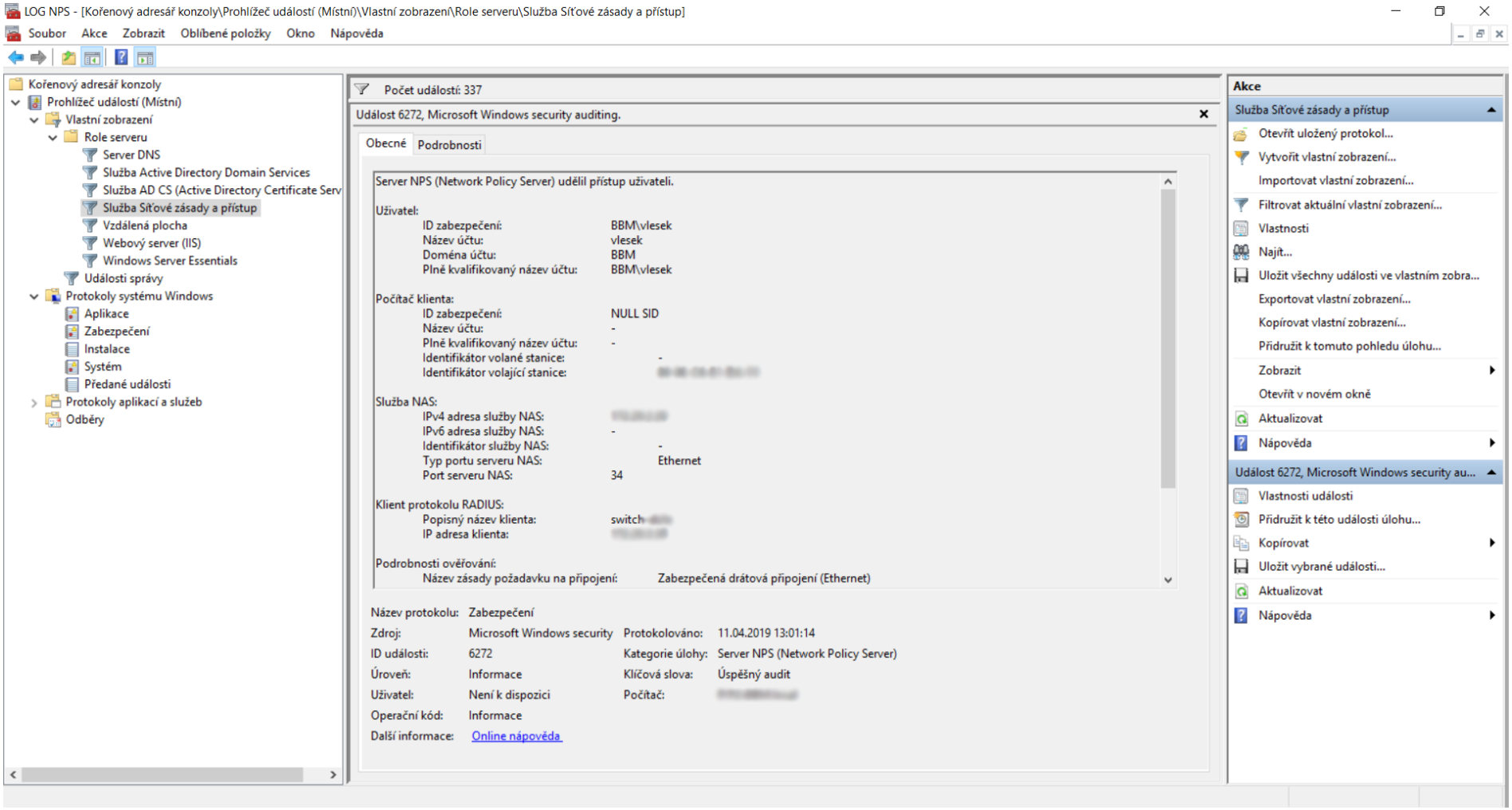
[18] Steve Willens et al. *Remote Authentication Dial In User Service (RADIUS)*. en. URL: https://tools.ietf.org/html/rfc2865 (cit. 04. 01. 2019).

[19] Glen Zorn et al. *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*. en. URL: https://tools.ietf.org/html/rfc3580#section-3.27 (cit. 04. 01. 2019).

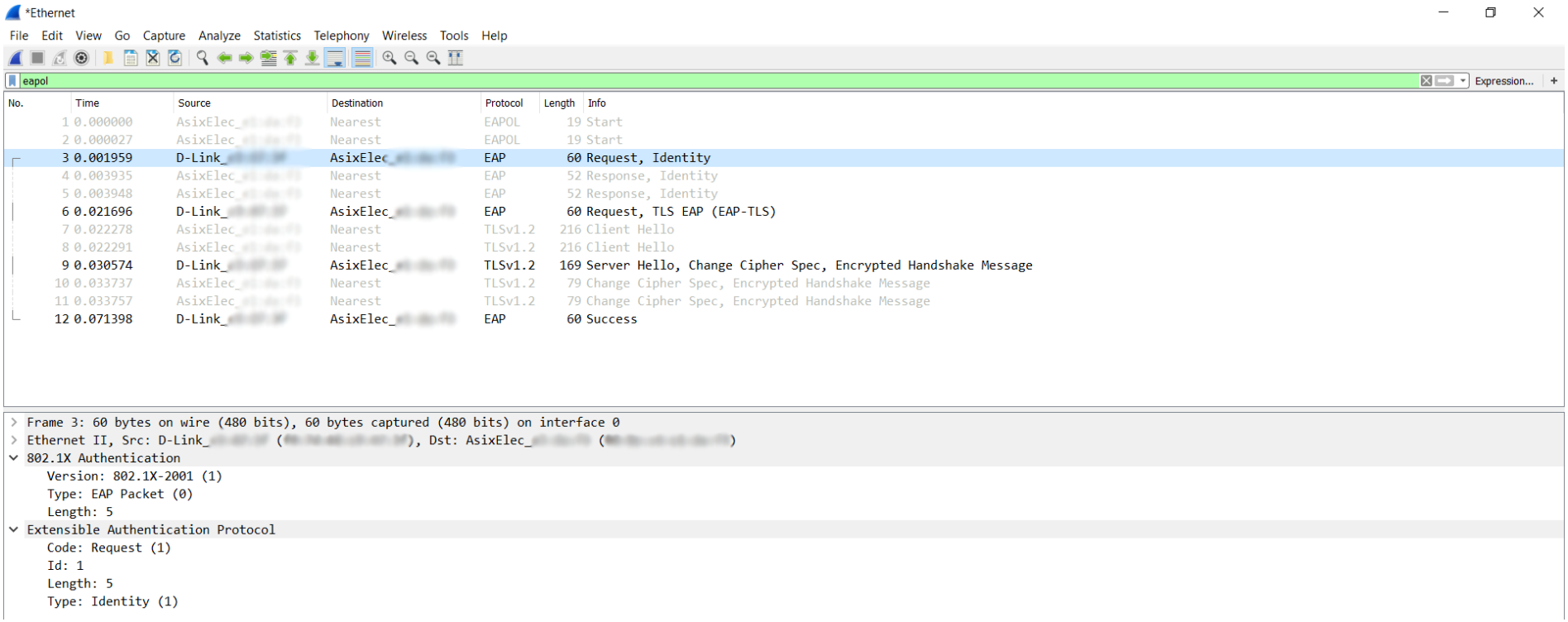
Přílohy



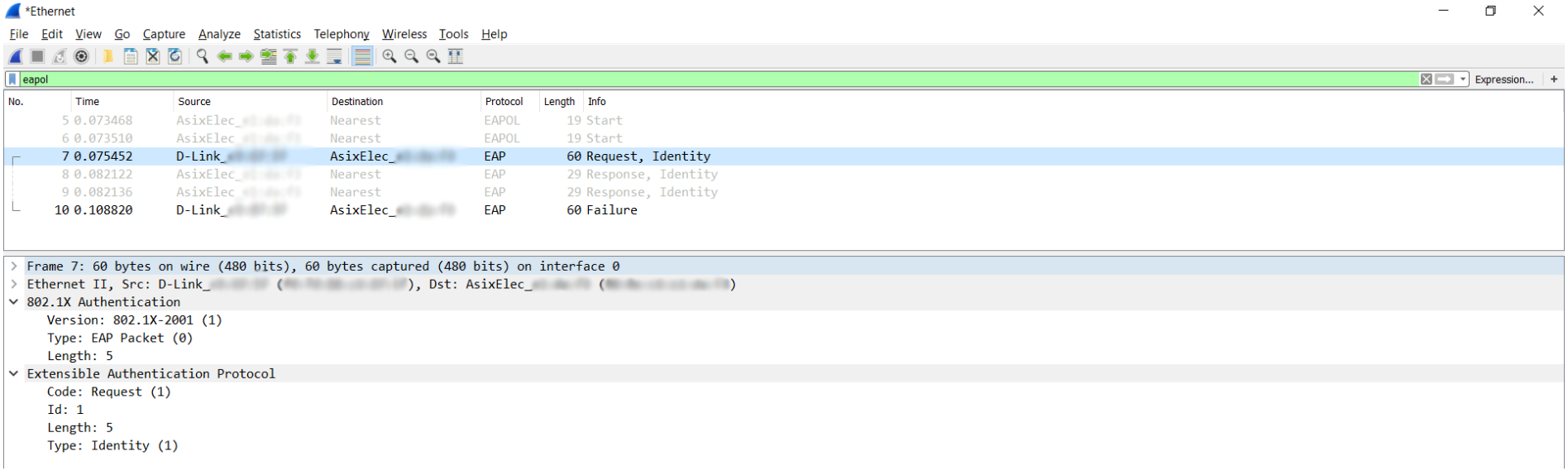
Obrázek 11.1: Kominukace IEEE 802.1X - WireShark - ověření MAC adresy



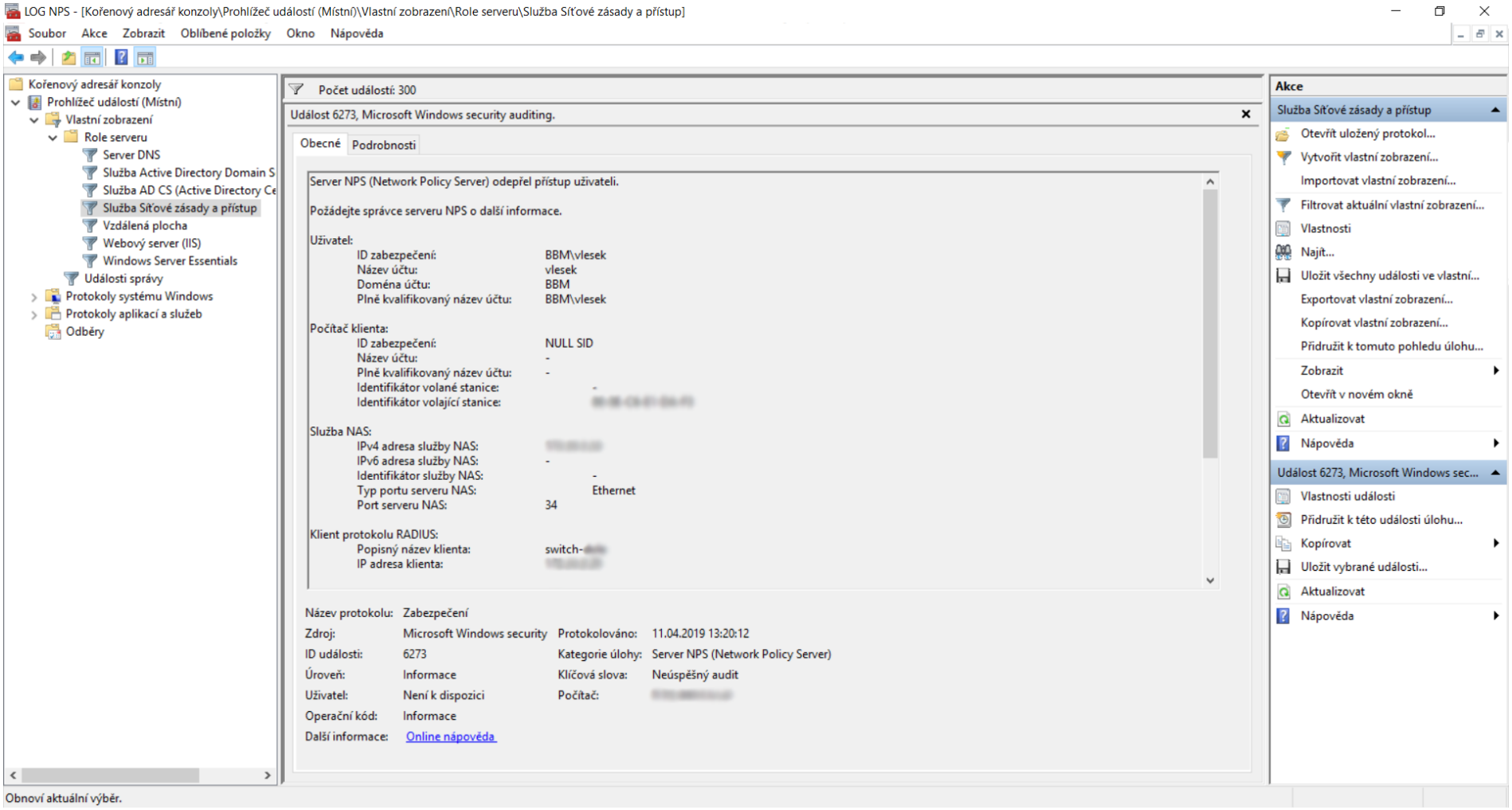
Obrázek 11.2: Prohlížeč událostí - úspěšné ověření



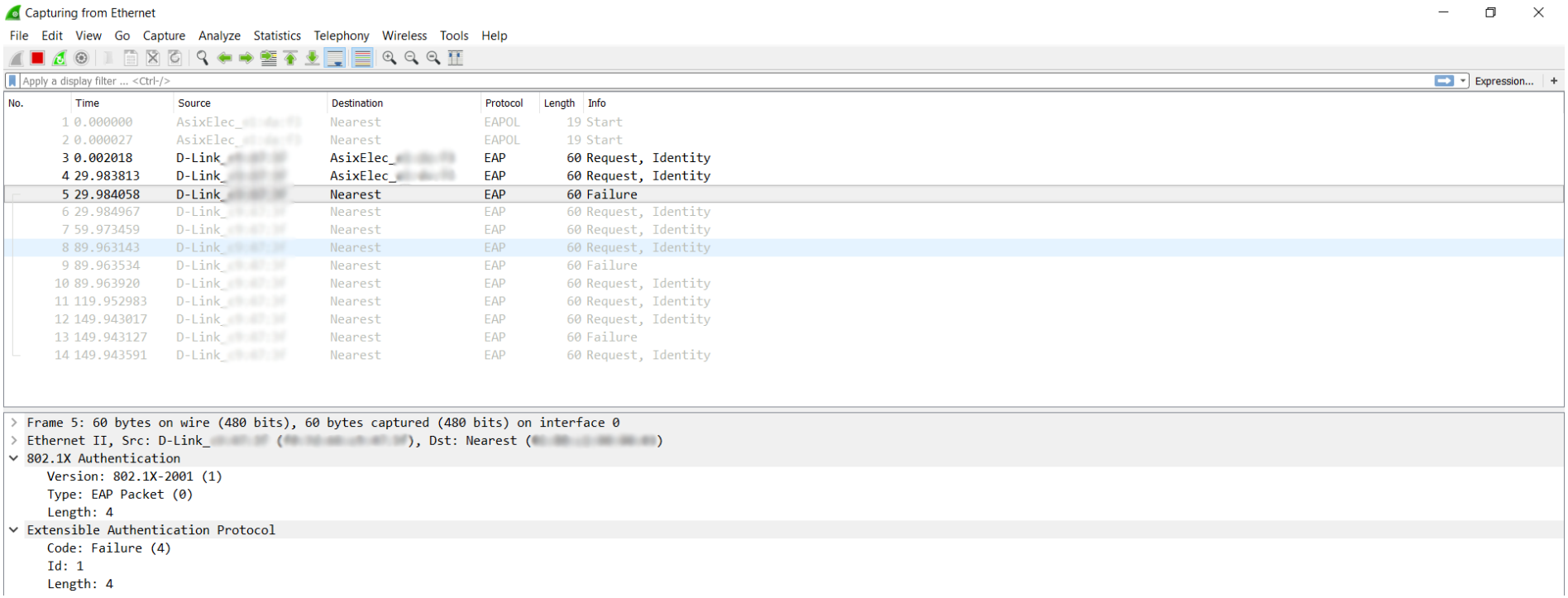
Obrázek 11.3: Kominukace IEEE 802.1X - WireShark - ověření certifikátu



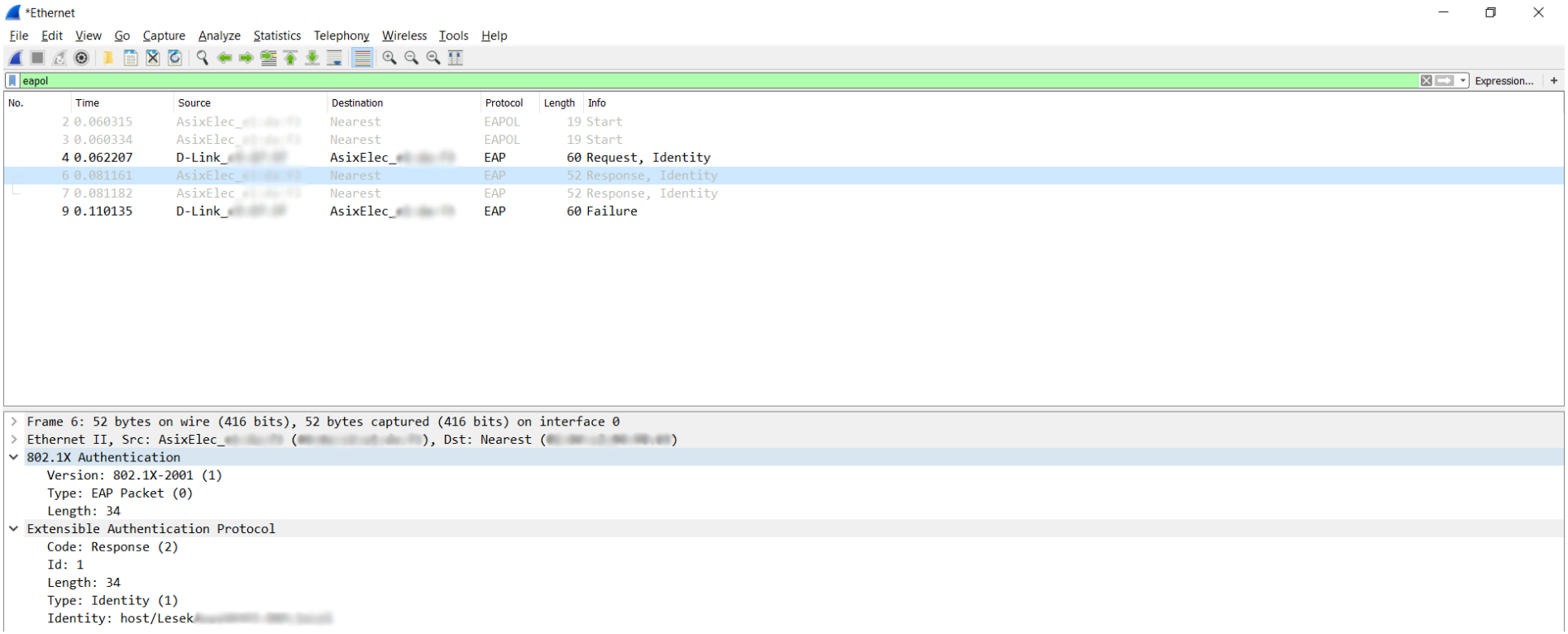
Obrázek 11.4: Kominukace IEEE 802.1X - WireShark - ověření s nepovolenou MAC adresou



Obrázek 11.5: Prohlížeč událostí - neúspěšné ověření



Obrázek 11.6: Kominukace IEEE 802.1X - WireShark - ověření bez certifikátu na koncové stanici



Obrázek 11.7: Kominukace IEEE 802.1X - WireShark - ověření s neplatným certifikátem na koncové stanici