Návrh zabezpečení přístupové vrstvy podnikové sítě založené na identitě uživatele

Bc. Peter Dupkala

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Peter Dupkala**
Osobní číslo:	**A12339**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh zabezpečení přístupové vrstvy podnikové sítě založené na identitě uživatele**
Téma anglicky:	**A Proposal for Securing Access to Corporate Network Layers Based on User Identity**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Vypracujte návrh zabezpečení přístupové vrstvy sítě založené na standardu IEEE 802.1X.**
3. **Vypracujte návrh optimálního postupu implementace Vámi navrženého řešení.**
4. **Popište možné útoky na L2 vrstvě a navrhnete protiopatření na jejich eliminaci.**
5. **Popište konfiguraci CISCO přepínačů, ACS a AD souvisejících se zabezpečením přístupové vrstvy.**
6. **Vyhodnoťte výhody a nevýhody Vámi navrženého řešení.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. 2nd print. Indianapolis: Cisco Press, 2009, 360 s. ISBN 978-1-58714-062-4.**
2. **SANTUKA, Vivek, Premdeep BANGA a Brandon CARROLL. AAA identity management security. Indianapolis, IN: Cisco Press, 2011, 443 p. ISBN 15-871-4144-2.**
3. **OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. 1. vyd. Brno: Computer Press, 2008, 444 s. ISBN 978-80-251-2048-4.**
4. **VYNCKE, Eric a Christopher PAGGEN. LAN switch security: what hackers know about your switches. Indianapolis, IN: Cisco Press, 2008, 340 s. ISBN 1-58705-256-3.**
5. **DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS: Vysvětlení nejpoužívanějších protokolů a konfigurace současných sítí. Internet i vnitřní podnikové sítě. Delegace domén, přidělování. 2. aktual. vyd. Praha: Computer Press, 2000, 426 s. ISBN 80-722-6323-4.**
6. **NORTHCUTT, S. Bezpečnost sítí: velká kniha. 1. vyd. Brno: CP Books, 2005, 589 s. ISBN 80-251-0697-7.**

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- Že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Táto práca sa zaoberá návrhom zabezpečenia prístupovej vrstvy podnikovej siete, v ktorom je nosným pilierom štandard 802.1X, ten umožňuje na základe autentizácie užívateľov vykonávať pravidlá definované v bezpečnostnej politike. V úvode sú popísané sieťové protokoly ako aj terminológia, ktoré sú v tejto technológii využívané. V druhá časť práce je venovaná akým spôsobom je možné postupovať pri nasadzovaní tejto technológie bez toho aby to negatívne ovplyvnilo užívateľov. V závere sú spomenuté výhody a nevýhody navrhovaného riešenia.

Klíčová slova: 802.1X, RADIUS, TACACS+, EAP, ACS

ABSTRACT

This thesis describes design security of enterprise network access layer, in which is the standard 802.1X core component, which allowing based authentication of users to the rules defined in the security policy. The introduction describes the network protocols and terminology that are used in this technology. The second part is devoted to how the model can be used to deploy with this technology without undermining users. At the end of are mentioned advantages and disadvantages of the proposed solutions.

Keywords: 802.1X, RADIUS, TACACS+, EAP, ACS

Touto cestou by som sa chcel poďakovať svojmu vedúcemu diplomovej práce Ing. Miroslavovi Matýskovi, Ph.D. za vedenie a poskytnuté odborné rady.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V súčasnej dobe sa kladie veľký dôraz na zabezpečenie podnikových sietí, či už je to z hľadiska aplikačnej, sieťovej bezpečnosti ICT. Avšak vo veľkej miere sa zabúda na zabezpečenie metalických LAN sietí. V drvivej väčšine je lepšie zabezpečená bezdrôtová sieť WIFI ako samotná LAN sieť.

Rozvod LAN sietí je realizovaný štruktúrovanou kabelážou s vývodmi do sieťových zásuviek na rôznych miestach budovy podniku. Pomocou metód sociálneho inžinierstva sa útočník môže dostať k prístupu do LAN siete (tlačiareň na chodbe, zásuvky v zasadacích miestnostiach a pod.) a realizovať útoky na prístupovej vrstve siete, prípadne realizovať sofistikované útoky naprieč celou infraštruktúrou. Prístup k podnikovým zdrojom je vo väčšine realizovaný pomocou rôznych bezpečnostných zariadení, ktoré povoľujú komunikáciu na základe zdrojovej a cieľovej IP adresy zariadení, ktoré sú do siete pripojené. Avšak týmto spôsobom nemôžeme jednoznačne zaručiť, že sa naozaj jedná o užívateľa ktorý sa vydáva, že ním naozaj je.

Ako príklad je možné uviesť situáciu, keď sa útočník pripojí do segmentu siete, kde chce vykonať útok, počká si pokiaľ zamestnanec podniku s požadovaným oprávnením vypne počítač. Pokiaľ na prístupových prepínačoch nie sú nastavené určité bezpečnostné nastavenia, stačí aby si nastavil IP adresu zamestnanca a dostane plný prístup s jeho oprávneniami.

Prevencia proti takýmto útokom nie je pritom zložitá a často je podporovaná na zariadeniach použitých v podnikových prístupových sieťach.

Technológia, ktorá umožňuje poskytovať prístup len k zdrojom na ktoré má užívateľ oprávnenie je uvedená pod štandardom IEEE 802.1X , v tejto práci je popísané, akým spôsobom je ju možné nasadiť práve v podnikovom prostredí, rovnako ako nastaviť základné bezpečnostné funkcionality ako protiopatrenia voči útokom používaných v prístupových sieťach.

Treba si uvedomiť, že každá sieť je bezpečná len tak, ako je zabezpečený jej najslabší článok. Z tohto hľadiska je nutné vynaložiť maximálne úsilie, aby každý prvok tejto siete bol zabezpečený na najvyššiu možnú úroveň.

I. TEORETICKÁ ČASŤ

1 DÔVODY ZABEZPEČENIA SIETE

Neoprávnený prístup prostredníctvom komunikačných sietí je jedným z najväčších ohrození bezpečnosti podnikovej komunikačnej infraštruktúry. V prípade, ak majú užívatelia alebo zariadenia nekontrolovaný a neriadený prístup do komunikačnej siete firmy, organizácia a jej dáta sa vystavujú možnosti najvážnejších napadnutí zo strany vírusov, malware prípadne iného sofistikovaného útoku. Toto môže viesť k tomu, že organizácia môže prísť o citlivé dáta, ktoré nadobúdala dlhé roky a jej postavenie na trhu sa môže výrazne zhoršiť, prípadne predstavovať iné nepriaznivé scenáre.

1.1 Identifikácia bezpečnostných slabín

V dnešnej dobe vznikajú z rôznych dôvodov bezpečnostné problémy, ktoré vo všeobecnosti delíme na tri základné zdroje slabých miest [1]:

- **Technologické.**
- **V bezpečnostnej politike.**
- **Konfiguračné.**

Technologické slabé miesta – každá technológia má niekoľko známych alebo neznámych slabín prípadne zraniteľností, ktoré môžu byť zneužívané dostatočne motivovaným útočníkom. Niektoré nedostatky sú v širokej miere publikované, pretože sú spojené s dobre známym a často používaným produktom. Ako príklad je možné uviesť slabé miesta v operačných systémoch, sieťových zariadeniach poprípade v protokoloch. Užívatelia by nemali podliehať falošnej ilúzii, že nejaký produkt je bezpečný pretože doposiaľ nepočuli o jeho slabých miestach. To, že sa niekto nezaujíma o prelomenie určitého produktu neznamená, že produkt je bezpečný.

Slabé miesta v bezpečnostnej politike – nedostatočne popísaná alebo nesprávne implementovaná bezpečnostná politika, čo môže viesť k bezpečnostným ohrozeniam sieťových systémov. Ako príklad je možné uviesť nedostatočné monitorovanie bezpečnosti, slabá kontrola používateľských prípadne systémových účtov, čo vedie k vytvoreniu zraniteľností ako aj možnosti neautorizovaného prístupu do siete.

Slabé miesta v konfigurácii – počas konfigurácie sieťových prípadne iných bezpečnostných zariadení administrátori nenakonfigurujú zariadenie správne podľa pravidiel bezpečnostnej politiky alebo neimplementujú protiopatrenia na známe zraniteľnosti. Ako príklad je možné uviesť prístup cez nezabezpečený kanál pomocou protokolu *telnet*, používanie

triviálnych hesiel ako je napr. *nbu123*, nesprávne nakonfigurovaný prístupový zoznam a podobne.

Samozrejme je možné definovať viacero bezpečnostných slabín ako je ľudsky faktor a podobne, ale hlavným cieľom bolo zadefinovať tie slabiny, ktoré je možné rozoznávať, riadiť, monitorovať, a zlepšovať v bezpečnostnej stratégii.

1.2 Bezpečnostná politika podniku

Aby sme dokázali predísť bezpečnostným rizikám a eliminovali bezpečnostné slabiny je potrebné zadefinovať bezpečnostnú politiku podniku, ktorá obsahuje súhrn bezpečnostných požiadaviek pre riešenie informačnej bezpečnosti. Bezpečnostná politika musí byť schválená vedením spoločnosti ako záväzná vnútropodniková smernica.

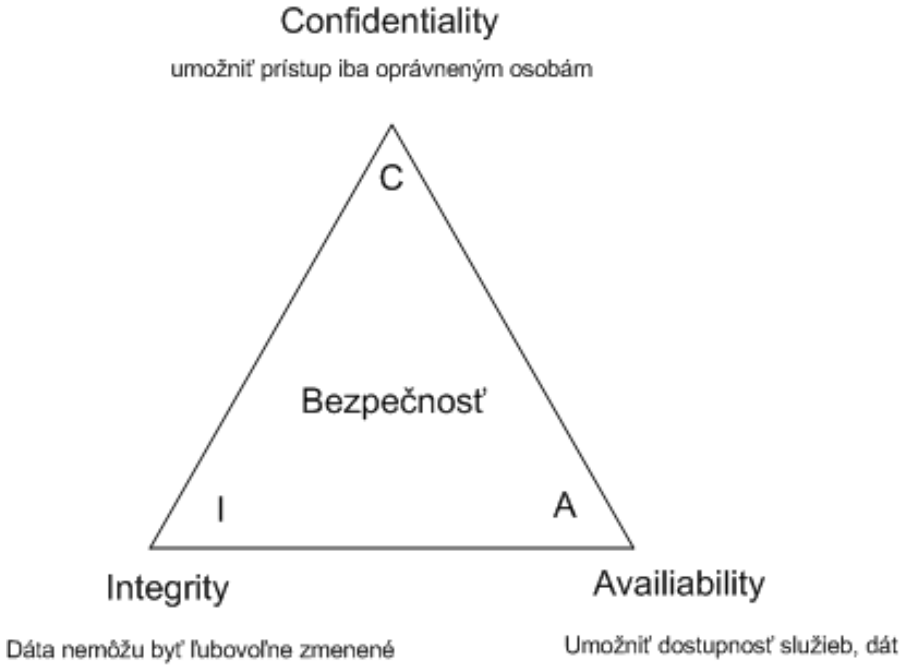
Bezpečnostná politika je chápaná ako písomný dokument podniku, obsahujúci predstavu vedenia spoločnosti o riešení bezpečnosti a základné požiadavky na jednotlivé bezpečnostné oblasti celého informačného systému. Cieľom bezpečnostnej politiky je vedieť odpovedať na niekoľko základných otázok:

- Čo chceme chrániť?
- Dôvod prečo to chceme chrániť?
- Akým spôsobom to chceme chrániť?
- Čo budeme robiť keď dôjde k zlyhaniu systému?

Hlavým cieľom bezpečnostnej stratégie je zabezpečenie základných funkcií informačných systémov, ktorý je definovaný podľa modelu CIA (Confidentality, Integrity, Availability)[2]:

- **Dôvernosť** (Confidentality) – umožniť prístup len autorizovaným subjektom, tj. zabránenie neoprávneným osobám prístupu k citlivým informáciám. Využívané sú rôzne kryptografické metódy, ktoré zaisťujú bezpečný prenos dát napr. cez zdieľané médium ako je Ethernet.
- **Integrita** (Integrity) **–** povoliť len autorizované zmeny, tj. zabránenie neoprávanej modifikácii dát, systémov, čo poskytuje istotu o správnosti údajov. Štandardným útokom na integritu je útok typu MITM (Man-In-The-Middle).
- **Dostupnosť** (Availability) – umožniť prístup v čase potreby, tj prevencia straty prístupu k zdrojom, informáciám v ľubovoľnom čase. Pre zaistenie dostupnosti služieb sa obvykle implementujú systémy vo vysokej dostupnosti to znamená je zvý-

šená redundancia jednotlivých prvkov. Jeden z bežných útokov na dostupnosť je DoS (Denial of Service) útok na odoprenie služby, teda dostupnosti systému, informácie.



Obr. 1. Bezpečnostný model CIA [2].

Riadenie prístupu a správa identít

V podnikovej sieti sa často rieši prístup k podnikovým zdrojom na základe IP adresy tz. pokiaľ subjekt potrebuje pristupovať k určitým zdrojom je identifikovaný na základe IP adresy a riadenie prístupu je štandardne riešené ACL (Access Control List), alternatívne riešenie je založené na princípe riadenia prístupu na základe identity, čo je omnoho sofistikovanejší spôsob, ktorý sa opiera o identifikáciu, autentifikáciu, autorizáciu a audit [2]:

- **Identifikácia**: zistenie mena subjektu (používateľské meno, poprípade IP adresa).
- **Autentizácia**: preverenie identity subjektu, typicky s použitím tajnej informácie najčastejšie heslo. Identifikácia bez autentifikácie nám prináša malú hodnotu dôvernosti.
- **Autorizácia**: nastavenie prístupových práv (určiť ktorý subjekt môže pristupovať k daným objektom). Primárne sa používajú ACL.
- **Audit (Accounting)**: zoznam prístupov a akcií vykonaných určitým subjektom.

Príklad použitia identifikácie, autentifikácie, autorizácie a auditu:

- **Identifikácia**: Kto si?
- **Autentizácia**: Dokáž to.
- **Autorizácia**: Čo môžeš robiť?
- **Audit (Accounting)**: Čo si vykonal?

Pre riadenie prístupu na základe identity užívateľa sa využíva štandard 802.1X, ktorý je nosným pilierom navrhovaného riešenia. Pre potreby identifikácie, autentizácie, autorizácie a auditu sa využíva bezpečnostný model AAA.

2 BEZPEČNOSTNÁ ARCHITEKTÚRA AAA

Architektúra AAA (Autentizácia, Autorizácia, Audit), poskytuje rozšírené zabezpečenie sieťovej infraštruktúry. Základom sú služby využívajúce nielen autentizáciu užívateľa alebo zariadenia, ale poskytuje aj mechanizmy prideľovania prístupových práv k zdrojom ako aj prostriedky pre audit využívania týchto zdrojov. Hlavnou myšlienkou je možnosť granulárneho zaistenia bezpečnostnej politiky, väčšinu parametrov AAA je preto možné nastaviť samostatne.

Autentizácia – úlohou autentizácie je preveriť, že prihlasujúci užívateľ je skutočne tým za koho sa vydáva a na strane druhej nepovoliť prístup neoprávneným osobám. Tento proces je realizovaný pomocou tajnej informácie ako je heslo, prípadne bezpečnostný predmet (generátor jedorázových hesiel, smart karta).

Autorizácia – sa vykonáva v prípade úspešnej autentizácie, tz priradiť užívateľovi oprávnenia ktoré jeho identite prislúchajú. Tieto oprávnenia môžu byť zabezpečené použitím prístupových zoznamov ACL, priradením užívateľa do určitej VLAN, poskytnutie privilegovanej úrovne 0 - 15 (pri CISCO IOS zariadeniach) a podobne.

Audit – cieľom tohto procesu je zhromažďovanie informácii o užívateľoch, ktorí boli alebo sú pripojení k sieťovým zariadeniam. Umožňuje sledovať využívanie sieťových prostriedkov a auditovať operácie, ktoré užívatelia vykonali.

Medzi najpoužívanejšie protokoly, ktoré sú založené na princípe AAA patria RADIUS a TACACS+, ktoré sú podrobnejšie popísané v kapitolách 2.1, 2.2.

2.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) je IETF (Internet Engineering Task Force) štandard, ktorý podporuje všetky tri komponenty AAA bezpečnostnej architektúry. Jedná sa o komunikačný model typu klient – server, čo znamená, klient pošle užívateľské informácie bezpečnostnému serveru RADIUS protokolom, následne bezpečnostný server odošle všetky informácie potrebné pre vykonanie autentizácie, autorizácie a auditu klienta za účelom zabezpečenia oprávnení a služieb užívateľovi, ktorý o ne žiadal. RADIUS podporuje viacero autentizačných metód napr. CHAP, PAP a EAP.

Protokol RADIUS komunikuje prostredníctvom UDP protokolu a používa porty 1645 a 1812 pre autentizačné a autorizačné požiadavky a porty 1646 a 1813 pre audit.

2.1.1 RADIUS Autentizácia, Autorizácia

Nižšie je popísaný princíp fungovania RADIUS protokolu pre autentizáciu a autorizáciu:

- V prvom kroku užívateľ odošle požiadavku na RADISU klienta (prístupový bod napr. access point alebo prepínač).
- Následne RADIUS klient vygeneruje požiadavku (Access-Request) a odošle ju na RADIUS server.
- RADIUS server odošle konkrétnu odpoveď (Access-Chalenge, Access-Accept, Access-Reject).

Access-Request paket obsahuje užívateľské meno, zašifrované heslo, IP adresu AAA klienta a port. Formát požiadavky obsahuje taktiež informáciu typu relácie, ktorú užívateľ žiada iniciovať. Niekedy pokiaľ RADIUS server potrebuje ďalšie informácie, pošle Access-Chalange odpoveď.

Tab. 1. Formát RADIUS paketu

Code	**Identifier**	**Length**
Request Authenticator		
Attributes		

Každý RADIUS paket obsahuje nasledujúce informácie [14].:

- **Code**: pole o veľkosti jedného bajtu, identifikuje typ RADIUS paketu. Keď je paket prijatý s neplatnou hodnotou, je potichu zahodený. Môže nadobúdať jednu z uvedených hodnôt:

    - Access-Request (1)
    - Access-Accept (2)
    - Access-Reject (3)
    - Accounting-Request (4)
    - Accounting-Response (5)

- Access-Chalenge (11)
- Status-Server (12) - experimentálny
- Status-Client (13) - experimentálny
- Reserved (255)

- **Access-Request (1)** – paket je odoslaný na RADIUS server a sprostredkúva informácie použité pre rozhodovanie, či má byť užívateľovi umožnený prístup cez daný prístupový server (RADIUS klienta). Klient musí RADIUS paket odoslať s hodnotou 1 v poli Code. Paket *Access-Reques*t musí obsahovať atribúty *User-Name* a *User-Password*, ďalej môže obsahovať atribúty *NAS-IP-Address, NAS-Identifier*, *NAS-Port* a *NAS-Port-Type*.
- **Access-Accept (2) –** paket je odoslaný RADIUS serverom a poskytuje špecifické konfiguračné informácie potrebné pre službu, ktorá je poskytovaná užívateľovi.
- **Access-Reject (3)** – pri odmietnutí požiadavky RADIUS serverom je posielaný paket Access-Reject, tento paket môže obsahovať informáciu ktorá je zobrazená užívateľovi.
- **Accounting-Request (4)** – pakety sú posielané z klienta na RADIUS server, a obsahujú informácie použiteľné pre zaznamenanie služby poskytnutej užívateľovi.
- **Accounting-Response (5)** – pakety sú odoslané RADIUS serverom klientovi pre potvrdenie, že *Accounting-Request* bol prijatý a zaznamenaný.
- **Access-Callenge (11)** – Niekedy pokiaľ RADIUS server potrebuje ďalšie informácie, pošle *Access-Chalange* odpoveď klientovi (využívané napr. pri autentizačnej metóde EAP-OTP).

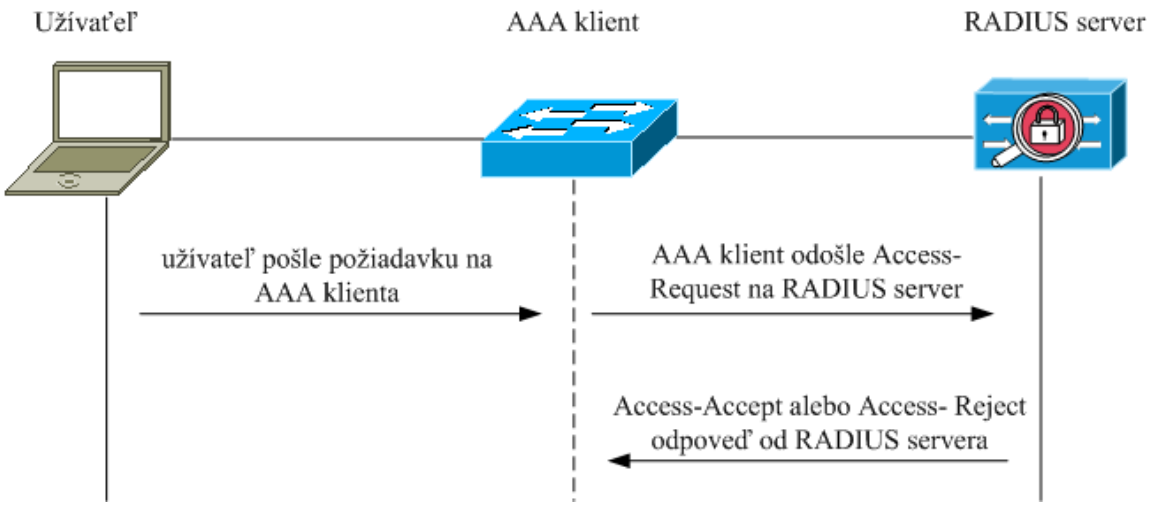
- **Identifier**: pole o veľkosti jedného bajtu, pomáha RADIUS serveru spárovať požiadavky a odpovede, zároveň detekuje duplicitné požiadavky.
- **Lenght**: pole o veľkosti dvoch bajtov, určuje veľkosť celého paketu, pokiaľ je paket menší ako je uvedené v poli Lenght, môže to znamenať chybu a paket môže byť potichu zahodený. Minimálna dĺžka je 20B, a maximálna je 4096B.

- **Request Authenticator:** pole o veľkosti šestnástich bajtov, jeho hodnota je použitá pri autentifikácii odpovede z RADIUS servera a ďalej použitá pri šifrovaní posielaného hesla.
- **Attributes**: nesú špecifické autentizačné, autorizačné informačné a konfiguračné detaily pre požiadavky a odpovede. Koniec zoznamu atribútov je určený dĺžkou RADIUS paketu. V tab. č.2 je zobrazená štruktúra atribútu.

Tab. 2. Štruktúra RADIUS Atribútu[14].

Type	Length	Value

- Type – pole o veľkosti jedného bajtu, definuje typ atribútu ako napr. User-Name, User-Password, NAS-IP-Address,...
- Lenght – pole o veľkosti jedného bajtu, označuje veľkosť atribútu zahrňujúce polia Type, Lenght, Value
- Value – pole má premenlivú veľkosť a obsahuje informácie, ktoré sú špecifické pre tento atribút.



Obr. 2. Princíp RADIUS autentizácie [7].

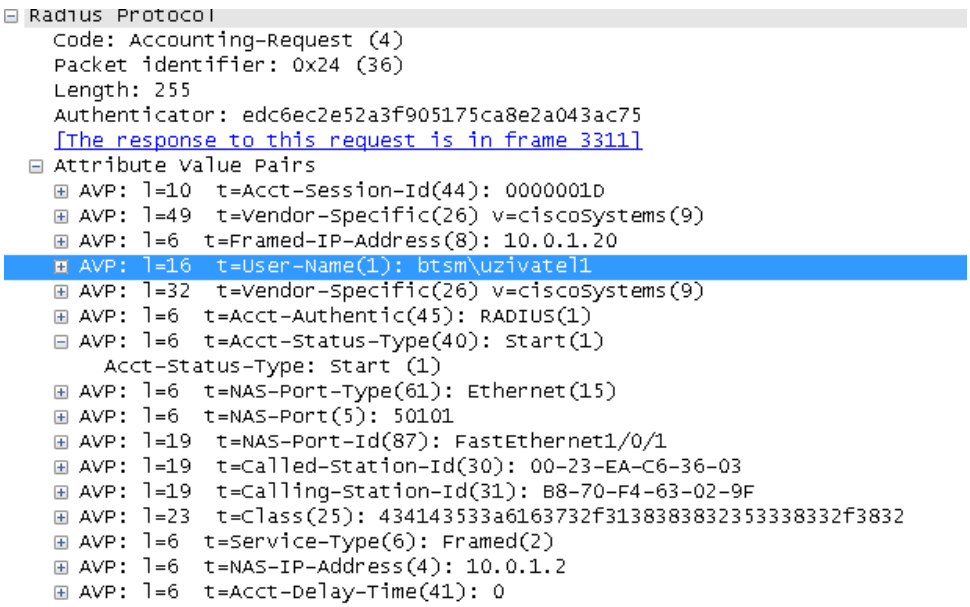
Treba si uvedomiť, že protokol RADIUS šifruje len heslo, ostatné časti sú posielané ako prostý text, teda voľne čitateľné.

2.1.2 RADIUS Audit

Tento protokol je rozšírením štandardného RADIUS protokolu, jeho rozšírenie spočíva v možnosti zasielania účtovacích informácií z prístupového servera RADIUS serveru. RADIUS audit sa je vykonávaný zaslaním *Accounting-Start viď* obr.č. 3 a *Accounting-Stop* paketu podľa toho, či sa jedná o začiatok alebo koniec relácie. V auditné pakety obsahujú informácie o relácii, typ poskytovanej služby, prenesené bajty, užívateľa ktorému je služba poskytovaná a iné dôležité informácie spojené s poskytovanými službami. Správy posielané medzi AAA serverom a AAA klientom sú *Accounting-Request* a *Accounting-Response* [14]:

- Accounting-Request – pakety sú posielané od klienta na RADIUS server a nesú informácie pre použitie pre audit služieb poskytovaných užívateľovi.

- Accounting-Response – pakety sú odoslané RADIUS serverom späť klientovi pre potvrdenie, že Accounting-Request bol v poriadku prijatý a zaznamenaný.



Obr. 3. RADIUS Accounting-Request

2.2 TACACS+

TACACS+ (Terminal Access Controller Access Control System Plus) je sieťový protokol slúžiaci pre zabezpečenie centralizovaného riadenia prístupu na sieťové zariadenia ako sú prepínače, smerovače, firewaly a pod. Deje sa tak za pomoci jedného alebo viacerých centralizovaných serverov. Tento server potom môže obsahovať kontrolu prístupu pre tieto sieťové prvky, čím sa výrazne uľahčí sledovanie a konfigurácia prístupových práv pre všetky sieťové zariadenia. Na rozdiel od RADIUS protokolu ponúka samostatne overovanie autentizácie, autorizácie a auditu. Jedná sa o proprietárny protokol spoločnosti Cisco, na rozdiel od RADIUS protokolu používa protokol TCP/49, teda spojovo orientovaný protokol, a celá komunikácia je šifrovaná. Samotný RADIUS protokol nemá príliš veľa možností na autorizáciu. Ideálne je kombinovať tieto dva protokoly, ktoré sa vhodne dopĺňajú.

Formát TACACS+ paketu

Tab. 3. Formát TACACS+ paketu [7].

major version (4bit)	**minor version** (4bit)	**type** (8bit)	**seq_no** (8bit)	**flags** (8bit)
session_id				
length				

- **Major version** – popisuje hlavnú verziu TACACS+ protokolu.
- **Minor version** – pospisuje minor verziu protokolu, využívanú pre spätnú kompatibilitu.
- **Type** – typ paketu ktorý môže nadobúdať hodnôt:
    - TAC_PLUS_AUTHEN = 0x01 (autentizácia).
    - TAC_PLUS_AUTHOR = 0x02 (autorizácia).
    - TAC_PLUS_ACCT = 0x03 (audit).
- **Seq_no** – sekvenčné číslo aktuálneho paketu v relácii. Prvý paket v relácii musí začínať sekvenčným číslom 1, následne každý ďalší paket v danej relácií je inkrementovaný o 1.
- **Flags** – Toto pole obsahuje príznaky ktoré môžu nadobúdať hodnôt:

- TAC_PLUS_UNENCRYPTED_FLAG.
- TAC_PLUS_SINGLE_CONNECT_FLAG.

TAC_PLUS_UNENCRYPTED_FLAG – tento príznak určuje, či sa v tele TACACS+ paketu vykonáva šifrovanie alebo nie. Pokiaľ je hodnota nastavená na 1, šifrovanie nie je vykonávané a opačne pokiaľ je hodnota nastavená na 0 paket sa šifruje. Možnosť vypnutia šifrovania by sa mala vykonávať len v prípade testovania a ladenia samotného protokolu.

TAC_PLUS_SINGLE_CONNECT_FLAG - príznak určuje či je podporované multiplexovanie viacerých TACACS+ relácii do jednej TCP relácie.

- **Session_id** – Náhodná hodnota, ktorá označuje aktuálnu reláciu medzi AAA klientom a TACACS+ serverom. Táto hodnota je rovnaká počas celej dĺžky trvania relácie.
- **Lenght** – Toto pole označuje celkovú dĺžku TACACS+ paketu, ale nezahrňuje záhlavie o veľkosti 12 bajtov.

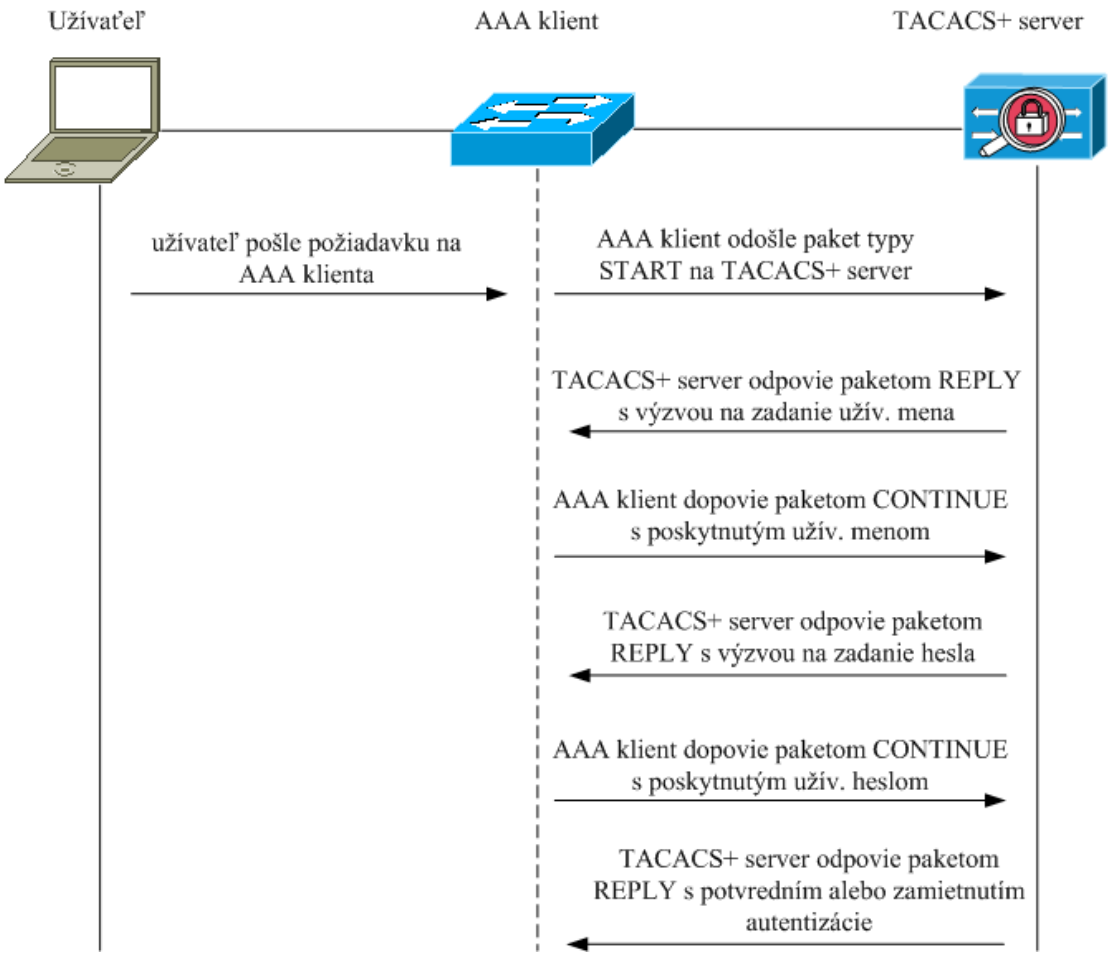
2.2.1 TACACS+ autentizácia

Pri priebehu autentizácie pomocou protokolu TACACS+ sa používajú tri možné typy paketov resp. výmeny správ [7]:

- **START**- tento paket je posielaný na začiatku komunikácie, keď sa užívateľ snaží pripojiť.
- **REPLY** – paket posielaný autentizačným serverov počas autentizačného procesu.
- **CONTINUE** - paket posielaný klientom k odoslaniu prihlasovacích údajov, ako je meno a heslo na autentizačný server.

Autentizácia nastáva v prípade, keď AAA klient dostane požiadavku od užívateľa so žiadosťou o autentizáciu, AAA klient vtedy odošle START paket na autentizačný server, pričom tento paket obsahuje informácie ohľadne typu autentizácie, ako je prihlasovacie meno a heslo. Ak je autentizačný proces ukončený server odpovedá správou REPLY s výsledkom procesu autentizácie, ktorý môže nadobúdať tieto hodnoty:

- **ACCEPT** – užívateľ je úspešne autentizovaný a môže mu byť poskytnutá požadovaná služba, v prípade, že je vyžadovaná autorizácia, začína práve v tomto kroku.
- **REJECT** – autentizácia bola neúspešná a užívateľ bol odmietnutý.
- **ERROR** - posielaný v prípade nejakej chyby na AAA servery, alebo v komunikácii, najčastejšie to môže znamenať nesprávne nastavené zdieľané tajomstvo (secret) medzi klientom a TACACS+ serverom.



Obr. 4. Princíp TACACS+ autentizácie [7].

Postup autentizácie je nasledovný:

Krok č.1 – AAA klient príjme požiadavku na pripojenie od užívateľa.

Krok č.2 – AAA klient pošle prvý paket typu START na TACACS+ server, ktorý obsahuje spôsob autentizácie.

Krok č.3 – TACACS+ server odošle REPLY paket späť na AAA klienta, vyžadujúci poslanie prihlasovacieho mena.

Krok č.4 – AAA klient odošle CONTINUE paket späť na TACACS+ server spolu s prihlasovacím menom poskytnutým od užívateľa.

Krok č.5 – TACACS+ server odošle paket typu REPLY späť na AAA klienta za účelom získania hesla.

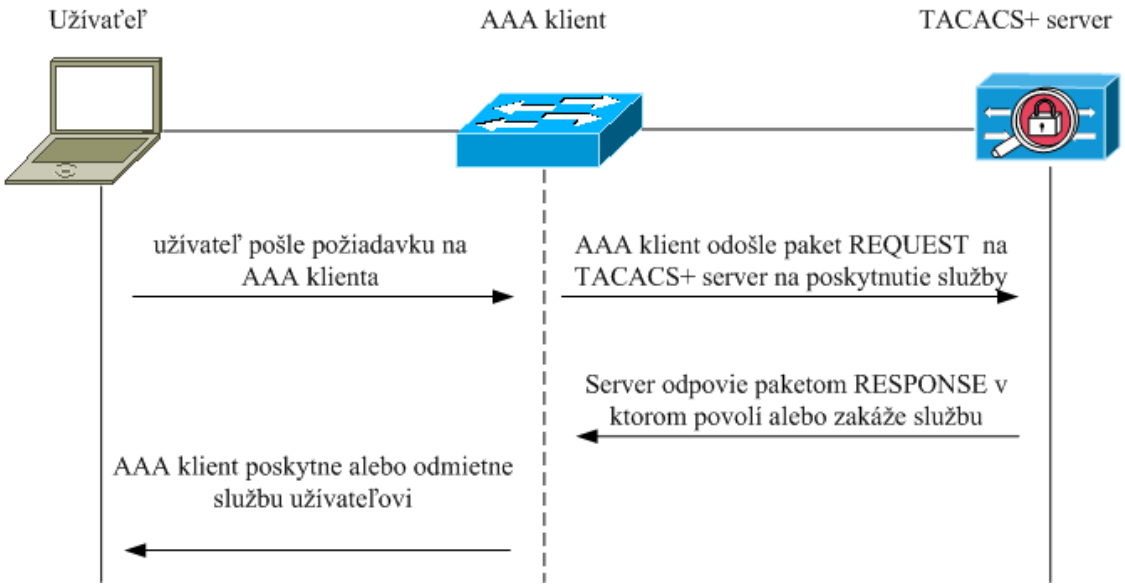
Krok č.6 – AAA klient odošle paket typu CONTINUE na TACACS+ server, ktorý obsahuje heslo užívateľa.

Krok č.7 – TACACS+ server následne odošle paket typu REPLY späť na AAA klienta ktorý indikuje úspešnú prípadne neúspešnú autentizáciu.

2.2.2 TACACS+ autorizácia

Počas priebehu autorizácie pomocou protokolu TACACS+ existujú dva možné typy paketov resp. výmeny správ [7]:

- **REQUEST** – obsahuje žiadosť na konkrétne služby napr. shell.
- **RESPONSE –** autorizácia môže obsahovať návratové parametre:
    - **FAIL –** posielaný v prípade, že autorizácia bola neúspešná
    - **PAS_ADD** – požiadavka na autorizáciu bola úspešná, ale sú vyžadované ďalšie informácie od klienta.
    - **PASS_REPL –** táto hodnota je vrátená klientovi v prípade, že TACACS+ server ignoruje REQUEST paket.
    - **FOLLOW –** sa posiela v prípade, keď AAA server požaduje vykonať autorizáciu na inom TACACS servery.
    - **ERROR –** posielaný v prípade nejakej chyby na AAA servery, alebo v komunikácii, najčastejšie to môže znamenať nesprávne nastavené zdieľané tajomstvo (secret) medzi klientom a TACACS+ serverom.



Obr. 5. Princíp TACACS+ autorizácie.

Porovnanie RADIUS a TACACS+ protokolov

Porovnanie jednotlivých vlastností oboch protokolov je popísane v tab. č. 4.

Tab. 4. Porovnanie vlastností RADIUS a TACACS+ protokolu[8].

RADIUS	TACACS+
Autentizácia a autorizácia sú zlúčené, ale audit je samostatný. Toto umožňuje menšiu pružnosť pri implementácii.	Separátne všetky tri funkcionality AAA, za účelom väčšej flexibility.
Šifrované len heslo.	Šifrovaný celý paket.
Nepodporuje logovanie vykonaných príkazov.	Podpora logovania vykonaných príkazov.
Minimálna podpora výrobcov zariadení pre autorizáciu (autorizácia príkazov vykonaných jednotlivými užívateľmi alebo skupinami).	Podporovaný väčšinou výrobcov.
UDP –nespojovo orientovaný protokol.	TCP - spojovo orientovaný protokol.
UDP - porty 1645/1646, 1812/1813.	TCP - port 49
Určený pre užívateľov požadujúcich služby AAA.	Určený pre prístup administrátorov na sieťové prvky.

2.3 Princíp činnosti štandardu 802.1X

IEEE (Institute of Electrical and Electronics Engineers) 802.1X je štandard, ktorý poskytuje riadenie prístupu na port prepínača za použitia autentifikácie, čo zabraňuje neautorizovaným klientom pripojiť sa k sieti LAN sieti. Autentizačný server overuje každého klienta pripojeného k portu prepínača, ešte pred tým než sú mu poskytnuté služby. Pokiaľ nie je klient autentizovaný, pomocou metódy 802.1X je povolená len komunikácia EAPoL (Extensible Authentication Protocol over Lan), CDP (Cisco Discovery Protocol) a STP (Spanning Tree Protocol). Po úspešnej autentifikácii a autorizácii je povolená štandardná prevádzka cez port prepínača[3].

Štandard 802.1X v kombinácií s existujúcimi protokolmi akými sú EAP a RADIUS, poskytuje vysokú úroveň zabezpečenia a riadenia prístupu ku sieti a ponúka oprávnenia prislúchajúce identite, ktoré zodpovedajú bezpečnostnej politike podniku.

Nasadenie štandardu 802.1X vyžaduje tri základné komponenty ktorými sú:

Suplikant – služba na koncovom zariadení inicializujúca a reagujúca na výzvy autentifikácie a autorizácie prostredníctvom protokolu EAPOL. Suplikant môže predstavovať softvér, ktorý je natívnou súčasťou operačných systémov ako Microsoft Windows 7, ale rovnako môže byť súčasťou firmvéru určitého zariadenia.

Autentizátor – prepínač, bezdrôtový prístupový bod prípadne smerovač vynucujúci identifikáciu a autentifikáciu a realizáciu bezpečnostnej politiky. Predstavuje akúsi bezpečnostnú bránu medzi suplikantom a prístupovou sieťou. Táto bezpečnostná brána (reálne port), ostane zatvorená, pokiaľ neprebehne autentizácia a realizuje sa autorizácia. Následne je suplikantovi umožnený prístup do chránenej siete.

Autentizačný server – RADIUS server overujúci identitu pripájajúceho sa zariadenia, používateľa a priraďujúci rozsah prístupu do vnútornej siete. RADIUS server v podnikových sieťach môže byť prepojený s externým zdrojom identít ako Active Directory, LDAP, RSA SecureID server a podobne.

Obr. 6. Komponenty v štandarde 802.1X.

2.4 EAPOL

RFC 2284 pre EAP (Extensible Authentication Protocol) protokol nešpecifikuje akým spôsobom sa majú EAP správy posielať, keďže EAP bol pôvodne vyvinutý pre použitie pomocou PPP (Point-to-Point) protokolu, je potrebné nejakým spôsobom zabezpečiť prenos EAP správ cez LAN sieť. Práve preto IEEE v štandarde 802.1X implementoval protokol s názvom EAP over LAN za účelom prenosu EAP správ od suplikanta k autentizátoru. To znamená, že EAP protokol je zapuzdrený do EAPOL rámca. Využíva sa päť rôznych typov EAPOL správ [9]:

- **EAPOL-Start** – posielaný na začiatku komunikácie suplikantom na autentizátor, ako inicializácia autentizácie.
- **EAPOL-Key** – v prípade povolenia prístupu do siete, autentizátor posiela šifrovacie kľúče suplikantovi.
- **EAPOL-Packet** – tento typ rámca je používaný pre posielanie EAP správ, predstavuje nejaký kontajner pre prenos EAP správ cez LAN sieť.
- **EAPOL-Logoff** – posielaný suplikantom a ukončuje EAP reláciu, deje sa v prípade keď sa zariadenie odpája.
- **EAPOL-Encapsulated-ASF-Alert** – povoľuje posielanie rôznych poplachových správ (napr. SNMP-trap) v prípade, že je port sa nachádza v neautorizovanom stave.

Tab. 5. Formát EAPOL rámca [9].

Ethernet MAC Header	Protocol Version	Packet type	Packet Body Length	Packet Body

Autentizačný proces začína, keď suplikant pošle EAPOL-Start rámec, ale obyčajne port na autentizátore je aktívny a spustí proces EAP automaticky. Deje sa tak poslaním správy EAP-Request/Identity. Dôležitým prvkom je správa EAPOL-Logoff , ktorá je posielaná suplikantom ku autentizátoru. Tento proces predstavuje koniec asociácie.

2.5 EAP

Pri protokole EAP nedochádza k vyjednaniu autentizačného protokolu pri nadviazaní spojenia, ako je to napr. pri použití protokolu CHAP (Challenge-Handshake Authentication Protocol), ale v tejto fáze dôjde len k dohode, že sa použije protokol EAP.

Skutočnosť, že medzi oboma koncami spojenia dôjde k dohode na použití protokolu EAP, ešte nepredurčuje použitie konkrétneho autentizačného algoritmu, ten sa vyjedná až samotným protokolom EAP. Protokol EAP tak umožňuje používať ľubovoľný autentizačný mechanizmus, stačí ho len implementovať na oboch stranách spojenia. Pokiaľ sa použije protokol EAP, skladá sa z fázy autentizácie na konkrétnom autentizačnom mechanizme, až následne na vlastnej autentizácii [4].

Dnes je mnoho dostupných EAP autentizačných metód, niektoré sú popísané v IETF RFC 3748 ako EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, existujú aj niektoré proprietárne metódy ako PEAP, LEAP.

EAP popisuje štyri typy správ ktoré môžu byť posielané:

- **Request**: používaný k posielaniu správ od autentizátora ku suplikantovi.
- **Response**: používaný k posielaniu správ od suplikanta k autentizátóru.
- **Success**: posielaný autentizátorom na povolenie prístupu.
- **Failure**: posielaný autentizátorom na odmietnutie prístupu.

Formát paketu EAP

V tab. č.6 je zobrazený formát EAP paketu.

Tab. 6. Formát EAP paketu [5].

Code	Identifier	Length	Data

- **Code**: Pole o veľkosti jedného bajtu, ktoré identifikuje o aký typ správy sa jedná (Request, Response, Success alebo Failure). V prípade ak sú poslané iné typy správ musia byť zahodené a to autentizátorom ako aj suplikantom.
- **Identifier**: Pole o veľkosti jedného bytu pomáha zabezpečiť spárovanie správ typu Response a Request. Každá nová správa typu request používa nové identifikačné číslo.
- **Lenght**: Pole o veľkosti dvoch bytov udáva súčet bytov v celom EAP pakete.
- **Data**: Hodnota premenlivej dĺžky, formát poľa Data je závislé na poli Code.

2.5.1 EAP autentizačné mechanizmy

EAP-MD5 – je autentizačný mechanizmus definovaný v RFC 3748, ponúka minimálne zabezpečenie, na autentizáciu klienta sa používa MD5 hash. Všeobecne sa neodporúča používať pretože je zraniteľný na slovníkové útoky ako aj útok MITM (Man In The Middle).

LEAP – (Lightweight Extensible Authentication Protocol) – je proprietárny autentizačný EAP mechanizmus vyvinutý spoločnosťou Cisco. Využíva sa predovšetkým v bezdrôtových sieťach. Dáta sú šifrované dynamicky generovaným WEP (Wired Equivalent Privacy) kľúčom. Hoci tento mechanizmus podporuje vzájomnú autentizáciu, prístupové údaje môžu byť ľahko kompromitované.

PEAP – (Protected Extensible Authentication Protocol) – jedná sa o autentizačný mechanizmus ktorý spolu vyvíjali spoločnosti Microsoft, Cisco a RSA Security. Táto autentizačná metóda poskytuje vysokú mieru zabezpečenia, nakoľko medzi klientom a autentizačným serverom sa najskôr vytvorí zabezpečený TLS (Transport Layer Security) tunel, a následne sa klient autentizuje voči serveru napr. MS-CHAP2 (Microsoft Challange-Handshake Authentication Protocol v2), alebo GTC (Generic Token Code) napr. s použitím tokenu generujúceho jednorazové heslo napríklad od spoločnosti RSA Security produkt SecurID.

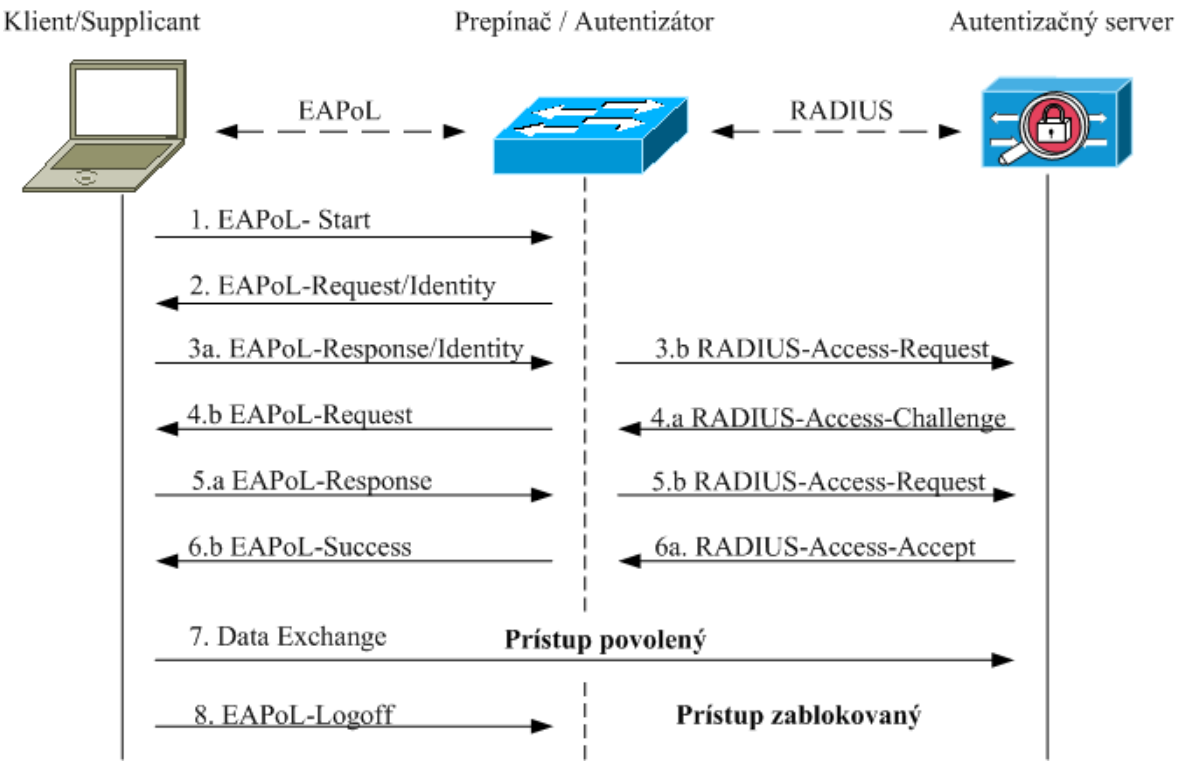
EAP-TLS (Transport Layer Security) je zadefinovaný v RFC 5216 a poskytuje najvyššiu mieru zabezpečenia, využíva PKI (Public Key Infrastructure) na zabezpečenie komunikácie. Rovnako ako pri PEAP je medzi klientom a autentizačným serverom vytvorený TLS tunel, avšak klient sa autentizuje klientskym certifikátom. V prípade, že je certifikát resp. jeho privátny kľúč nainštalovaný na smart karte jedná sa o dvojfaktorovú autentizáciu.

EAP-TTLS – (Tunneled Transport Layer Security) je autentizačný mechanizmus vyvinutý za účelom aby poskytoval silnú autentizáciu ako je to u mechanizmu EAP-TLS ale nevyžaduje vybudovanú PKI infraštruktúru, namiesto toho je vytvorený TLS tunel ako v prípade PEAP mechanizmu. To znamená že v prvej fáze si klient overí či je autentizačný server dôveryhodný na základe jeho certifikátu následne poskytne prihlasovacie údaje cez už zabezpečený TLS tunel.

EAP autentizačné mechanizmy, ktoré spoliehajú na autentizáciu na základe užívateľského mena a hesla (PEAP,TTLS, LEAP) môžu odhaliť informácie o identite užívateľa (užívateľské meno), ktoré sú sieťou prenášané v podobe obyčajného textu. Táto skutočnosť môže pre niektoré organizácie predstavovať riziko odhalenia informácií, nakoľko umožňuje útočníkovi získať zoznam platných užívateľských mien, čo predstavuje solídny základ pre ďalšie útoky proti sieti [6].

2.6 Autentizácia v 802.1X

Ako bolo popísané v kapitole2.3. štandard 802.1X definuje tri základné komponenty tj. suplikant, autentizátor, a autentizačný server. Výmena správ v závislosti od uvedených troch základných komponentov sa v procese 802.1X uskutočňuje prostredníctvom EAP respektíve EAPOL paketov, počnúc od suplikanta cez autentizátor a autentizačný server za použitia RADIUS protokolu, enkapsulovaním EAP protokolu do RADIUS protokolu, niekedy nazývaného ako *EAP over RADIUS.* Obr. č.7 popisuje výmenu správ v procese 802.1X.



Obr. 7. Výmena správ v procese 802.1X [7].

Proces autentizácie 802.1X s použitím EAP protokolu je nasledovný:

Krok č.1 – Autentizátor najprv pošle správu typu *EAPOL-Request* pre zistenie identity Suplikanta, ktorý môže taktiež naštartovať uvedený proces poslaním správy typu *EAPOL-Start.*

Krok č.2 – Pokiaľ suplikant odošle správu typu *EAPOL-Start*, autentizátor následne odošle požiadavku na overenie identity suplikanta. Toto sa deje zaslaním správy typu *EAPOL-Request/Identity*.

Krok č.3– Suplikant odošle informácie prostredníctvom rámca *EAPOL-Response/Identity* a autentizátor dekapsuluje z EAPOL rámca prepošle EAP informácie prostredníctvom RADIUS protokolu ako *RADIUS-Access-Request*.

Krok č.4 – RADIUS server si vyjedná komunikáciu so suplikantom a to poslaním *RADIUS-Access-Challange* paketu, ktorý zašle autentizátoru. Ten následne enkapsuluje EAP informáciu do rámca EAPOL a pošle ju suplikantovi ako *EAPOL-Request*.

Krok č.5 – v odpovedi na *EAPOL-Request* suplikant odpovie správou *EAPOL-Response* prostredníctvom autentizátora, ktorý opäť dekapsuluje EAP informáciu a odošle ju RADIUS serveru ako *RADIUS-Access-Request*.

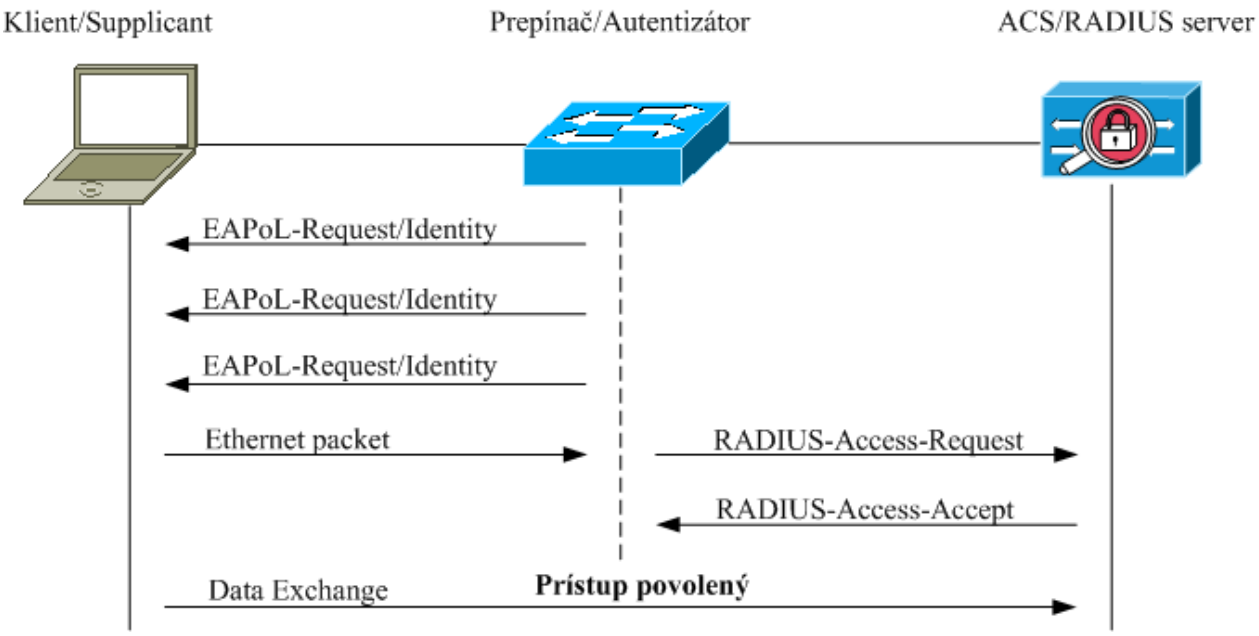
Krok č.6 – RADIUS server odpovie klientovi, že je úspešne autentizovaný. Proces prebieha poslaním správy *RADIUS-Access-Accept*. Autentizátor túto správu opätovne dekapsuluje a EAP informácie pošle na suplikanta prostredníctvom správy *EAPOL-Success*. Od toto momentu je port autorizovaný a klientovi je umožnená komunikácia.

Krok č.7 – v tomto štádiu je suplikantovi umožnená komunikácia a môže prenášať dáta.

Krok č.8 – po ukončení komunikácie suplikant pošle správu *EAPOL-Logoff* smerom ku autentizátoru, ktorý uvedie port do neautorizovaného stavu.

Proces autentizácie s použitím MAB (Mac Authentication Bypass)

MAB sa používa v prípade, keď je na port prepínača pripojené zariadenie, ktoré nevie využiť žiadnu autentizačnú metódu. Štandardne sa jedná o tlačiarne, IP kamery prípadne iné zariadenia typu „NONPC“. Tento spôsob je vhodné využívať len v čo najmenšom množstve. Princíp fungovania je názorne zobrazený na obr. č.8, ktorý popisuje proces autentizácie za použitia metódy MAB.



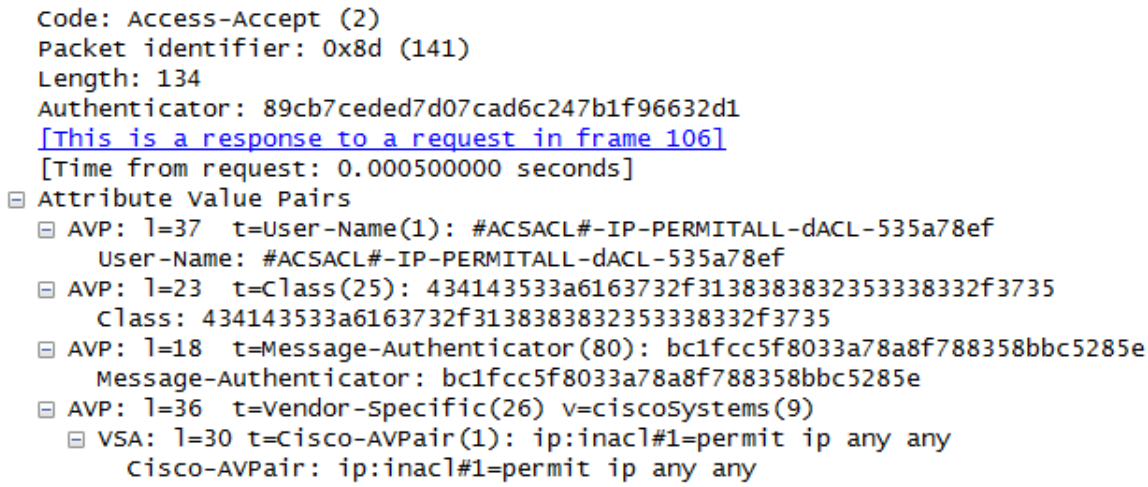
Obr. 8. Proces autentizácie za použitia metódy MAB [7].

Na začiatku komunikácie sa port na autentizátore sa nachádza v neautorizovanom stave. Po pripojení zariadenia zašle prepínač EAPOL *Request/Identity* paket. Po uplynutí 30 sekundového limitu (prednastavená hodnota), opätovne zašle EAPOL Request/Identity paket. Tento proces sa zopakuje spolu tri krát. Následne autentizátor zašle *RADIUS-Access-Request* na autentizačný server, ako prihlasovacie meno použije MAC adresu zariadenia. Pokiaľ autentizačný server overí oprávnenie koncovej stanici zašle naspäť na autentizátor paket typu *RADIUS-Access-Accept* a prepínač prepne port do autorizovaného stavu. V prípade, že autentizačný server neoverí identitu zariadenia, odošle autenizátoru paket *RADIUS-Access-Reject*.

2.7 Autorizácia v 802.1X

Štandard 802.1X umožňuje dva rôzne autorizačné prístupy, ktorými je možné autorizovať resp. poskytnúť oprávnenia prislúchajúce užívateľovi, alebo zariadeniu pripojenému na port prepínača. Spôsob akým autentizátor komunikuje s autentizačným serverom je podobný, ako v prípade autentizácie. Funguje na princípe posielania RADIUS atribútov, ktoré sú odlišné pri použití každej metódy. Autorizáciu je možné vykonať dvoma spôsobmi:

- **Aplikovanie prístupového zoznamu ACL na port prepínača** – po úspešnej autentizácií, autentizačný server odosiela *RADIUS-Access-Accept* paket. V tomto pakete sú posielané rôzne RADIUS atribúty, jeden z nich je označovaný ako *VSA* (Vendor Specific Attribute), ktorý obsahuje prístupový zoznam ACL, použitý ako výsledok autorizácie. Na obr. č.9 je zobrazený fragment RADIUS paketu s definovaným ACL. Tento prístupový zoznam sa je pomenovaný *PERMITALL-dACL* a obsahuje prístupový zoznam *permit ip any any*. Prístupové zoznamy konfigurované na autentizačnom servery sa nazývajú dACL (downloadableACL).



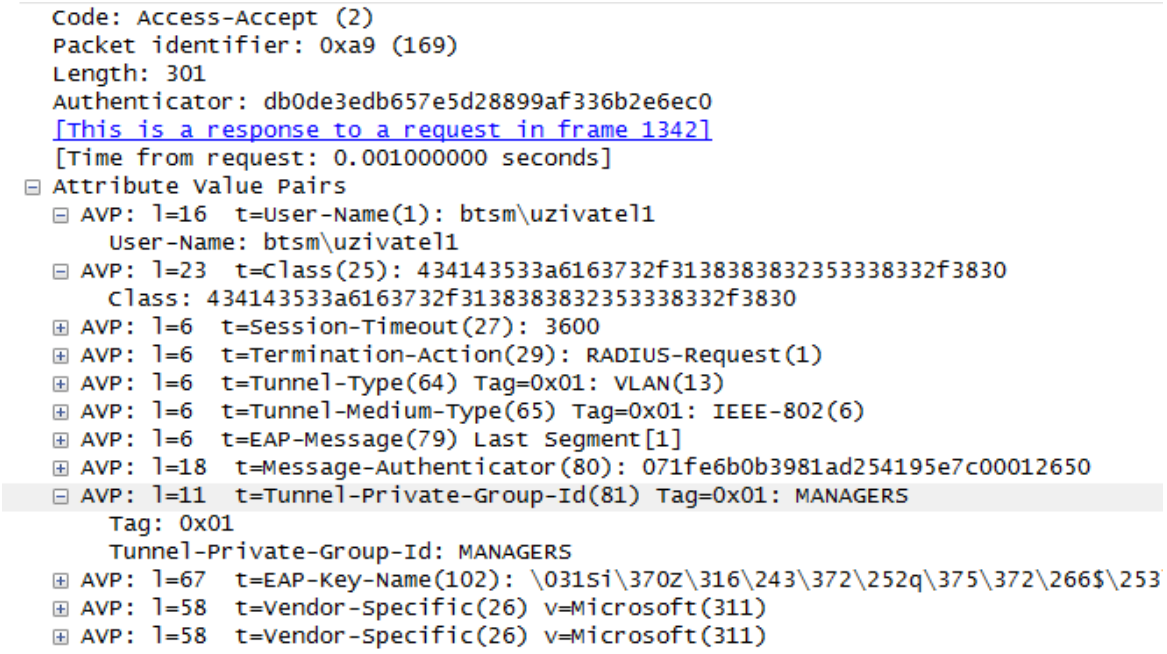
Obr. 9. RADIUS-Access-Accept paket pri použití dACL

- **Priraďovanie zariadení do dynamických VLAN** – po úspešnej autentizácii, autentizačný server posiela *RADIUS-Access-Accept* paket, v ktorom je zadefinovaný atribút s parametrom *Tunnel-Private-Group-Id.* Ten určuje identifikátor VLAN siete, do ktorej je užívateľ autorizovaný.

  Na obr. č. 10 je zobrazený fragment RADIUS-Access-Accept paketu, kde sa klient *užívatel1* úspešne autentizoval a autentizačný server povolil pripojenie do siete VLAN s názvom *MANAGERS.* Pri dynamickom prideľovaní VLAN sietí sú posielané nasledujúce atribúty [19]:

  - Tunnel-Type: VLAN (13).
  - Tunnel-Medium-Type: 802 (6).
  - Tunnel-Private-Group-ID: ID VLAN.

- Tunnel-Type – identifikuje, že sa jedná o VLAN sieť.
- Tunnel-Medium-Type – určuje, že sa jedná o štandard IEEE 802.
- Tunnel-Private-Group – určuje identifikátor, alebo názov VLAN siete.



Obr. 10. RADIUS paket pri dynamickom prideľovaní VLAN.

3 SIEŤOVÁ BEZPEČNOSŤ

Je dôležité si uvedomiť, aké je veľmi ťažké objaviť a zabezpečiť všetky bezpečnostné hrozby, pretože útočníkovi stačí využiť len jednu bezpečnostnú slabinu k útoku. Na rozdiel je od správcov systémov, ktorí musia zabezpečovať všetky prvky ako celok, je teda vhodné aby boli dodržiavané odporúčania na zamedzenie doposiaľ známych typov útokov. Základné typy útokov používaných v prístupovej vrstve siete, ako aj protiopatrenia na ich elimináciu sú uvedené v kapitole 3.2.

3.1 Rozdelenie sieťových útokov

Vo všeobecnosti delíme sieťové útoky na tri skupiny[1]:

- Prieskumný útok.
- Prístupový útok.
- DoS útok (Odopretie služby).

Prieskumný útok – jedná sa o pasívny útok, kedy útočník vykonáva prieskum, alebo skenovanie siete do ktorej je pripojený a môže že sa pripravovať na ďalší útok (prístupový, alebo DoS). Útočník na to využíva viacero techník, ktorými môže zistiť základné informácie o sieti do ktorej je pripojený, aké zariadenia sa na sieti nachádzajú, otvorené porty, zraniteľnosti zariadení a podobne. Medzi najznámejšie používané nástroje na skenovanie siete sú: nmap, netcat, wireshark, telnet, ping.

Prístupový útok – ide o aktívny útok, kedy sa útočník snaží dostať k neoprávnenému prístupu k systémom, alebo dosiahnuť požadované informácie a následne vykonať ich modifikáciu. Najčastejšie sa jedná o prelomenie autentizácie, presmerovanie prevádzky cez iné zariadenie (Man-In-The-Middle) a podobne.

DoS – jedná sa o aktívny útok, kedy sa útočník snaží úmyselne znefunkčniť alebo odoprieť nejakú službu určenú legitímnym užívateľom. Službou je možné chápať rôzne pojmi ako je napr. sieťová infraštruktúra, prístup k aplikácii, a pod. Odopretie služby môže byť vykonané rôznymi spôsobmi napr. využitie slabiny v aplikácii, dosiahnutie limitu systému, sieťového rozhrania, poprípade systémových prostriedkov. Medzi najznámejšie DoS útoky patrí zahltenie TCP/SYN paketmi.

3.2 Sieťové útoky na linkovej vrstve a protiopatrenia na ich elimináciu

V tejto časti sú popísané možné útoky na linkovej vrstve OSI referenčného modelu, a návrh protiopatrení na ich elimináciu. V tab. č.7 je prehľad základných bezpečnostných nástrojov Cisco IOS softvéru, ktoré je možné použiť na ich elimináciu. Konfigurácia jednotlivých bezpečnostných nástrojov je uvedená v kapitole 6.2.1.

Tab. 7. Bezpečnostné nástroje Cisco IOS.

Bezpečnostný nástroj	Popis
Port Security	Obmedzuje počet MAC adries, ktoré sa prepínač povolí na prístupovom porte.
BPDU guard	V prípade, že sa na porte prepínača objaví BPDU rámec, prepínač nastaví port do err-disable.
Root guard	Riadenie, ktoré porty na prepínači sa nesmú stať root portami.
Dynamic ARP inspection	Zabraňuje podvrhnutiu MAC adresy.
802.1x	Autentizuje užívateľov, ešte pred prístupom do siete.
DHCP snooping	Zabraňuje použitiu falošného DHCP servera.
ACL	Riadenie prevádzky za účelom splnenia bezpečnostnej politiky.

3.2.1 STP

STP (Spanning Tree Protocol) sa využíva za účelom odstránenia slučiek v sieti, STP na fyzickej topológii, (ktorá môže obsahovať slučky) vytvorí virtuálnu topológiu , ktorá už slučky neobsahuje.

Protokol STP vyžíva zasielanie špeciálnych správ medzi prepínačmi, tieto správy sa označujú ako BPDU (Bridge Protocol Data Unit) a sú primané aj blokovanými portami prepínačov.

Používajú sa dva typy BPDU správ[10]:

- **CBPDU (Configuration)** – posiela sa pravidelne a obsahuje konfiguráciu siete.
- **TCN BPDU (Topology Change Notification)** – posiela sa v prípade zmeny topológie siete.

Základné funkcie protokolu STP sú voľba koreňového prepínača označovaného ako koreňový prepínač (Root switch) a výpočet trasy cez všetky prepínače v topológii, ktoré tvoria kostru grafu. Na voľbe koreňového prepínača sa zúčastňujú všetky pripojené prepínače, pričom prepínač ktorý má najnižšie identifikačné číslo ID sa stáva koreňovým prepínačom. Identifikačné číslo je možné manuálne nakonfigurovať, preto pri rovnosti identifikačného čísla sa volí poľa najnižšej MAC adresy. Keď po voľbe koreňového prepínača nastane zmena v topológii siete dôjde k prepočtu ciest pomocou STP. Rovnako dochádza k prepočítavaniu ciest v prípade odpojenia koreňového prepínača alebo po pripojení prepínača s nižším ID.

Zmeny topológie siete musia byť oznámené všetkým zariadeniam v sieti, čo znamená, že prepínač notifikuje zmeny topológie koreňovému prepínaču, a ten oznamuje zmeny topológie do celej siete.

Treba si uvedomiť, že protokol STP je „dôverčivý“ protokol a neposkytuje žiadny autentizačný mechanizmus, preto je možné vykonávať rôzne typy útokov na tento protokol.

Ovládnutie koreňového prepínača

Útočník sa stane koreňovým prepínačom, poslaním nižšieho identifikačného čísla ID, ako samotný koreňový prepínač. To vykoná odchytením BPDU správy. Po prepočítaní ciest a zvolení za koreňový prepínač, prestane reagovať na *TCN – BPDU* správy a následne nastane nestabilita siete.

DoS s použitím Configuration – BPDU

Útočník permanentne posiela *CBPDU* správy (niekoľko tisíc správ za sekundu), čoho výsledkom je vytvorenie dojmu, že do siete sa pripojilo niekoľko tisíc zariadení a vyvolá tak permanentné prepočítavanie STP. V dôsledku tejto skutočnosti dochádza k nestabilite siete. Obdobou tohto útoku je posielanie *TCN – BPDU* paketov.

Protiopatrenia voči STP útokom:

Uvedené útoky sa eliminujú zapnutím funkcionality BPDU – Guard, ktorá zabezpečí by sa BPDU rámec nedostal na prístupový port prepínača. Teda port na ktorom sú pripojené koncové zariadenia ako je napr. počítač alebo server.

Zároveň je potrebné všetky prístupové porty nastaviť do módu portfast. Pri tomto nastavení sa port automaticky prepne zo stavu blocking do stavu forwarding.

V prípade, že sa na prístupovom porte objaví BPDU rámec, port sa prepne do stavu *error-disable* (vypnutie portu). Ďalšou možnosťou je zapnutie funkcionality BPDU – Filtering, ktorá potichu zahadzuje BPDU rámce (v oboch smeroch). Toto je mimoriadne účinné práve pri brute –force (útok hrubou silou) útokoch typu DoS.

Ďalším protiopatrením je nakonfigurovanie RootGuard, čo zabezpečí, že ak príde na port prepínača BPDU rámec s vhodnejšími parametrami ako koreňový prepínač, port sa prepne do stavu, kedy neposiela dáta ale len prijíma BPDU rámce.

3.2.2 DHCP

DHCP (Dynamic Host Configuration Protocol) sa používa pre automatickú konfiguráciu zariadení pripájaných do počítačovej siete. DHCP protokol umožňuje prostredníctvom DHCP servera nastavovať zariadeniam v počítačovej sieti sadu parametrov, nutných pre komunikáciu pomocou IP protokolu (IP adresa, maska siete, default-gateway, DNS server,)

Komunikáciu inicializuje klient a to poslaním paketu DHCPDISCOVER, ktorý je poslaný broadcastom. Server odpovie paketom DHCPOFFER s ponukou IP adresy DHCP servera, následne klient požiada konkrétny DHCP server paketom DHCPREQUEST o nastavenia na čo mu ich DHCP server v odpovedi DHCPACK vráti[15].

DoS útok voči DHCP serveru

Princíp útoku spočíva v tom, že útočník generuje veľké množstvo paketov s náhodnou MAC adresou a unikátnou DHCPDISCOVER požiadavkou pre každú MAC adresu. Toto zapríčiní, že DHCP server minie všetky IP adresy z adresného priestoru určeného pre danú VLAN sieť, a ďalším klientom nie je poskytnutá z DHCP servera IP adresa.

Presmerovanie komunikácie za použitia cudzieho DHCP Servera

Ďalším útokom na DHCP protokol je použitie cudzieho DHCP servera v LAN sieti a následný útok MITM (Man In The Middle). Keďže DHCP server môže vrátiť parametre default-gateway, DNS, za ním ovládané zariadenia.

Protiopatrenia voči DHCP útokom

Útoky na DHCP protokol, resp. server vieme eliminovať použitím funkcionality Port Security, ktorá umožňuje nastaviť počet MAC adries priradených k určitému portu prepínača. Toto však nie je možné vo väčších sieťach kde je veľký počet klientov, alebo v prípadoch

kde klienti často migrujú. Preto ideálnym riešením voči DHCP útokom je DHCP Snooping, čo je monitorovanie a povoľovanie DHCP požiadaviek na určitej VLAN sieti. Základom je definovanie dôveryhodných a nedôveryhodných portov, pričom nedôveryhodné porty nesmú posielať DHCP odpovede. DHCP Snooping uchováva tabuľku vzájomných vzťahov medzi MAC adresami a IP adresami. Táto tabuľka má názov DHCP Snooping Binding Database. V prípade, že príde komunikácia na nedôveryhodné rozhranie, dochádza ku jej kontrole vo vzťahu k databáze a v prípade nezhody sa paket zahadzuje.

3.2.3 802.1Q

Protokol IEEE 802.1Q je verejnou špecifikáciou, ktorá popisuje formát paketov prechádzajúcich trunkovými linkami. Nakoľko sa jedná o otvorený štandard bol prijatý väčšinou výrobcov a používa sa pre trunk porty. Nie je však jediný, spoločnosť Cisco vyvinula svoj vlastný proprietárny protokol ISL (Inter-Switch Link).

Keď prepínač príjme rámec, pridá značku (tag) pomocou protokolu 802.1Q o veľkosti štyroch bajtov, následne prepočíta hodnotu FCS (Frame Check Sequence) a upravený paket odošle na trunk linku. V poliach pridaných protokolom 802.1Q sa nachádza aj hodnota VID (VLAN identifier), ktorá môže nadobúdať hodnôt od 1 – 4096 [10].

VLAN Hopping

Pri tomto útoku sa útočník snaží dostať do časti siete, ktorá na sa nachádza vo VLAN sieti, kde útočník nemá prístup. Môže sa jednať o metódu Switch spoofing, alebo Double Tagging.

Switch Spooofing – spočíva v tom, že sa útočníkova stanica vydáva za prepínač a získava dáta z trunk portu prepínača, kde je prenášané množstvo VLAN sietí. Jedná sa o zneužitie protokolu DTP (Dynamic Trunking Protocol), kedy stanica vyjedná na svojom porte trunk.

Double Tagging – útočník odosiela rámec s dvoma pridanými 802.1Q tagmi. Prvý prepínač na ktorý je pripojený útočník príjme rámec, odstráni prvý tag a prepošle rámec druhému prepínaču kde je pripojená obeť. Druhý prepínač prevezme rámec, ktorý obsahuje druhý 802.1Q tag čo spôsobí, že útočník sa dostane do inej VLAN na ktorú mal oprávnenia. Tento útok funguje len za predpokladu, že útočník patrí do VLAN ktorá je nakonfigurovaná ako natívna.

Protiopatrenia voči VLAN hopping útoku

Switch Spoofing: všetky porty je potrebné nastavovať manuálne (*switch port mode access, switch port mode trunk*), nepoužívať DTP.

DoubleTagging: Ubezpečiť sa, že natívna VLAN nie je priradená na žiadny prístupový port.

3.2.4 MAC

MAC Address Flooding

Útočník sa snaží vyčerpať pamäť prepínača, určenú pre ukladanie MAC adries (CAM table). Útok spočíva v posielaní veľkého množstva rámcov s rôznymi falošnými zdrojovými MAC adresami, čo spôsobí zaplnenie CAM tabuľky. Vo chvíli, keď je CAM tabuľka plná, tak sa nevytvárajú nové záznamy a komunikácia, ktorá je určená len pre cieľovú MAC adresu je zasielaná na všetky porty prepínača (s výnimkou zdrojového portu). Znamená to, že prepínač sa začne chovať ako obyčajný rozbočovač (hub) a útočník sa môže dostať ku každému rámcu v danej VLAN sieti [2].

MAC Spoofing Attack

Útočník odosiela podvrhnutú MAC adresu (MAC adresa obete) prepínaču, ktorý si upraví CAM tabuľku, následne rámce určené pre obeť sú posielané útočníkovi. Toto platí dovtedy pokiaľ obeť opätovne odošle rámec a CAM tabuľka sa upraví.

Protiopatrenia voči MAC útokom

Na prevenciu tohto útoku sa používa DHCP Snooping, prípadne Port Security. Ideálnym riešením je aj monitoring aktivity MAC adries s následnou notifikáciou (SNMP trap).

3.2.5 ARP

ARP (Address Resolution Protocol) protokol bol vytvorený za účelom získavania fyzickej adresy (MAC) z logickej adresy (IP). Keďže ARP protokol nedisponuje žiadnym bezpečnostným prvkom, ako je autentizácia, útočník môže posielať ARP pakety s podvrhnutým obsahom.

ARP Spoofing

Útok typu ARP spoofing taktiež známy ako ARP poisoning, spočíva v zneužití slabín tohto protokolu. Útočník prinúti obeť myslieť si, že komunikuje so smerovačom, resp. s bránou, no v skutočnosti bude komunikovať s útočníkom. Útočník posiela ARP reply správy obeti, ktorá má následne upravenú svoju ARP tabuľku. Jedná sa teda o typ útoku MITM (Man In The Middle).

Protiopatrenia na ARP útoky

Najúčinnejším protiopatrením je funkcionalita DAI (Dynamic ARP Inspection), ktorá zabraňuje preposielanie neplatných ARP dotazov a odpovedí na iné porty prepínača v rovnakej VLAN sieti.

Pre tento prípad sa používa funkcionalita DHCP Snooping, ktorá vytvára databázu DHCP Snooping Binding Database. Táto databáza udržuje vzájomný vzťah medzi IP a MAC adresami.

Jednou z hlavných funkcií DAI je kontrolovať celú ARP prevádzku prichádzajúcu na port prepínača a zahadzovať rámce, ktoré neodpovedajú tejto databáze. Ďalšou z funkcionalít DAI je *rate-limiting* – obmedzovanie množstva ARP rámcov, z dôvodu zabránenia DoS útokom. Štandardne je táto hodnota nastavená na hodnotu 15, teda pokiaľ príde na port viac ako 15 ARP rámcov za sekundu port sa vypne resp. prepne do stavu *err-disabled*.

3.2.6 CDP

CDP (Cisco Discovery Protocol) je proprietárny protokol vyvinutý spoločnosťou Cisco, a používa sa k zdieľaniu určitých informácií o inom priamo pripojenom zariadení napr. verzia IOS, hostname, VTP doména, IP adresa, hardwarová platforma a iné.

Údaje, ktoré by mohol útočník získať, môžu byť použité pri príprave na ďalšie útoky. Ďalšou možnosťou je, že sa útočník bude tváriť ako sieťové zariadenie a bude posielať CDP rámce. Takto môže zmiasť administrátorov sieťovej infraštruktúry.

V prípade posielania veľkého množstva CDP rámcov, môže to spôsobiť vyčerpanie systémových zdrojov priľahlého sieťového zariadenia (v prípade útoku na staršie zariaenie). CDP protokol neposkytuje žiadny spôsob autentifikácie a informácie, ktoré sú posielané sú voľne čitateľné.

Protiopatrenia voči zneužitiu CDP informácii.

Je potrebné zabezpečiť aby CDP nebol šírený do prístupových portov a na všetky nedôveryhodné porty. CDP protokol by mal byť použitý len na portoch ktorými sú prepojené samotné sieťové zariadenia.

3.2.7 VTP

VTP (VLAN Trunking Protocol) protokol je určený k správe a konfigurácii VLAN prostredníctvom pridávania, mazania alebo premenovania VLAN naprieč celou sieťovou infraštruktúrou.

Útoky na VTP protokol spočívajú v snahe neautorizovane pozmeniť databázu VLAN, čím je možné znefunkčniť celú sieťovú infraštruktúru.

Protiopatrenia voči VTP útokom

Najúčinnejšie protiopatrenie je VTP protokol vôbec nepoužívať, avšak v prípadoch, kedy je to nevyhnutné, treba zabezpečiť VTP doménu netriviálnym heslom.

II. PRAKTICKÁ ČASŤ

4 NÁVRH ZABEZPEČENIA PRÍSTUPOVEJ VRSTVY SIETE ZALOŽENEJ ŠTANDARDE 802.1X

Pre zabezpečenie prístupovej vrstvy podnikovej siete bude použitý štandard 802.1X, teda budeme autentizovať užívateľov na portoch prepínača. Pre realizáciu tohto konceptu sú potrebné viaceré zariadenia, ktoré pri spojení do jedného celku ponúkajú možnosť lepšie zabezpečiť sieťovú infraštruktúru ako aj podnikové zdroje, ktoré často obsahujú cenné informácie.

Pri zabezpečení sieti pomocou štandardu 802.1X je možné zvýšiť bezpečnosť ako aj zjednodušiť manažment prístupových práva s nimi súvisiaci životný cyklus užívateľských oprávnení. V neposlednom rade táto technológia umožňuje aj komfort konečným užívateľom, keďže umožňuje ich mobilitu a to bez zníženia úrovne zabezpečenia siete. Pri návrhu som vychádzal z konceptu spoločnosti Cisco označovaný pod názvom IBNS (Identity Based Networking Services) [11], [12], [13]. IBNS ponúka tri režimy použitia štandardu 802.1X monitorovací, low-impact (označovaný aj ako selektívny) a zabezpečený mód. Jednotlivé módy nasadenia sú popísané v kapitole 5.1, až 5.3.

Ako centrálny zdroj identít bude použitý Active Directory od spoločnosti Microsoft inštalovaný na operačnom systéme Windows 2008 R2 na ktorom budú spustené aj doplnkové služby ako DNS, DHCP a certifikačná autorita. Pre riadenie prístupu užívateľov do siete budeme používať produkt od spoločnosti Cisco ACS (Secure Access Control System) verzie 5.2, ktorý podporuje oba protokoly RADIUS pre riadenie sieťového prístupu ako aj TACACS+ pre riadenie prístupu k sieťovým zariadeniam.

4.1 Špecifikácia siete

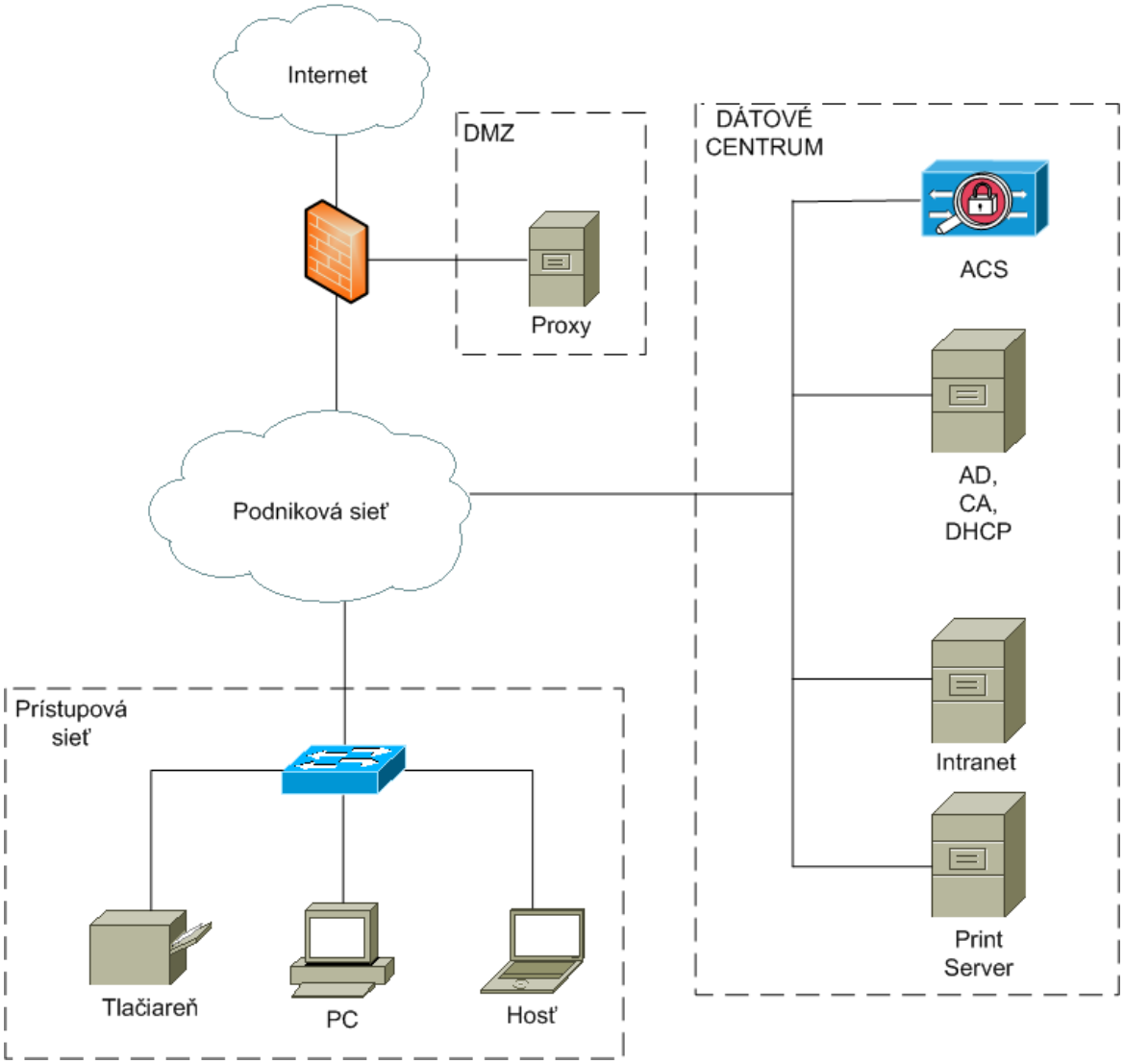
Fiktívna podniková sieť pozostáva prístupového prepínača rady Cisco 3750 IOS 12.2.(55), ktorý je pripojený do distribučnej vrstvy podnikovej siete a tá následne prepojená do chrbticovej vrstvy, keďže v podnikových sieťach sa využíva táto trojvrstvový sieťová hierarchia.

Prístupová vrstva predstavuje prepínač na ktorý sú pripojené jednotlivé zariadenia akými sú počítače a tlačiarne, ktoré môžu byť rozdelené do rôznych segmentov siete. Niekedy je táto časť nazývaná ako užívateľská sieť.

V distribučnej časti siete sa nachádzajú agregačné prepínače, ktoré oddeľujú užívateľskú časť siete od najvýkonnejšej chrbticovej siete.

Všetky servery poskytujúce služby užívateľom sa nachádzajú v dátovom centre, čím sa myslí bezpečnostná zóna, ktorá je od užívateľskej časti siete oddelená firewallom. Prístup k internetu je zabezpečený proxy serverom, ktorý sa nachádza v demilitarizovanej zóne DMZ, ktorá je taktiež oddelená externým firewallom.

Tieto zariadenia predstavujú nástroj, ktorým sú vynucované prístupové politiky (v prípade prideľovania užívateľov do VLAN), pri použití dACL, sú tieto oprávnenia vykonávané priamo na prístupovom prepínači. Na obr. č.11 je zobrazená schéma podnikovej siete.



Obr. 11. Logická schéma podnikovej siete.

Keďže v tejto práci sa zaoberám problematikou zabezpečenia prístupovej vrstvy siete, nebudem popisovať akým spôsobom sú zabezpečené ostatné dve vrstvy tejto podnikovej siete, dátového centra a DMZ.

V reálnom prostredí je prístupová vrstva siete tvorená viacerými prepínačmi. V navrhovanom riešení je použitý len jeden, avšak princíp aplikovania bezpečnostnej politiky je identický. Preto je uvedená konfigurácia jedného prístupového prepínača a ostatných komponentov súvisiacich so zabezpečením prístupovej vrstvy siete ako sú ACS a Active Directory.

4.2 Prístupová politika

Cieľom navrhovaného riešenia je zabezpečiť prechod z neriadeného prístupu užívateľov na riadený prístup s možnosťou mobility užívateľov po podniku a poskytnúť užívateľom prístup len k zdrojom na ktoré majú oprávnenie.

Administrátori pre prístup na konzolu a terminál prepínačov sa musia autentizovať voči Active Directory serveru. Ako autentizačný protokol je použitý TACACS+ z dôvodu väčšej flexibility a bezpečnosti.

Užívatelia sú rozdelený do viacerých skupín a to administrátori, manažéri, účtovníci a v neposlednej rade hostia alebo dodávatelia. Manažéri a majú povolený prístup na serverA, serverB a proxy server. Účtovníci môžu pristupovať na serverB a proxy server. Dodávatelia a hostia, majú povolený prístup len na internet prostredníctvom proxy servera. Tlačiarne, ktoré nepodporujú 802.1X autentizáciu sú zadefinované v samostatnej organizačnej jednotke (ou v rámci Active Directory) PRINTERS. Tieto zariadenia majú povolený prístup na print serverC. Adresný plán uvedených serverov je zobrazený v tab. č.10.

Tab. 8. Servery poskytujúce služby pre koncových užívateľov.

Hostname	IP Adresa	Popis
Podniková doména:	btsm.local	
ad.btsm.local	10.10.10.11	Win 2k8, AD, DHCP,DNS,CA
acs.btsm.local	10.10.10.12	ACS server
serverA.btsm.local	10.10.20.11	Intranet portal(TCP/443)
serverB.btsm.local	10.10.30.11	Účtovnícky server (TCP/443)
serverC.btsm.local	10.10.40.11	Print server (TCP/515)
proxy.btsm.local	192.168.0.11	Proxy server pre prístup na internet(TCP3128)

Ako autentizačný mechanizmus bola zvolená metóda EAP-PEAP(MS-CHAPv2), ktorá je považovaná za bezpečnú a nie je potrebné mať administratívne komplikovanú infraštruktúru PKI ako v prípade metódy EAP-TLS, kde je na autentizáciu požitý užívateľský certifikát.

Každý užívateľ je priradený do jemu prislúchajúcej skupiny v Active Directory, ktorá určuje oprávnenia prístupu podľa uvedenej tab. č.8. popisujúcu prístupovú politiku.

Tab. 9. Návrh prístupovej politiky.

Meno	**MS Skupina**	**Povolený prístup**
net-admin1	NETADMIN	povolené všetko
uzivatel1	MANAGERS	server A, Server B, proxy
uzivatel2	ACCOUNTING	server A, proxy
$MAC-ADDR Tlačiarne	PRINTERS	server C
$hosť, dodávateľ	-	proxy

Keďže v navrhovanom riešení boli použité rôzne režimy nasadenia, bolo potrebné definovať aj VLAN siete s adresným priestorom. prislúchajúcim navrhnutým VLAN sieťam. V prípade použitia monitorovacieho a selektívneho módu sú užívatelia pripojený do rovnakej dátovej VLAN siete s názvom DATA. V prípade použitia zabezpečeného módu sa užívatelia priraďujú do rôznych VLAN sietí, podľa výsledku autorizácie. Popis adresného priestoru a návrh VLAN sietí je uvedený v tab. č.10.

Tab. 10. Adresný priestor a konfigurácia VLAN sietí.

Názov VLAN	**VLAN ID**	**Adresný priestor**
Monitorovací a Selektívny mód		
DATA	10	10.0.1.0/24
Zabezpečený mód		
MANAGERS	20	10.0.2.0/24
ACCOUNTING	30	10.0.3.0/24
PRINTERS	40	10.0.4.0/24
NETADMIN	50	10.0.5.0/24
GUEST	100	10.0.10.0/24

5 POSTUP IMPLEMENTÁCIE NAVRHOVANÉHO RIEŠENIA

Implementácia navrhovaného riešenia sa skladá z troch krokov, ktoré ponúkajú postupný prechod zvyšovania úrovne bezpečnosti, bez vážnejších dopadov na chod prevádzky. Monitorovací mód ako aj selektívny mód je špecifický tým, že užívatelia a zariadenia sa nachádzajú rovnakej dátovej VLAN, avšak pri zabezpečenom móde sú užívatelia priraďovaný do samostatných VLAN.

5.1 Monitorovací mód

Monitorovací mód ponúka možnosť implementácie 802.1X bez negatívneho dopadu na užívateľov a koncové zariadenia ako sú tlačiarne, prípadne iné „NONPC“ zariadenia. Táto metóda ponúka otvorený prístup, ktorý umožňuje klientom autentifikáciu prostredníctvom 802.1X alebo MAB. V prípade neúspešnej autentizácie port prepínača poskytuje stále normálny prístup bez obmedzení. Nasadením toho módu administrátor môže podľa auditných log záznamov z AAA servera preveriť, či sú správne nakonfigurovaný jednotlivý suplikanti, prípadne vytvoriť databázu zariadení, ktoré nepodporujú autentizáciu a priradiť ich do skupiny pre určených pre MAB autentizáciu.

Ďalšou výhodou tohto módu je možnosť preveriť aké zariadenia sa vyskytujú na sieti, nakoľko pri väčších sieťach nie je možné monitorovať každé zariadenie a nasadenie tejto technológie to umožňuje. Základom tohto režimu nasadenia je fakt, že autentizácia je zapnutá pričom autorizácia je vypnutá.

- **Autentizácia zapnutá**
- **Autorizácia vypnutá**

5.2 Selektívny mód

Po odladení všetkých problémov (najčastejšie nastavenie suplikanta na koncových staniciach a zadefinovaní zariadení, ktoré nepodporujú 802.1X autentifikáciu) je možné prejsť na selektívny mód, ktorý umožňuje postupné zvýšenie úrovne bezpečnosti, použitím dACL, ktoré sú spravované na ACS servery.

Toto umožňuje centralizovanú správu ACL a nie je potreba definovať prístupové zoznamy na každom prepínači v sieti, čo samozrejme uľahčuje správu pre administrátorov siete.

Porty prepínača na ktoré sú pripojený dodávatelia a hostia a neautentizovali sa žiadnou podporovanou metódou (802.1X alebo MAB) je aplikovaný ACL, ktorý povoľuje len obmedzený prístup (proxy server).Takto definovaný prístupový zoznam musí obsahovať aj povolenia použitia protokolov DNS a DHCP. ACL je aplikovaný na všetkých portoch prepínača s nastavením selektívneho módu.

- **Autentizácia zapnutá**
- **Autorizácia zapnutá dACL + ACL pre limitovaný prístup.**

5.3 Zabezpečený mód

Tento mód poskytuje najväčšiu mieru zabezpečenia a to takým spôsobom, že na základe autentizácie sa zariadenia priraďujú do rôznych VLAN sietí, ktoré sú výsledkom autorizačného procesu. Zariadeniam ktoré sa nevedia autentizovať žiadnou autentizačnou metódou (802.1X alebo MAB) je povolený prístup do samostatnej VLAN s názvom GUEST.

- **Autentizácia zapnutá**
- **Autorizácia zapnutá s priraďovaním VLAN**

5.4 Postup implementácie 802.1X

Prvým krokom implementácie je nasadenie monitorovacieho módu, ktorý slúži na zmonitorovanie podnikového prostredia bez negatívneho dopadu na koncových užívateľov. Táto časť je určená hlavne na preverenie funkčnosti autentizačných metód 802.1X a MAB. Zároveň ponúka priestor na otestovanie rôznych EAP autentizačných mechanizmov, čo umožňuje vybrať najvhodnejšiu variantu.

Najčastejšie problémy sú spojené práve s nastavením suplikantov a to hlavne v prípade, kedy je heterogénne prostredie z pohľadu použitia operačných systémov.

Popri preverovaní funkčnosti suplikantov, je potrebné vytvoriť zoznam zariadení, nepodporujúcich autentizáciu 802.1X. Tieto zariadenia následne zaznamenať do centrálneho zdroju identít, ktorým je napr. Active Directory. Zariadenia budú využívať sekundárnu autentizačnú metódu ktorou je MAB. Znamená to, že klient sa autentizuje MAC adresou zariadenia. Túto možnosť treba využívať v čo najmenšej miere, nakoľko pre útočníka je

jednoduché podvrhnúť MAC adresu zariadenia. Toto je asi najväčšia slabina tejto technológie.

Po odladení a preverení funkčnosti v monitorovacom móde nasleduje ďalší krok, kedy sa už reálne zvýši úroveň zabezpečenia podnikovej siete. Touto fázou je selektívny mód. Zariadenia a užívatelia pripojený na prístupový port prepínača budeme nielen autentizovať, ale začneme ich aj autorizovať. Na základe identity užívateľa sa prideľujú prístupové zoznamy, ktoré sú aplikované na porte prepínača.

Tieto ACL sú nakonfigurované na ACS serveri podľa definovanej prístupovej politiky a prepínač si ich stiahne a aplikuje na konkrétneho používateľa resp. port prepínača.

Treba si uvedomiť, že každý prepínač má obmedzenú možnosť použitia ACL (podľa hardvérovej platformy sa počet ACL líši), preto je potrebné pri definovaní samotných ACL na túto skutočnosť myslieť a optimalizovať veľkosť ACL.

Keďže je potrebné umožniť aj prístup pre dodávateľov a hostí, pre tento účel sa používa samostatný ACL, v našom prípade s názvom GUEST-ACCESS-ACL, ktorý je aplikovaný na prístupový port prepínača.

Ďalšou možnosťou je použitie zabezpečeného módu, kedy priraďujeme užívateľov do konkrétnej VLAN siete, ktorá zodpovedá prístupovej politike. Toto je považované za najviac bezpečné riešenie, avšak pri používaní veľkého množstva VLAN sietí administratívne náročné. Predstavme si situáciu, že v podniku sa nachádza 800 užívateľov a je použitých napríklad 30 prepínačov, podľa počtu autorizačných skupín je potrebné zadefinovať množstvo VLAN sietí, ktoré musia byť nakonfigurované na každom prepínači (predpokladom je, že sa nepoužíva VTP protokol). Obecne povedané použitie zabezpečeného módu je možné len v menších prostrediach, kde nie je veľký počet prepínačov a autorizačných skupín.

V prípravnej fáze implementácie tejto technológie je dobré otestovať všetky varianty, a podľa získaných skúseností sa rozhodnúť sa pre najvhodnejšiu variantu.

6 KONFIGURÁCIA ZARIADENÍ

6.1 Inštalácia a konfigurácia Cisco ACS

Jedným zo základných stavebných prvkov každej podnikovej siete je silný prostriedok pre autentizáciu, autorizáciu a audit, ktorý umožňuje aplikovanie pravidiel definovaných v prístupovej politike. Práve na tento účel sa využíva ACS server, ktorý umožňuje granulárne definovanie prístupových politík na základe identity alebo role užívateľa.

Základná konfigurácia ako aj nastavenie primárnych služieb je uvedená v tab. č.11.Všetky nastavenia sú pôvodné, avšak bola vypnutá služba CDP pomocou príkazu ***no CDP run***. Aby správne fungovala autentizácia voči Active Directory serveru je potrebné správne nastaviť časovú zónu a synchronizáciu s NTP (Network Time Protocol) serverom, v opačnom prípade by autentizácia bola neúspešná.

Tab. 11. Základná konfigurácia ACS servera.

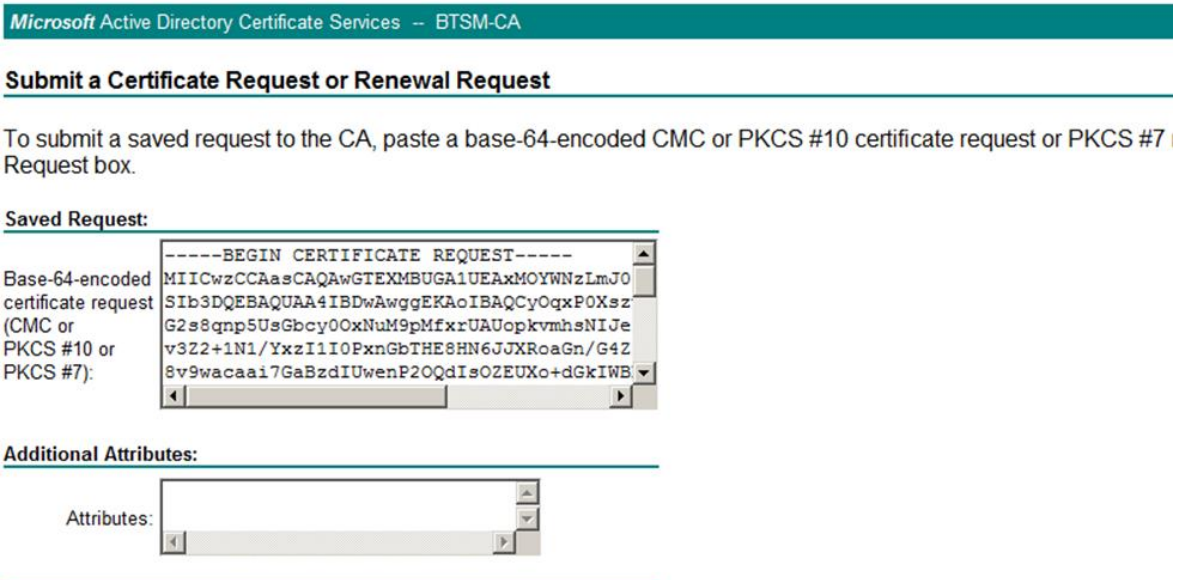
```
!
hostname acs
!
ip domain-name btsm.local
!
interface GigabitEthernet 0
  ip address 10.10.10.12 255.255.255.0
!
ip name-server 10.10.10.11
!
ip default-gateway 10.10.10.1
!
clock timezone Europe/Bratislava
!
ntp server ntp.btsm.local
!
username admin password hash $1$CHcHGEvV$v/PvwPsRoLFMNESd11 role ad-
min
!
service sshd
!
repository tftp
  url tftp://10.10.10.128
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 8
!
logging localhost
logging loglevel 6
!
icmp echo on
```

Pre tento dôvod bol použitý NTP server inštalovaný na Active Directory s DNS záznamom *ntp.btsm.local*. Toto samozrejme nie je prípustné v reálnej prevádzke. Na tento účel sa používa samostatný server, ideálne dva pre zabezpečenie vysokej dostupnosti tejto služby.

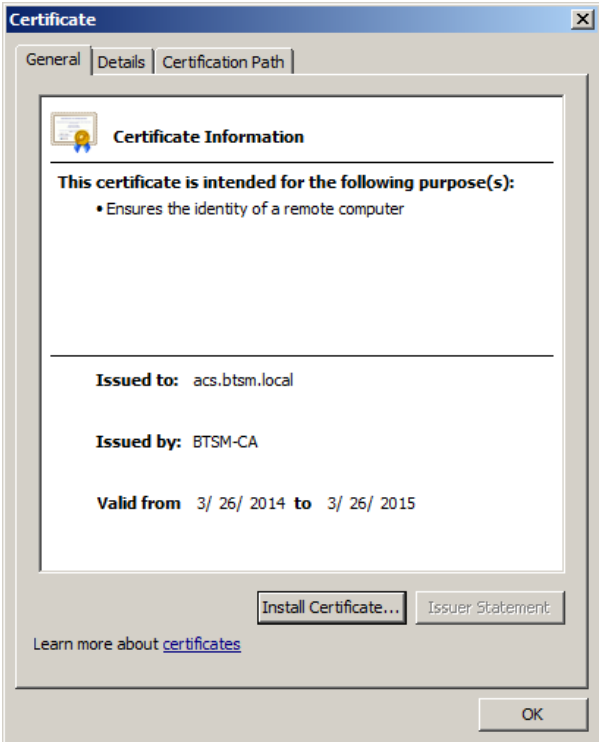
6.1.1 Konfigurácia SSL certifikátu

Keďže v podnikovom prostredí je používaná certifikačná autorita je potrebné nakonfigurovať aj SSL certifikát, ktorý bude slúžiť pre zabezpečený prístup k webovej konzole samotného ACS servera, ale aj pre tunelovanie EAP protokolu. Obr. č. 12 zobrazuje vygenerovanie CSR (certificate signing request), ktorý je následne podpísaný koreňovou certifikačnou autoritou BTSM-CA (obr. č.13). Ako Common Name (bežné meno), musí byť použité FQDN (Fully Qualified Domain Name) ACS servera v našom prípade sa jedná o *acs.btsm.local*.

Obr. 12. Vygenerovanie CSR pre ACS server.



Obr. 13. Podpísanie CSR na certifikačnej autorite BTSM-CA.



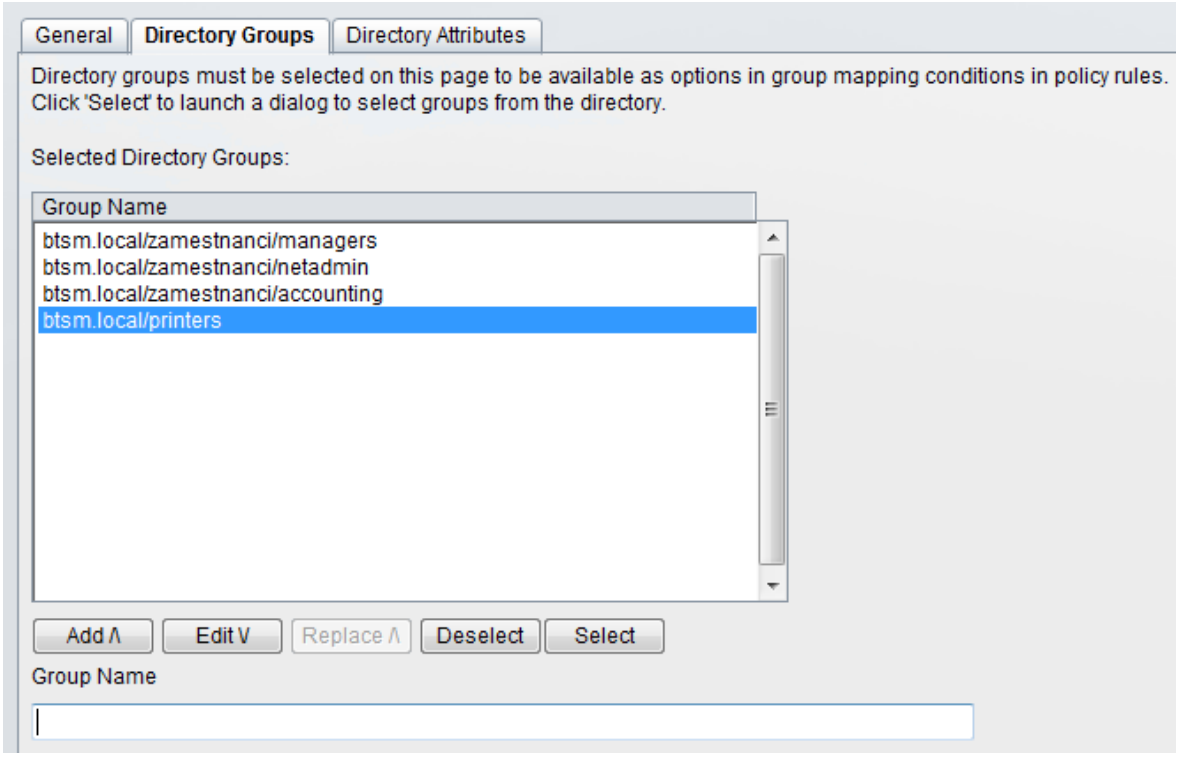
Obr. 14. Certifikát ACS servera.

6.1.2 Prepojenie ACS s Active Directory

Aby sme mohli užívateľov autentizovať voči Active Directory, je potrebné ACS server pripojiť do domény. Na základe členstva v doméne je potom možné vykonávať autentizáciu a autorizáciu užívateľov a zariadení, ktoré sú definované v adresárovej štruktúre Active directory servera. Na prepojenie sa používa administrátorské doménové konto, ktoré má oprávnenie ACS server pripojiť do domény *btsm.local.*

Obr. 15. Prepojenie ACS servera s Active Directory.

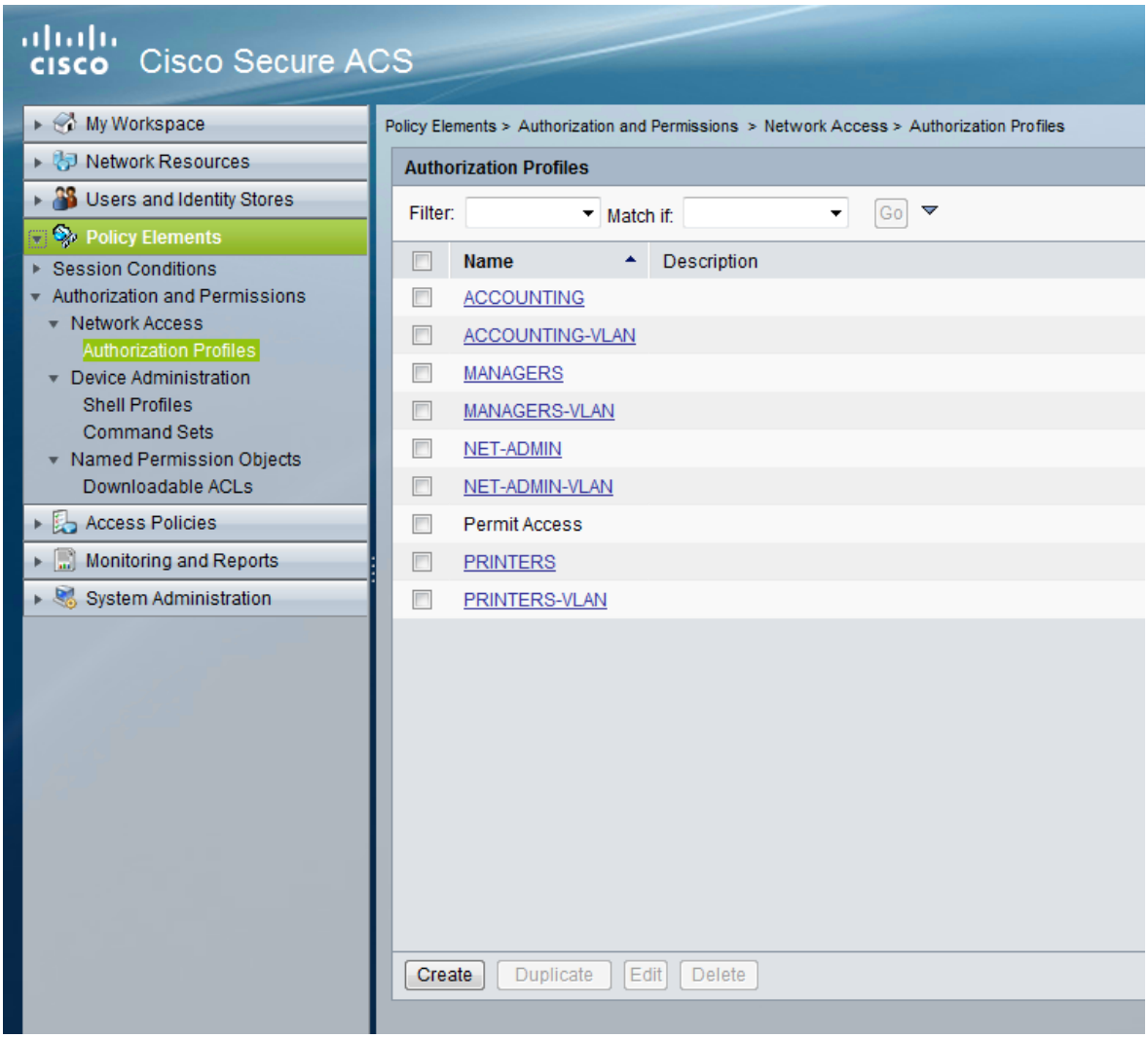
Aby bolo možné užívateľov a zariadenia autorizovať podľa príslušnosti v skupinách Active Directory je potrebné mapovať používané skupiny, ktoré sa následne budú používať pri vytváraní autorizačných politík, postup je zobrazený na obrázku č.16.



Obr. 16. Mapovanie skupín AD so serverom ACS.

6.1.3 Konfigurácia prístupových politík

Prístupové politiky musia spĺňať politiku popísanú v tab. č.8, ktorá je vytvorená variantne pre možnosť použitia priraďovania užívateľov, buď do konkrétnych VLAN alebo za použitia dACL, ktoré sú nakonfigurované na ACS servery a aplikovaný na každého používateľa resp. port prepínača. Aby bola splnená táto podmienka je potrebné najprv nakonfigurovať autorizačný profil pre každú skupinu užívateľov samostatne. Na obr. č.17 sú zobrazené vytvorené autorizačné profily.



Obr. 17. Vytvorenie autorizačných profilov.

Nastavenie ACL pre prístup v selektívnom móde

Na ACS servery je potrebné nakonfigurovať rozšírené (extended) dACL, ktoré si prepínač stiahne a aplikuje na konkrétny port. Nižšie je zobrazená tabuľka zoznamu ACL definovaná podľa prístupovej politiky, ktorá je nakonfigurovaná na ACS servery.

Tab. 12. Zoznam ACL konfigurovaných na ACS servery

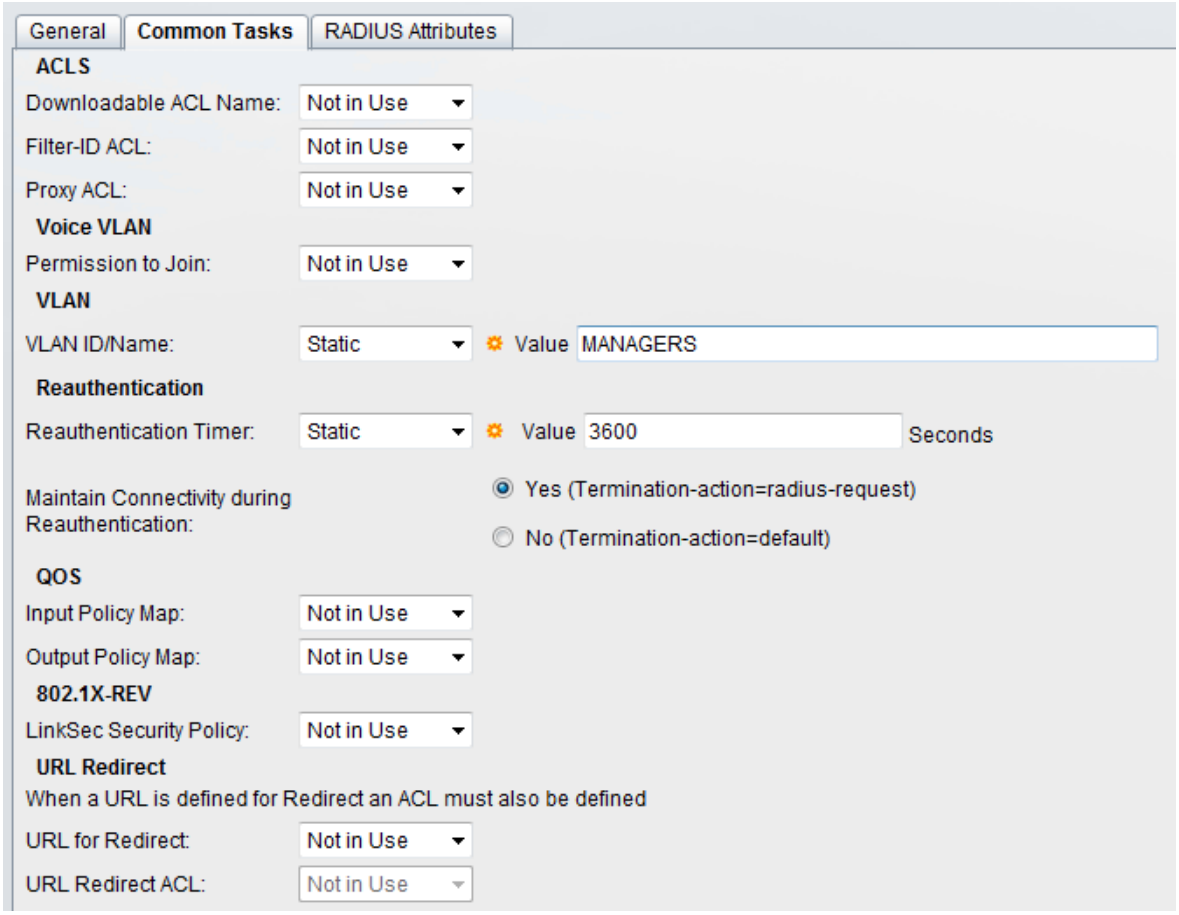
MS Skupina	ACL
MANAGERS	permit tcp any host 10.10.20.11 eq 443 permit tcp any host 10.10.30.11 eq 443 permit tcp any host 192.168.0.11 eq 3128
ACCOUNTING	permit tcp any host 10.10.20.11 eq 443 permit tcp any host 192.168.0.11 eq 3128
NETADMIN	permit ip any any
PRINTERS	permit tcp any host 10.10.40.11 eq 515
GUEST	permit udp any eq bootpc any eq bootps permit udp any any eq domain permit tcp any host 192.168.0.11 eq 3128

Nastavenie VLAN pre prístup v zabezpečenom režime

Rovnako ako v prípade selektívneho módu je potrebné nakonfigurovať VLAN siete pre jednotlivé autorizačné profily. Konfiguráciu je možné urobiť podľa ID VLAN siete, alebo pod názvom VLAN napr. *MANAGERS.* Obe možnosti fungujú korektne, avšak je dôležité aby uvedená VLAN sieť bola nakonfigurovaná aj na prepínači, v opačnom prípade by bol autorizačný proces neúspešný. Na obr. č.18 je uvedený príklad tejto konfigurácie.

Tab. 13. Zoznam VLAN konfigurovaných na ACS a prepínači.

MS Skupina	VLAN NAME	VLAN ID
MANAGERS	MANAGERS	20
ACCOUNTING	ACCOUNTING	30
NONPC	NONPC	40
NETADMIN	NETADMIN	50
-	GUEST	100



Obr. 18. Príklad konfigurácie autorizačného profilu s použitím VLAN.

Pri komunikácii prepínača s ACS serverom pomocou RADIUS protokolu, sa pri každej autentizačnej metóde posielajú v pakete *RADIUS-Access-Request* odlišné *Service-Type* atribúty. Podľa toho aká autentizačná metóda je použitá (802.1X alebo MAB) je posielaný aj tento RADUIS atribút. Aby sme mohli na ACS servery vytvárať servisné politiky musíme rozlišovať aký Service-Type atribút dorazil na ACS server.

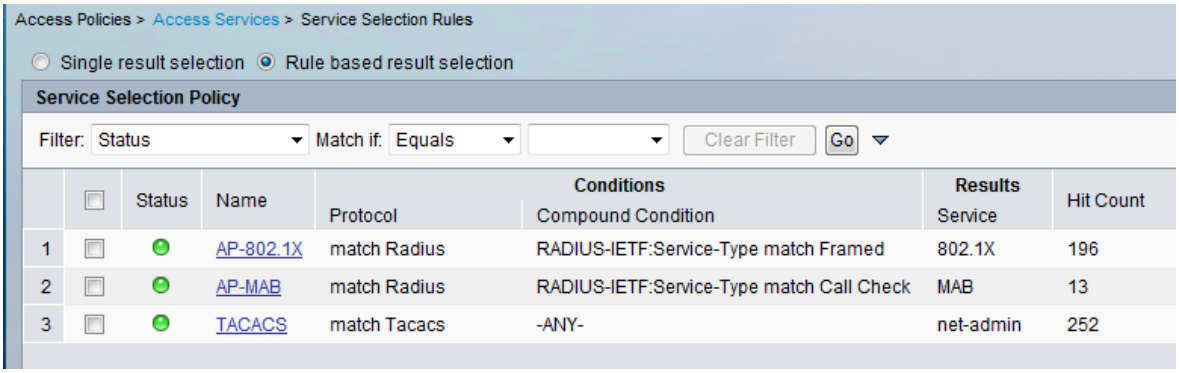
Rozdelenie Service-Type atribútov vzhľadom na typ autentizácie je nasledovný[12]:

- 802.1X posiela atribút **Framed.**
- MAB posiela atribút **Call Check.**
- WebAuth posiela atribút **Outbound.**

Ako je vidno podľa rozdelenia Service-Type atribútov, technológia IBNS umožňuje použiť, ešte jeden spôsob autentizácie, ktorou je webová autentizácia (WebAuth). Táto autentizačná metóda poskytuje možnosť overenia identity užívateľa prostredníctvom webového

portálu. Princíp je podobný ako pri hotspotoch používaných vo WIFI sieťach. Po pripojení užívateľa do siete je prevádzka presmerovaná na webový portál, kde je vyžadovaná autentizácia užívateľa. Keďže ACS server nemá implementovaný webový portál (guest portal), ktorý by tento spôsob autentizácie podporoval nebol použitý ani v navrhovanom riešení.

Pre účely manažmentu prepínača sieťovými administrátormi je používaný protokol TACACS+. V servisnej politike je preto nastavené jednoduché pravidlo, ktoré definuje, ak bude použitý protokol TACACS+ bude aplikovaný autorizačný profil s názvom *net-admin.* Obr. č. 18 popisuje servisnú politiku vo vzťahu na použitý protokol a Service-Type atribút.



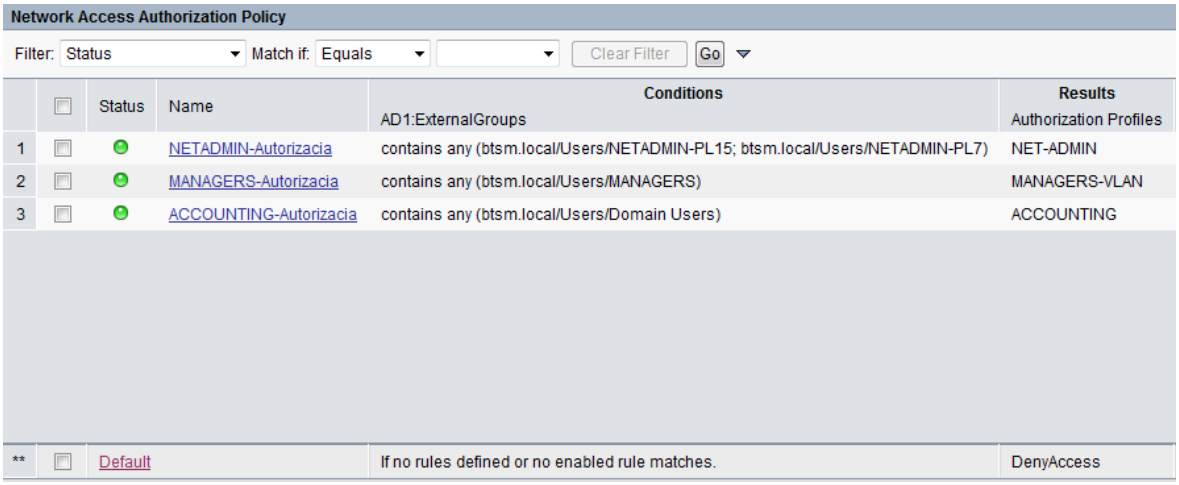
Obr. 19. Vytvorenie servisnej politiky

Nastavenie autentizácie a autorizácie

V navrhovanom riešení je použitý autentizačný mechanizmus PEAP(MS-CHAPv2), ktorý sa nastavuje samostatne v každej prístupovej politike. Okrem tejto metódy sú podporované aj nasledovné autentizačné mechanizmy:

- PAP.
- CHAP.
- MS-CHAPv1.
- MS-CHAPv2.
- EAP-MD5.
- EAP-TLS.
- LEAP.
- PEAP.
  - MS-CHAPv2.
  - GTC.
- EAP-FAST.

Autorizácia sa nastavuje samostatne pre každú užívateľskú skupinu, pričom dôležitým bodom je nastavenie zablokovania prístupu v prípade nesplnenia, žiadaných kritérií. Táto voľba je štandardne nastavená na hodnotu *Permit Access*. Čo znamená, že bude povolený prístup aj v prípade, kedy sa užívatelia neautentizujú (vypnutie autorizácie). Na obr. č. 20 je uvedený príklad konfigurácie autorizačnej politiky.



Obr. 20. Konfigurácia autorizačnej politiky.

6.1.4 Audit a monitoring

Audit je veľmi dôležitou súčasťou v každej organizácii, na základe auditných logov je možné dohľadať kto, kde a kedy bol pripojený a aké služby mu boli poskytnuté. Log záznamy sú niekedy jediným dôkazom úspešného útoku. Veľa organizácií uchováva auditné log záznamy na centralizovanom logovacom servery.

ACS server v tomto prípade zastáva aj funkciu log servera, kde sú ukladané všetky poskytnuté prístupy, teda nielen sieťové prístupy použité za pomoci RADIUS protokolu, ale aj TACACS+ servera. V auditných logoch je možné spätne dohľadať informácie prípadne dôkaz o tom, ktorý administrátor vykonal určitý príkaz na sieťovom zariadení.

ACS server umožňuje preposielanie auditných logov na ďalšie zariadenia, ktoré potom môžu automaticky vyhodnocovať, či sa vyskytol bezpečnostný incident a notifikovať určitú skupinu ľudí, ktorí potom vyhodnocujú, či sa jednalo o reálny bezpečnostný incident alebo planý poplach. Zariadenia, ktoré automaticky vyhodnocujú resp. korelujú auditné log záznamy sa nazývajú SIEM (Security Information and Event Monitoring).

Tieto zariadenia sa využívajú z dôvodu, aby administrátori nemuseli sledovať každý log záznam a vyhodnocovať ho. Vyhodnocovanie log záznamov ľudskou bytosťou v reálnom čase nie samozrejme možné.

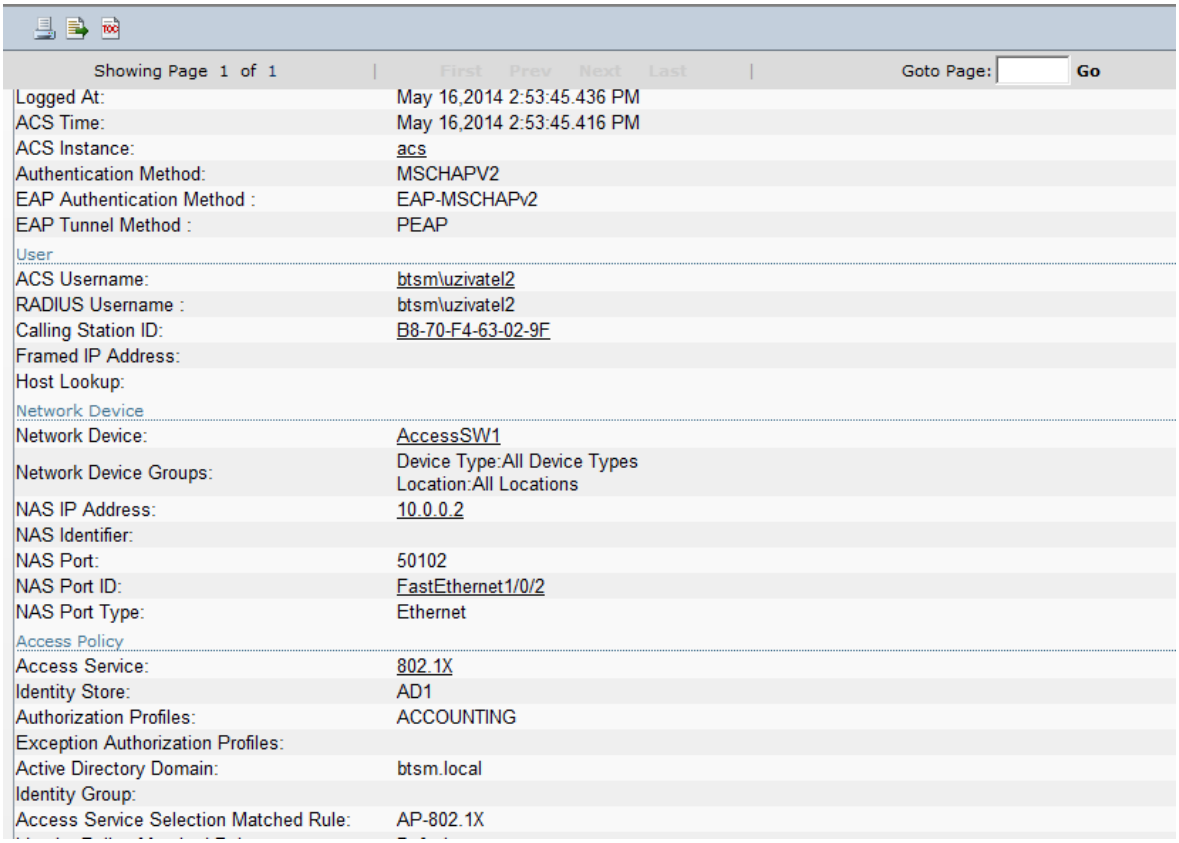
Autentizačné logy sú dôležité hlavne v prvej fáze implementácie, kedy administrátor monitoruje celé prostredie s použitým nastavením 802.1X. Z týchto logov je potom jednoduché určiť správanie jednotlivých autentizačných metód, nastavenia suplikantov a v neposlednej rade aj zmonitorovať celé prostredie prístupovej vrstvy.

Podľa výstupu z autentizačných log záznamov sa dajú jednoducho zistiť zlyhania použitých autentizačných metód . Ako príklad je možné uviesť situáciu, kedy je suplikant správne nakonfigurovaný, avšak nemá importovanú koreňovú certifikačnú autoritu, ktorá podpísala certifikát pre ACS server. Príklad autentizačných logov je zobrazený na obr. 21. a 22.

✔=Pass ✖=Fail =Click for details =Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
May 16,14 3:06:57.496 PM	✔			00-00-00-00-00-11	00-00-00-00-00-11	MAB	Lookup
May 16,14 3:03:19.506 PM	✖			B8-70-F4-63-02-9F	B8-70-F4-63-02-9F	MAB	Lookup
May 16,14 3:00:45.966 PM	✖			B8-70-F4-63-02-9F	B8-70-F4-63-02-9F	MAB	Lookup
May 16,14 2:55:08.336 PM	✖			btsm\uzivatel1	B8-70-F4-63-02-9F	802.1X	PEAP (EAP-MSCHAPv2)
May 16,14 2:53:45.496 PM	✔			#ACSACL#-IP-ACCOUNTING-dACL-5375d2c6			
May 16,14 2:53:45.436 PM	✔			btsm\uzivatel2	B8-70-F4-63-02-9F	802.1X	PEAP (EAP-MSCHAPv2)
May 16,14 2:53:11.186 PM	✔			btsm\uzivatel1	B8-70-F4-63-02-9F	802.1X	PEAP (EAP-MSCHAPv2)
May 16,14 2:50:38.646 PM	✔			btsm\uzivatel1	B8-70-F4-63-02-9F	802.1X	PEAP (EAP-MSCHAPv2)
May 16,14 2:48:55.056 PM	✖			B8-70-F4-63-02-9F	B8-70-F4-63-02-9F	MAB	Lookup
May 16,14 2:43:25.183 PM	✔			btsm\uzivatel1	B8-70-F4-63-02-9F	802.1X	PEAP (EAP-MSCHAPv2)
May 16,14 2:40:47.113 PM	✖			B8-70-F4-63-02-9F	B8-70-F4-63-02-9F	MAB	Lookup
May 16,14 10:52:16.270 AM	✔			#ACSACL#-IP-ACCOUNTING-dACL-536cfbb3			
May 16,14 10:52:16.250 AM	✔			btsm\uzivatel2	B8-70-F4-63-02-9F	802.1X	PEAP (EAP-MSCHAPv2)

Obr. 21. Autentizačné logy z ACS servera pre RADIUS protokol.



Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

Logged At:	May 16,2014 2:53:45.436 PM
ACS Time:	May 16,2014 2:53:45.416 PM
ACS Instance:	acs
Authentication Method:	MSCHAPV2
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
User	
ACS Username:	btsm\uzivatel2
RADIUS Username :	btsm\uzivatel2
Calling Station ID:	B8-70-F4-63-02-9F
Framed IP Address:	
Host Lookup:	
Network Device	
Network Device:	AccessSW1
Network Device Groups:	Device Type:All Device Types Location:All Locations
NAS IP Address:	10.0.0.2
NAS Identifier:	
NAS Port:	50102
NAS Port ID:	FastEthernet1/0/2
NAS Port Type:	Ethernet
Access Policy	
Access Service:	802.1X
Identity Store:	AD1
Authorization Profiles:	ACCOUNTING
Exception Authorization Profiles:	
Active Directory Domain:	btsm.local
Identity Group:	
Access Service Selection Matched Rule:	AP-802.1X

Obr. 22. Detailný log z ACS servera.

6.2 Prístupový prepínač Cisco rady 3750

6.2.1 Bezpečnostné nastavenia

Po prvotnej inštalácii sú na prepínačoch spustené určité služby, ktoré by mohli negatívne ovplyvniť bezpečnosť zariadenia ako aj celú infraštruktúru podniku, preto je potrebné takéto služby vypnúť a vykonať niektoré nastavenia, ktoré naopak môžu efektívne zvýšiť bezpečnosť.

V tejto časti je uvedená odporúčaná konfigurácia základných bezpečnostných nastavení, ako aj protiopatrenia na niektoré útoky používané v prístupových sieťach. Uvedená konfigurácia sa môže v malých detailoch líšiť v závislosti od použitej platformy, verzie IOS a podobne.

CDP (Cisco Discovery Protocol) – je potrebné vypnúť na všetkých nedôveryhodných rozhraniach. Tento protokol by mal byť zapnutý len na portoch, ktorými sú prepojené samotné sieťové zariadenia.

```
interface FastEthernet1/0/1
 no cdp enable
```

Šifrovanie hesiel – z dôvodu, aby neboli heslá v lokálnej konfigurácií voľne čitateľné (a to nielen používateľských, enable ale aj RADIUS či TACACS+ secret) sa zapína služba na šifrovanie hesiel.

```
service password-encryption
```

Lokálne užívateľské účty – Heslá pre lokálne používateľské účty sa konfigurujú výlučne s parametrom **secret** a nie password.

```
username localadmin privilege 15 secret Pa$$W0rd
ebable secret Pa$$W0rd1
```

Nepoužívané rozhrania

Nepoužité rozhrania prístupovej vrstvy by mali byť nastavené do módu access.

```
interface FastEthernet1/0/1
 switchport mode access
```

Nepoužité rozhrania mimo prístupovej vrstvy by mali byť vypnuté.

```
interface FastEthernet1/0/1
 shutdown
```

Vypnutie http/https servera

```
no ip http server
no ip secure-server
```

Nastavenie EXEC idle timeout

Toto nastavenie určuje čas nečinnosti užívateľa na konzole alebo termináli po ktorom bude odpojený.

```
line con 0
 exec-timeout 5 0 ![minúty, sekundy]
line vty 0 4
 exec-timeout 5 0 ![minúty, sekundy]
```

Obmedzenie prístupu na terminál

Vzdialený prístup na vty terminál by mal byť obmedzený prístupovým zoznamom, ktorý je v konfigurácii uvedený pod názvom SSH, zároveň každý pokus o nepovolený prístup je logovaný. Pre vzdialený prístup je nutné používať zabezpečený protokol SSH (Secure Shell).

```
ip access-list extended SSH
 permit ip 10.0.99.0 0.0.0.255 any
 deny ip any any log
line vty 0 4
 transport input ssh
 transport output none
 access-class SSH in
```

Šifrovanie vzdialeného prístupu

Pre možnosť použitia protokolu SSH je nutnosť vygenerovať RSA kľúč. Pred samotným generovaním RSA kľúča je potrebné najprv nastaviť doménu, až potom vygenerovať RSA kľúč.

```
ip domain-name btsm.local
crypto key generate rsa general-keys modulus 2048
```

STP (Spanning Tree Protocol)

V prípade použitia možnosti portfast (štandardne port na ktorý je pripojené koncové zariadenie ako počítač pod.) je potrebné použiť zároveň funkcionalitu BPDU guard, ktorá zabezpečí, zablokovanie portu v prípade, že dorazí BPDU rámec na tento port.

```
spanning-tree portfast bpduguard default
```

Port Security

Ako protiopatrenie proti MAC Flooding útoku je potrebné na prístupovej vrstve a všetkých portoch v móde *access* nakonfigurovať port-security.

```
interface fa 1/0/1
  switchport port-security maximum 10
  switchport port-security aging time 1
  switchport port-security violation restrict
  switchport port-security aging type inactivity
  switchport port-security
```

DHCP Snooping

Ako protiopatrenie na útoky s DHCP protokolom sa používa funkcionalita DHCP Snooping. Globálne zapnutie DHCP Snooping a následne aktivovanie pre konkrétnu VLAN je zobrazené nižšie.

```
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40,50,100
```

Nastavenie uplink portov na dôveryhodné tj. odkiaľ môže prísť DHCP ACK, DHCP OFFER odpoveď, sa nastavuje na porte, ktorý je pripojený do distribučnej vrstvy.

```
interface fa 1/0/48
  ip dhcp snooping trust
```

ARP inspection

Ako protiopatrenie na ARP útoky sa používa bezpečnostná funkcionalita ARP inspection, ktorá sa zapína pre každú používanú VLAN sieť.

```
ip arp inspection vlan 10,20,30,40,50,100
```

Záverečné odporúčania:

- Prístup na manažment prepínača by mal byť použitý zabezpečený protokol SSH s použitím ACL.
- Protokol CDP by mal vyť zapnutý len na dôveryhodných rozhraniach.
- Nikdy nepoužívať VLAN1.
- Všetky nepoužívané porty je potrebné vypnúť a priradiť do nepoužívanej VLAN.
- Nepoužívať DTP protokol na prístupových portoch.
- Pri použití VTP protokolu nastaviť autentizáciu.
- Využívať bezpečnostné funkcionality ako protiopatrenia na L2 útoky (Port Security, ARP Inspection, DHCP Snooping, BPDU Guard).

6.2.2 Konfigurácia AAA

TACACS+

Pre nastavenie konfigurácie bezpečnostného modelu AAA je potrebné zadefinovať jednotlivé komponenty AAA architektúry. Prístup na terminál alebo na konzolu prepínača je nakonfigurovaný pomocou TACACS+ protokolu. Pre prípad nedostupnosti ACS servera je vhodné nastaviť aj „fallback“ autentizáciu a autorizáciu, ktorá je použitá ako druhá metóda. Pre tento prípad sa konfiguruje lokálny užívateľský účet viď kapitola 6.2.1.

Súčasťou konfigurácie TACACS+ i RADIUS servera je tajný kľúč (secret), ktorý musí byť nastavený rovnaký na oboch stranách (prepínač, ACS server). Ďalej budú uvedené spôsoby konfigurácie jednotlivých komponentov aj s popisom [20]:

- ***aaa-new model*** – zapne bezpečnostnú architektúru AAA na prepínači.
  tacacs-server host 10.10.10.12 key 123456 – nastavenie TACACS+ servera a zdieľaného tajomstva.
- ***aaa authentication login default group tacacs+ local –*** nastavuje autentizáciu pre prihlásenie na konzolu alebo terminál ***(login)***, ako prednastavená metóda (***default***) je použitá skupina ***(group)*** tacacs+ serverov čo definuje ***(tacacs+)***. Posledným bodom je použitie fallback autentizácie ***(local)***.

- ***aaa authentication enable default group tacacs+ enable –*** nastavuje autentizáciu pri prihlásení do privilegovaného režimu. Nastavenia sú identické ako v predošlom

prípade. Parameter ***(enable)***, určuje fallback autentizáciu do privilegovaného režimu. Teda heslo ktoré je definované príkazom ***enable secret***.

- ***aaa authorization commands 0 default group tacacs+ local –*** nastavuje autorizáciu podľa úrovne privilegovaného režimu. Štandardne sa nastavujú všetky úrovne od 0 – 15.

- ***aaa accounting exec default start-stop group tacacs+ –*** nastavuje audit, teda logovanie vykonaných príkazov. Parameter ***start-stop*** určuje okamžité logovanie, po vykonaní každého príkazu.
- ***aaa accounting system default start-stop group tacacs+*** – vykonáva audit pre všetky systémové udalosti, ktoré nie sú asociované s užívateľom.

RADIUS

Konfigurácia RADIUS servera je obdobná ako v prípade TACACS+ servera.

- ***aaa authentication dot1x default group radius*** – používané ako autentizácia používaná v prípade protokolu 802.1X.

- ***aaa authorization network default group radius*** – používané pre účely autorizácie, využívané pre pridelovanie užívateľov do VLAN sietí prípadne na aplikovanie ACL.
  aaa accounting dot1x default start-stop group radius – nastavenie auditu pre zariadenia pripojené do siete metódou 802.1X.

- ***radius-server host 10.10.10.12 auth-port 1812 acct-port 1812 –*** nastavenie RADIUS servera s možnosťou definovať porty na používané na ACS servery. Samostatne sa nastavujú pre autentizáciu , autorizáciu ***(auth-port 1812)*** a samostatne pre audit **(*acct-port 1812*).**

- ***radius-server key 123456*** – nastavenie zdielaného tajomstva (secret).

6.2.3 Konfigurácia 802.1X

Prístupové porty na prepínači môžu byť nastavené do rozličných režimov *switchport*. V štandardnom nastavení je možné pripojiť len jedno zariadenie na jeden prístupový port. Je viacero možností použitia tohto nastavenia [16]:

- **single-host** – možnosť pripojenia len jednej MAC adresy, tz. jedného zariadenia na daný port, neumožňuje pripojenia viacero zariadení cez ďalší prepínač alebo rozbočovač,
- **multi-domain** – rovnaký spôsob ako *single-host,* avšak s možnosťou použitia VOICE VLAN pre IP telefóny,

- **multi-auth** – povolené jedno zariadenie v hlasovej VLAN (voice VLAN) a viacero v dátovej VLAN (DATA VLAN),
- **multi-host** – povoľuje viacero pripojených zariadení po autorizácii portu prvým pripojeným zariadením (prvé pripojené zariadenie autorizuje port a ostatné majú rovnaké oprávnenia ako autentizované zariadenie). Z bezpečnostného hľadiska tento režim nie je odporúčaný,

Globálne nastavenia

Pri použití metódy v zabezpečenom móde s priraďovaním užívateľov do VLAN sietí sa pre neautorizované zariadenia používa VLAN sieť s názvom GUEST. Toto sa využíva v prípade, keď na zariadení nie je spustený suplikant, alebo keď nereaguje na *EAPoL* rámce. Spustenie funkcie GUEST VLAN sa vykonáva príkazom ***dot1x guest-vlan supplicant.*** Obdobným spôsobom funguje princíp priraďovania užívateľov do tz. reštriktívnej (restricted) VLAN siete, ktorá je používaná v prípade neúspešnej autentizácie. V tomto prípade suplikant reaguje na autentizačné výzvy zasielané autentizátorom, ale autentizácia je neúspešná. Ako príklad je možné uviesť situáciu, kedy má užívateľ zablokované alebo exspirované užívateľského konto na Active Directory. V navrhovanom riešení tento spôsob nie je použitý.

Pri používaní dACL sa informácie o prístupových zoznamoch medzi prepínačom a ACS serverom posielajú prostredníctvom RADIUS VSA atribútov, túto funkciu zapneme pomocou ***radius-server vsa send authentication***.

Aby bolo možné aplikovať dACL na konkrétne zariadenie, ktoré je pripojené na port prepínača, využíva sa funkcionalita ***ip device tracking***. Pomocou protokolov ARP a DHCP sa prepínač naučí IP adresu pripojeného zariadenia a aplikuje ACL na užívateľa teda, so zdrojovou IP adresou jeho zariadenia.

Globálne nastavenie 802.1X je uvedené nižšie:

```
dot1x system-auth-control
dot1x guest-vlan supplicant
radius-server vsa send authentication
ip device tracking
```

Monitorovací mód

V testovanom prostredí bol monitorovací režim aplikovaný na porte *FastEthernet1/0/3*. Port bol nastavený do prístupového (access) módu, čo definuje príkaz ***switchport mode access,*** priradenie portu do dátovej VLAN siete určuje ***switchport access vlan 10.***

Režim *switchport* popisovaný na začiatku tejto kapitoly sa nastavuje *authentication host-mode [single-host | multi-domain | multi-auth | multi-host]*.

V konfigurácii je použitý *single-host* mód s nastavením ***authentication host-mode single-host,*** pretože v navrhovanom riešení sa nepredpokladá použite IP telefónov ani viacerých zariadení pripojených na jeden port cez ďalší prepínač. Nastavenie monitorovacieho prístupu je vykonané s použitím príkazu ***authentication open***, pričom zapnutie 802.1X funkcionality na porte prepínača určuje ***authentication port-control auto.*** Pre zariadenia nepodporujúce 802.X autentizáciu je využívaná MAB, ktorá je definovaná parametrom ***mab.*** Táto metóda je použitá ako nasledujúca po tom, ako prepínač tri krát za sebou pošle *EAPOL Request/Identity* a nedostane žiadnu odpoveď (štandardné nastavenie 3 x 30 sekúnd). Povolenie 802.1X na rozhraní vykonáva príkaz ***dot1x pae authenticator.*** Nastavenie portu v monitorovacom režime je uvedené nižšie:

```
interface FastEthernet1/0/3
 description Monitorovaci-mod
 switchport access vlan 10
 switchport mode access
authentication host-mode single-host
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Selektívny mód

Pri použití selektívneho módu sa využíva prístupový zoznam pomocou ktorého, je povolená len prevádzka definovaná pre neautentizované zariadenia (dodávatelia, hostia). V navrhovanom riešení je povolený prístup len na DHCP, DNS a proxy server, čo definuje ACL zobrazený nižšie:

```
ip access-list extended GUEST-ACCESS-ACL
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit tcp any host 192.168.0.11 eq 3128
```

Konfigurácia selektívneho módu je identická ako v prípade monitorovacieho módu len s tým rozdielom, že na porte je aplikovaný prístupový zoznam pomocou príkazu ***ip access-group GUEST-ACCESS-ACL in***.

Nastavenie portu v selektívnom režime je uvedené nižšie:

```
interface FastEthernet1/0/2
 description Selektivny-mod
 switchport access vlan 10
 switchport mode access
 ip access-group GUEST-ACCESS-ACL in
 authentication host-mode single-host
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Zabezpečený mód

Tento režim sa považuje za najviac bezpečný, ale v niektorých prípadoch nepoužiteľný. Príkladom môže byť situácia, kedy sa použije napr. nastavenie portu *authentication host-mode multi-auth,* a je požadované aby sa na porte pripájali viaceré zariadenia cez ďalší prepínač. Toto by znamenalo, že jeden fyzický port by musel byť pripojený súčasne do viacerých dátových VLAN sietí, čo ale na prístupovom porte nie je možné.

Nastavenie portu do zabezpečeného módu je v základnej časti rovnaké ako v prípade monitorovacieho režimu, len s tým rozdielom, že nie je použitý príkaz *authentication open.* Na-

stavenie switchport *authentication host-mode* je použitý ***multi-domain***. Je to z dôvodu, že režim *single-host* nepodporuje zmenu portu do viacerých dátových VLAN sietí. Použitie GUEST VLAN je nastavené pomocou príkazu ***authentication event no-response action authorize vlan 100.***

Nastavenie portu v zabezpečenom režime je uvedené nižšie:

```
interface FastEthernet1/0/1
 description Zabezpeceny-mod
 switchport access vlan 10
 switchport mode access
 authentication event no-response action authorize vlan 100
 authentication host-mode multi-domain
 authentication port-control auto
 mab
dot1x pae authenticator
```

Ukážka autentizácie v monitorovacom móde, kedy je klient *btsm/uzivatel1* autentizovaný pomocou 802.1X (*dot1x Authc Success*), v ďalšom prípade zariadenie s MAC adresou použitou ako *User-Name B8-70-F4-63-02-9F* a s použitím MAB autentizačnej metódy (*mab Authc Success*):

```
Switch#sh authentication sessions interface fa 1/0/3
Interface:  FastEthernet1/0/3
        MAC Address:  b870.f463.029f
         IP Address:  10.0.1.21
User-Name:  btsm\uzivatel1
         Status:  AuthzSuccess
Domain:  DATA
SecurityPolicy:  ShouldSecure
Security Status:  Unsecure
 Oper hostmode:  single-host
 Oper controldir:  both
Authorized By:  Authentication Server
VlanGroup:  N/A
Sessiontimeout:  N/A
Idletimeout:  N/A
CommonSession ID:  C0A802AB00000001000D343F
AcctSession ID:  0x0000000B
Handle:  0xAC000001
Runnablemethods list:
Method   State
      dot1x    Authc Success
mab Not run
```

Switch#sh auth sessions inter fa 1/0/3
Interface: FastEthernet1/0/3
MAC Address: b870.f463.029f
IP Address: 10.0.1.21
User-Name: B8-70-F4-63-02-9F
Status: AuthzSuccess
Domain: DATA
SecurityPolicy: ShouldSecure
Security Status: Unsecure
Oper host mode: single-host
Oper controldir: both
Authorized By: Authentication Server
Vlan Group: N/A
Session timeout: N/A
Idletimeout: N/A
Common Session ID: C0A802AB0000000200196462
Acct Session ID: 0x0000000D
Handle: 0xCC000002

Runnablemethods list:
MethodState
dot1x Failed over
mab Authc Success

Tab. 14. Základné príkazy používané pri riešení problémov [16].

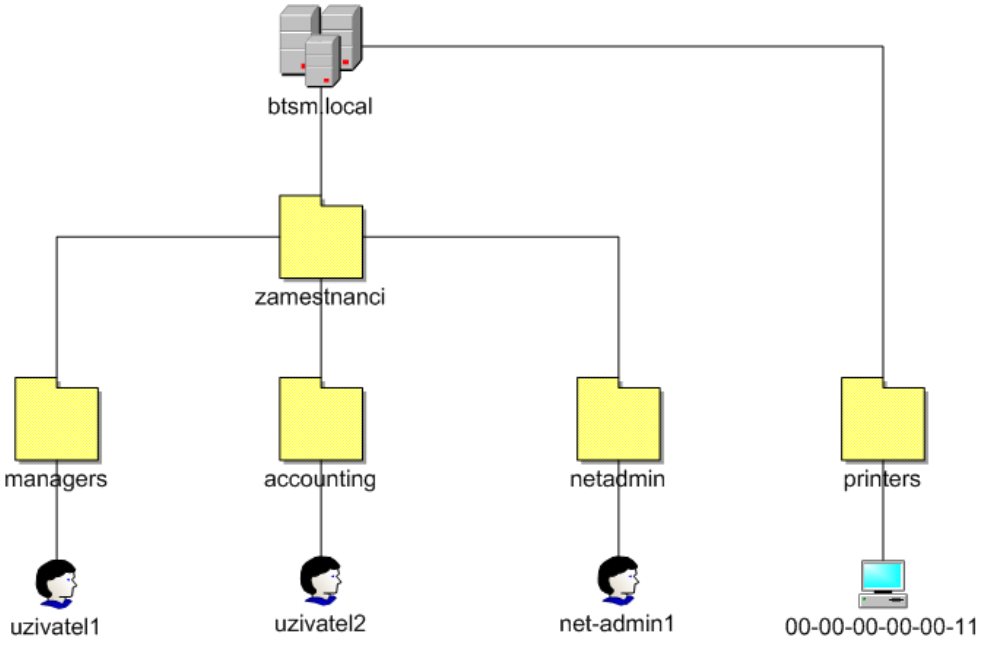
Príkaz	**Popis**
show authentication sessions fastEthernet 1/0/1	Zobrazí sumárne informácie autentizačnej relácie na konkrétnom rozhraní.
show dot1x interface fastEthernet 1/0/1details	Zobrazí detailné informácie autentizačnej relácie na konkrétnom rozhraní.
show errdisable detect	Zobrazí nastavenie errdisable funkcionality, a ak je nejaký port v errdisable stave zobrazí dôvod prečo bol zablokovaný.
show ip device tracking all	Zobrazí IP informácie o zariadeniach naučených cez ARP alebo DHCP protokol.
show ip access-list interface	Zobrazí aplikovaný ACL na aplikovaných na rozhranie spolu so štatistikou.

6.3 Konfigurácia Microsoft Active Directory

V navrhovanom riešení je použitý Microsoft Windows Server 2008 R2, so službou Active Directory, ktorá ponúka prostriedky pre správu identít a vzťahov v rámci siete organizácie. Active Directory je integrovaná v systéme Windows Server 2008 a ponúka funkcie nutné na centrálnu konfiguráciu a správu nastavení systému, používateľov a aplikácií. Pomocou služby Active Directory je možné zjednodušiť správu používateľov a počítačov, povoliť prístup k sieťovým prostriedkom a vylepšiť ochranu a zabezpečenie uložených informácií a komunikácie. Active Directory je centrálnym umiestnením pre konfiguračné informácie, požiadavky na overovanie a informácie o všetkých objektoch uložených v doménovej štruktúre. Pomocou služby Active Directory je možné efektívne spravovať používateľov, počítače, skupiny, tlačiarne, aplikácie a ďalšie objekty využívajúce adresárovú službu z jedného zabezpečeného, centralizovaného umiestnenia [17].

Jedná sa teda o centrálny zdroj identít, ktorý sa používa vo väčšine podnikových sietí. Pre testovacie účely boli na uvedenom servery nainštalované doplnkové služby ako podniková certifikačná autorita označovaná ako Active Directory Certificate Services (pre zabezpečenie správnej funkčnosti PEAP-MS-CHAPv2 autentizácie), DNS a DHCP server (pre poskytnutie základných sieťových služieb).Podniková doména bola zvolená pod názvom *btsm.local.*

Užívatelia, ktorí pristupujú do podnikovej siete a autentizujú sa pomocou metódy 802.1X sú priradený do organizačných jednotiek, ktoré prislúchajú ich pracovnej pozícii (managers, accounting, netadmin). Tlačiarne, ktoré používajú autentizáciu pomocou MAB sú priradené do organizačnej jednotky *printers.* Pomocou takto vytvorenej štruktúry sa na ACS servery vytvárajú autorizačné profily, ktoré sú používané na povolenie prístupu do podnikovej siete. Schéma organizačnej štruktúry, ktorá je využívaná na vytváranie autorizačných profilov je zobrazená na obr. č23.

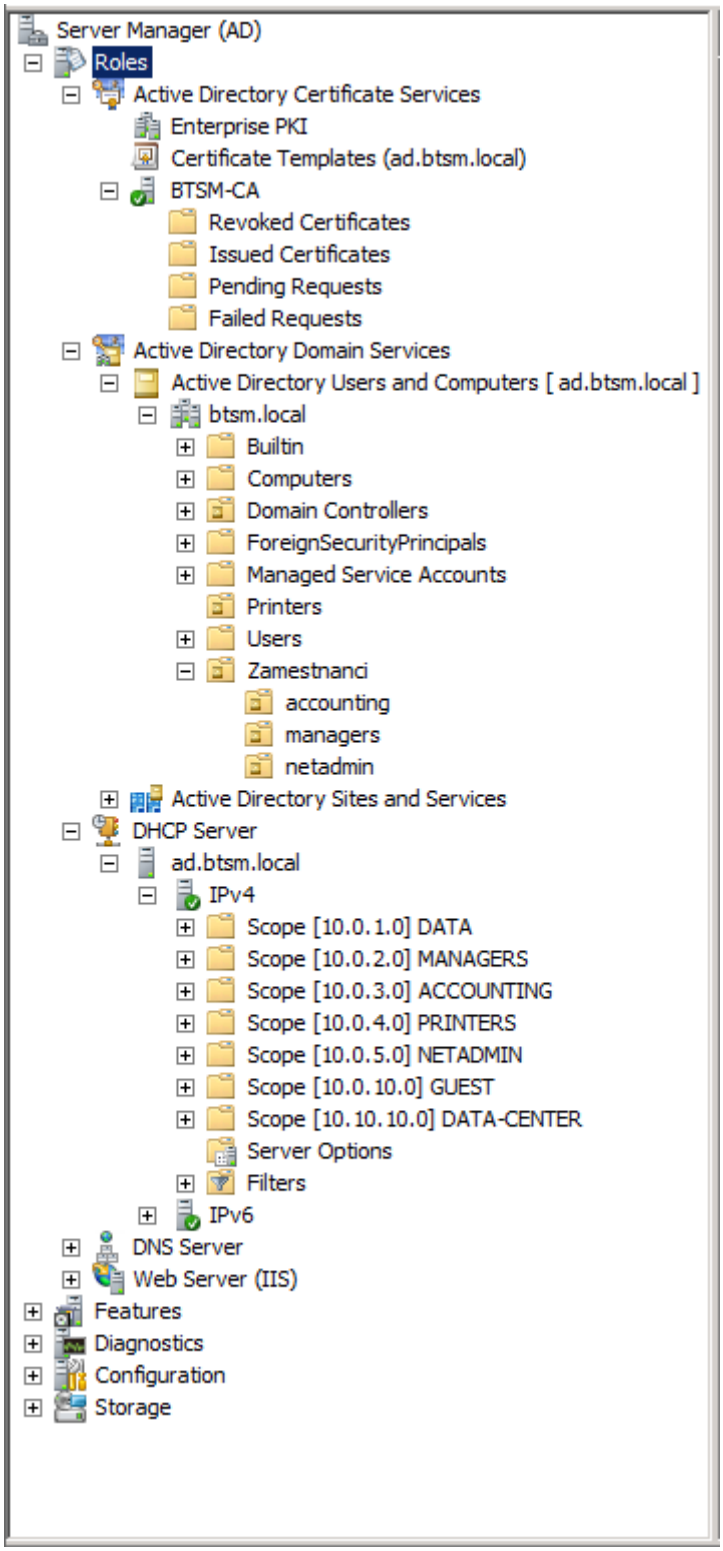


Obr. 23. Schéma organizačnej štruktúry Active Directory.

Doplnkové služby použité v testovacom prostredí.

V testovacom prostredí bola použitá podniková certifikačná autorita BTSM-CA, avšak v produkčnom prostredí by certifikačná autorita nemala, byť nainštalovaná na rovnakom servery ako Active Directory a hierarchický model podnikovej PKI infraštruktúry by mal byť trojúrovňový.

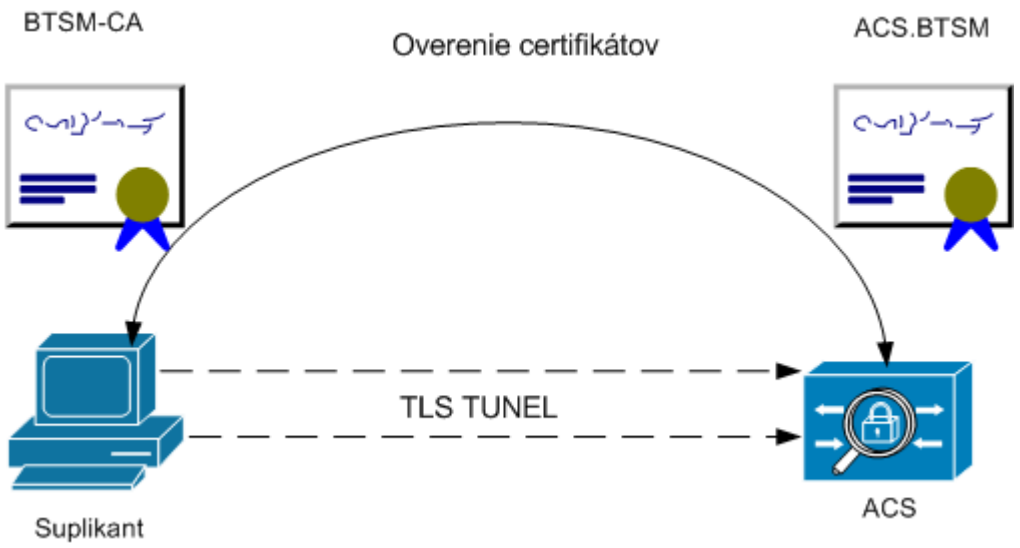
Ďalšou doplnkovou službou bol DHCP server, ktorý zabezpečoval prideľovanie IP adries pre zariadenia pripojené do podnikovej siete. V navrhovanom riešení bolo používaných päť VLAN sietí, pre ktoré boli vytvorené adresné rozsahy podľa tab. č. 9. DNS server zabezpečoval preklad doménových mien na IP adresy pre jednotlivé používané služby. Náhľad na administratívnu konzolu je zobrazený na obr. č. 24.



Obr. 24. Prehľad doplnkových služieb na Active Directory.

6.4 Konfigurácia klientov

Autentizačná metóda používaná v navrhovanom riešení je PEAP(MS-CHAPv2), ako bolo popísané v kapitole 2.5.1, medzi klientom a autentizačným serverom sa najskôr vytvorí zabezpečený TLS kanál. V takto zabezpečenom kanále sa vytvorí ďalšia EAP autentizačná metóda, ktorou je MS-CHAPv2. Obr. č.25 popisuje základný princíp PEAP(MS-CHAPv2) autentizácie.



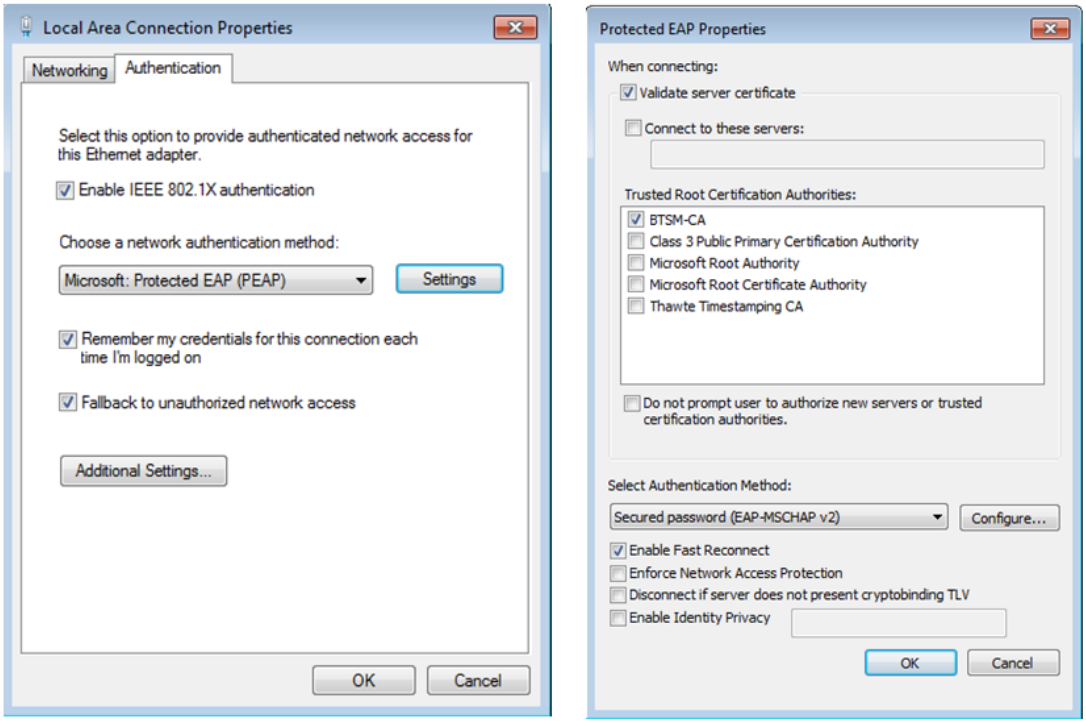
Obr. 25. Princíp PEAP autentizácie.

V prvom kroku ACS server pošle certifikát suplikantovi, následne si klient overí či sa jedná o dôveryhodný server a vytvorí sa zabezpečený TLS tunel, cez ktorý suplikant pošle prihlasovacie údaje (meno, heslo). V poslednej fáze ACS server overí platnosť prihlasovacích údajov.

Je teda zrejmé, že je potrebné mať na klientoch nainštalovaný certifikát z dôveryhodnej koreňovej certifikačnej autority, ktorá vydala certifikát pre ACS server. V našom prípade sa jedná o certifikačnú autoritu *BTSM-CA*.

Pre počítače s operačným systémom MS Windows (Windows Vista, Windows 7, Windows 8) činnosť suplikanta zabezpečuje natívna služba *Wired Auto Config*, ktorá musí byť nastavená v režime automatického spúšťania pri štarte počítača. Konfigurácia suplikanta môže byť vykonaná nasledujúcimi spôsobmi:

- **Manuálne pomocou nastavení sieťového adaptéra**, k tomu sú potrebné administrátorské oprávnenia viď. obr. č.26.
- **Centralizovane za pomoci doménových politík GPO** (Group Policy Object), s predpokladom, že počítač je členom domény.



Obr. 26 Manuálne nastavenie suplikanta.

V navrhovanom riešení je definovaný prístup na internet prostredníctvom proxy servera, čo v prípade použitia počítačov pripojených do podnikovej domény nie je problém. Toto sa nastavuje pomocou GPO politík. Ale ako to vyriešiť v prípade dodávateľov a hostí, ktorí nemajú počítače zaradené do podnikovej domény? Jedným z riešení je nastaviť proxy server ručne, to znamená, že by si hostia museli nastaviť proxy server v internetových prehliadačoch manuálne. Tento spôsob nie je moc transparentný pre koncových užívateľov. Vhodnejšie je nastaviť proxy server pomocou WPAD (Web Proxy Auto-Discovery) technológie.

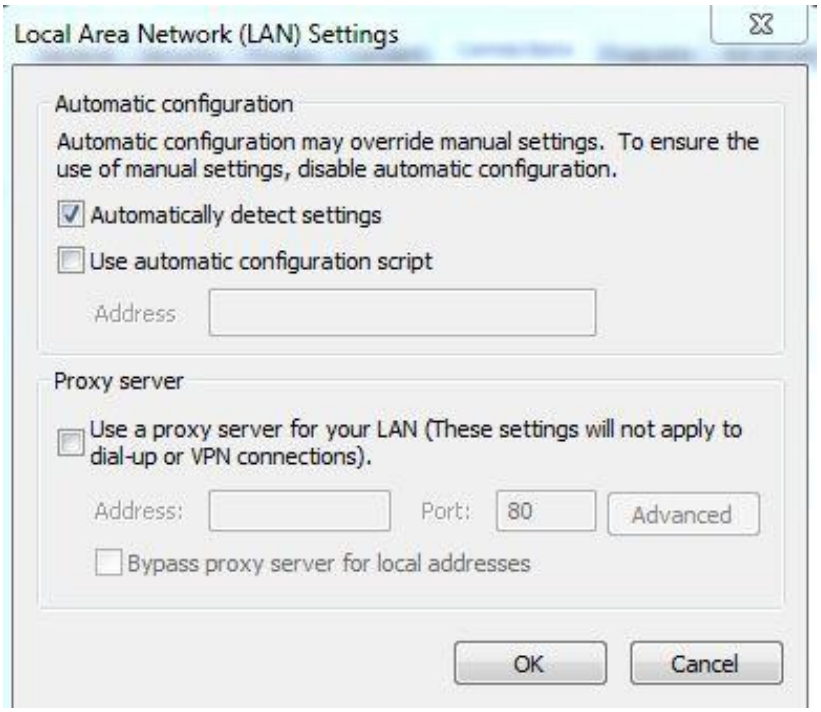
WPAD technológia umožňuje dve metódy nastavenia proxy servera:

- Nastavenie WPAD pomocou DNS.
- Nastavenie WPAD pomocou DHCP servera

Nastavenie WPAD pomocou DNS

Princíp WPAD technológie je taký, že klient po pripojení do počítačovej siete si stiahne konfiguračný súbor wpad.dat (príklad konfigurácie je uvedený v prílohe PI), ktorý býva umiestnený na vždy dostupnom mieste, najčastejšie sa používa umiestnenie práve na samotnom proxy servery. Tento súbor obsahuje nastavenie proxy servera.

Klient po pripojení do počítačovej siete automaticky hľadá server s DNS záznamom napr. wpad.domena.com v našom prípade *wpad.btsm.local*. Z toho vyplýva, že je potrebné v DNS vytvoriť záznam, ktorý bude smerovať na web server kde je uložený wpad.dat. V konečnom dôsledku si užívateľ stiahne súbor z adresy napr. http://wpad.btsm.local/wpad.dat. Toto nastavenie je štandardne na klientoch, resp. v prehliadači Internet Expolorer zapnuté. V prípade, že je konfigurácia zmenená treba ju nastaviť podľa obr. č 27.



Obr. 27. Nastavenie proxy konfigurácie pomocou WPAD a DNS.

Nastavenie WPAD pomocou DHCP servera

Toto nastavenie proxy servera na klientoch je identické ako v predchádzajúcom prípade, len s tým rozdielom, že namiesto DNS záznamu je použitý DHCP server, ktorý pošle nastavenie proxy serveru (pomocou dhcp option 252).

7 VÝHODY A NEVÝHODY NAVRHOVANÉHO RIEŠENIA

7.1 Výhody použitia štandardu 802.1X

Hlavnou výhodou navrhovaného riešenia je podstatné zvýšenie zabezpečenia prístupovej vrstvy siete, ktoré so sebou ale nesie neduh zvýšenia komplexnosti siete. Keďže sa jedná o komplexnú službu v reálnom nasadení je potrebné zabezpečiť vysokú dostupnosť autentizačného servera. Pretože v prípade jeho výpadku, by boli ohrození všetci užívatelia, nakoľko by sa nemohli pripojiť do siete. Na druhej strane si treba uvedomiť, že toto riešenie prináša množstvo výhod ktorými sú:

- **Riadený prístup k podnikovým zdrojom –** centralizovaný prístup pre riadenie užívateľov a zariadení do podnikovej siete s možnosťou granulárneho definovania prístupových oprávnení a zjednodušenie manažmentu týchto oprávnení. Umožnenie rýchlej zmeny oprávnení napr. po zmene pracovnej pozície, alebo zakázanie prístupu po ukončení pracovného pomeru, prípadne časové obmedzenie v ktorom bude povolený prístup a pod.

- **Monitoring užívateľov –** z logov autentizačného servera je možné spätne dohľadať:
    - Kto bol pripojený do podnikovej siete.
    - Kedy bol pripojený do podnikovej siete.
    - Kam bol pripojený (cez aký prepínač).

- **Mobilita užívateľov –** keďže v štandard 802.1x umožňuje riadenie prístupových oprávnení na základe identity užívateľa a nie je viazané na koncové zariadenie prípadne lokalitu, užívatelia môžu využívať všetky podnikové zdroje kdekoľvek v rámci prístupovej infraštruktúry podnikovej siete, čo so sebou prináša ďalšiu výhodu ktorou je zvýšenie produktivity a komfortu pre koncových používateľov.

- **Selektívny mód** – jednoduché spravovanie sieťovej prevádzky pomocou prístupových zoznamov na centralizovanom mieste, netreba konfigurovať prístupové zoznamy na každom prepínači. Ďalšou výhodou je jednoduchá migrácia, s minimálnym dopadom na koncových užívateľov (netreba meniť sieťovú architektúru, ponechanie existujúcich VLAN sietí).

- **Zabezpečený mód**– priraďovanie užívateľov do VLAN sietí je podporované väčšinou výrobcov, takže je možné tento mód použiť aj v prípade iných prístupových prepínačoch ako Cisco.

7.2 Nevýhody použitia štandardu 802.1X

- **Komplexnosť siete** – s nárastom bezpečnosti sa zvýši komplexnosť podnikovej siete. Samotné prihlásenie do počítačovej siete je závislé na ďalších službách.

- **Selektívny mód** – pri použití dACL je možné na prepínačoch použiť, len určitý počet prístupových zoznamov (v závislosti na použitej platforme), je teda nutná optimalizácia prístupových zoznamov.

- **Zabezpečený mód** – Priraďovanie užívateľov do VLAN je vo veľkých sieťach komplikované, pripadne až nereálne (viacero VLAN sietí, ktoré musia byť smerované, všetky VLAN siete musia byť nakonfigurované na každom prístupovom prepínači).

- **Nutnosť použitia suplikanta** – môže predstavovať problém v závislosti na použitom operačnom systéme.

- **MAB** – prináša určité riziko zneužitia, v prípade podvrhnutia falošnej MAC adresy, preto by sa mala táto metóda autentizácie nastavovať len na portoch prepínača, kde sú zariadenie nepodporujúce 802.1X.

ZÁVER

Cieľom tejto práce bolo poukázať na možnosti zabezpečenia podnikových sietí s využitím autentizačných metód, ktoré umožňujú poskytovať užívateľom len tie oprávnenia, ktoré prislúchajú ich pracovnej pozícii alebo roli. Tento koncept môže efektívnym spôsobom zabezpečiť podnikové zdroje, za použitia bežne dostupných technológií.

Prvá časť tejto práce obsahuje základné informácie spojené s problematikou zabezpečenia podnikových sietí založenej na identite užívateľa, ktorá využíva štandard 802.1X, ako aj základné princípy sieťových protokolov používaných pomocou tejto technológie. Ďalšia časť práce bola venovaná popisu možných útokov používaných v prístupových sieťach a návrhu protiopatrení, ktoré efektívne eliminujú tieto hrozby.

Praktická časť obsahuje základný návrh zabezpečenia prístupovej siete založený na štandarde 802.1X, ako aj možným spôsobom nasadenia pri procese implementácie, ktorý by nemal negatívne ovplyvniť koncových užívateľov.

Ako kľúčový prvok bol použitý ACS server od spoločnosti Cisco, ktorý ako bolo počas reálneho testovacieho nasadenia overené, dokáže vynucovať vyžívanie prístupových politík definovaných v bezpečnostnej politike podniku. Pri realizácii boli použité tri módy nasadenia, ktoré umožňujú použitie technológie 802.1X. Prvou je monitorovací mód, ktorý umožňuje nasadenie technológie bez afektovania užívateľov a zároveň ponúka možnosť zmonitorovať si prostredie v ktorom bude technológia 802.1X nasadená.

Tento režim však neposkytuje zvýšenie bezpečnosti. Na tento účel sú používané ostatné dva módy, selektívny mód a zabezpečený mód, ktoré používajú odlišný spôsob zabezpečenia. Selektívny mód používa na zabezpečenie prevádzky prístupové zoznamy. Počas testovania som nezaznamenal žiaden problém a z hľadiska nasaditeľnosti považujem za najviac použiteľný. V prípade použitia zabezpečeného módu, ktorý používa priraďovanie do VLAN sietí som zaznamenal problémy spojené s DHCP protokolom. Konkrétne po zmene VLAN siete, niekedy zariadenie pripojené na prepínač nedostalo IP adresu z DHCP servera. Je možné, že to bolo spôsobené chybnou konfiguráciou niektorého z použitých komponentov. Rozhodnutie, ktorá metóda je najvhodnejšia je individuálne, závisí od konkrétneho prostredia v ktorom bude použitá. Celkovo je možné hodnotiť túto technológiu pozitívne, nakoľko dokáže relatívne jednoduchým spôsobom zvýšiť celkovú bezpečnosť podnikovej infraštruktúry.

ZOZNAM POUŽITEJ LITERATÚRY

[1] LARSON, Robert. Cisco security specialist 1 certification: exam guide. Berkeley, Calif: Osborne, 2003, 805 s. ISBN 00-722-2691-9.

[2] VYNCKE, Eric a Christopher PAGGEN. LAN switch security: what hackers know about your switches. Indianapolis, Cisco Press, 2008, 340 s. ISBN 15-870-5256-3

[3] Configuring IEEE 802.1x Port-Based Authentication [online]. [cit. 2014-03-24]. Dostupný z www: http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/ht_8021x.html.

[4] DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS: Vysvětlení nejpoužívanějších protokolů a konfigurace současných sítí. Internet i vnitřní podnikové sítě. Delegace domén, přidělování. Vyd.2 Praha: Computer Press, 2000, 426 s. ISBN 80-722-6323-4.

[5] RFC3748 Extensible Authentication Protocol [online]. [cit. 2014-03-24]. Dostupný z www: http://tools.ietf.org /html/rfc3748.

[6] OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. Vyd. 1. Brno: Computer Press, 2008, 444 s. ISBN 978-80-251-2048-4.

[7] SANTUKA, Vivek, Premdeep BANGA a Brandon CARROLL. AAA identity management security. Indianapolis, Cisco Press, 2011, 443 s. ISBN 15-871-4144-2.

[8] The Advantages of TACACS+ for Administrator Authentication [online]. [cit. 2014-03-24]. Dostupný z www: http://www.tacacs.net/docs/TACACS+ Advantages.pdf

[9] EAPOL [online]. [cit. 2014-03-24]. Dostupný z www: http://etutorials.org/Networking/802.11+security.+wi fi+protected+access+and+802.11i/P art+II+The +Design+of+WiFi+Security/Chapter+8.+Access+Control+IEEE+802.1X+EAP+and+RADIUS/EAPOL/

[10] ANDRÉS, Alfredo a David BARROSO. Útoky na druhou vrstvu síťového modelu OSI. Hakin9. Warszawa: Software-Wydawnictwo Sp z o.o, 2005, č. 6.

[11] Identity Based Networking Services [online]. [cit. 2014-03-24]. Dostupný z www: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/data_sheet_c78-542121.html.

[12] IBNS: Web Authentication Deployment and Configuration Guide [online]. [cit. 2014-03-24]. Dostupný z www: http://www.cisco.com/c/en/us/products/ios-nx-os-software/identity-based-networking-services/index.html.

[13] IBNS: IP Telephony In IEEE 802.1X-Enabled Networks Deployment and Configuration Guide [online]. [cit. 2014-03-24]. Dostupný z www: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-605524.html.

[14] RFC 2865 Remote Authentication Dial In User Service [online]. [cit. 2014-03-24]. Dostupný z www: http://tools.ietf.org/html/rfc2865.

[15] RFC 2131 Dynamic Host Configuration Protocol [online]. [cit. 2014-03-24]. Dostupný z www: http://tools.ietf.org/html/rfc2131.

[16] IBNS quick reference guide [online]. [cit. 2014-03-24]. Dostupný z www: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_c27-574041.pdf.

[17] Active Directory [online]. [cit. 2014-03-24]. Dostupný z www: http://www.microsoft.com/slovakia/windowsserver2008/active-directory.aspx

[18] FindProxyForURL [online]. [cit. 2014-03-24]. Dostupný z: http://findproxyforurl.com/example-pac-file/

[19] MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. Vyd.2. Indianapolis: Cisco Press, 2009, 333 s. ISBN 978-1-58714-062-4.

[20] Catalyst 3750 Software Configuration Guide [online]. [cit. 2014-03-24]. Dostupný z www: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/ software/release/12-2_55_se/configuration/guide/scg3750.html

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
ACS	Secure Access Control Server
AD	Active Directory
BPDU	Bridge Protocol Data Unit
CBPDU	Configuration Bridge Protocol Data Unit
CDP	Cisco Discovery Protocol
CSR	Certificate Signing Request
dACL	downloadable ACL
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarizovaná zóna
DNS	Domain Name Systém
DoS	Denial of Service
DTP	DynamicTrunking Protocol
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over Lan
EAP-TLS	Transport Layer Security
EAP-TTLS	Tunneled Transport Layer Security
FCS	Frame Check Sequence
FQDN	Fully Qualified Domain Name
GPO	Group Policy Object
GTC	Generic Token Code
CHAP	Challenge-Handshake Authentication Protocol

IBNS	Identity Based Networking Services
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
ISL	Inter Switch Link
LEAP	Lightweight Extensible Authentication Protocol
LLDP	Link Layer Discovery Protocol
MAB	MAC Authentication Bypass
MAC	Medium Access Control
MITM	Man In The Middle
NTP	Network Time Protocol
PAP	Password authentication protocol
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infractructure
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SIEM	Security Information and Event Monitoring
SNMP	Simple Network Management Protocol
SPOF	Single Point Of Failure
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access-Control System Plus
TCN BPDU	Topology Change Notification Bridge Protocol Data Unit
TLS	Transport Layer Security

TTLS	Tunneled Transport Layer Security
VID	VLAN Identifier
VLAN	Virtual LAN
VSA	Vendor Specific Attribute
VTP	VLAN Trunking Protocol
WPAD	Web Proxy Auto-Discovery

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: KONFIGURÁCIA PROXY S POUŽITÍM WPAD TECHNOLÓGIE.

Tab. 15. Konfigurácia proxy servera s použitím wpad.dat [18].

```
functionFindProxyForURL(url, host) {


// If the hostname matches, send direct.
    if(dnsDomainIs(host, ".intranet.btsm.local") ||
        shExpMatch(host, "(*.btsm.local)"))
        return"DIRECT";


// If the protocol or URL matches, send direct.
    if(url.substring(0, 4)=="ftp:"||
        shExpMatch(url, "http://intranet.btsm.local/*"))
        return"DIRECT";


// If the requested website is hosted within the internal network, send di-
rect.
    if(isPlainHostName(host) ||
        shExpMatch(host, "*btsm.local") ||
        isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
        isInNet(dnsResolve(host), "172.16.0.0",  "255.240.0.0") ||
        isInNet(dnsResolve(host), "192.168.0.0",  "255.255.0.0") ||
        isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
        return"DIRECT";
// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
    if(isInNet(myIpAddress(), "10.0.10.0", "255.255.255.0"))
        return"PROXY proxy.btsm.local:3128";
}
```