VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

AUTENTIZÁCIA AKTÍVNYCH PRVKOV V SIEŤACH IBNS (IDENTITY-BASED NETWORKING SERVICES)

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE MAREK LOMNICKÝ
AUTHOR

BRNO 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

AUTENTIZÁCIA AKTÍVNYCH PRVKOV V SIEŤACH IBNS (IDENTITY-BASED NETWORKING SERVICES)

AUTHENTICATING DEVICES IN IBNS (IDENTITY-BASED NETWORKING SERVICES) NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MAREK LOMNICKÝ
AUTHOR

VEDOUCÍ PRÁCE — ING. PETR MATOUŠEK, PH.D.
SUPERVISOR

BRNO 2007

ZADANIE

1. Zoznámte sa s architektúrou IBNS (Internet-Based Networking Services) na autentizáciu aktívnych zariadení (prepínačov, prístupových bodov AP Wifi) podľa štandardu IEEE 802.1x.

2. Zoznámte sa s podporou týchto technológií na zariadeniach od firmy Cisco (prepínače, smerovače). Popíšte všeobecnú schému riadenia prístupu k sieťovým zdrojom pomocou IBNS.

3. Preštudujte dostupnosť a podporu serverov na autentizáciu (RADIUS, TACACS+, LDAP).

4. Navrhnite bezpečnostnú politiku na pripojovanie zariadení pomocou rôznych VLAN sietí. Nakonfigurujte zariadenia v laboratóriu tak, aby podporovali navrhnutú bezpečnostnú politiku.

5. Otestujte funkčnosť systému a spoluprácu klientov v operačných systémoch Linux, Windows, FreeBSD počas autentizácie podľa implementovanej schémy.

6. Zhodnoťte využitie IBNS na zabezpečenie LAN sietí.

LICENČNÁ ZMLUVA

Licenčná zmluva je uložená v archíve Fakulty informačních technologií Vysokého učení technického v Brně.

ABSTRAKT

Cieľom tejto práce je preštudovať a otestovať sieťové riešenie IBNS, ktoré dovoľuje navrhnúť flexibilnú bezpečnostnú politiku založenú na identite a právach užívateľov, nezávislú na fyzických zariadeniach a spojeniach, ktoré títo užívatelia používajú.

KĽÚČOVÉ SLOVÁ

IBNS, 802.1x, EAP, RADIUS, AAA, LAN, autentizácia, port, prepínač, smerovač, Cisco, bezpečnosť, autorizácia, VLAN, sieť, LDAP

ABSTRACT

Main goal of this thesis is to study and test network access based on IBNS technology giving possibility to design flexible security policy based on user's identity and rights that is transparent to physical network components.

KEYWORDS

IBNS, 802.1x, EAP, RADIUS, AAA, LAN, authentication, port, switch, router, Cisco, security, authorization, VLAN, network, LDAP

CITÁCIA

Lomnický, M. Autentizácia aktívnych prvkov v sieťach IBNS (Identity-Based Networking Services). Brno, 2007. FIT VUT v Brně. bakalárska práca.

AUTENTIZÁCIA AKTÍVNYCH PRVKOV V SIEŤACH IBNS (IDENTITY-BASED NETWORKING SERVICES)

PREHLÁSENIE

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením Ing. Petra Matouška, Ph.D. a že som uviedol všetky literárne pramene a publikácie, z ktorých som čerpal.

Marek Lomnický
11. mája 2007

POĎAKOVANIE

Týmto ďakujem pánovi Ing. Petrovi Matouškovi, Ph.D. za podporu a pomoc pri riešení tohto projektu.

OBSAH

1 ÚVOD

S nárastom využitia počítačových sietí v spoločnosti úzko súvisí potreba tieto siete zabezpečiť. Či sa jedná o otázku dostupnosti siete, dôvernosti dát alebo kontrolu využívania služieb, bezpečnosť sa vyvinula z doplnkovej zložky na jednu z najdôležitejších zložiek sieťového návrhu.

Umožnenie prístupu do siete a k sieťovým zariadeniam znamená zvýšené riziko a neautorizovaný prístup do siete internetového poskytovateľa, mobilnej kancelárie či školy môže viesť k prezradeniu citlivých informácií. Spôsobov ako zabezpečiť sieť existuje veľké množstvo. Nelíšia sa pritom len typom siete, ktorú zabezpečujú, ale aj možnosťami sieťových služieb, ktoré poskytujú.

Bezpečnosť sietí s užívateľmi pripojenými vytáčanými pripojeniami je na vysokej úrovni vďaka možnosti použiť služby architektúry AAA. Ako však zabezpečiť sieť, do ktorej sa užívatelia pripájajú LAN technológiami ako 802.3 (Ethernet), 802.11 (Wifi) alebo 802.5 (Token Ring)? Odpoveď nájde čitateľ v tejto práci.

Často zaužívaný spôsob zabezpečenia založený na hardwarovej adrese zariadenia, ktorým sa užívateľ do siete pripája má niekoľko nevýhod. Keďže sa viaže na fyzické zariadenie a nie na užívateľa, je možné rozlišovať sieťové práva len na úrovni týchto zariadení. Sieť sa tým pádom stáva neflexibilná a ťažko rozšíriteľná, pretože už pri malej zmene, akou je napr. výmena sieťového adaptéru či kúpa nového zariadenia, je na zachovanie integrity bezpečnostnej politiky nutná jej úprava. Navyše, pokiaľ užívateľ vlastní viac zariadení, musia byť jeho práva pre každé zariadenie definované osobitne, pretože každé z nich má odlišnú hardwarovú adresu. Správa takejto sieti sa tým výrazne komplikuje.

Ďalšou nevýhodou spojenou s používaním hardwarovej adresy je otázka jej dôveryhodnosti. V prostredí LAN sietí nemá útočník problém ju odchytiť a pod falošnou identitou získať prístup k zdanlivo zabezpečených zdrojom.

Táto práca sa zaoberá zabezpečením sietí pomocou IBNS, čo je technologické riešenie bezpečnosti využívajúce štandard 802.1x s protokolmi EAP, RADIUS alebo TACACS+, umožňujúce sieťam prevádzkovať všetky služby architektúry AAA aj nad klientmi pripojenými do siete technológiami LAN. Použitím služieb AAA sa zariadenie v procese autentizácie identifikuje nie adresou sieťového adaptéru, ale užívateľom pracujúcim na tomto zariadení, čím sa sieť stáva flexibilnejšou a ľahko rozšíriteľnou. Umožní sa využívanie jedného zariadenia viacerými užívateľmi s rozličnými právami a zvýši sa ich mobilita, kedy nie je dôležité, čím, odkiaľ a ako sa užívateľ do siete

pripája, ale na základe jeho identity sa dynamicky aplikujú bezpečnostné pravidlá napr. pomocou technológie VLAN. Aby sa odstránili bezpečnostné riziká spojené s použitím hardwarovej adresy ako identity pri autentizácii, používajú sa autentizačné protokoly, ktoré poskytujú rozsiahle možnosti zabezpečenia prenášaných identifikačných údajov a ich bezpečnosť nie je ohrozená ani pri použití bezdrôtového prístupu v sieťach WLAN.

Správu užívateľov siete založenej na AAA značne uľahčuje použitie štandardných univerzálnych databázových riešení ako napr. SQL server alebo LDAP server.

Kapitola číslo 1 uvádza čitateľa do problematiky a pojednáva o téme tejto bakalárskej práce.

Druhá kapitola zoznamuje čitateľa s architektúrou AAA, popisuje úlohy jednotlivých prvkov siete a predstavuje rôzne používané protokoly.

V tretej kapitole je vysvetlený význam štandardu 802.1x, spôsob autentizácie pripájajúcich sa zariadení a tunelovací protokol EAPOL.

Štvrtá kapitola je zameraná na praktickú ukážku návrhu siete mobilnej kancelárie, ktorá na zabezpečenie využíva technológie predstavené v predchádzajúcich kapitolách.

V piatej kapitole sa čitateľ zoznámi s detailmi implementácie navrhnutej siete, konkrétne s konfiguráciou použitých zariadení a softvéru.

Šiesta kapitola nesie názov „Testovanie siete“. Detailne opisuje 6 testov vykonaných na implementovanej sieti a ich výsledky dokladuje priloženými ukážkami komunikácie jednotlivých zariadení.

Poslednú kapitolu tvorí zhrnutie prínosu práce a názor autora na spôsob zabezpečenia sietí, ktorým sa celá práca zaoberá.

2 ARCHITEKTÚRA AAA

Táto kapitola pojednáva o sieťovej architektúre, ktorej cieľom je poskytnúť rozšírené zabezpečenie siete. Jej základ tvoria služby, ktoré sú určené nie len na autentizáciu zariadenia pred vstupom, ale ponúkajú mechanizmy, ako mu prideliť sieťové práva alebo ako jeho činnosť následne účtovať. Zariadeniam pritom určuje špecifické úlohy a pri komunikácii využíva špecifické protokoly.

2.1 Služby AAA

AAA (angl. Authentication, Authorization and Accounting) je architektúrou, ktorá definuje 3 nezávislé bezpečnostné služby:

- **autentizáciu** – poskytuje metódy identifikácie užívateľa pracujúceho na zariadení, deje sa na linkovej, resp. aplikačnej vrstve TCP/IP sieťového modelu (ďalej len vrstve) a jej bezpečnosť závisí na zvolenom autentizačnom protokole
- **autorizáciu** – po umožnení zariadeniu do siete vstúpiť sa stará o obmedzenie jeho činnosti, pričom na to využíva dodatočné informácie získané počas procesu autentizácie
- **účtovanie** – poskytuje možnosti, ako činnosť autorizovaného zariadenia v sieti monitorovať a kontrolovať

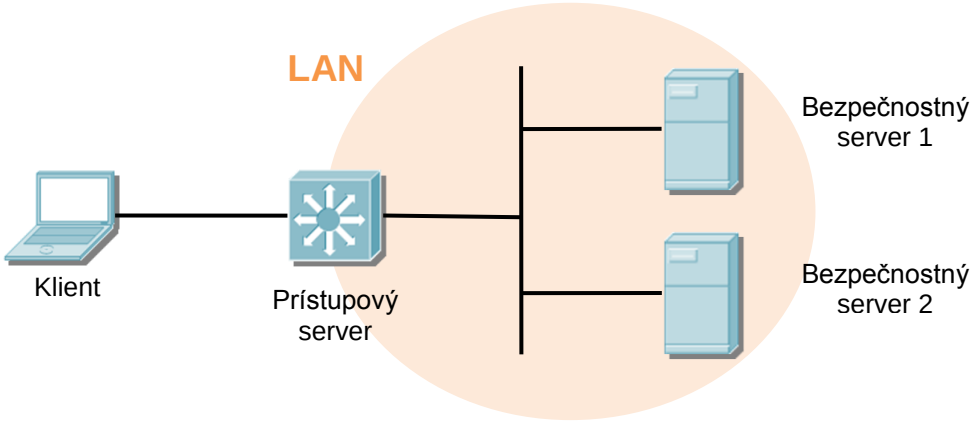
Všetky tieto služby sú založené na identite užívateľa zariadenia a umožňujú aplikovať flexibilnú a ľahko rozšíriteľnú bezpečnostnú politiku.

2.2 Zariadenia AAA

Architektúra AAA popisuje nasledujúce úlohy zariadení zúčastňujúcich sa na autentizácii, autorizácii alebo účtovaní:

- klient
- prístupový server
- bezpečnostný server

Schéma zapojenia zariadení v sieti LAN založenej na AAA viď Obrázok 1.



Obrázok 1 - Schéma zapojenia zariadení v sieti LAN založenej na AAA

2.2.1 Klient

Zariadenie, ktorým sa užívateľ pripája do siete sa volá AAA klient. Typicky sa jedná o počítač pripojený pevným alebo bezdrôtovým spojením k prístupovému serveru.

2.2.2 Prístupový server

Prístupový server je hraničné zariadenie stabilne zapojené v sieti, ku ktorému sa pripája klient. Do ukončenia procesov autentizácie a autorizácie má klient právo komunikovať iba s prístupovým serverom a komunikácia s ostatnými zariadeniami siete je mu odopretá už na linkovej vrstve.

Po pripojení klienta ho prístupový server vyzve k autentizácii a ďalej už do tohto procesu nezasahuje. Následne posiela celú komunikáciu od klienta bezpečnostnému serveru a funguje tak ako most medzi dvomi spojeniami. Po úspešnej, resp. neúspešnej autentizácii na základe informácií od bezpečnostného servera prístupový server komunikáciu s klientom buď ukončí alebo pokračuje vo vykonávaní ďalších AAA služieb podľa potreby.

2.2.3 Bezpečnostný server

Bezpečnostný server je zariadenie, na ktorom bežia služby AAA. Počas procesu autentizácie komunikuje s klientom cez prístupový server a rozhoduje o povolení resp. zamietnutí žiadosti klienta o prístup do siete. Má prístup do databázy užívateľov, ktorá sa môže nachádzať buď priamo na serveri alebo môže byť umiestnená externe napr. na databázovom serveri (SQL server, LDAP server a pod.). Súčasne s údajmi potrebnými na autentizáciu užívateľov sú v databáze umiestnené aj údaje o ich právach a údaje potrebné k účtovaniu.

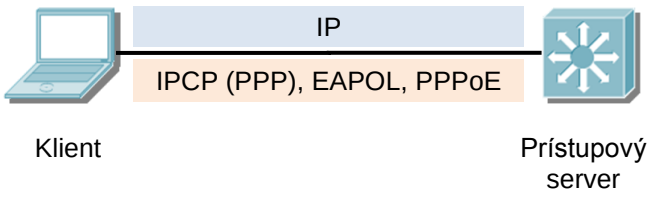
2.3 Komunikácia medzi AAA zariadeniami z hľadiska protokolov

Komunikácia medzi jednotlivými AAA zariadeniami využíva množstvo protokolov, ktoré sa líšia nielen svojou funkciou, ale aj vrstvou, na ktorej pracujú.

2.3.1 Komunikácia medzi klientom a prístupovým serverom

Použitie protokolov medzi klientom a prístupovým serverom úzko súvisí s typom pripojenia, pomocou ktorého sa klient do siete pripája, pričom všetky tieto protokoly pracujú na linkovej vrstve.

Najznámejšie protokoly linkovej vrstvy sú PPP, PPPoE a EAPOL.



Obrázok 2 – Vzťah linkových protokolov k protokolu IP

PPP (Point-to-Point Protocol)

Medzi najtypickejšie patrí protokol PPP, ktorý sa používa najmä pri vytáčaných spojeniach a umožňuje pokročilú autentizáciu tým, že v sebe zapuzdruje rôzne typy autentizačných protokolov (viď kapitola 2.3.3).

PPPoE (PPP over Ethernet)

Absencia podobných autentizačných možností pri pripájaní pomocou Ethernetu viedla k vzniku protokolu PPPoE (RFC 2516), tunelovaciemu protokolu, ktorý umožňuje preniesť pakety protokolu PPP v Ethernet rámcoch.

Keďže protokol PPP, sám zaobalený do paketov PPPoE, zapuzdruje všetky dáta prichádzajúce z vyšších vrstiev, dochádza k zvýšeniu réžie pri spracovávaní jednotlivých rámcov a k zníženiu množstva „užitočných“ dát prenesených sieťou.

EAPOL (EAP Over LAN)

Nakoľko sa PPPoE na vysokorýchlostných pripojeniach neujalo, konzorcium IEEE uviedlo v štandarde 802.1x protokol EAPOL s novým spôsobom autentizácie, ktorý riešil nevýhody spojené s použitím PPPoE.

Pretože je EAPOL používaný len na autentizáciu klienta, počas normálnej komunikácie nedochádza k prebytočnému zapuzdrovaniu paketov ako v prípade protokolu PPPoE.

Podrobnejšie informácie o tomto štandarde a protokole viď kapitola 3.

2.3.2 Komunikácia medzi prístupovým a bezpečnostným serverom

Komunikácia medzi prístupovým a bezpečnostným serverom sa deje až na aplikačnej vrstve, čo umožňuje využitie služieb nižších vrstiev ako napr. smerovania protokolom IP, šifrovania spojenia protokolom TLS alebo spoľahlivého prenosu dát protokolom TCP.

Hlavnou úlohou použitých protokolov je prenášať autentizačné informácie prevzaté od klienta prístupovým serverom prostredníctvom autentizačného protokolu až k bezpečnostnému serveru. Fungujú tak ako tunelovacie protokoly zapuzdrujúce

autentizačný protokol, pričom umožňujú prenášať dodatočné informácie dôležité pre celkový proces autentizácie, autorizácie alebo účtovania.

Medzi najpoužívanejšie protokoly patria RADIUS a TACACS+.

TACACS+ (Terminal Access Controller Access-Control System Plus)

Podľa (1) je TACACS+ rozšírením proprietárneho protokolu TACACS firmy Cisco špecifikovaného v RFC 1492. Umožňuje nezávislý prenos všetkých troch AAA služieb a tým dáva priestor pre modularitu implementácií klienta a servera. Na svoj prenos využíva protokol TCP, čím zaisťuje spoľahlivé spojenie medzi prístupovým a bezpečnostným serverom.

Kvôli zaisteniu lepšej integrity prenášaných dát podporuje obojstrannú autentizáciu autentizačným protokolom CHAP medzi prístupovým a bezpečnostným serverom a zároveň šifruje celé telo prenášaného paketu symetrickou šifrou.

RADIUS (Remote Authentication Dial In User Service)

Jedná sa o binárny protokol špecifikovaný v RFC 2865. Podľa (1) združuje procesy autentizácie a autorizácie, účtovanie je stále nezávislé. Oproti protokolu TACACS+ používa na prenos dát protokol UDP, čím zjednodušuje implementáciu prístupového a bezpečnostného servera. Nevýhodou tohto prístupu môže byť nespoľahlivosť spojenia.

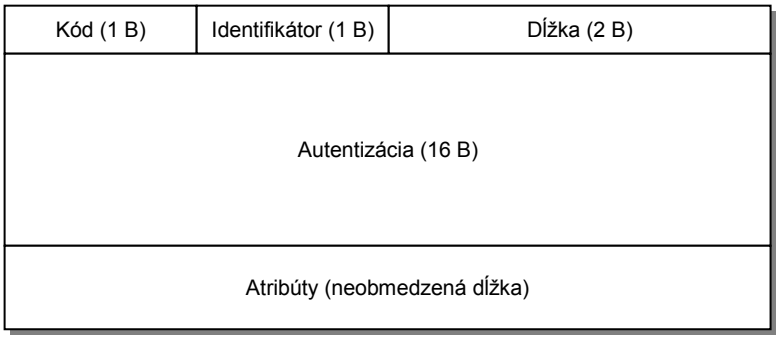
Podporuje len jednostrannú autentizáciu prístupového a bezpečnostného servera protokolom CHAP a zdieľaným kľúčom šifruje v pakete len prenášané heslo.

Využíva klasickú schému „žiadosť – odpoveď“, kedy je iniciátorom komunikácie vždy prístupový server, ktorý zasiela žiadosti serveru bezpečnostnému a ten na ne odpovedá.

Na prenos (tunelovanie) autentizačného protokolu využíva špecifické atribúty, ktoré sú súčasťou každého paketu (viď nižšie).

Formát paketu

Na základe informácií uvedených v (2) využíva protokol RADIUS rovnaký formát paketu pre všetky typy správ. Každá zo správ sa líši iba hodnotami častí paketu a svojou dĺžkou podľa počtu prenášaných atribútov. Presný formát správy viď Obrázok 3. Jednotlivé časti paketu majú nasledujúci význam.

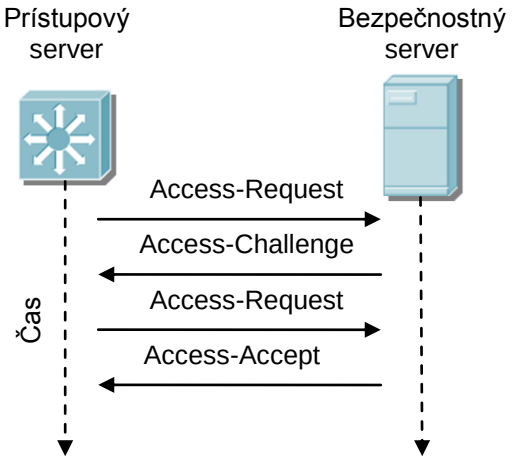


Obrázok 3 - Formát RADIUS paketu

Časť „*Kód*“ určuje typ správy, pričom procesu autentizácie a autorizácie sa týkajú nasledujúce typy:

- „Access-Request“ – prístupový server žiada bezpečnostný server o povolenie prístupu klienta do siete, resp. posiela dodatočné informácie o klientovi
- „Access-Challenge“ – bezp. server vyžaduje dodatočné informácie o klientovi
- „Access-Accept“ – bezp. server povoľuje klientovi prístup do siete
- „Access-Reject“ – bezp. server zamieta žiadosť o prístup klienta do siete

Príklad komunikácie RADIUS protokolom viď Obrázok 4.



Obrázok 4 - Príklad RADIUS komunikácie

„*Identifikátor*“ určuje, ktorej žiadosti je priradená ktorá odpoveď. Zaručí sa spoľahlivosť doručenia aj pri použití protokolu UDP. V časti „*Dĺžka*“ je uložená dĺžka celého paketu so všetkými atribútmi. Časť „*Autentizácia*“ zaručuje dôveryhodnosť zdroja správy.

Pomocou časti „*Atribúty*“ si prístupový a bezpečnostný server vymieňajú špecifické informácie týkajúce sa autentizácie, autorizácie alebo konfigurácie. Jedná sa o zoznam dvojíc s menom a hodnotou, ktorých podpora závisí od konkrétnych implementácií prístupového a bezpečnostného servera. Medzi atribúty využívané pri autentizácii patria napr.:

- „User-Name“ – meno užívateľa
- „EAP-Message“ – telo autentizačného protokolu EAP
- „User-Password“ – heslo užívateľa
- „Tunnel-Private-Group-Id“ – identifikátor VLAN siete, do ktorej patrí užívateľ
- Ďalšie atribúty sú popísane v (2) a (3).

2.3.3 Úloha autentizačných protokolov

Protokoly spomenuté v kapitolách 2.3.1 a 2.3.2 využívajú na autentizáciu klienta autentizačné protokoly, ktoré sú nezávislé na type spojenia medzi klientom a bezpečnostným serverom. Tieto protokoly sú zapuzdrené vo vyššie uvedených protokoloch a zvyšujú bezpečnosť prenosu citlivých dát od klienta napr. využívaním šifrovania hesla alebo použitím metód založených na TLS. Medzi najpoužívanejšie patria PAP, CHAP, EAP a i.

PAP (Password Authentication Protocol)

Jednoduchý protokol umožňujúci autentizáciu menom a heslom. Napriek svojej jednoduchosti sa v praxi nepoužíva, pretože nešifrovaný prenos dát tvorí značné bezpečnostné riziko.

CHAP (Challenge-Handshake Authentication Protocol)

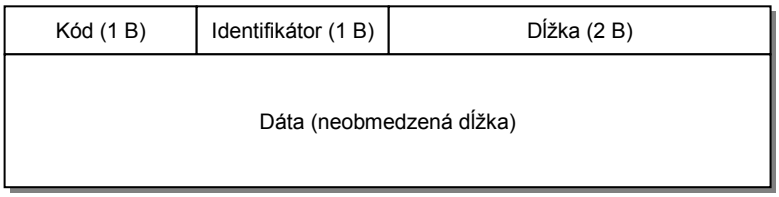
Jedná sa o autentizačný protokol, ktorý poskytuje lepšie zabezpečenie dát ako protokol PAP. Vo svojom tele neprenáša samotné heslo, ale špeciálny reťazec, ktorý vznikne zakódovaním niekoľkých častí správy a užívateľského hesla samotného.

EAP (Extensible Authentication Protocol)

Binárny autentizačný protokol, ktorý umožňuje zvoliť si autentizačný mechanizmus v závislosti na konkrétnej situácii a bezpečnostných požiadavkách. Je ľahko rozšíriteľný a komunikuje na základe schémy „žiadosť – odpoveď“, kde je iniciátorom komunikácie vždy prístupový server.

Formát paketu

Podľa (4) je formát paketu protokolu EAP rovnaký pre všetky typy správ. Presný formát viď Obrázok 5, pričom majú časti tohto paketu nasledujúci význam.



Obrázok 5 - Formát EAP paketu

Časť „*Kód*“ definuje typ prenášanej správy, pričom v (4) sú definované nasledujúce typy:

- „Request“ – žiadosť zasielaná prístupovým serverom
- „Response“ – odpoveď na žiadosť zaslaná klientom
- „Success“ – oznam klientovi o úspešnej autentizácii
- „Failure“ – oznam klientovi o neúspešnej autentizácii

„*Identifikátor*“ je časťou paketu, ktorá, podobne ako pri protokole RADIUS, určuje, ku ktorej žiadosti sa viaže ktorá odpoveď. Číslo reprezentujúce dĺžku celého paketu je uložená v časti „*Dĺžka*“.

Ak sa jedná o správu typu „Request“ alebo „Response“, v časti „*Dáta*“ sú prenášané údaje súvisiace so zvoleným autentizačným mechanizmom. Na jej začiatku je uložená informácia o podtype správy a za ňou nasledujú autentizačné dáta. Medzi základné podtypy správ patria napr.:

- „Identity“ – jedná sa o správu týkajúcu sa úvodnej identifikácie klienta
- „Nak“ – klient nesúhlasí zo zvoleným autentizačným mechanizmom ponúknutým prístupovým serverom

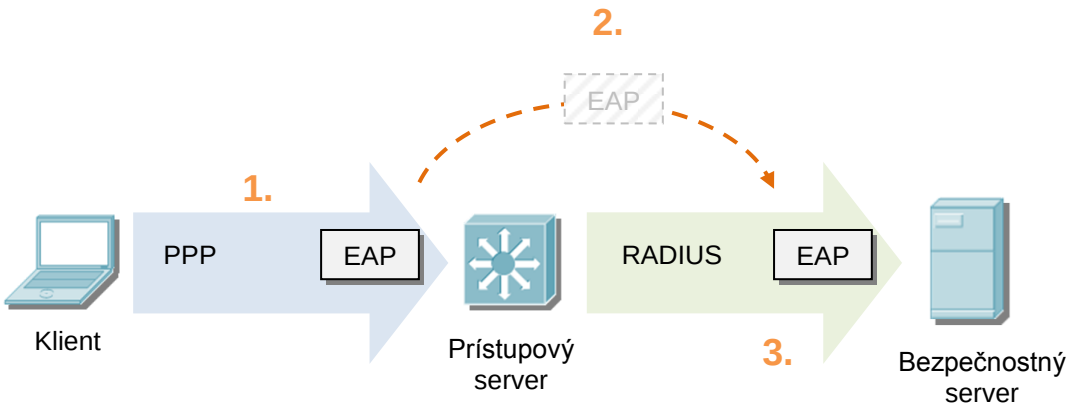
- „MD5-Challenge“ – správa sa týka autentizačného mechanizmu EAP-MD5

Proces prenosu EAP paketu od klienta až k bezpečnostnému serveru

Keďže je formát EAP paketu rovnaký pre každý autentizačný mechanizmus, prístupový server nemusí pre každý mechanizmus implementovať rôznu funkcionalitu. Stačí, ak funguje len ako agent, ktorý vybalí EAP paket z paketu protokolu použitého v komunikácii s klientom a zabalí ho do paketu protokolu, ktorým komunikuje s bezp. serverom. Proces má nasledujúci postup:

1. klient zašle prístupovému serveru EAP paket zapuzdrený v protokole linkovej vrstvy (napr. PPP)
2. prístupový server vybalí EAP paket z linkového protokolu a zapuzdrí ho do paketu vyššej vrstvy (napr. RADIUS)
3. prístupový server zašle paket bezpečnostnému serveru

Rovnakým spôsobom to funguje aj pri komunikácii v opačnom smere. Ilustrácia vyššie uvedeného procesu viď Obrázok 6.



Obrázok 6 – Proces prenosu EAP paketu od klienta k bezp. serveru

Prehľad autentizačných mechanizmov

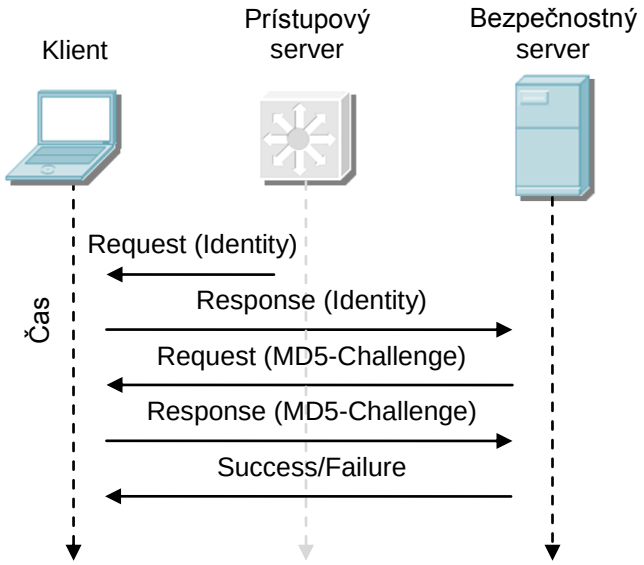
EAP-MD5 – najjednoduchší autentizačný mechanizmus, ktorý využíva na autentizáciu klienta MD5 hash. Keďže je hash posielaný cez sieť nešifrovane, je tento spôsob autentizácie zraniteľný voči útokom typu „sniffing“ (odchytávanie paketov) a slovníkovým útokom. Odporúča sa používať len v dôveryhodných sieťach.

EAP-TLS – bezpečný autentizačný mechanizmus autentizujúci klienta a server pomocou kryptografie verejných kľúčov (digitálny certifikát, Smart Card). Celá komunikácia je šifrovaná tunelom TLS, čo ju robí voči slovníkovým útokom rezistentnou.

EAP-TTLS – autentizačný mechanizmus, ktorý na autentizáciu bezp. servera používa rovnako ako mechanizmus EAP-TLS jeho digitálny certifikát (alebo Smart Card). Počas komunikácie vytvorí TLS tunel, v ktorom je schopný klienta autentizovať akoukoľvek inou autentizačnou metódou (PAP, CHAP a i.). Jeho bezpečnosť nesúvisí len so šifrovaním komunikácie tunelom TLS, ale závisí aj od odolnosti autentizačnej metódy použitej vo vnútri tunela.

EAP-PEAP – jedná sa o veľmi podobný autentizačný mechanizmus ako EAP-TTLS. Z hľadiska funkcií ponúka rovnaké možnosti, pričom sa líši len v spôsobe zabaľovania správ do TLS tunela. Viac informácií viď (5).

Príklad komunikácie protokolom EAP viď Obrázok 7.



Obrázok 7 – Príklad EAP komunikácie pri použití autentizačného mechanizmu EAP-MD5 (v zátvorkách je uvedený podtyp správy)

3 ŠTANDARD 802.1X

V tejto kapitole sa čitateľ zoznámi so štandardom 802.1x, ktorý definuje proces autentizácie klienta pripojeného do siete pomocou LAN technológií. Definuje úlohy zariadení, vzťahy medzi nimi, ich správanie sa pred, počas a po procese autentizácie a v neposlednom rade spôsob ich komunikácie protokolom EAPOL.

3.1 Úvod do problematiky

Proces autorizácie a účtovania prebieha len medzi prístupovým a bezpečnostným serverom a vďaka použitým protokolom aplikačnej vrstvy je táto komunikácia na fyzickom spojení nezávislá. Do procesu autentizácie je však zainteresovaný aj klient, pričom proces v komunikácii medzi klientom a prístupovým serverom používa protokoly linkovej vrstvy závislé na technológii, akou je klient do siete pripojený.

Aby bolo možné klienta autentizovať, musí použitý linkový protokol podporovať prenos autentizačných protokolov. Takýmto protokolom je napr. protokol PPP prítomný v spojeniach typu „point-to-point“, ktorý má schopnosť autentizačný protokol v sebe zapuzdrovať. Počas počiatočnej fázy komunikácie dohodne medzi komunikujúcimi stranami druh autentizačného protokolu a následne ho v ďalšej fáze komunikácie použije na autentizáciu.

Problém nastáva v autentizácii klientov pripojených k prístupovému serveru technológiami LAN. Protokoly linkovej vrstvy technológii 802.11 alebo 802.3 totiž nemajú podporu zapuzdrenia autentizačného protokolu a teda priamo neumožňujú využívať službu autentizácie. Ako bolo uvedené v kapitole 2.3.1, použitie protokolu PPPoE na tieto účely sa ukázalo byť nevýhodné, hoci poskytovalo rovnaké možnosti autentizácie ako samotné PPP. Riešením sa stal štandard konzorcia IEEE s označením 802.1x.

3.2 Autentizácia na základe portu

Prostredie LAN je charakterizované ako prostredie so zariadeniami spojenými zdieľaným médiom, na ktoré môže pristupovať viac zariadení a autentizácia zariadení

v takomto prostredí sa deje na základe hardwarovej adresy im pridelenej. Ako bolo uvedené v kapitole 1, založiť bezpečnosť siete na autentizácii tohto typu nie je vždy výhodné.

Každé zariadenie pripájajúce sa do siete má však aspoň jeden bod pripojenia zvaný port. Ak sa jedná o pevné spojenie, spojenie končí vo fyzických portoch umiestnených na spojovaných zariadeniach. Avšak ak sa jedná o spojenie bezdrôtové, tiež možno považovať jeho konce za porty, ale virtuálne.

Štandard 802.1x definuje nový spôsob autentizácie, v ktorom sa klient identifikuje nie hardwarovou adresou, ale portom na prístupovom serveri, do ktorého sa pripája. Takto definované spojenie získava charakter spojenia typu „point-to-point".

3.2.1 Princíp operácie

Nakoľko port ako taký je iba fyzické ukončenie spojenia, ktoré nemá v sebe žiadnu logiku, je mu pridelená tzv. *prístupová entita* (ďalej len entita), ktorá ovláda jeho stav a prostredníctvom ktorej sú vykonávané jednotlivé služby architektúry AAA. Entita môže v procese autentizácie nadobúdať dve úlohy:

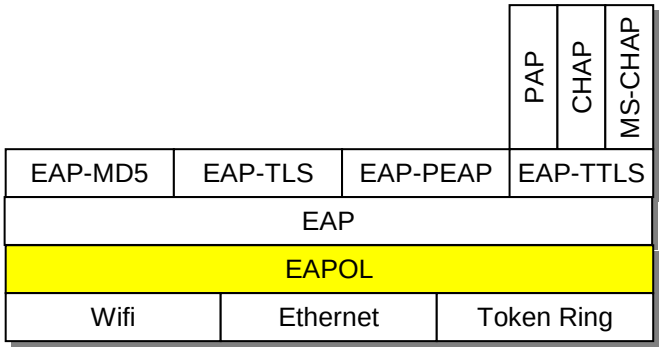
- *žiadateľ* (angl. supplicant) – nadobúda ho entita portu na klientovi
- *overovateľ* (angl. authenticator) – nadobúda ho entita portu na prístupovom serveri

Port na strane žiadateľa ako aj port na strane overovateľa môže byť v stave „*autorizovaný*" alebo „*neautorizovaný*". Komunikácia cez autorizovaný port prebieha bez obmedzení na všetkých vrstvách, ale pokiaľ sa port nachádza v stave „neautorizovaný", komunikácia cezeň je obmedzená, pričom môže cez port posielať dáta iba jeho prístupová entita.

Po pripojení klienta k prístupovému serveru sú porty na oboch stranách v stave „neautorizovaný". Žiadateľ alebo overovateľ začne proces autentizácie protokolom EAPOL, pričom je autentizačný protokol EAP ďalej posielaný bezpečnostnému serveru (viď Obrázok 6). Po úspešnom skončení procesu autentizácie a procesu autorizácie sa oba porty dostanú do stavu „autorizovaný" a klientovi je umožnené bez obmedzení komunikovať s ostatnými zariadeniami v sieti.

3.3 Protokol EAPOL (EAP Over LAN)

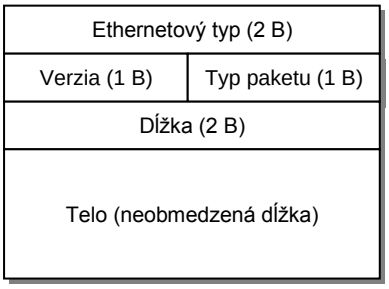
Podľa (6) je protokol EAPOL protokolom pracujúcim na LLC vrstve nad Ethernetom, Wifi alebo technológiou Token Ring. Jeho úlohou je zapuzdrovať pakety autentizačného protokolu EAP a umožniť tak jeho prenos aj na protokoloch LAN technológií, ktoré túto schopnosť natívne nemajú. Vzťah protokolov EAP a EAPOL k ostatným technológiám viď Obrázok 8.



Obrázok 8 – Vzťah protokolov EAP a EAPOL

3.3.1 Formát paketu

Formát paketu sa líši podľa použitej LAN technológie. Štandard 802.1x definuje rôzny formát pre 802.3/Ethernet a pre Token Ring/FDDI. Presný formát paketu pre 802.3 viď Obrázok 9.



Obrázok 9 – Formát paketu EAPOL pre 802.3/Ethernet

Časť „*Ethernetový typ*“ udáva typ protokolu neseného v rámci technológie 802.3. Podľa (7) sa v rámcoch technológie Ethernet nenachádza pole, ktoré by určovalo

typ zapuzdreného paketu a práve z tohto dôvodu sa do EAPOL paketov explicitne udáva hodnota 0x888E, čo je podľa (8) číslo pridelené konzorciom IEEE označujúce protokol EAPOL. Na technológii Ethernet II sa táto časť vynecháva, pretože typ zapuzdreného paketu je už súčasťou Ethernet II rámca.

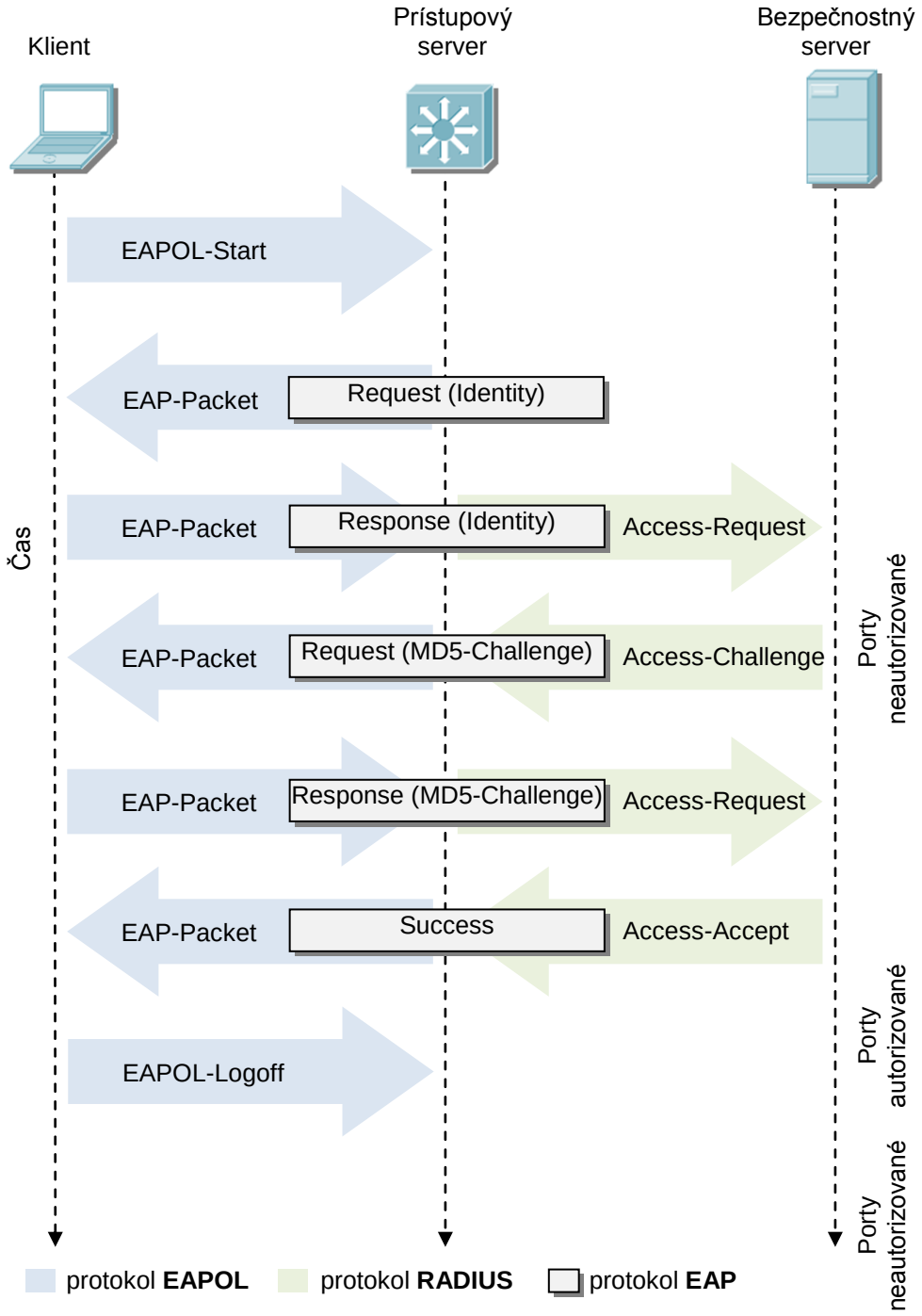
Typ nesenej správy sa nachádza v oblasti s názvom „*Typ paketu*“. Podporované typy sú nasledujúce:

- „EAP-Packet“ – indikuje, že rámec EAPOL prenáša paket protokolu EAP
- „EAPOL-Start“ – klient žiada prístupový server o autentizáciu
- „EAPOL-Logoff“ – klient žiada prístupový server o odhlásenie
- „EAPOL-Key“ – rámec EAPOL prenáša kľúč pri použití zabezpečenia WPA technológie 802.11 (pre viac informácii o vzťahu protokolu EAPOL k WPA viď (9))
- „EAPOL-Encapsulated-ASF-Alert“ – používa sa na prenos špecifických SNMP nevyžiadaných správ (angl. „traps“) cez neautorizovaný port prístupového servera

Číslo určujúce verziu protokolu EAPOL je v časti „*Verzia*“. V časti „*Dĺžka*“ je uložená celková dĺžka EAPOL rámca a v časti „*Telo*“ sa nachádzajú prenášané dáta.

3.3.2 Príklad autentizácie

Príklad autentizácie klienta protokolom EAPOL viď Obrázok 10.



Obrázok 10 - Príklad autentizácie mechanizmom EAP-MD5 vyvolanej žiadateľom

4 NÁVRH SIETE IBNS

Úlohou tejto kapitoly je ukázať čitateľovi praktický návrh bezpečnostnej politiky siete, ktorá bude na poskytovanie služieb autentizácie a autorizácie využívať technológie uvedené v kapitolách predchádzajúcich. Popisuje špecifikáciu siete, zoznamuje čitateľa s použitými zariadeniami a taktiež popisuje použitý softvér ako na strane bezpečnostného serveru, tak na strane jednotlivých klientov.

4.1 Neformálna špecifikácia siete

Špecifikovaná sieť má charakter LAN siete mobilnej kancelárie. Kancelária sa nachádza na dvoch poschodiach, pričom možnosť pripojiť sa je dostupná pre každé poschodie zvlášť.

Keďže niektorí užívatelia siete kancelárie vlastnia notebook, je im umožnené pripojiť sa do siete podľa potreby na jednotlivých poschodiach, pričom sa nenaruší integrita bezpečnosti siete. Konvergencia bezpečnosti siete po takomto presune sa deje bez zásahu administrátora úplne automaticky.

Z hľadiska činnosti v sieti sú užívatelia rozdelení na *pracovníkov* a *administrátorov*. Pracovníci využívajú sieť na každodennú prácu, pričom nemajú možnosť pristupovať k zariadeniam siete ako sú prepínače, smerovače, bezpečnostné servery a pod. Administrátori majú rovnaké práva ako pracovníci, avšak oproti nim môžu spravovať jednotlivé zariadenia v LAN napr. pomocou spojenia Telnet.

Každému užívateľovi je priradené unikátne meno a heslo, ktorým sa po pripojení do siete identifikuje. Zoznam užívateľov (viď Tabuľka 1), ich práv a ich hesiel je kvôli možnosti neskoršej integrácie umiestnený na univerzálnom databázovom serveri LDAP.

Meno užívateľa	Prihlasovacie meno	Prihlasovacie heslo	Typ
Marek	marek	hello	administrátor
Andrej	andrej	hello	administrátor
Michal	michal	hello	pracovník
Zuzana	zuzana	hello	pracovníčka

Tabuľka 1 - Zoznam užívateľov siete

4.2 Návrh bezpečnostnej politiky

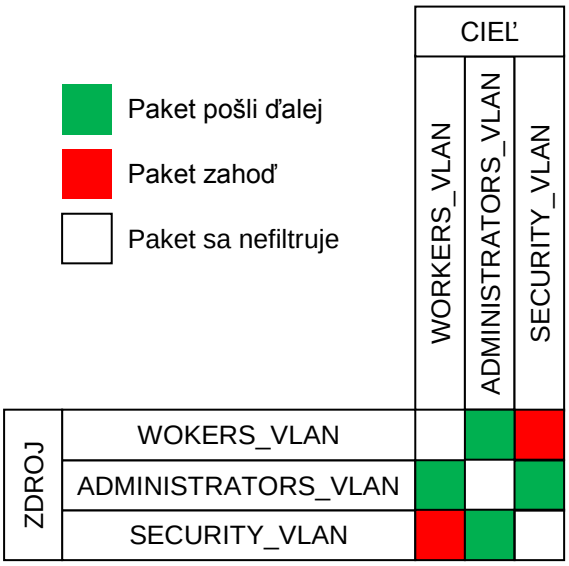
Prvým bodom zabezpečenia je autentizácia klienta. Keďže sa jedná o sieť LAN a klienti sú autentizovaní prihlasovacím menom a heslom užívateľa, je nutné využiť autentizáciu na základe portu definovanú v štandarde 802.1x s autentizačným protokolom EAP. Dôveryhodnosť užívateľov zjednodušuje proces autentizácie tým, že dovoľuje použiť menej zabezpečený autentizačný mechanizmus EAP-MD5. Pre neskoršiu podporu bezdrôtového pripojenia je užitočné nakonfigurovať sieťové zariadenia tak, aby boli schopné autentizovať klienta aj mechanizmom PEAP, ktorý zabezpečuje prenos identifikačných údajov v prostredí Wifi omnoho viac.

Druhým bodom je obmedzenie prístupu pracovníkov k určitým zariadeniam za pomoci VLAN a paketového filtrovania. Po úspešnej autentizácii klienta je port prístupového servera, do ktorého je klient pripojený, pridelený do VLAN na základe informácii z databázy užívateľov. Administrátori, pracovníci a zariadenia sú rozdelení do nasledujúcich virtuálnych sietí:

- WORKERS_VLAN – virtuálna sieť pracovníkov
- ADMINISTRATORS_VLAN – virtuálna sieť administrátorov
- SECURITY_VLAN – virtuálna sieť zariadení

Výhodnosť definície osobitnej VLAN pre každý typ zamestnanca spočíva v jednoduchej identifikácii cieľa a zdroja správy. Keďže každá z uvedených VLAN má definovanú svoju vlastnú IP adresu, určiť kto sa snaží s kým komunikovať je otázkou zistenia adresy zdrojovej a adresy cieľovej siete. Potom stačí aplikovať pravidlo filtrujúce komunikáciu na základe IP adresy na port smerovača smerujúceho pakety medzi virtuálnymi sieťami.

Matica pre filtrovanie komunikácie medzi jednotlivými virtuálnymi sieťami viď Obrázok 11.



Obrázok 11 – Matica pre filtrovanie komunikácie medzi jednotlivými virtuálnymi sieťami

4.3 Voľba zariadení

Sieť pozostáva z piatich zariadení. Na pripojenie klientov do siete je na každom poschodí umiestnený viacvrstvový prepínač Cisco Catalyst 2950, ktorý je schopný pracovať s VLAN a podporuje autentizáciu štandardom 802.1x.

Na smerovanie komunikácie medzi jednotlivými VLAN sieťami je použitý smerovač Cisco 2800, ktorý plní zároveň funkciu paketového filtra a tým zabraňuje komunikácii pracovníkov so zariadeniami na úrovni sieťovej vrstvy.

Funkciu bezpečnostného a databázového servera plní jedno zariadenie typu PC, ktoré je spolu s prístupovými prepínačmi jednotlivých poschodí a smerovačom pripojené do centrálneho viacvrstvového prepínača (tiež Cisco Catalyst 2950).

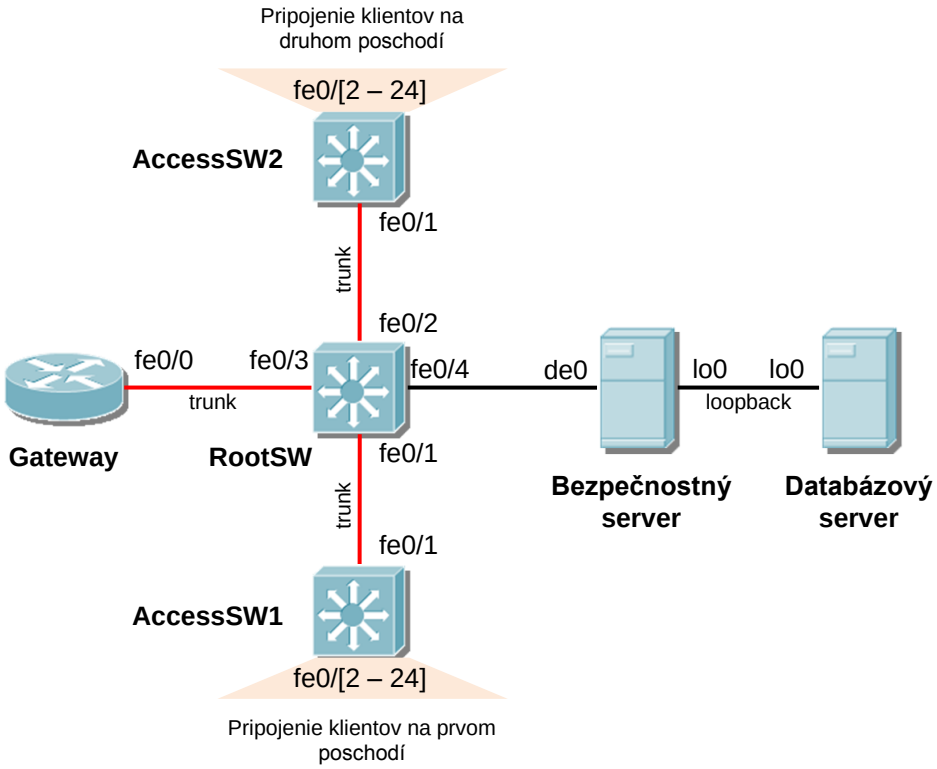
Verzia IOS jednotlivých Cisco zariadení viď Tabuľka 2.

Zariadenie	Verzia IOS
Cisco Catalyst 2950	12.1 (22) EA9
Cisco 2800	12.4 (1C)

Tabuľka 2 - Verzia IOS jednotlivých Cisco zariadení

4.4 Schéma siete

Detailná schéma siete viď Obrázok 12. Sú v nej uvedené informácie o zapojení jednotlivých zariadení. Spolu s rozhraniami sú na schéme zobrazené aj údaje o type spojenia medzi jednotlivými zariadeniami.



Obrázok 12 – Schéma siete

Bezpečnostný a databázový server sú chápané ako zariadenia virtuálne, hoci, ako je uvedené v kapitole 4.3, bežia ako programy na jednom fyzickom zariadení (PC). Bezpečnostný server komunikuje s ostatnými fyzickými zariadeniami siete cez fyzické rozhranie de0 a z databázovým serverom prostredníctvom lokálneho rozhrania lo0.

4.5 Rozdelenie adresového priestoru

Kvôli zjednodušeniu je IP adresácia jednotlivých virtuálnych sietí a zariadení (viď Tabuľka 3 a Tabuľka 4) založená na privátnych adresách triedy C s hodnotou prvých dvoch oktetov 192 a 168.

Adresy sú priradené rozhraniam na zariadeniach, pričom rozhranie fe0/0 na smerovači Gateway je rozdelené na podrozhrania pre každú VLAN.

Číslo	Názov	IP adresa / maska
10	SECURITY_VLAN	192.168.10.0 / 24
20	ADMINISTRATORS_VLAN	192.168.20.0 / 24
30	WORKERS_VLAN	192.168.30.0 / 24

Tabuľka 3 – IP adresy VLAN

Názov zariadenia	IP adresa	Rozhranie
Bezpečnostný server	192.168.10.254 127.0.0.1	de0 lo0
Gateway	192.168.10.1 192.168.20.1 192.168.30.1	fe0/0.1 fe0/0.2 fe0/0.3
RootSW	192.168.10.10	vlan10
AccessSW1	192.168.10.11	vlan10
AccessSW2	192.168.10.12	vlan10
Databázový server	127.0.0.1	lo0

Tabuľka 4 – IP adresy zariadení

4.6 Voľba softvéru

4.6.1 Bezpečnostný server

Nakoľko v dobe písania tejto bakalárskej práce nebolo možné nájsť implementáciu servera protokolu TACACS+, ktorá by podporovala autentizáciu protokolom EAP a teda autentizáciu 802.1x, rozhodol som sa využiť server protokolu RADIUS.

Bezpečnostný server tvorí server balíka FreeRADIUS verzie 1.1.4 bežiaci na PC s operačným systémom FreeBSD verzia 6.1. Má v sebe zabudovanú podporu rôznych autentizačných protokolov využívajúcich rôzne autentizačné mechanizmy.

Údaje o užívateľoch získava buď z lokálneho súboru alebo z niektorého z podporovaných databázových serverov ako napr. LDAP alebo SQL. Je jednoducho konfigurovateľný pomocou niekoľkých konfiguračných súborov a v prípade LDAP je schopný spracovať získané záznamy pomocou nadefinovaných filtrov.

4.6.2 Databázový server

Funkciu databázového servera plní server zahrnutý v balíku OpenLDAP verzie 2.3.34, ktorý beží paralelne s bezpečnostným serverom na tom istom PC.

Údaje o užívateľoch uskladňuje v stromoch s vopred nadefinovanou štruktúrou prístupných pomocou protokolu LDAP.

4.6.3 Softvér na klientoch

Použitie softvéru na komunikáciu medzi prístupovým serverom a klientom úzko súvisí s použitým operačným systémom bežiacim na klientovi.

Operačný systém Microsoft Windows XP má zabudovanú podporu autentizácie 802.1x a to konkrétne mechanizmami EAP-MD5 (prihlasovacie meno a heslo), EAP-TLS (verejný certifikát, Smart Card) a EAP-PEAP (rôzne). Po pripojení klienta sa automaticky zobrazí podľa zvoleného mechanizmu okno umožňujúce užívateľovi zadať potrebné údaje (viď Obrázok 13).

Obrázok 13 –Okno na zadanie prihlasovacích údajov vo Windows XP

Klienti pracujúci na systémoch založených na UNIX-e musia siahnuť po softvéri z tretích strán. Medzi najpoužívanejšie patrí program WPA Supplicant, ktorý poskytuje podobné možnosti autentizácie ako Microsoft Windows XP. Beží na pozadí v systéme a v prípade, že je požadovaná autentizácia autentizuje klienta na základe informácii uložených v konfiguračnom súbore. Testovaná verzia bola 0.5.7.

5 IMPLEMENTÁCIA SIETE

Táto kapitola sa venuje implementácii siete navrhnutej v kapitole 4. Popisuje konfiguráciu jednotlivých sieťových zariadení a softvéru ako na strane pripájajúcich sa klientov, tak na strane oboch serverov.

Informácie potrebné na konfiguráciu som čerpal z (1), (3), (10), (11), (12) a (13). Všetky spomenuté konfiguračné súbory sa nachádzajú v prílohe A.

5.1 Konfigurácia zariadení

Nasledujúce podkapitoly predstavujú individuálnu konfiguráciu každého zo zapojených zariadení.

5.1.1 Prepínače AccessSW1 a AccessSW2

Prepínače AccessSW1 a AccessSW2 majú úlohu prístupového servera a preto sú nakonfigurované tak, aby dokázali pripojeného klienta autentizovať a zaradiť do príslušnej virtuálnej siete. Konfigurácia je uložená v súboroch AccessSW1.cfg a AccessSW2.cfg.

Popis konfigurácie

1. Konfigurácia jednotlivých VLAN

Aby mohol prepínač dynamicky priraďovať jednotlivé rozhrania do VLAN, musí poznať ich názvy a čísla (viď Tabuľka 3). Tieto údaje sa neuchovávajú v konfiguračnom súbore, ale v lokálnej databáze na prepínači.

2. Nastavenia AAA

Po založení nového AAA modelu sú vytvorené základné zoznamy autentizačných a autorizačných metód, ktoré sa majú na prepínači používať. Ako

autentizácia klienta štandardom 802.1x, tak aj autorizácia pri prístupe klienta do siete komunikujú so serverom RADIUS, ktorý je špecifikovaný v konfigurácii spolu s IP adresou a zdieľaným heslom používaným počas komunikácie („testing123“). Autentizácia pri prihlásení na prepínač terminálom využíva heslo nastavené na konkrétnom konzolovom alebo terminálovom rozhraní.

```
!
aaa new-model
aaa authentication login default line
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

Výpis 1 – Fragment konfigurácie AAA

3. Konfigurácia rozhraní

Rozhranie fe0/1 je rozhraním, ktoré prenáša dáta zo všetkých VLAN. Používa na to protokol 802.1q a jeho typ je nastavený na typ „trunk“.

Ostatné fyzické rozhrania sú určené na pripojenie klientov. Ich typ je preto typ „access“ s autentizáciou štandardom 802.1x.

Aby mohol prepínač v úlohe prístupového servera, komunikovať na sieťovej vrstve s bezpečnostným serverom a zároveň bol adresovateľný pri neskoršej konfigurácii spojením Telnet, je zapnutému virtuálnemu rozhraniu vlan10 pridelená IP adresa (viď Tabuľka 4). Fragment konfigurácie rozhraní fe0/1 a fe0/2 viď Výpis 2.

```
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
```

Výpis 2 – Fragment konfigurácie rozhraní zariadenia AccessSW1

4. Heslá

Kvôli bezpečnosti je na všetkých virtuálnych termináloch a na prechode do privilegovaného režimu nastavené heslo.

5.1.2 Prepínač RootSW

Prepínač RootSW funguje ako spojovací bod spájajúci smerovač, bezpečnostný server a oba prístupové prepínače. Sám aktívne nevykonáva žiadne služby AAA. Jeho konfigurácia sa nachádza v súbore RootSW.cfg

Popis konfigurácie

1. Konfigurácia jednotlivých VLAN

Prepínač pracuje s rámcami jednotlivých VLAN a preto sú do databázy pridané informácie o všetkých VLAN podobne ako v prípade prepínačov AccessSW1 a AccessSW2.

2. Konfigurácia rozhraní

Keďže sa rozhraniami fe0/1, fe0/2 a fe0/3 prenášajú protokolom 802.1q pakety všetkých VLAN, je ich typ nastavený na typ „trunk“.

Rozhranie fe0/4, do ktorého sa pripája bezpečnostný server je kvôli zabezpečeniu staticky priradené do SECURITY_VLAN.

Aby mohol byť prepínač konfigurovateľný aj cez spojenie Telnet, je aktivované rozhranie vlan10 rovnako ako v prepínačoch AccessSW1 a AccessSW2 a je mu priradená adresa. Konfigurácia jednotlivých rozhraní viď Výpis 3.

```
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
```

Výpis 3 – Konfigurácia rozhraní prepínača RootSW

3. Heslá

Na všetkých virtuálnych termináloch a na prechode do privilegovaného režimu je nastavené heslo.

5.1.3 Smerovač Gateway

Smerovač Gateway smeruje a filtruje pakety medzi jednotlivými virtuálnymi sieťami. Podobne ako RootSW, ani on priamo nevykonáva žiadne z AAA služieb. Konfigurácia viď súbor Gateway.cfg.

Popis konfigurácie

1. Konfigurácia rozhraní

Aby mohli byť smerované pakety jednotlivých virtuálnych sietí tým istým rozhraním, akým do smerovača vstúpili, je rozhranie fe0/0 rozdelené na podrozhrania. Pre každú VLAN je určené jedno podrozhranie, ktorému je pridelená adresa z adresového priestoru virtuálnej siete. Pakety sú zapuzdrované protokolom 802.1q.

2. Nastavenia paketového filtra

Paketový filter zabraňuje komunikácii medzi klientmi z WORKERS_VLAN a zariadeniami zo SECURITY_VLAN. Pozostáva z jedného prístupového zoznamu (angl. ACL) aplikovaného na výstup z podrozhrania fe0/0.1.

```
!
access-list 1 permit 192.168.20.0 0.0.0.255
!
```

Výpis 4 – Konfigurácia prístupového zoznamu na smerovači Gateway

3. Heslá

Rovnako ako v prípade konfigurácie predchádzajúcich zariadení, je na všetkých virtuálnych termináloch a na prechode do privilegovaného režimu nastavené kvôli bezpečnosti heslo.

5.2 Konfigurácia softvéru

Proces konfigurácie softvéru pozostával z niekoľkých bodov. Prvým bodom bolo nastavenie parametrov LDAP adresára a jeho naplnenia informáciami o užívateľoch siete. Druhým bodom bola konfigurácia samotného bezpečnostného servera, aby bol schopný spracovávať požiadavky na autentizáciu rôznymi autentizačnými mechanizmami protokolu EAP a po autentizácii poslať prístupovému serveru potrebné autorizačné informácie. V poslednom bode bolo potrebné nastaviť parametre softvéru na jednotlivých klientoch ako napr. použitý autentizačný mechanizmus alebo použitie certifikátu na overenie identity bezpečnostného servera.

Nasledujúce podkapitoly popisujú výslednú konfiguráciu jednotlivých softvérových prvkov siete.

5.2.1 Konfigurácia LDAP adresára

Súčasťou balíka OpenLDAP je server „slapd“ a ďalšie pomocné nástroje určené na prácu s údajmi v databáze. Celá konfigurácia pozostáva z niekoľkých súborov implicitne umiestnených v systéme FreeBSD v adresári „/usr/local/etc/openladp“.

Popis konfigurácie

1. Konfigurácia pripojenia k LDAP serveru

Aby nebolo treba pri práci s pomocnými nástrojmi ako napr. „ldapadd“ neustále do príkazového riadku zadávať údaje týkajúce sa pripojenia k LDAP serveru, uložia sa do súboru „ldap.conf“.

2. Konfigurácia servera „slapd“

Nastavenia servera „slapd“ sú uložené v súbore „slapd.conf“ a súvisia najmä so spravovanou databázou. Koreňovým uzlom v strome je uzol „mobileoffice.com“ a právo upravovať databázu má každý LDAP klient autentizovaný ako „Admin.mobileoffice.com“ s heslom „secret“. Fragment súboru „slapd.conf“ viď Výpis 5.

```
suffix          "dc=mobileoffice,dc=com"
rootdn          "cn=Admin,dc=mobileoffice,dc=com"
rootpw          secret
```

Výpis 5 – Konfigurácia parametrov databázy

Keďže dáta adresára tvoria objekty, server musí poznať presnú štruktúru triedy, ktorej sú inštanciami. Definícia tried objektov a ich atribútov je uložená v súboroch schém.

Množinou tried objektov špecifikovaných v základnom súbore „core.schema“ by bolo zložité vytvoriť databázu užívateľov, ich prihlasovacích mien, hesiel, identifikácie VLAN a pod. a preto je vhodné vyžiť schému distribuovanú s balíkom FreeRADIUS. Jej súbor nesie názov „radius.schema“ a do konfigurácie servera je zahrnutý parametrom „include“.

Definuje 2 triedy, ktoré abstrahujú práve reálneho užívateľa: „radiusprofile“ a „radiusObjectProfile“. Názvy ich atribútov plne korešpondujú s názvami atribútov protokolu RADIUS (viď kapitolu 2.3.2).

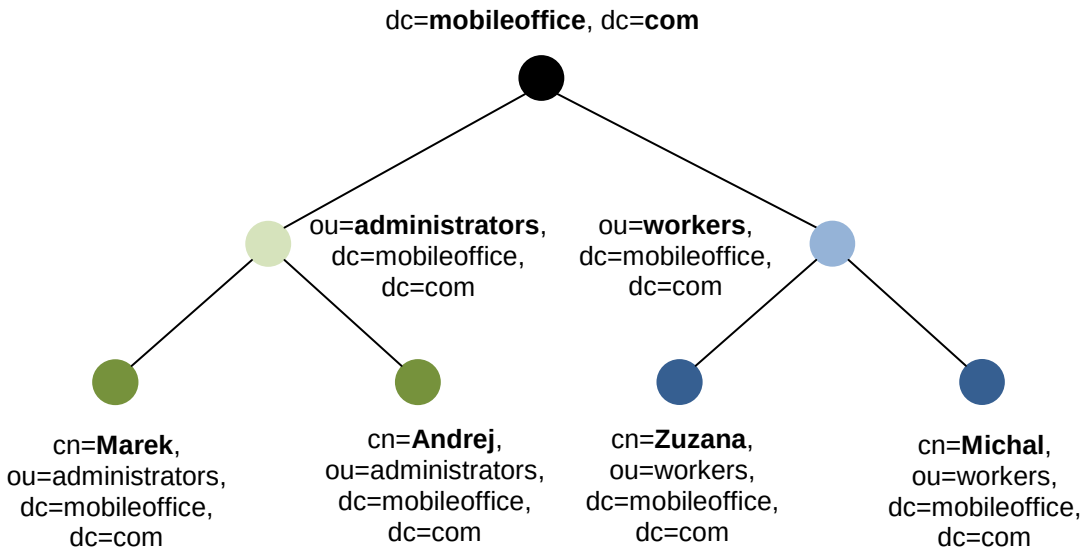
3. Dáta adresára

Objekty adresára sú vzájomne hierarchicky poprepájané do stromu. Sú spolu s ich prepojeniami definované v tzv. LDIF súboroch, ktoré boli následne importované do databázy nástrojom „ldapadd“.

Každý objekt je identifikovaný atribútom „dn“ (angl. Distinguished Name), ktorý sa skladá z mena objektu a atribútov „dn“ objektov predchádzajúcich (pri prechode stromom zhora nadol).

Jednotlivé objekty databázy mobilnej kancelárie (viď Obrázok 14) sú definované v súbore „mobileoffice.com.ldif“. Koreňovým objektom adresára je objekt „mobileoffice.com“, ktorý spolu s objektmi „administrators.mobileoffice.com“ a „workers.mobileoffice.com“ pôsobí ako organizačná jednotka štruktúrujúca databázu.

Objekt „administrators.mobileoffice.com“ má pritom funkciu vstupného bodu do vetvy s administrátormi a „workers.mobileoffice.com“ do vetvy s pracovníkmi.



Obrázok 14 – Hierarchia objektov v databáze mobilnej kancelárie

Každého užívateľa reprezentuje objekt tried „radiusObjectProfile“ a „radiusprofile“. Pre potreby autentizácie a autorizácie sú u každého užívateľa nastavené hodnoty nasledujúcich atribútov:

- „dn“ – identifikátor objektu
- „objectClass“ – trieda, ktorej je objekt inštanciou
- „cn“ – meno užívateľa
- „uid“ – prihlasovacie meno

- „userPassword“ – prihlasovacie heslo
- „description“ – slovný popis objektu

Na uloženie informácií o VLAN, do ktorej užívateľ patrí slúžia atribúty „radiusTunnelMediumType“, „radiusTunnelType“ a „radiusTunnelPrivateGroupId“. Podľa (14) majú mať tieto atribúty nasledujúce hodnoty:

- „radiusTunnelMediumType“ – IEEE-802 (6)
- „radiusTunnelType“ – VLAN (13)
- „radiusTunnelPrivateGroupId“ – názov VLAN siete

Výpis 6 zobrazuje definíciu objektu užívateľa Mareka zo súboru „mobileoffice.com.ldif“.

```
dn: cn=Marek,ou=administrators,dc=mobileoffice,dc=com
objectClass: radiusprofile
objectClass: radiusObjectProfile
cn: Marek
uid: marek
description: Administrator Marek
userPassword: hello
radiusTunnelMediumType: IEEE-802
radiusTunnelType: VLAN
radiusTunnelPrivateGroupId: ADMINISTRATORS_VLAN
```

Výpis 6 – Definícia objektu Marek.administrators.mobileoffice.com zo súboru „mobileoffice.com.ldif“

5.2.2 Konfigurácia bezpečnostného servera

Súčasťou balíka FreeRADIUS je server „radiusd“, ktorý beží ako program v systéme a obsluhuje požiadavky od prístupových serverov. Je silne modulárny, pričom proces vybavenia žiadosti pozostáva z postupného prechodu jednotlivými modulmi. Moduly spracovávajú žiadosť v presnom poradí a určenie nasledujúceho modulu sa dynamicky odvíja od výsledku operácie modulu predchádzajúceho.

Jeho nastavenia sú uložené vo viacerých súboroch implicitne umiestnených v operačnom systéme FreeBSD v adresári „/usr/local/etc/raddb“.

Popis konfigurácie

1. Nastavenia týkajúce sa prístupových serverov

Nastavenia typov prístupových serverov AccessSW1 a AccessSW2 spolu so zdieľaným heslom používaným počas komunikácie sa nachádzajú v súbore „clients.conf“. Príslušnosť nastavení k jednotlivých prístupovým serverom je určená ich IP adresami. Konfigurácia parametrov prístupového servera viď Výpis 7.

```
client 192.168.10.12 {
      secret = testing123
      shortname = AccessSW2
      nastype = cisco
}
```

Výpis 7 – Konfigurácia parametrov prístupového servera AccessSW2

2. Konfigurácia autentizačných mechanizmov

Keďže sieť mobilnej kancelárie využíva na autentizáciu štandard 802.1x, hlavným autentizačným protokolom je protokol EAP. O autentizáciu týmto protokolom sa stará osobitný modul, ktorého konfigurácia sa nachádza v súbore „eap.conf“ a umožňuje konfigurovať jednotlivé mechanizmy tohto protokolu.

Základným autentizačným mechanizmom použitým v sieti mobilnej kancelárie je mechanizmus EAP-MD5.

Server „radiusd“ je nakonfigurovaný tak, aby v prvej poslanej žiadosti klienta vyzval na autentizáciu práve týmto mechanizmom. Ak to však klientovi nevyhovuje (ako napr. v prípade pripojenia pomocou Wifi), zašle serveru správu typu „Nak“, v ktorej špecifikuje požadovaný mechanizmus.

Kvôli rozšírenej podpore bezdrôtového spojenia je nevyhnutná konfigurácia aj ďalších mechanizmov ako EAP-TLS a EAP-PEAP.

EAP-TLS je autentizačný mechanizmus, ktorý na vzájomnú autentizáciu klienta a servera využíva metód verejnej kryptografie. Pri vytváraní šifrovaného tunela medzi klientom a bezp. serverom využíva verejný certifikát servera podpísaný certifikačnou autoritou, ktorej dôveruje. Zároveň sa ním server autentizuje klientovi.

Autentizácia klienta certifikátom odstraňuje riziká súvisiace s použitím hesiel. Vyžaduje však vydanie certifikátu užívateľovi a jeho podpísanie certifikačnou autoritou,

ktorej obaja dôverujú. Následne sa musí certifikát nainštalovať na pripájajúce sa zariadenie. V prípade použitia certifikátov v prostredí Microsoft Windows XP musí byť podľa (10) presne špecifikovaný účel, za ktorým boli vydané.

Nastavenia mechanizmu EAP-TLS sa nachádzajú v sekcii „tls“, kde sú špecifikované cesty k certifikátu certifikačnej autority, certifikátu servera a privátnemu kľúču, ku ktorému je prístup chránený heslom „whatever“.

Výpis 8 zobrazuje fragment konfiguračného súboru „eap.conf“ s nastaveniami mechanizmu EAP-TLS.

```
tls {
      private_key_password = whatever
      private_key_file = ${raddbdir}/certs/server.key

      certificate_file = ${raddbdir}/certs/server.crt
      CA_file = ${raddbdir}/certs/ca.crt

      dh_file = ${raddbdir}/certs/dh
      random_file = /dev/urandom
}
```

Výpis 8 – Konfigurácia mechanizmu EAP-TLS

V prípade, že je potrebné klienta autentizovať inou metódou, ale šifrovať pritom spojenie, je možné použiť napr. mechanizmus EAP-PEAP. Vytvorí tunel TLS, v ktorom je následne možné využívať autentizáciu ľubovoľnou inou autentizačnou metódou.

Aby však fungoval, musí byť nakonfigurovaný aj mechanizmus EAP-TLS, ktorý sa stará o vytváranie šifrovaného spojenia a o autentizáciu servera klientovi.

Konfigurácia mechanizmu EAP-PEAP pozostáva z prázdnej sekcie „peap“ v konfiguračnom súbore.

3. Konfigurácia pripojenia k LDAP serveru

Server „radiusd“ v základnom nastavení získava údaje o užívateľoch zo súboru „users“. Avšak v prípade mobilnej kancelárie posiela požiadavky aj LDAP serveru.

Adresa LDAP servera spolu s identifikátorom prípojného bodu adresára a ďalšími nastaveniami sú uložené v súbore „radiusd.conf“ v sekcii „ldap“ (viď Výpis 9). Pre jednoduchosť je server „radiusd“ autentizovaný rovnako ako administrátor databázy špecifikovaný pri nastavovaní servera „slapd“ (viď kapitola 5.2.1).

```
ldap {
      server = "localhost"
      identity = "cn=Admin,dc=mobileoffice,dc=com"
      password = secret
      basedn = "dc=mobileoffice,dc=com"

      filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
}
```

Výpis 9 – Konfigurácia pripojenia k LDAP serveru

Súčasťou posielanej požiadavky na LDAP server je reťazec, na základe ktorého sa filtrujú záznamy v adresári. Výraz tvoriaci tento reťazec je špecifikovaný parametrom „filter“ a pri jeho tvorbe je možné používať hodnoty atribútov získaných zo žiadostí od prístupového servera. Výsledkom výrazu „(uid=%{Stripped-User-Name:-%{User-Name}})“ v prípade autentizácie Mareka je reťazec „(uid=marek)“, ktorý sa zašle LDAP serveru v správe typu „searchRequest“.

Modul „ldap“ je pridaný do zoznamu modulov používaných na autorizáciu v sekcii „authorize“.

Vzťahy atribútov objektov uložených v LDAP adresári ku atribútom protokolu RADIUS sú špecifikované v súbore „ldap.attrmap“. Každému vzťahu je určené, či majú byť vzájomné hodnoty jeho členov v prípade žiadosti od prístupového servera kontrolované na zhodu (kľúčové slovo „checkItem“) alebo či má byť hodnota atribútu LDAP zaslaná v odpovedi servera v príslušnom atribúte protokolu RADIUS (kľúčové slovo „replyItem“).

Medzi vzťahy patriace do prvej skupiny patrí vzťah atribútov „User-Password“ a „userPassword“. Vzťahy atribútov týkajúcich sa informácií o VLAN užívateľa patria do druhej skupiny (viď Výpis 10).

```
replyItem   Tunnel-Type                 radiusTunnelType
replyItem   Tunnel-Medium-Type          radiusTunnelMediumType
replyItem   Tunnel-Private-Group-Id     radiusTunnelPrivateGroupId
```

Výpis 10 – Vzťah atribútov týkajúcich sa VLAN

5.2.3 Konfigurácia softvéru na klientoch

Nakoľko sa vyskytli pri práci s programom WPA Supplicant problémy s ovládačmi sieťovej karty, nebolo možné otestovať správnosť jeho nastavení. Z tohto

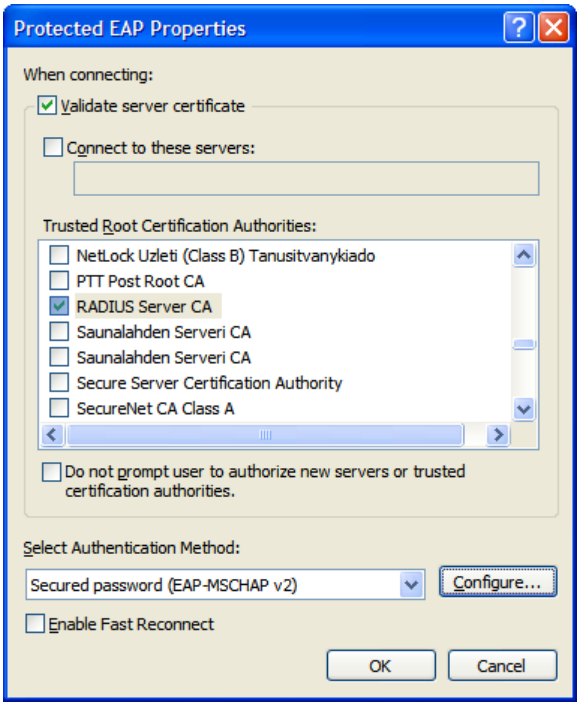
dôvodu všetci klienti používali systém Microsoft Windows XP, ktorý autentizáciu 802.1x natívne podporuje.

Konfigurácia autentizácie je v systéme Microsoft Windows XP definovaná pre každé rozhranie osobitne. Ak sa jedná o Wifi rozhranie, viaže sa navyše na konkrétnu bezdrôtovú sieť.

V závislosti na type pripojenia je na konkrétnom rozhraní, ktorým sa klient do siete pripája zvolená jedna autentizačná metóda. Nakoľko je implementovaná sieť považovaná za dôveryhodnú, väčšine klientov stačí autentizácia mechanizmom **EAP-MD5**, ktoré nemá žiadne ďalšie nastavenia.

Keďže systém Microsoft Windows XP od Service Pack 2 nedovoľuje nastaviť pre bezdrôtovú sieť mechanizmus EAP-MD5 kvôli slabému zabezpečeniu, potenciálni Wifi klienti musia použiť mechanizmus **EAP-PEAP**.

Ako bolo uvedené v kapitole 2.3.3 v časti o protokole EAP, mechanizmus EAP-PEAP umožňuje autentizovať okrem klienta aj bezpečnostný server. Aby to bolo možné, systém musí dôverovať certifikačnej autorite, ktorá certifikát servera podpísala. Preto je jej verejný certifikát pridaný do zoznamu certifikačných autorít, ktorým systém dôveruje. V nastaveniach mechanizmu EAP-PEAP je povolená autentizácia bezp. servera a je zvolený práve certifikát tejto certifikačnej autority (viď Obrázok 15).



Obrázok 15 – Okno s nastaveniami mechanizmu EAP-PEAP

Na autentizáciu klienta vo vnútri vytvoreného TLS tunela je použitý mechanizmus EAP-MSCHAP verzie 2, ktorý klienta autentizuje prihlasovacím menom a heslom užívateľa. Implicitné posielanie prihlasovacích údajov užívateľa používaných pri prihlasovaní sa do systému je vypnuté a systém si vždy vyžiada prihlasovacie údaje od užívateľa pri pripojení (viď Obrázok 13).

6 TESTOVANIE SIETE

Táto kapitola sa venuje testovaniu siete navrhnutej a implementovanej v kapitolách 4 a 5. Hovorí o princípe testovania a detailne popisuje jednotlivé vykonané testy.

6.1 Súbor testov

Proces testovania je rozdelený do šiestich testov, ktoré nasledujú v presnom poradí za sebou. Koncový stav siete v teste predchádzajúcom je východiskovým stavom testu nasledujúceho.

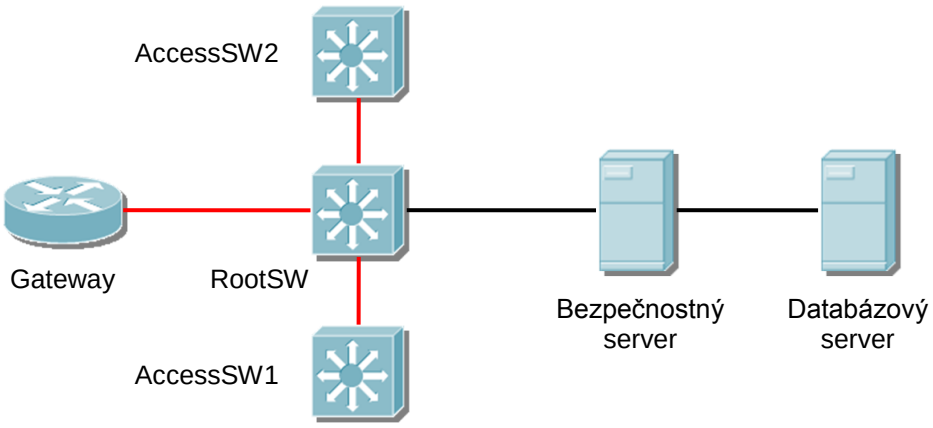
Pri jednotlivých testoch bola monitorovaná komunikácia medzi klientom a prístupovým serverom, medzi prístupovým serverom a bezpečnostným serverom a medzi bezpečnostným a databázovým serverom. Použité monitorovacie programy boli Wireshark a Tcpdump.

6.1.1 Test 1

Cieľ

Otestovať funkciu prepínača AccessSW2, schopnosť bezpečnostného servera autentizovať mechanizmom EAP-MD5 a schopnosť databázového servera vyhľadať užívateľa v databáze.

Východiskový stav siete



Obrázok 16 – Východiskový stav siete 1. testu

Očakávané výsledky

Po pripojení klienta k AccessSW2 na rozhranie fa0/2 je užívateľ Marek vyzvaný na zadanie mena a hesla. Po zadaní mena „marek“ a hesla „hello“ je klient úspešne pripojený do siete a rozhranie fa0/2 je priradené do ADMINISTRATORS_VLAN.

Dosiahnuté výsledky

Tabuľka 5 ukazuje zachytený priebeh autentizácie protokolom EAP. Zaslanie EAP paketu typu „Success“ v rámci č. 5 je dôkazom, že sa klient úspešne pripojil.

Komunikácia protokolom LDAP (viď Tabuľka 6) končí úspešným nájdením záznamu „Marek.administrators.mobileoffice.com“ (rámec č. 2).

Výpis 11 zobrazuje stav priradenia jednotlivých rozhraní na prepínači AccessSW2 do VLAN po prebehnutí autentizácie a autorizácie. Rozhranie fa0/2 je podľa výpisu priradené do ADMINISTRATORS_VLAN.

Možno konštatovať, že dosiahnuté výsledky sa zhodujú s očakávanými.

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	Cisco_32:a8:82	Spanning-tree-(for-bridges)_03	EAP	Request, Identity [RFC3748]
2	0.000358	Intel_2b:9f:db	Spanning-tree-(for-bridges)_03	EAP	Response, Identity [RFC3748]
3	0.250905	Cisco_32:a8:82	Spanning-tree-(for-bridges)_03	EAP	Request, MD5-Challenge [RFC3748]
4	0.254053	Intel_2b:9f:db	Spanning-tree-(for-bridges)_03	EAP	Response, MD5-Challenge [RFC3748]
5	0.486074	Cisco_32:a8:82	Spanning-tree-(for-bridges)_03	EAP	Success

Tabuľka 5 – Tunelovaná komunikácia medzi klientom a bezp. serverom

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	::1	::1	LDAP	searchRequest(6) dc=mobileoffice,dc=com wholeSubtree
2	0.092222	::1	::1	LDAP	searchResEntry(6) cn=Marek,ou=administrators,dc=mobileoffice,dc=com
3	0.096778	::1	::1	LDAP	searchResDone(6)

Tabuľka 6 – Komunikácia medzi bezp. serverom a databázovým serverom

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   SECURITY_VLAN                    active
20   ADMINISTRATORS_VLAN              active    Fa0/2
30   WORKERS_VLAN                     active
```

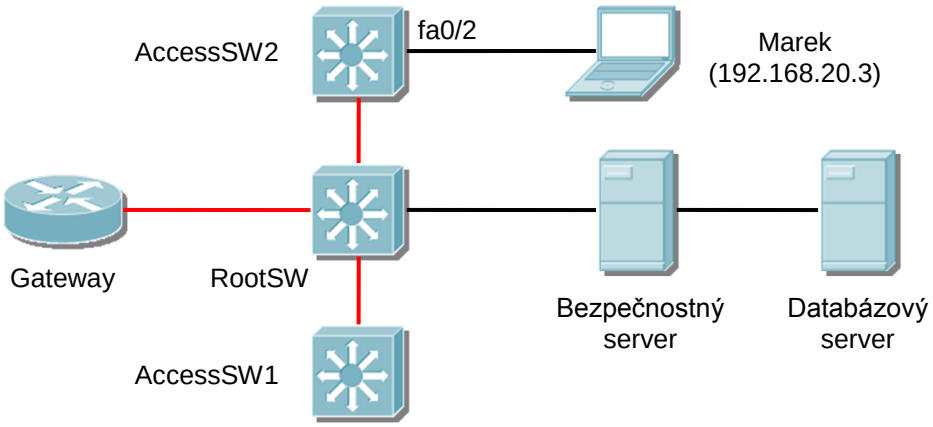
Výpis 11 –Fragment výpisu príkazu `show vlan` z AccessSW2

6.1.2 Test 2

Cieľ

Otestovať funkciu prepínača AccessSW1, schopnosť bezpečnostného servera autentizovať mechanizmom EAP-MD5 a schopnosť databázového servera vyhľadať užívateľa v databáze.

Východiskový stav siete



Obrázok 17 – Východiskový stav siete 2. testu

Očakávané výsledky

Po pripojení klienta k AccessSW1 na rozhranie fa0/2 je užívateľ Michal vyzvaný na zadanie mena a hesla. Po zadaní mena „michal“ a hesla „hello“ je klient úspešne pripojený do siete a rozhranie fa0/2 je priradené do WORKERS_VLAN.

Dosiahnuté výsledky

Tabuľka 7 ukazuje zachytený priebeh autentizácie protokolom EAP. Zaslanie EAP paketu typu „Success“ v rámci č. 5 je dôkazom, že sa klient úspešne pripojil.

Výpis 12 ukazuje stav priradenia jednotlivých rozhraní na prepínači AccessSW1 do VLAN po prebehnutí autentizácie a autorizácie. Rozhranie fa0/2 je podľa výpisu priradené do WORKERS_VLAN.

Možno konštatovať, že dosiahnuté výsledky sa zhodujú s očakávanými.

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	Cisco_32:44:c2	Spanning-tree-(for-bridges)_03	EAP	Request, Identity [RFC3748]
2	0.000503	Intel_fe:1c:71	Spanning-tree-(for-bridges)_03	EAP	Response, Identity [RFC3748]
3	0.429624	Cisco_32:44:c2	Spanning-tree-(for-bridges)_03	EAP	Request, MD5-Challenge [RFC3748]
4	0.432720	Intel_fe:1c:71	Spanning-tree-(for-bridges)_03	EAP	Response, MD5-Challenge [RFC3748]
5	0.984317	Cisco_32:44:c2	Spanning-tree-(for-bridges)_03	EAP	Success

Tabuľka 7 – Tunelovaná komunikácia medzi klientom a bezp. serverom

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   SECURITY_VLAN                    active
20   ADMINISTRATORS_VLAN              active
30   WORKERS_VLAN                     active    Fa0/2
```

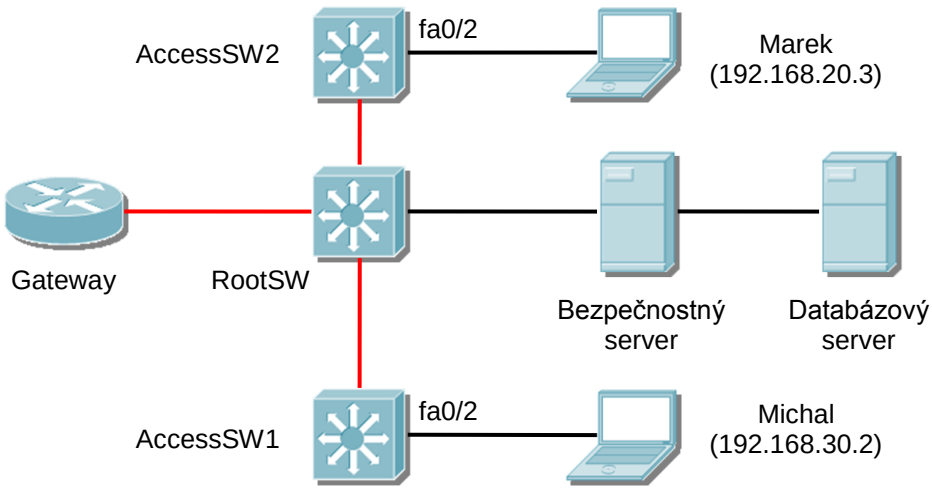
Výpis 12 – Fragment výpisu príkazu `show vlan` z AccessSW1

6.1.3 Test 3

Cieľ

Otestovanie funkčnosti filtra na smerovači Gateway pri filtrovaní nedovolenej komunikácie medzi virtuálnymi sieťami WORKERS_VLAN a SECURITY_VLAN.

Východiskový stav siete



Obrázok 18 – Východiskový stav siete 2. testu

Očakávané výsledky

AccessSW1 (IP adresa viď Tabuľka 4) neodpovie ani na jednu zo štyroch ICMP správ vyslaných z PC Michala programom Ping na jeho adresu. Dôvodom je zachytenie komunikácie filtrom na strane smerovača Gateway.

Dosiahnuté výsledky

Po zaslaní každej z ICMP správ klientom na adresu prepínača AccessSW1 (viď Tabuľka 8) neprišla klientovi odpoveď z cieľového zariadenia, ale zo smerovača Gateway (IP adresa viď Tabuľka 4). Táto odpoveď informovala klienta o nedostupnosti

zariadenia v dôsledku zachytenia správy filtrom. Dosiahnuté výsledky sa zhodujú s očakávanými.

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	192.168.30.3	192.168.10.11	ICMP	Echo (ping) request
2	0.000665	192.168.30.1	192.168.30.3	ICMP	Destination unreachable (Communication administratively filtered)
3	0.988141	192.168.30.3	192.168.10.11	ICMP	Echo (ping) request
4	0.988795	192.168.30.1	192.168.30.3	ICMP	Destination unreachable (Communication administratively filtered)
5	1.988175	192.168.30.3	192.168.10.11	ICMP	Echo (ping) request
6	1.988823	192.168.30.1	192.168.30.3	ICMP	Destination unreachable (Communication administratively filtered)
7	2.988267	192.168.30.3	192.168.10.11	ICMP	Echo (ping) request
8	2.988943	192.168.30.1	192.168.30.3	ICMP	Destination unreachable (Communication administratively filtered)

Tabuľka 8 – Ukážka filtrovania komunikácie protokolom ICMP medzi WORKERS_VLAN a SECURITY_VLAN

6.1.4 Test 4

Cieľ

Otestovanie funkcie smerovača Gateway pri smerovaní a filtrovaní povolenej komunikácie medzi virtuálnymi sieťami SECURITY_VLAN
a ADMINISTRATORS_VLAN.

Východiskový stav siete

Nezmenený (viď kapitola 6.1.3).

Očakávané výsledky

AccessSW1 (IP adresa viď Tabuľka 4) odpovie na každú zo štyroch ICMP správ vyslaných z PC Mareka programom Ping na jeho adresu.

Dosiahnuté výsledky

Po zaslaní každej z ICMP správ klientom na adresu prepínača AccessSW1 (viď Tabuľka 9) prišla klientovi odpoveď z cieľového zariadenia. Táto odpoveď znamená, že je cieľové zariadenie dostupné a komunikácia nie je zachytená filtrom.

Dosiahnuté výsledky sa zhodujú s očakávanými.

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	192.168.20.2	192.168.10.11	ICMP	Echo (ping) request
2	0.001632	192.168.10.11	192.168.20.2	ICMP	Echo (ping) reply
3	0.998619	192.168.20.2	192.168.10.11	ICMP	Echo (ping) request
4	1.001301	192.168.10.11	192.168.20.2	ICMP	Echo (ping) reply
5	1.998725	192.168.20.2	192.168.10.11	ICMP	Echo (ping) request
6	2.000312	192.168.10.11	192.168.20.2	ICMP	Echo (ping) reply
7	2.998825	192.168.20.2	192.168.10.11	ICMP	Echo (ping) request
8	3.000382	192.168.10.11	192.168.20.2	ICMP	Echo (ping) reply

Tabuľka 9 – Úspešná komunikácia protokolom ICMP medzi ADMINISTRATORS_VLAN a SECURITY_VLAN

6.1.5 Test 5

Cieľ

Otestovanie funkcie smerovača Gateway pri smerovaní a filtrovaní povolenej komunikácie medzi virtuálnymi sieťami WORKERS_VLAN a ADMINISTRATORS_VLAN.

Východiskový stav siete

Nezmenený (viď kapitola 6.1.3).

Očakávané výsledky

PC Mareka odpovie na každú zo štyroch ICMP správ vyslaných z PC Michala programom Ping na jeho adresu.

Dosiahnuté výsledky

Po zaslaní každej z ICMP správ Marekom na adresu PC Michala (komunikácia viď Tabuľka 10) prišla Marekovi odpoveď z cieľového zariadenia. Táto odpoveď znamená, že je cieľové zariadenie dostupné a komunikácia nie je zachytená filtrom.

Dosiahnuté výsledky sa zhodujú s očakávanými.

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	192.168.20.2	192.168.30.3	ICMP	Echo (ping) request
2	0.000817	192.168.30.3	192.168.20.2	ICMP	Echo (ping) reply
3	0.987964	192.168.20.2	192.168.30.3	ICMP	Echo (ping) request
4	0.988297	192.168.30.3	192.168.20.2	ICMP	Echo (ping) reply
5	1.988074	192.168.20.2	192.168.30.3	ICMP	Echo (ping) request
6	1.988416	192.168.30.3	192.168.20.2	ICMP	Echo (ping) reply
7	2.988178	192.168.20.2	192.168.30.3	ICMP	Echo (ping) request
8	2.988508	192.168.30.3	192.168.20.2	ICMP	Echo (ping) reply

Tabuľka 10 – Úspešná komunikácia protokolom ICMP medzi PC Mareka a PC Michala

6.1.6 Test 6

Cieľ

Otestovať schopnosť bezpečnostného servera a klienta nadviazať medzi sebou tunel TLS a autentizovať mechanizmom EAP-PEAP.

Východiskový stav siete

Nezmenený (viď kapitola 6.1.3).

Očakávané výsledky

Po pripojení klienta k AccessSW2 na rozhranie fa0/3 je užívateľka Zuzana vyzvaná na zadanie mena a hesla. Po zadaní mena „zuzana“ a nesprávneho hesla „hello2“ sa nadviaže medzi klientom a bezpečnostným serverom tunel TLS a prebehne proces autentizácie. Keďže je zadané heslo nesprávne autentizácia zlyhá.

Dosiahnuté výsledky

Na základe komunikácie protokolom EAP medzi klientom a bezp. serverom (viď Tabuľka 11) možno konštatovať, že sa dosiahnuté výsledky zhodujú s očakávanými.

Po identifikovaní bol klient vyzvaný na autentizáciu mechanizmom EAP-MD5. Ten však autentizáciu takýmto mechanizmom odmietol a vyžadoval mechanizmus EAP-PEAP (rámec č. 4). Následne sa medzi ním a bezpečnostným serverom vytvoril tunel TLS a prebehla autentizácia. Keďže nebolo heslo správne, autentizácia skončila neúspešne (rámec č. 19).

Č.	Čas	Zdroj	Cieľ	Protokol	Info
1	0.000000	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	EAP	Request, Identity [RFC3748]
2	0.000263	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	EAP	Response, Identity [RFC3748]
3	0.469207	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	EAP	Request, MD5-Challenge [RFC3748]
4	0.469502	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	EAP	Response, Legacy Nak (Response only) [RFC3748]
5	0.995232	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	EAP	Request, PEAP [Palekar]
6	1.003888	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	TLSv1	Client Hello
7	1.564554	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	TLSv1	Server Hello, Certificate, Server Hello Done
8	1.564890	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	EAP	Response, PEAP [Palekar]
9	2.136670	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	TLSv1	Server Hello, Certificate, Server Hello Done
10	2.206899	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
11	2.906312	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	TLSv1	Change Cipher Spec, Encrypted Handshake Message
12	2.993288	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	EAP	Response, PEAP [Palekar]
13	3.568276	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	TLSv1	Application Data
14	3.568782	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	TLSv1	Application Data
15	4.746955	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	TLSv1	Application Data
16	4.748243	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	TLSv1	Application Data
17	6.283297	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	TLSv1	Application Data
18	6.283746	Intel-Hf_6e:f2:94	Spanning-tree-(for-bridges)_03	TLSv1	Application Data
19	8.280457	Cisco_32:a8:83	Spanning-tree-(for-bridges)_03	EAP	Failure

Tabuľka 11 – Tunelovaná komunikácia medzi klientom a bezp. serverom

7 ZÁVER

Hlavným cieľom tejto práce bolo zaoberať sa problematikou autentizácie a autorizácie klientov využívajúcich na svoje pripojenie do sietí technológie LAN. Teóriu som v potrebnej miere popísal v kapitolách 1, 2 a 3 a je písaná tak, že aj neskúsený čitateľ sa dokáže po jej prečítaní orientovať v technológiách, ktoré táto rozsiahla problematika zahrňuje.

Už počas návrhu siete mobilnej kancelárie som sa stretával s problémami týkajúcimi sa podpory jednotlivých technológií na zariadeniach. Pôvodný návrh, ktorý počítal aj s bezdrôtovým pripojením klientov technológiou 802.11 (Wifi) som musel zavrhnúť, pretože prístupový bod Proxim Orinoco AP-700, ktorý som mal k dispozícii nepodporoval dynamické priraďovanie pripojených klientov do VLAN sietí.

Taktiež som pôvodne počítal s existenciou dvoch bezpečnostných serverov. Jeden by komunikoval s prístupovými servermi protokolom TACACS+ a druhý protokolom RADIUS. Keďže sa mi však nepodarilo nájsť implementáciu serveru TACACS+, ktorá by podporovala autentizáciu protokolom EAP, musel som od tohto zámeru odstúpiť.

Avšak aj napriek spomenutým redukciám v návrhu má výsledná implementovaná sieť všetky vlastnosti, ktoré sa od nej očakávali. Umožňuje rozšírenú autentizáciu klientov na báze užívateľa, je ľahko rozšíriteľná a v neposlednom rade použitie LDAP ako databázového servera na ukladanie údajov o užívateľoch dáva široký priestor napr. pre neskoršiu integráciu do informačného systému firmy.

Celkovo hodnotím spôsob takéhoto zabezpečenia sietí veľmi kladne. Väzba len na užívateľa, možnosť použiť rôzne metódy autentizácie od klasického prihlasovania menom a heslom až po digitálny certifikát a obmedzenie komunikácie len na základe IP adries sú jej silnými stánkami.

Práca mi priniesla množstvo skúseností z oblasti sietí. Dovolila mi rozšíriť si svoje znalosti z oboru sieťovej bezpečnosti a v neposlednom rade ma naučila orientovať sa v sieťových štandardoch a dokumentáciách k zariadeniam. Všetky tieto získané znalosti využijem pri práci na ďalších projektoch.

ZOZNAM POUŽITEJ LITERATÚRY

1. **Cisco Systems, Inc.** *Fundamentals of Network Security Companion Guide.* 4. vydanie. s.l. : Cisco Press, 2004. ISBN 9781587131226.
2. **Rigney, C. et al.** *Remote Authentication Dial In User Service (RADIUS).* [Online] Jún 2000. [Dátum: 13. apríla 2007.] http://www.ietf.org/rfc/rfc2865.txt.
3. **Zorn, G. et. al.** *RADIUS Attributes for Tunnel Protocol Support.* [Online] jún 2000. [Dátum: 18. apríla 2007.] http://www.ietf.org/rfc/rfc2868.txt.
4. **Aboba, B. et al.** *Extensible Authentication Protocol (EAP).* [Online] jún 2004. [Dátum: 18. apríla 2007.] http://www.ietf.org/rfc/rfc3748.txt.
5. **Interlink Networks.** Application Note. *Configuring EAP-PEAP & EAP-TTLS in the RAD-Series RADIUS Server.* [Online] [Dátum: 6. mája 2007.] http://www.interlinknetworks.com/app_notes/eap-peap.htm.
6. **IEEE Computer Society.** *IEEE Std. 802.1X-2004, IEEE Standard for Local and metropolitan area networks - Port-Based Newtork Access Control.* [Online] 13. decembra 2004. [Dátum: 18. apríla 2007.] http://standards.ieee.org/getieee802/download/802.1X-2004.pdf. ISBN 0-7381-4529-7.
7. **Synapse: Networks.** SYNAPSE: BANalyzer - Online Network Protocol Database. [Online] [Dátum: 25. apríla 2007.] http://www.banalyzer.de/ban/.
8. **IEEE Computer Society.** *EtherType Field Public Assignments.* [Online] 25. apríla 2007. [Dátum: 26. apríla 2007.] http://standards.ieee.org/regauth/ethertype/eth.txt.
9. **Davies, J.** *Wi-Fi Protected Access Data Encryption and Integrity.* [Online] 7. júna 2006. [Dátum: 26. apríla 2007.] http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx.
10. **Microsoft Corporation.** *Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS.* [Online] 30. októbra 2006. [Dátum: 20. marca 2007.] http://support.microsoft.com/kb/814394/en-us.
11. **Vuksan, V.** *FreeRADIUS + 802.1x/WPA + OpenLDAP HOWTO.* [Online] 14. mája 2005. [Dátum: 18. apríla 2007.] http://vuksan.com/linux/dot1x/802-1x-LDAP.html.
12. **Roser, K.** *HOWTO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant.* [Online] 18. apríla 2002. [Dátum: 20. marca 2007.] http://www.freeradius.org/doc/EAPTLS.pdf.
13. **Strand, L.** *802.1X Port-Based Authentication HOWTO.* [Online] 18. októbra 2004. [Dátum: 20. marca 2007.] http://www.tldp.org/HOWTO/8021X-HOWTO/index.html.
14. **Congdon, P. et al.** *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.* [Online] september 2003. [Dátum: 5. mája 2007.] http://www.ietf.org/rfc/rfc3580.txt.

15. **Phifer, L.** *Deploying 802.1X for WLANs: EAP Types.* [Online] 10. septembra 2003. [Dátum: 23. apríla 2007.] http://www.wi-fiplanet.com/tutorials/article.php/3075481.
16. **Funk, P. et al.** *EAP Tunneled TLS Authentication Protocol Version 1.* [Online] marec 2006. [Dátum: 6. mája 2007.] http://tools.ietf.org/wg/eap/draft-funk-eap-ttls-v1-01.txt.

ZOZNAM POUŽITÝCH SKRATIEK

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
IBNS	Identity-Based Networking Services
IOS	Internetworking Operating System
IP	Internet Protocol
ISO	International Standard Organization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Files
LLC	Logical Link Control
OSI	Open System Interconnect
PC	Personal Computer
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
Wifi	Wireless Fidelity
WLAN	Wireless LAN
WPA	Wired Equivalent Privacy

ZOZNAM PRÍLOH

Príloha A – CD s konfiguračnými súbormi