VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV AUTOMATIZACE A INFORMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF AUTOMATION AND COMPUTER SCIENCE

BEZPEČNOST LOKÁLNÍCH POČÍTAČOVÝCH SÍTÍ

SOLVING OF SECURITY PROBLEMS IN LOCAL NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN MAREK
AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN ROUPEC, Ph.D.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav automatizace a informatiky
Akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Martin Marek

který/která studuje v **magisterském navazujícím studijním programu**

obor: **Aplikovaná informatika a řízení (3902T001)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Bezpečnost lokálních počítačových sítí

v anglickém jazyce:

Solving of Security Problems in Local Networks

Stručná charakteristika problematiky úkolu:

Pojednejte o bezpečnostních problémech v lokálních počítačových sítích a uveďte metody jejich řešení. Formulujte doporučení pro firemní počítačové sítě a realizujte je ve vzorové aplikaci.

Cíle diplomové práce:

1. Studie bezpečnostních problémů se zaměřením na firemní počítačové sítě.
2. Doporučení pro hw a sw řešení ve firemních sítích s ohledem na bezpečnost.
3. Ověření navržených zásad v konkrétní realizaci.

Seznam odborné literatury:

Ludvík, M. - Štědroň, B.: Teorie bezpečnosti počítačových sítí. Computer Media, Praha, 2008.
Harper, A. - Harris, S. - Eagle, C. - Ness, J. - Lester, M.: Hacking - manuál hackera. Grada, Praha, 2008.
Northcutt, S. - Zeltser, L. - Winters, S. - Kent Frederick, K. - Ritchey, R. W.: Bezpečnost počítačových sítí. Computer Press, Praha, 2005.

Vedoucí diplomové práce: Ing. Jan Roupec, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2009/2010.

V Brně, dne 26.11.2009

L.S.

Ing. Jan Roupec, Ph.D. Ředitel ústavu	prof. RNDr. Miroslav Doupovec, CSc. Děkan fakulty

ABSTRAKT

Diplomová práce se zabývá vybudováním bezpečnosti lokálních počítačových sítí. Hlavní část práce se zabývá řešením autorizace bezdrátových klientů proti RADIUS serveru a návrhem doménového kontroléru pomocí open-source produktů a nástrojů s operačním systémem GNU/Linux.

ABSTRACT

The diploma thesis is concerned with solving security problems in local computer networks. The main part deals with the solution of authorization of wireless clients against the RADIUS server and with the proposal of domain controller using open-source products and the tools of operating system GNU/Linux..

KLÍČOVÁ SLOVA

RADIUS, Free-RADIUS, MySQL, MikroTik, autentizace, autorizace, Wi-Fi, Wireless, Acces Point, LDAP, Samba.

KEYWORDS

RADIUS, Free-RADIUS, MySQL, MikroTik, authentication, authorization, Wi-Fi, Wireless, Acces Point, LDAP, Samba.

PODĚKOVÁNÍ

Chtěl bych poděkovat Ing. Janu Roupcovi, Ph.D., za cenné rady, informace, připomínky a vedení celé mé práce.

Obsah:

ÚVOD

Informační technologie vstoupily do všech oblastí života lidského jedince a každým dnem se jejich působnost dál rozšiřuje. Ať už se jedná o využívání služeb Internetu, komunikace přes počítačové sítě, nebo návštěvy knihoven a prostorů budov veřejného a soukromého sektoru. Zde se všude setkáváme se zpracováním informací, které se mohou vyskytovat v mnoha formách. Mohou být například v tištěné podobě, nebo elektronicky uložené. Informace by se měly vždy přiměřeně chránit nezávisle na podané formě, společném užívání nebo ukládání.

Ochrana informací a bezpečná manipulace s nimi se stává důležitou součástí celkových bezpečnostních strategií firem a společností. Mezi bezpečnostní strategii firmy patří zavedení bezpečnostní politiky pro firemní počítačovou síť, kterou se zabývá tato diplomová práce. Bezpečnostní politika slouží jako návod a podpora k zavedení bezpečnosti informací.

Na začátku teoretické části diplomové práce se seznámíme s existujícími hrozbami počítačových sítí, protože nejčastější útoky na firemní síť bývají z vnitřní sítě. Tyto útoky využívají bezpečnostních děr, jako jsou například jednoduchá uživatelská hesla, chyby v aplikacích a jejich konfigurací, špatně nastavených síťových zařízení. Součásti obrany proti těmto hrozbám jsou také standardy a management řízení rizik.

Následující tři kapitoly pojednávají o síťových protokolech TCP/IP a referenčním modelu ISO/OSI, architektuře počítačových sítí a vytvoření virtuálních sítí.

V páté kapitole jsou uvedeny nejběžnější používané operační systémy v počítačových sítích a jejich softwarové řešení bezpečnosti. Jedná se o možnosti využití operačního systému platformy Windows a svobodného operačního systému GNU/Linux.

Poslední kapitola teoretické části pojednává o problematice bezdrátových sítí, protože jejich popularita ve firemním prostředí vzrostla natolik, že je nutno zohlednit její bezpečnost a soukromí uživatelů. U bezdrátových sítí je relativně jednoduché odposlechnout jakýkoliv přenos dat a zjistit tak uživatelská jména a hesla, proto je nutné před útočníky veškerý přenos šifrovat. Uživatelům můžeme přístup do sítě povolit, nebo zakázat některým z autorizačních serverů, například RADIUS server.

V praktické části je návrh autorizace bezdrátových klientů proti RADIUS serveru. Pro tento účel je použita aplikace FreeRADIUS a databázový systém MySQL. Součástí návrhu je nastavení limitu download a upload dat z internetu u bezdrátových klientů. Závěrem je návrh doménového serveru s operační systémem GNU/Linux.

1. BEZPEČNOST POČÍTAČOVÝCH SÍTÍ

Následující text vychází z uvedených norem v textu této kapitoly a monografických publikací uvedených v diplomové práci. [6] [7] [12] [13]

1.1 Nebezpečí v počítačových sítích

Nejčastější útoky bývají z vnitřní sítě, proto jim musíme předcházet a analyzovat možná rizika. Zajistit aby útok nebyl možný, popřípadě došlo k co nejmenším škodám.

Škody můžeme rozdělit na:

- napadení serverů, pracovních stanic,
- napadení síťové infrastruktury,
- napadení na úrovni aplikací,
- odcizení soukromých dat,
- nechtěný přenos dat,
- zablokování služeb.

Člověk může tyto škody napáchat:

- neúmyslně – nedopatřením, programová chyba programátora,
- úmyslně nezlomyslný – úmyslně prolomí bezpečnostní opatření, ve smyslu nepoškodit organizaci (testování bezpečnosti administrátorem),
- oportunistický – zlomyslný útok poškodit organizaci, odcizení soukromých dat.

Z hlediska bezpečnosti v organizaci musíme definovat postavení zaměstnanců, pracovní vztah a přístup do firmy. Ve firmě mohou být pracovníci pracující jako externisti, brigádnici (dočasní pracovníci), pracovníci cizích firem, administrátoři serverů a infrastruktury.

U každé pozice zaměstnance je možné analyzovat různá rizika bezpečnosti, podle jejich přístupových práv a potřeb pro výkon své práce. Škody mohou také vzniknout špatnou disciplínou zaměstnanců, kteří nedodržují vnitřní bezpečnostní předpisy firmy (např. uživatelé si zapisují svá hesla do kalendáře, což představuje obrovský bezpečnostní incident).

Mezi bezpečnostní rizika také patří mechanické opotřebení a stárnutí hardware a vliv přírodních jevů na informační technologie. Řešením této problematiky je vytvoření zálohování dat na více míst, tím snížíme pravděpodobnost ztráty dat. Zálohovat můžeme na disky, externí disky, pásky. Další potřebnou ochranou jsou přepěťové ochrany a UPS. Mezi důležitou součást bezpečnosti také patří využití klimatizace proti přehřátí serverů a ostatního zařízení.

Zásady pro zmenšení bezpečnosti rizik:

- Vytvořit dokumentaci a předpisy pro firmu a její zaměstnance – zavedením standardu, více v podkapitole 1.2,
- Pravidelné školení zaměstnanců,
- Definovat a nastavit uživatelská práva zaměstnanců podle jejich pracovní pozice.

Uživatelé používají silná hesla složená z velkých a malých písmen, čísel a speciálních znaků. Změna hesel pro přístup do doménové sítě je vynucována každý měsíc. Přístup do aplikací, sdílených disků omezíme podle pracovní pozice zaměstnance a jeho potřeb k výkonu práce. Mezi další bezpečnostní přístup k síti patří například využití čipové karty, na které jsou uloženy digitální certifikáty s určitou platností spjaté na PIN a PUK kód uživatele. K počítači je připojena čtečka karet (klávesnice umožňující zastrčení karty), do které se zastrčí čipová karta a po zadání uživatelského kódu PIN se uživatel přihlásí na stanici a získá přístup do počítačové sítě. Čipová karta vlastní PIN a PUK kód, po třetím špatném zadání PIN kódu se karta uzamkne a lze ji odemknout pouze PUK kódem. Pokud se povede třetím špatným pokusem uzamknout PUK kód, tak je potřeba čipovou kartu smazat a znova na ni nahrát certifikáty. Bude také vytvořen nový PIN a PUK kód.

U bývalých zaměstnanců firmy je potřeba uzamknout, nebo smazat uživatelský účet. V tomto směru by měli existovat dvě žádosti ve formě formuláře:

- nový zaměstnanec – kde jsou údaje zaměstnance a žádost o práva k síti a aplikací,
- zrušení zaměstnance – žádost na zrušení a smazání uživatelských práv odchozího zaměstnance.

- Zabezpečit fyzicky síťovou infrastrukturu a co nejvíce omezit přístup zaměstnancům. Do místnosti kde se nachází servery a zálohovací a jiné zabezpečovací zařízení by měl být omezen co nejvíce přístup, kromě administrátora a úzkého vedení. V některých případech přístup pod dohledem administrátora. Místnost by měla být zvlášť zabezpečena a obsahovat speciální zámky. V místnosti by měl být trezor, kam se ukládají jednotlivé zálohy a dokumenty. Dodržovat by se mělo například:

  - citlivá data a hesla neukládejte na disky uživatelských stanic. Vyřazené disky je potřeba smazat a přepsat nesmyslnými daty, nebo také mechanicky poškodit.
  - v Rack skříni používejte přepínač (switch), nikoliv rozbočovač (hub). V této době každý switch a podobný aktivní prvek umožňuje přístup pomocí www rozhraní, kde se dá konfigurovat. Heslo a jméno změňte, protože je z výroby standardně nastavené a útočník si přihlašovací údaje může najít v každém manuálu.

- Vytvořit zásady pro pracovní stanice a zabezpečit proti virům - zakázat uživateli vypnout různá nastavení a antivirový program, omezit přístup k www stránkám na internetu. Zakázat zobrazovaní přihlašovacího jména posledního přihlášeného uživatele, nastavit zamknutí stanice po určité době nečinnosti. Zakázat uživateli použít vyměnitelná média a možnosti použít nosiče dat (DVD,DVD-RW…).
- Pravidelně kontrolovat systémy a procedury,
- Testovat bezpečnost proti průnikům a používat systémy pro jejich detekci,
- Pravidelně zálohovat data – vytvoření pravidelného kalendáře zálohování. Využít inkrementální zálohování, zálohy image disků a diskových polí RAID.
- kontrola a servis hardware, záložních zařízení, přepěťových ochran a UPS.

1.2 Standardy v bezpečnosti

Jak již bylo nastíněno v předchozí kapitole, existuje mnoho bezpečnostních rizik a jejich řešení. Problém bezpečnosti informačních technologií se stal součástí managementu organizace, kdy je zpravidla iniciován projektovými pracovníky managementu nebo

pracovníky IT. Musíme si uvědomit, že zajištění větší bezpečnosti informačních technologií můžeme zlepšit nejen technickými pomůckami, ale zvýšením stávající bezpečnostní úrovně prostřednictvím směrnic a administrativních postupů. Jako součást bezpečnosti můžeme považovat řízení kvality. Například pokud vybíráme antivirový program pro zajištění bezpečnosti, zajímá nás také jeho kvalita z hlediska použitelnosti.

Kritéria pro určení kvality v IT:

- rychlost,
- dostupnost,
- důvěrnost,
- použitelnost,
- akceptovatelnost.

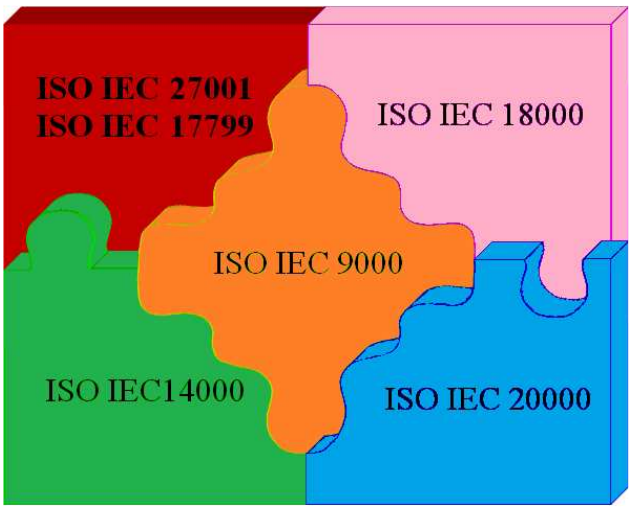
Aby se celková bezpečnost informačních technologií řešila jako komplexní proces, nabízí se soubory standardních kritérií, obsahující obsahovou a metodickou část zaměřující se na různé cílové skupiny.

Rok 1987 považujeme za počátek normy ISO 17799 / ISO 27001, která má za cíl vytvořit systém řízení bezpečnosti informací (ISMS) zahrnující nejvyšší pozice podniku a administrativní pracovníky.

Základní role ISMS:

- akceptovatelnost,
- důvěrnost,
- integrita,
- dostupnost.

S neustále rostoucím požadavkem na informační technologie a zvyšující se závislost na nich vzniká stále větší tlak na rozsáhlá bezpečnostní opatření. Pro co největší minimalizaci nákladů na bezpečnost IT se využívají standardy a normy, které zodpovědné osoby za bezpečnost po metodické a obsahově stránce podporují. Kritéria pro bezpečnost se v normách částečně obsahově překrývají, ale zaměřují se na různé cílové skupiny (viz obr. 1).



Obr. 1 *Vazby mezi standardy*

Standardy s největší relevancí v oblasti bezpečnosti IT:

- Příručka základní ochrany IT – cílem je vybudovat standardní bezpečnostní úroveň IT na základě infrastrukturních, personálních a technických standardů. Příručka obsahuje katalogy a postupy se standardními opatřeními z této oblasti. Postupy zahrnují analýzu struktur IT, zjištění potřeby ochrany, modelování, základní prověření, doplňující analýzu a realizace bezpečnostních opatření IT. Zaměření je v zásadě na úřady a podniky, kromě soukromých osob. U přidělených opatření příslušným pracovníkům začíná text každého opatření „Odpovědný za iniciování“ a „Odpovědný za realizaci“. Existuje 40 definovaných rolí v rámci podniku, například vedoucí IT, osoba pověřená bezpečnosti IT, administrátor, uživatel IT apod. Příručka se převážně hodí pro poskytovatele služeb zveřejňující a vytvářející data na internetu, výrobce hardware a software (vývoj software je zde brán okrajově). Administrátoři zde naleznou obsáhlé a podrobné technické informace.

- ISO / IEC 17799 a ISO 27001 – cílem je poskytnout rozsáhlou sbírku opatření vyhovující koncepci nejlepších postupů či praktik v bezpečnosti informací. Úkolem ISO 17799 je prezentace vhodných opatření a ISO 27001 je kriteriální norma pro certifikaci ISMS. Posuzuje se pro danou organizaci použití ekonomických kritérií a kritérií prostředí. V normě ISO 17799 se sledují tyto aspekty:

  - organizace bezpečnosti,
  - klasifikace a kontroly hodnot,
  - personální bezpečnost,
  - fyzická bezpečnost,
  - bezpečnost prostředí,
  - řízení komunikace provozu,
  - vstupní kontroly,
  - vývoj systému a údržba,
  - řízení kontinuity činnosti organizace a dodržování závazků.

Zaměření těchto norem je v zásadě na úřady a podniky kromě soukromých uživatelů. Cílová skupina v normách není definována, ale za cílovou skupinu lze považovat všechna místa, která jsou odpovědná za realizaci, výběr a řízení bezpečnostních opatření (administrátoři IT, bezpečnostní ředitel IT, interní auditoři, atd.).

- ISO TR 13335 – v současné době se tato norma přepracovává, skládá se ze čtyř částí, po přepracování dojde ke sloučení prvních dvou částí v jednu a třetí část bude sloučena se čtvrtou. Norma je zaměřená na vedoucí pracovníky podniku resp. organizace. V první části se obrací na vedoucí pracovníky na úrovni představenstva. V druhé části se zaměřuje na vedoucí pracovníky, kteří jsou odpovědní a kompetentní za IT systému podniku. V části třetí a čtvrté se obrací na ty, kteří v rámci životního cyklu projektu potýkají s bezpečností informačních technologií.

- ITSEC/ Common Criteria – cílem těchto kritérií je definovat kontrolní postup pro zkoumání bezpečnostní vlastnosti produktů a systémů IT. Definují se soubory kritérií funkční a kvalitativní požadavky na konkrétní předměty šetření tak, aby výsledky šetření byly srovnatelné. Cílovou skupinou jsou výrobci IT systémů, IT produktů a IT komponentů, kteří plánují jejich použití s požadavky na bezpečnost. Výrobci obdrží hodnotící mřížku, s jejíž pomocí mohou utvářet a ošetřovat své produkty tak, aby měly

definované bezpečnostní vlastnosti a aby tyto vlastnosti byly doložitelné pro třetí subjekty. Výrobci mohou zlepšit a standardizovat tyto vlastnosti u svých produktů tak, že svůj vývoj zaměří na bezpečnostní profily definované pro Common Criteria.

- CobiT – intenzivní používání IT na podporu a realizaci obchodních postupů vyžaduje zavedení vhodného kontrolního prostředí. Umožňuje prověřovat úplnost a efektivitu takového kontrolního prostředí k omezení vznikajících rizik. Cílové skupiny, které rozlišuje CobiT jsou management (na podporu při zvažování investic a rizik), uživatelé (pro lepší odhad spolehlivosti a kontroly IT), kontroloři (ke zdůvodnění kontrol a poradenství v rámci vybudování a provozu interních kontrol) a osoby zodpovědné za procesy nebo IT.

Z výše uvedených norem je zřejmé, že je hodně rozdílných cílů a cílových skupin, proto přiměřenou úroveň bezpečnosti IT pro celkové řešení lze dosáhnou pouze tehdy, když k tomu přispějí výrobci i uživatelé IT.

Kombinace norem pro dosáhnutí větší bezpečnosti:

- ISO 17799 + Příručka základní ochrany IT – norma ISO 17799 se zabývá řízením bezpečnosti informací nabízející procesně orientovaný přístup. Důležitou součástí je zde katalog s generickým opatřením ve smyslu nejlepších postupů a praktik. Pro zabezpečení celkového řešení před hrozbami je nutné tato opatření zavést do praxe pomocí konkrétních i technických návodů. K tomuto nám slouží příručka základní ochrany IT se svým katalogem opatření. Z této kombinace vyplývá postup, který striktně odděluje řízení bezpečnosti IT od praktické realizace. Také zde, pokud existují speciální požadavky na bezpečnost, můžeme ve speciálních případech sáhnout po Common Criteria.

- ISO 17799 + ISO 9000 – požadavky na systémy kvality zde popisuje norma ISO 9000 a definuje příslušný kontrolní postup. Postup lze aplikovat v podnicích a organizacích, ale nezabývá se zde specificky aspektem bezpečnosti informací. Stanovená jsou pouze pověření, zda IT vyhovují požadavkům a činnosti organizace. Aby bylo možné pokrýt více oblast bezpečnosti informací, lze ji doplnit o doplněk ve formě normy ISO 17799.

1.3 ISO 27001 / ISO 17799, obsahy normy a realizace v praxi

Úvodem se norma popisuje pojmem bezpečnost informací a jejího významu pro organizaci. V další části se norma zabývá informačními médii, protože informace se mohou vyskytovat v mnoha formách. (např. vytištěném papíře, elektronicky uložené, ve filmech apod.). Dále je uváděna důležitost informace z hlediska zajištění:

- důvěrnosti - zaručení přístupu k informacím pouze pro oprávněné osoby,
- integrity - zajištění správnosti a úplnosti informací a metod jejich zpracování,
- dostupnosti - zaručení přístupu k informacím podle potřeb a přístupu k příslušným hodnotám pro oprávněné uživatele.

Pro nutnost bezpečnosti informací, procesů, systémů a sítě jsou důležitá komerční aktiva firmy, zachování jejich důvěrnosti, integrity a dostupnosti, mohou přispět k zachování náskoku před konkurencí, likvidity, rentability, dodržování zákonných předpisů a obchodní

autority. Důležitým faktorem je závislost obchodní činnosti na službách a informačních systémech.

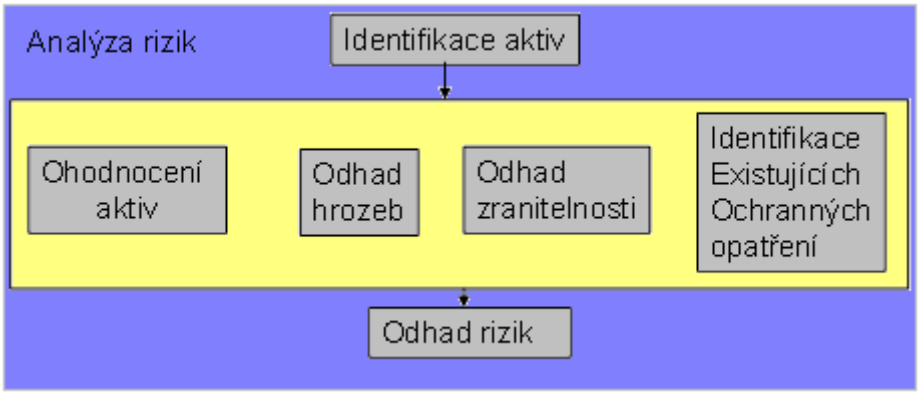
Norma uvádí tři zdroje pro řešení bezpečnostních požadavků:

- Analýza rizik – umožňuje identifikování hrozeb pro aktiva, pravděpodobnosti výskytu rizika, analýzu možných dopadů a hodnocení slabých míst.
- Požadavky – vyplývají ze zákonů, politiky, směrnic a smluv, které musí být splněny
- Specifické principy – cíle a požadavky organizace na zpracování informací, které podnik vytvořil na podporu svých procesů.

1.3.1 Analýza rizik

Systematickou analýzou bezpečnostních rizik identifikujeme bezpečnostní požadavky, v rámci analýzy se nalezená rizika kvantifikují a stanoví se jejich priority. Náklady na vytvoření opatření je nutné porovnat s ekonomickými škodami, které mohou nastat při vzniku rizika. Zaměření analýzy se může vztahovat na celou organizaci, její část nebo konkrétního systém. Osoby s rozhodovací pravomocí určí zaměření analýzy, kterou doloží argumenty. Analýza rizik se zpravidla omezují na tyto faktory (viz obr. 2):

- aktiva (složky, jejichž chybné chování by mohlo v obchodních procesech ohrozit dostupnost, důvěrnost a integritu),
- hrozby specifické pro komponenty,
- slabá místa.



Obr. 2 *Analýza rizik*

Každá metoda analýzy rizik má vlastní postupy ve formě kroků, které musíme projít, tak abychom dospěli k výsledku.

Níže bude představen model pro většinu aplikací IT v každém sektoru.

Mezi faktory úspěšnosti analýzy patří kvalitní složení týmu, který analýzu provádí. Tým musí mít k dispozici kompetentní kontaktní osoby pro všechny sledované složky. Při provádění analýzy, která je časově velmi náročná, musí vedení poskytnout týmu potřebné prostředky. V týmu by měl být zkušený účastník, který převezme moderování. Důležité je stanovení metodiky a dokumentačního postupu. První analýza rizik by se měla zaměřit na jednu dílčí oblast, aby bylo možné zjistit, zda zvolená metoda, nástroje a dovednosti účastníků jsou dostatečné.

Podrobná analýza rizik zahrnuje tyto kroky:

- Vymezení oblasti analýzy – specifikovat IT systém a uvést zahrnutí jiných aktiv (budovy, infrastruktura).
- Identifikování ohrožených aktiv – zaevidovat všechna ohrožená aktiva ležící uvnitř analyzované oblasti stanovené v předchozím kroku.
- Hodnotová analýza – zjišťuje se hodnota ohrožených aktiv, analýza obsahuje stanovení základny pro hodnocení věcných a nehmotných aktiv, zjištění závislosti mezi aktivy a hodnocení ohrožených aktiv.
- Analýza hrozeb – aktiva jsou vystavena mnoha hrozbám, mohou vyplynout z úmyslu, nedbalosti a nedopatření. Analýza hrozeb zahrnuje pravděpodobnost výskytu hrozby, identifikování možných hrozeb (katastrofy apod.) a možných útočníků (zaměstnanci, externí zaměstnanci).
- Analýza slabých míst – hrozba se může stát účinnou, pokud existuje slabé místo. Do oblasti slabých míst organizace může patřit hardware a software, personál a infrastruktura.
- Identifikování stávajících bezpečnostních opatření – je nutné provést evidenci již existujících bezpečnostních zařízení, jejich dopady z hlediska jejich správné funkce a zabránění zbytečným nákladům. Nová opatření musí být kompatibilní s existujícími.
- Hodnocení rizik – hodnotí se jednotlivá rizika a celkové riziko. Zda jsou rizika akceptovatelná nebo neakceptovaná se provádí zohledněním těchto faktorů: výši škody a pravděpodobnost výskytu.
- Vyhodnocení – výsledkem je vyhodnocení a zpracování příslušné dokumentace.

Výsledky analýzy slouží k hledání řešení v řízení rizik a výběr příslušných opatření zajišťuje dodržení národních a mezinárodních zákonů, realizaci podnikových cílů, splnění provozních požadavků a nákladů na jejich implementaci v rozumném poměru se snížením rizik.

V normě ISO 17799 jsou navržena tato opatření:

- Bezpečnostní politika – přijatá vedením společnosti, slouží jako návod a podpora k zavedení bezpečnosti informací. Dokument bezpečnostní politiky musí obsahovat definici bezpečnosti informací, cíl a oblast použití. Dále podpoření managementu k naplnění cíle ve formě prohlášení a strukturní popis řízení rizik. Další součástí dokumentu by mělo být stručné vysvětlení bezpečnostní politiky, principů a norem, například:

  - dodržování zákonných předpisů,
  - požadavky na výcvik v oblasti bezpečnosti,
  - zabránění a identifikace virů a jiného škodlivého softwaru,
  - důsledky při porušení bezpečnostních směrnic.

- Organizování bezpečnosti – stanoví se systém řízení, který stanovuje odpovědnosti a úkoly. Systém integruje všechny plánovací, realizační a kontrolní činnosti. Z normy je směrodatné:

  - Osobní angažovanost a iniciativa – odpovědnost za bezpečnost informací má vedení organizace,
  - Koordinace ISMS – ve velké organizaci může být konsorcium osob s komplexní

pravomocí, složené ze zástupců managementu, administrátorů, uživatelů a auditorů. Konsorcium koordinuje implementaci opatření zaměřených na bezpečnost informací. Typické úkoly konsorcia jsou organizační dohody o určitých rolích a odpovědností, záruky bezpečnosti jako součást plánovacího procesu pro informace a jejich zpracování, prověření bezpečnostních incidentů aj.

- Přidělení samostatných odpovědností – je nutné přesně definovat místní specifické odpovědnosti za bezpečnostní procesy, věcná a informační aktiva.
- Důležité oblasti úkolů pro organizace IS – je nutné definovat a zavést proces upravující používání nového IT zařízení a proces pro odborné poradenství k bezpečnosti informací (např. z důvodů školení).
- Dohody o důvěrnosti.
- Spolupráce mezi organizacemi – definování informací, které budou k dispozici ostatním.

    - Bezpečnost ve spolupráci s cizími podniky – pro zachování bezpečnosti je potřeba monitorování cizích firem. Uvědomit si, že analýza rizik je velice citlivá a je nutné prověření smluv.

- Bezpečnostní požadavky při styku se zákazníky – musí se postupovat obzvlášť citlivě, musíme chránit informace před odcizením, narušením integrity, kopírování. Řešením je kontrola přístupu, vstupní kontrola, monitorování činnosti zákazníka. Požadavky na ochranu autorských práv a dat. Zákazníka instruovat ohledně bezpečnostních podnikových pravidel.
- Bezpečnostní požadavky ve smlouvách s cizími podniky – dodržování zavedených opatření a bezpečnostních požadavků je nutné s firmami smluvně upravit

- Klasifikace a řízení aktiv – aby bylo možné majetek chránit, je nutná jeho klasifikace prováděná inventarizaci.
- Personální bezpečnost – přijetí a ukončení pracovních poměrů je nutné naplánovat podle organizačních směrnic. Nový zaměstnanci musí projít zaškolením v rámci bezpečnostní politiky organizace. Jsou jim přiděleny role a odpovědnosti. Podepisují dohody o důvěrnosti, které specifikují informace jako citlivé, důvěrné nebo tajné. U ukončení pracovních poměrů, kdy zaměstnanec odchází z firmy, jsou mu jeho přístupy odebrány a deaktivovány, s možností použití dat jeho nástupcem.
- Fyzická bezpečnost a bezpečnost prostředí – je potřeba definovat bezpečnostní zóny a hranice a přístup do nich. Fyzickou ochranou lze zabezpečit přístupy do budov, kanceláří apod. jak pro neoprávněné tak i oprávněné osoby. Bezpečnostní zóny by měly být chráněny příslušnými kontrolami přístupu (identifikační karty). Kromě ochrany fyzického přístupu se musí zavést tato opatření:

    - Ochrana přístupu – omezením přístupu k zařízení a zavedením opatření před krádeží, požárem, vodou apod.
    - Zásobování elektrickou energií – chránění zařízení před výpadky sítě a jinými elektrickými poruchami. Možnost zabezpečení je náhradní zásobovací vedení, záložní zdroje (UPS), záložní agregáty.
    - Údržba IT zařízení – pravidelný servis zařízení a kontrola stavu doporučené specifikace v dokumentaci výrobce zařízení.
    - Bezpečnost zařízení mimo prostor podniku,
    - Bezpečná likvidace a opětovné použití zařízení – data s citlivými informacemi musí být fyzicky zničena, nebo přepsána bezpečným způsobem.

- Řízení komunikací a řízení provozu,
- Řízení přístupu – přístupy k informacím musí být definovány podle uživatelských rolí a řízeny vhodnými opatřeními. Pravidla pro přístupová oprávnění definují a dokumentují uživatele a skupiny s požadavky pro přístup k informacím. Správa uživatelů a skupin zaručí, že přidělená práva skupině, uživateli jsou aktuální. Práva by měla být platná pro období jejich používání. K přístupovým právům potřebujeme ověření totožnosti uživatele, k tomu slouží hesla. Pravidla pro hesla uživatelů a jejich používání (změna hesla, složitost) by měla být uvedena ve směrnici.
- Vývoj a údržba systémů – aby se snížilo riziko ztráty dat, porušení integrity, nebo zneužití, je nutné vypracovat příslušné směrnice zabývající se:

    - Validace vstupních dat – kontrola zadaných dat (neplatné znaky, chybějící data), postupy pro jejich prověření, definování kompetencí zaměstnanců podílejících na zadávání dat systému.
    - Kontrola systémového zpracování – data správně zadaná se mohou poškodit chybami při zpracování systému. Do systému by se měla integrovat zkouška validace dat.
    - Správné a bezchybné zpracování dat – možné chyby aplikačního softwaru při zpracování mohou zkreslovat výsledky. Předejít těmto problémům můžeme kontrolou logů souborů při zpracování. Kontrolou integrity aplikačního softwaru a prověřením generovaných vstupních dat.
    - Autentizace zpráv – technika k rozpoznání zfalšovaných, upravených dat. Využívá šifrovací metody zajišťující důvěrnost, autentičnost nebo integritu informací K zajištění autentičnosti a integrity elektronických dokumentů slouží digitální podpis.
    - Zachování integrity systémů – prověření software před jeho integrací do operačního systému. Softwarové záplaty a aktualizace knihoven by se měly instalovat, pokud přispějí k odstranění bezpečnostních slabin. O aplikování by se měly vést záznamy.

- Řízení bezpečnostních incidentů – zavést odpovědnosti a postupy pro řízení bezpečnostních incidentů, aby bylo možné na ně rychle reagovat. Měly by se zavést postupy k evidenci bezpečnosti incidentů (např. výpadky IT systému, chyby kvůli neúplným datům, přestupky proti důvěrnosti). Dalším postupem je zavedení havarijních plánů zahrnujících analýzu a identifikaci příčin vzniklého incidentu. Součástí havarijních plánu jsou protiopatření proti opakování incidentu a shromažďují se potřebné záznamy vzniklého incidentu.

2. SÍŤOVÉ PROTOKOLY

Zkratka TCP/IP označuje sadu protokolů, jejíž součásti jsou dva protokoly používané v internetu a to Transmission Control Protocol a Internet Protocol.

Tato sada protokolů poskytuje metody pro přenos dat mezi počítači, konkrétněji mezi jejich síťovými komponenty. Tato sada protokolů TCP/IP zabezpečuje přenos dat pro všechny služby, které jsou dostupné současnému uživateli sítě. Služby např. zajišťují přenos elektronické pošty, přenos souborů, zasílání zpráv a přístup na WWW

Referenční model ISO OSI – Open Systems Intercontenction byl navržen kvůli standardizaci různých technologií souvisejících s komunikací sítových zařízení. Reprezentuje sedm vrstev tvořící architekturu protokolů pro datovou komunikaci. Lze si jej představit jako zásobník, kde jednotlivé vrstvy leží na sobě (viz obr. 3). Každá vrstva obsahuje služby definované protokoly sloužící ke komunikaci a kontrole.

Referenční model ISO OSI

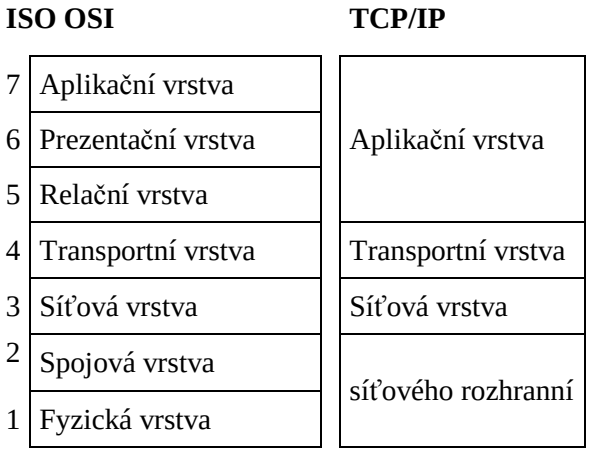
7	Aplikační vrstva
6	Prezentační vrstva
5	Relační vrstva
4	Transportní vrstva
3	Síťová vrstva
2	Spojová vrstva
1	Fyzická vrstva

Obr. 3 *Referenční model ISO OSI (RFC)*

Popis vrstev referenčního modelu ISO OSI, uvedených na obrázku 3:

- Vrstva 7 (aplikační) – nejvyšší vrstva modelu reprezentuje a definuje způsoby komunikace aplikací se sítí a mezi systémy.
- Vrstva 6 (prezentační) – obsahuje protokoly, které jsou součástí operačního systému. Vrstva definuje způsob, jak budou data prezentovaná a jaký budou mít formát. V této vrstvě mohou být data šifrována i dešifrována.
- Vrstva 5 (relační) – koordinuje komunikaci (relace) mezi koncovými body. Zajišťuje stav relace pro bezpečnostní, protokolovací a administrativní funkce.
- Vrstva 4 (transportní) – zde jsou data definována do struktur a kontrolují se u nich chyby. U webových prohlížečů zde probíhá šifrování.
- Vrstva 3 (síťová) – protokoly sloužící pro směrování dat mezi systémy, na této vrstvě dochází k adresování cílového bodu zabezpečující, že data se dostanou k cílovému bodu.
- Vrstva 2 (spojová – linková vrstva) – jsou zde definována pravidla pro zasílání a přijímání informací v lokání síti (LAN)
- Vrstva 1 (fyzická) – hardwarová vrstva zajištující fyzický přenos informací mezi uzly sítě, kódující bajtový tok přenosu.

Sada protokolů TCP/IP a referenční model ISO OSI byly navrženy současně a jsou si hodně podobné (viz obr. 4), ale protokoly TCP/IP představují realitu v praxi. Každá skupina referenčního modelu ISO OSI a TCP/IP má vlastní definici vrstev a jejich protokolů. Rodina protokolů TCP/IP využívá čtyři vrstvy – aplikační, transportní, síťovou a síťové rozhraní. Na obrázku č. 11 je porovnání referenčního modelu ISO OSI s TCP/IP. Za povšimnutí stojí, že pod aplikační vrstvou TCP/IP se skrývají služby a protokoly tří nejvyšších vrstev modelu ISO OSI, transportní a síťová vrstva zůstala shodná. Vrstva síťového rozhraní zahrnuje spojovou a fyzickou vrstvu.

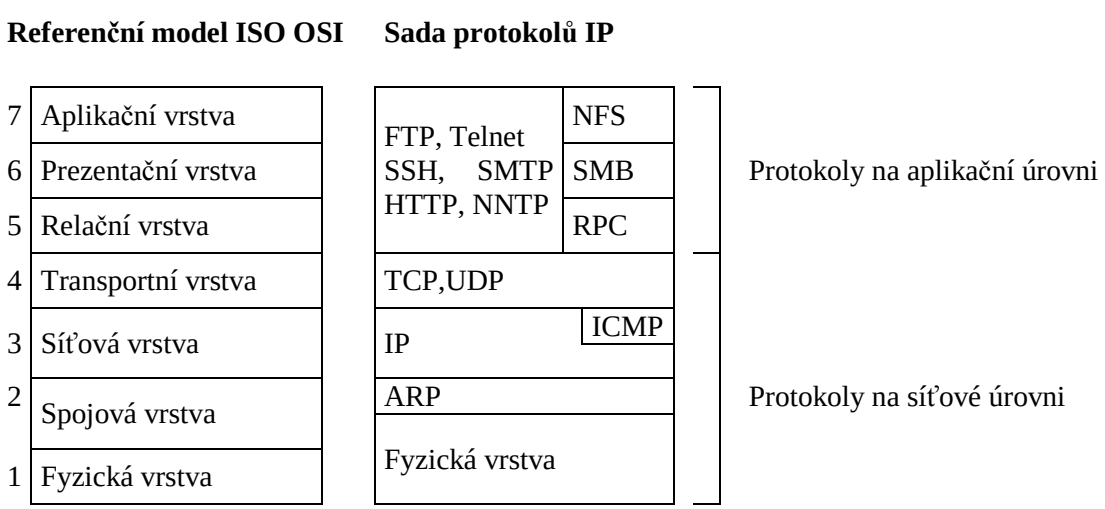


Obr. 4 *Porovnání modelů ISO OSI a TCP/IP (RFC)*

Běžné protokoly na těchto vrstvách jsou např.:

- aplikační vrstva: HTTP (Hypertext Transfer Protocol),
- transportní vrstva: TCP (Transmission Control Protocol),
- síťová vrstva: IP (Internet Protocol),
- spojová vrstva: ARP (Address Resolution Protocol).

Tyto protokoly lze rozdělit na síťové a aplikační (viz obr. 5):



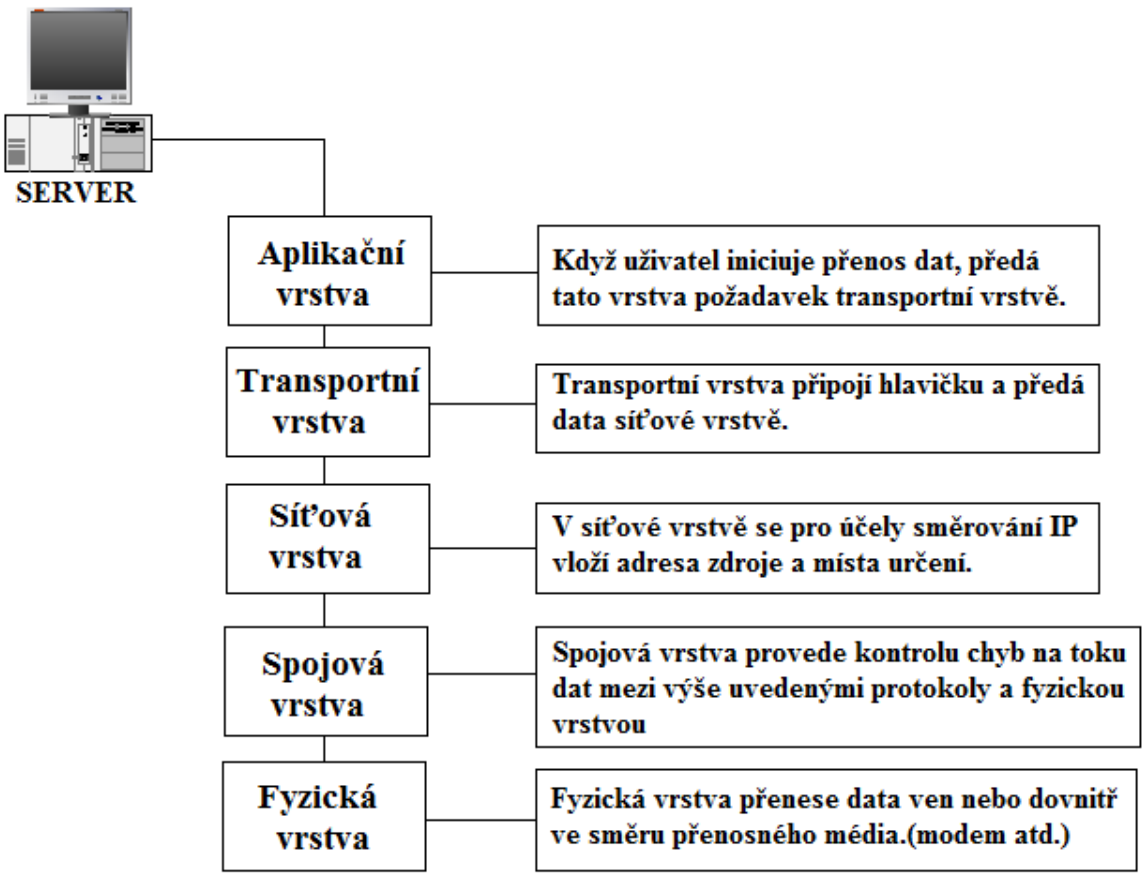
Obr. 5 *Zásobníky protokolu IP a modelu ISO OSI (RFC)*

Protokoly na síťové úrovni jsou řídicí mechanismy pro přenos dat. Zabezpečují zasílání informací mezi počítači v paketech na základě různých typů dat, např. u IP protokolu směrování informací pomocí IP adres počítačů do jejich místa určení. V průběhu této komunikace komunikuje IP protokol s jinými protokoly zapojenými do přenosu informace na síťové úrovni.

Protokoly na aplikační úrovni jsou přístupné pro uživatele, např. u interaktivního protokolu http vidíme výsledky přenosu dat. Tyto informace nalezneme v chybových hlášeních a zprávách o přenosu.

Jak to všechno funguje?

Oba modely TCP/IP a ISO OSI funguji na principu protokolového zásobníku. Zásobník představuje úhrn činností a protokolů pro přenos informací mezi dvěma počítači. Pro představu, každý počítač tvoří jeden tento zásobník. Pokud chceme předat nějaké informace (data) druhému počítači, tak data putují a jsou předávána mezi vrstvami až do nejnižší vrstvy odesílajícího počítače, který předá data k cílovému počítači. Zde jsou předána stejné vrstvě a data putuji od nejnižší k nejvyšší vrstvě cílového počítače (viz obr. 6)



Obr. 6 *Protokol IP (RFC)*

2.1 Protokoly na síťové úrovni:

Každá vrstva obsahuje několik samostatných protokolů, mezi důležité síťové protokoly patří:

- Address Resolution Protocol (ARP),
- Internet Control Message Protocol (ICMP),
- Internet Protocol (IP),
- Transmission Control Protocol (TCP),
- User diagram protokol (UDP).

Address Resolution Protocol (ARP)

Využívá směrování mezi počítači lokální sítě a sítě internet a také při mapování internetových adres do hardwarových adres (MAC address) a překladu adres síťové vrstvy na adresy spojové vrstvy.

Před odesláním se data zabalí do IP paketů pro přenos po internetu. Pakety obsahují IP adresu odesílatele a příjemce, ale neznají hardwarovou adresu příjemce. Za pomocí dotazovací zprávy protokolu ARP můžeme získat hardwarovou adresu příjemce, pokud cílová adresa je dostupná v lokální síti, cílový počítač odešle odpověď pomocí hardwarové adresy a přenos dat může začít.

Internet Control Message Protocol (ICMP)

Tento protokol poskytuje chybové a kontrolní zprávy, které protokol umožňuje sdílet, nebo mohou být předávány mezi počítači, servery. Užitečné zprávy:

- zprávy nesoucí echo a odezvu pro testování dostupnosti sítě,
- zprávy o přesměrování umožňující efektivnější směrování,
- zprávy o překročení časového limitu, které informují zdroje, že paket překročil přidělený čas v rámci sítě.

Pakety používané k zjištění síťové konektivity, zda je cíl dostupný a aktivní.

- ICMP_ECHO_REQUEST
- ICMP_ECHO_REPLY

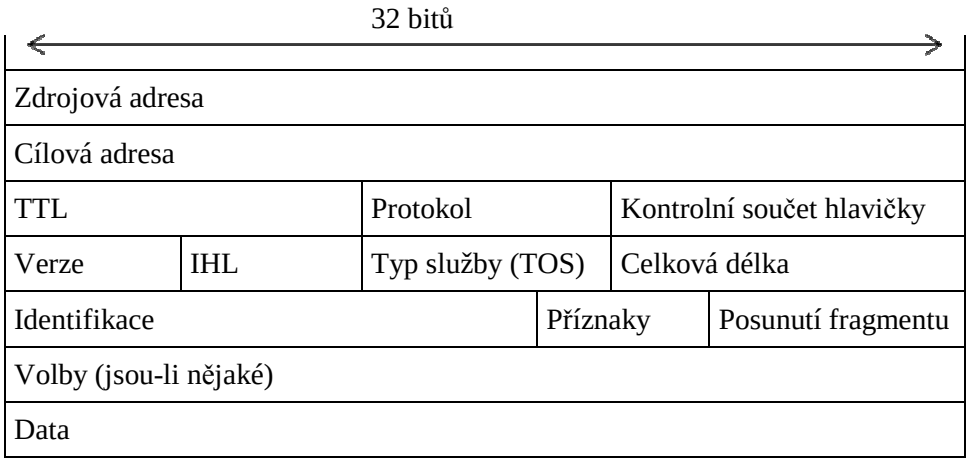
Internet Protocol (IP)

Zajišťuje doručování paketů (datagramů) v síti. IP datagram je prostředek pro doručování dat TCP/IP, je složen z několika částí:

- hlavička – obsahuje zdrojovou a cílovou adresu, veškeré síťové informace,
- veškerá odesílaná data,
- TTL pole – numerická hodnota, při každém průchodu routrem se snižuje o jedničku, pokud hodnota bude nulová, dojde k vyřazení diagramu.

IP protokol umožňuje data fragmentovat a komplementovat. Na síti se data mohou odesílat pouze v jednotlivých blocích, pokud při přenosu je blok větší než je velikost MTU (MaximumTransmission Unit – označení maximální velikosti IP paketu, který je možné přenést z jednoho síťového zařízení na druhé), nelze jej přenášet. Data jsou rozdělena do menších bloků, aby bylo možné data přenést po síti k cílovému zařízení. Struktura IP protokolu je na obrázku 7.

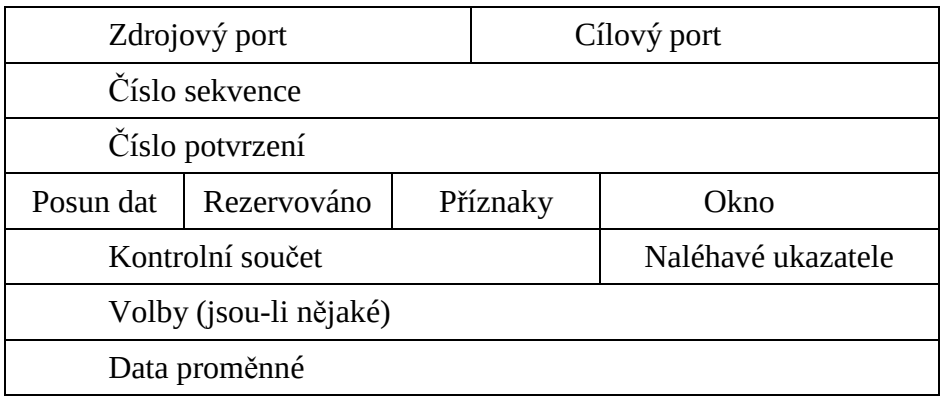
IP adresa je 32 bitů dlouhá adresa, představující jedinečný identifikátor systému v síti. Obvykle je zapsána čtveřicí čísel odpovídajících hodnotám bajtů oddělené tečkou (127.0.0.1). Každý bajt (oktet) může mít hodnotu 0 až 255. Souvislý rozsah IP adres definuje IP síť. IP adresa s maskou sítě tvoří rozsah sítě. Maska sítě je 32 bitů (255.255.255.248).



Obr. 7 *Protokol IP (RFC)*

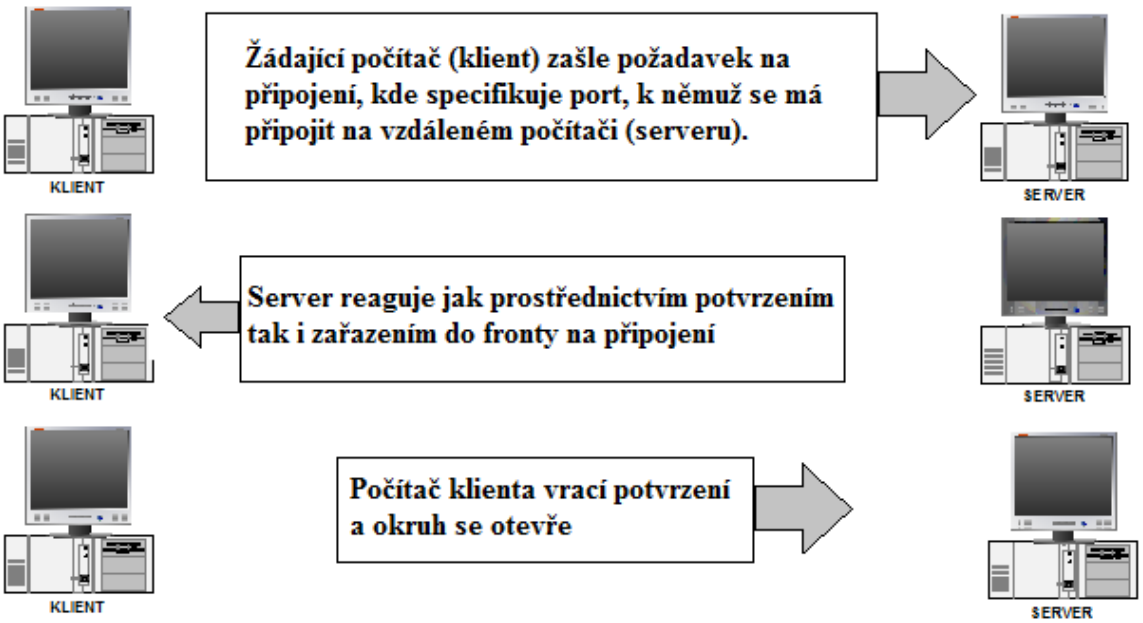
Transmission Control Protocol (TCP)

Je jedním z hlavních protokolů využívaných na Internetu. Pracuje na transportní úrovni a umožňuje přenos souborů a vzdálené relace. Má vlastní strukturu paketu (viz obr. 8). Pořadové číslo slouží k určení pořadí, ve kterém se data zasílají. Kontrolní součet (checksum) slouží k ověření, zda data byla poškozena během přenosu. Příznaky ovládající stav připojení (zřízeno, používá, zavřeno)



Obr. 8 *Struktura TCP paketu (RFC)*

Třícestný handshake – TCP spoléhá na virtuální okruh klient – server, mezi počítačem zasílající požadavek a jeho cílem (viz obr. 9).



Obr. 9 *Zřízení handshake*

User diagram protokol (UDP)

Nespojový protokol transportní vrstvy. Zabezpečuje kontrolu integrity dat přes kontrolní součet.

2.2 Protokoly na aplikační úrovni

Hypertext Transfer Protocol (HTTP)

Nejznámější protokol běžící standardně na TCP portu 80, díky tomuto protokolu může uživatel surfovat po internetových stránkách WWW. Nevýhodou tohoto protokolu je slabá bezpečnost přenosu dat, data nejsou při přenosu šifrována. Řešením je přidání podpory šifrování přes SSL/TLS (HTTPS) běžící standardně na portu TCP portu 443.

Domain Name Systém (DNS)

V počítačové síti je počítač, server definován vlastní IP adresou, jak v lokální nebo ve veřejné síti. Pro uživatele se lépe pamatuje textové jméno serveru www.seznam.cz, než aby zadával do internetového prohlížeče adresu 77.75.72.3. DNS slouží k překladu textových jmen počítačů na IP adresu.

Telnet

Tento nešifrovaný protokol slouží pro emulaci terminálu a komunikuje přes síťovou kartu se vzdáleným serverem. Nevýhodou je slabá bezpečnost tohoto protokolu, přihlašovací údaje a hesla se dají útočníkem odchytit a tím získat přístup na server. Obousměrný osmibitový protokol běží standardně na TCP portu 23.

File Transfer Protocol (FTP)

Díky tomuto protokolu můžeme přenášet data z jednoho systému do druhého. Pomocí FTP zašleme požadavek spojení na server, kde běží FTP server. Následně budeme vyzváni na přihlašovací údaje od serveru, po potvrzení se vytvoří spojení a můžeme přenášet data ze serveru a zpět. File Transfer Protocol běží standardně na TCP portu 20 nebo 21. FTP přenos není šifrovaný, přenášená data je možné odchytit.

Simple Mail Transfer Protocol (SMTP)

Zajišťuje přenos elektronické pošty mezi servery a klient – server. Cílem je zajistit spolehlivý a efektivní přenos elektronické pošty. Simple Mail Transfer Protocol standardně na TCP portu 25. Nakonfigurovat SMTP server je velice složité z hlediska bezpečnosti.

Secure Shell Protocol (SSH)

Jak bylo uvedeno, protokol FTP a Telnet z hlediska bezpečnosti je špatný, proto pro podobné služby byl implementován protokol SSH zajištující větší bezpečnost, při přenosu jsou všechna data šifrována. SSH běží standardně na TCP portu 22.

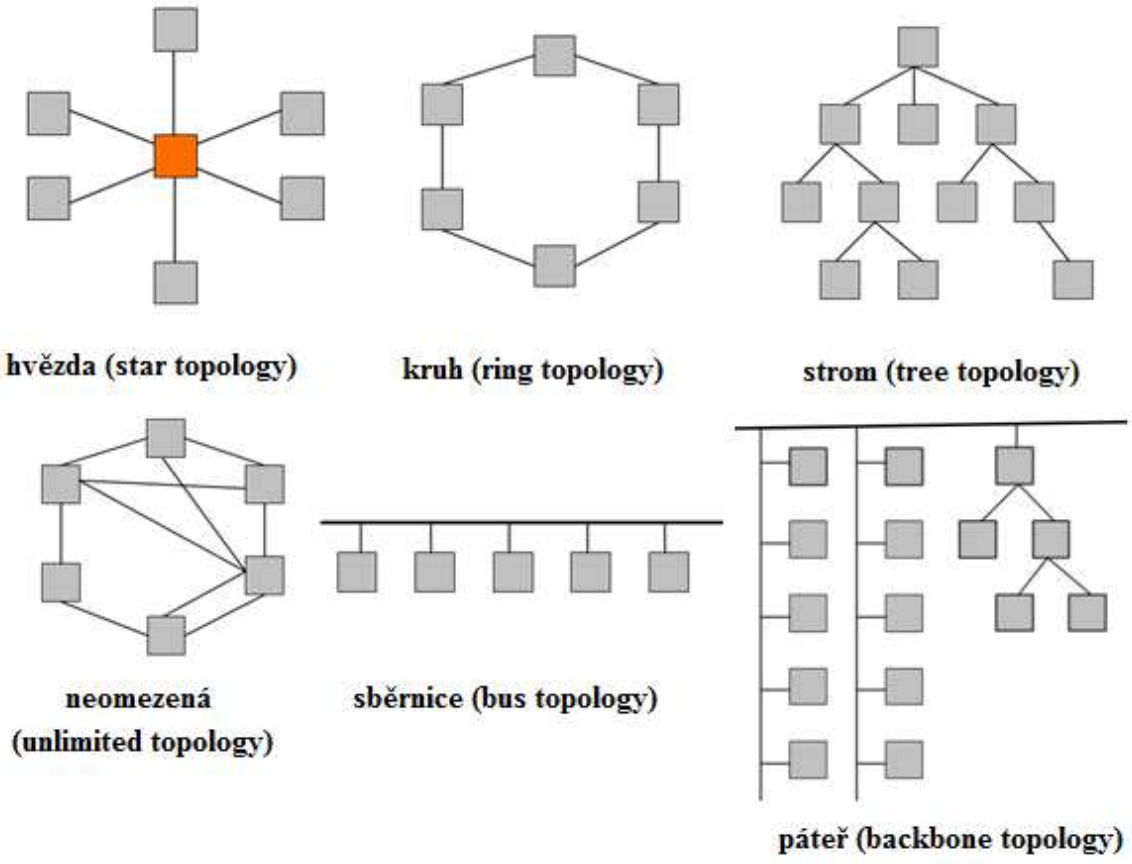
3. ARCHITEKTURA SÍTÍ

3.1 Síťová topologie a architektura

Počítačové sítě můžeme rozdělit podle jejich rozsahu na LAN (Local Are Network), MAN (Metropolitan Area Network) a WAN (Wide Area Network). Pod každou z těchto sítí si musíme představit několik počítačů a prvků, které jsou nějak propojeny. Způsob jejich propojení můžeme vyjádřit grafem. Uzly představují počítače a prvky, jejich propojení nám představuje většinou jejich kabelové propojení. Celkové jejich uspořádání tvoří topologii sítě.

3.1.1 Topologie sítí

Na obrázku 10 jsou znázorněny topologie sítí, uzly mohou představovat počítačové stanice a zřízení jako hub, switch apod.



Obr. 10 *Topologie počítačových sítí*

Popis topologií:

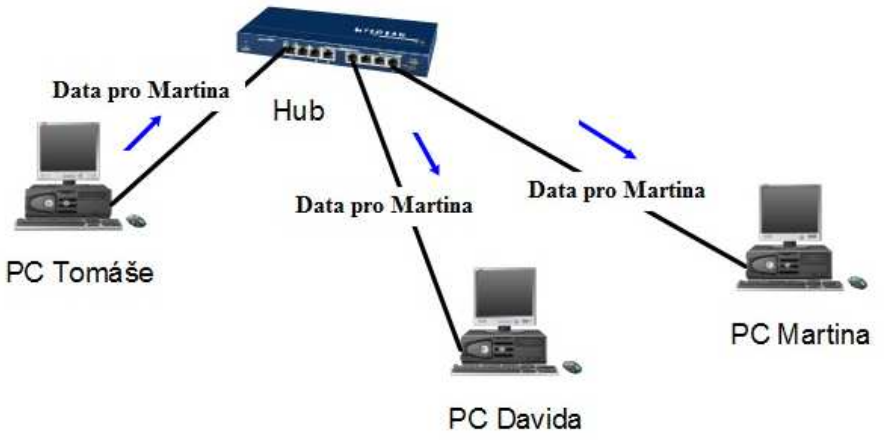
- Hvězdicová topologie – stanice jsou propojeny s rozbočovačem (hub). Často bývá kombinována se stromovou topologií.
- Kruhová topologie – stanice jsou propojeny do souvislého kruhu, data jsou přenášena od jedné stanice ke druhé.

- Stromová topologie – rozšíření hvězdy, nejpoužívanější v LAN
- Sběrnicová topologie – jednotlivé stanice jsou připojeny konektory k průběžnému vedení tvořené segmenty. Výhodou topologie je nižší spotřeba vedení, nevýhodou je hledání poruchy.

3.1.2 Aktivní prvky

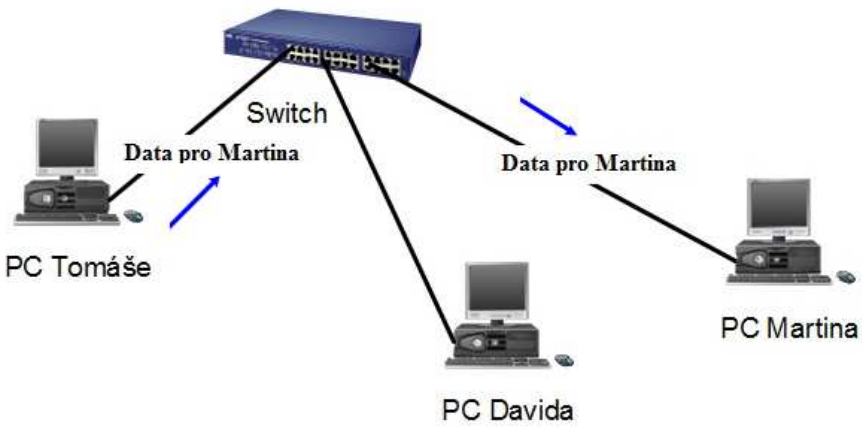
Dva osobní počítače mezi sebou komunikují pomocí vlastní síťové karty, propojené kabelem. Přidáním třetího počítače bychom potřebovali další kartu a kabel pro propojení. Ve velkém množství počítačů je tento způsob řešení neefektivní, řešením je vést z každého počítače jeden kabel a zapojit je do speciálního síťového zařízení, kterému se říká aktivní prvek. Mezi tyto prvky patří:

Rozbočovač (hub) - z každého počítače je k němu přiveden kabel. Pouze naslouchá, všechny příchozí elektrické signály opakuje do všech připojených zařízení (viz obr. 11).



Obr. 11 *Hub – přenos dat*

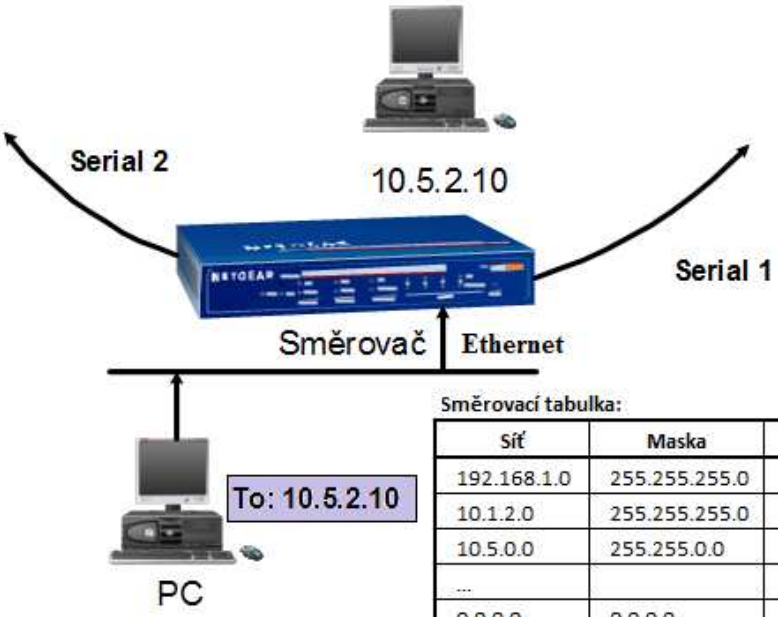
Přepínač (switch) – obvykle pracuje na druhé (linkové) vrstvě, příchozí elektrické signály od vysílajícího jsou přepínačem zaslány pouze příjemci. Umožňuje paralelní komunikaci mezi porty (viz obr. 12).



Obr. 12 *Switch – přenos dat*

Směrovač (router)

Často se považuje za zařízení sítí WAN, přesto však mohou najít své místo v LAN. Komunikuje na vrstvě datových spojů a síťové vrstvě. V síti LAN může plnit úlohu gateway, segmentaci přístupových domén a domén nesměrového vysílání. Směrovač rozhoduje, kam příchozí IP-datagramy bude posílat, zda do svého nebo do jiného rozhraní. Na následujícím obrázku směrovač obdržel od počítače IP-datagram adresovaný stanici 10.5.2.10 a musí rozhodnout, do kterého rozhraní ho může poslat dál (Seriál 1 nebo Serial2), nebo zpět do svého rozhraní. K rozhodování používá směrovací tabulku, v našem příkladě uvedenou na obrázku 13.



Směrovací tabulka:

Síť	Maska	Next Hop	Síťové rozhraní	Metrika
192.168.1.0	255.255.255.0	192.168.254.5	Serial 1	4
10.1.2.0	255.255.255.0	Lokální rozhraní	Ethernet	0
10.5.0.0	255.255.0.0	10.5.5.5	Serial 2	2
...				
0.0.0.0	0.0.0.0	10.10.10.2	Seriál 2	1

Obr. 13 *Rozhodování směrovače a jeho směrovací tabulka*

Při rozhodování se vezme z prvního řádku (seřazené tabulky) maska cílové sítě, která se bit po bitu vynásobí s IP adresou příjemce. Pokud se výsledek bude rovnat první IP adrese v sloupci, směrovač otestuje následující řádek, zdali neexistuje stejná adresa v tabulce s menší metrikou. [1]

Access Point

Zařízení pro bezdrátovou komunikaci slouží jako přístupový bod, klienti se k němu připojují pomocí rádiového spojení. Většinu přístupových bodů je možné konfigurovat pomocí WWW rozhraní, nebo přiloženého instalačního média. Mezi jeho služby patří DHCP server, NAT (překlad veřejných IP na soukromé), autentizace klientů proti RADIUS serveru. Může fungovat jako bridge, kde je součástí sítě LAN, nebo jako router, kde tvoří podsíť.

3.1.3 Firewall

Lze označit jako ochranný systém, který zajišťuje a vynucuje zásady přístupu mezi dvěma nebo více sítěmi. Povoluje, nebo zamítá průchod síťového provozu podle stanovených kritérií. Ochranný systém může tvořit počítač, nebo více počítačů popřípadě jiné zařízení na hraně sítě. Firewally můžeme rozdělit do následujících tří kategorií:

- Paketové filtry – zpravidla analyzují síťový provoz na transportní vrstvě, případně síťové vrstvě protokolů TCP/IP. Vytvářená pravidla paketového filtru jsou definována jako zdroj nebo cíl komunikace. Jednotlivá pole každého paketu jsou dobře známá a konfigurace pravidel se mohou řídit těmito informacemi:

  - zdrojová IP adresa,
  - cílová IP adresa,
  - protokol,
  - zdrojových port,
  - cílový port.

  Důležitou vlastností je, že pakety jsou buď zamítnuty, nebo povoleny a filtr se k nim už nevrací. Nevýhodou je, že fragmentované a libovolně sestrojené pakety mohou projít filtrem, konfigurace a udržovatelnost složitých pravidel je obtížná a některé služby se filtrovat nedají (neznáme port, než dojde ke spuštění relace)

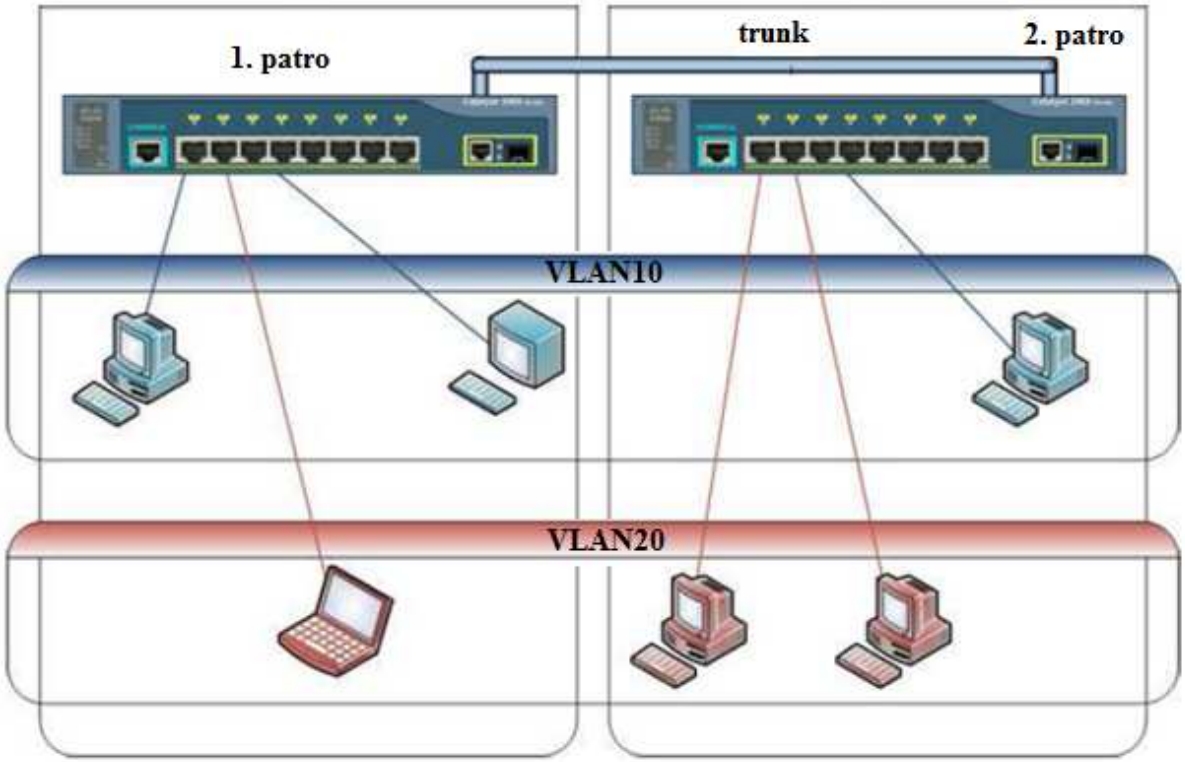
- Proxy filtry – zkoumají pakety z pohledu vyšších vrstev referenčního modelu ISO OSI, nejčastěji na vrstvách 4 až 7. Uživatel komunikuje se zabezpečeným proxy serverem, pomocí kterého se autentizuje do sítě a uplatní se zásady pro oprávnění. Nevýhodou je, že firewall tvoří v síti jediné zranitelné místo (při napadení je ohrožena bezpečnost celé sítě), obtížně se doplňují nové služby a často využívá služeb operačního systému na kterém je postaven, a zde může útočník využít slabých míst operačního systému. Pod zatížením pracuje pomaleji.

- Stavové paketové filtry – jsou kombinací nejlepších vlastností předchozích kategorií. Stavový paketový filtr si pamatuje informace pro každou relaci vedenou přes firewall. Při každém navázaní nového spojení jsou informace ukládány do stavové tabulky relačních toků. Výhody jsou v rychlosti, informace jsou ukládány do tabulky, ke které se firewall vrací a porovnává vůči navázaným komunikačním zařízením. [4]

4. ZABEZPEČENÍ SÍTĚ POMOCÍ VLAN

4.1 Co je to VLAN

Virtuální LAN slouží k logickému rozdělení sítě na menší sítě uvnitř fyzické struktury původní sítě. Následujícím obrázkem se dá jednodušeji vysvětlit VLAN (viz obr. 14).



Obr. 14 *Návrh VLAN v budově*

Na obrázku je návrh sítě v budově s dvěma patry. Na každém z nich jsou přepínače navzájem propojené. Chceme-li zařízení na patrech propojit, musel by se na každé patro zabudovat duplicitní přepínač pracující pro vlastní síť nezávislé na druhé. Toto řešení je nepraktické a neekonomické. S použitím VLAN můžeme tyto dvě sítě vytvořit a nastavit se současným zařízením.

VLAN se v dnešní době začala využívat z těchto důvodů:

- Snížení broadcastů – vytvořením více, menších broadcastových domén se snížením provozu zlepšuje výkon sítě.
- Zjednodušená správa – k přesunu zařízení z jedné sítě do druhé stačí překonfigurovat zařízení do jiné VLAN.
- Zvýšení zabezpečení – oddělením komunikace mezi zařízeními a jejich zařazení do speciálních VLAN, kam není jiný přístup.

- Oddělením speciálního provozu – součástí provozu mohou být například IP telefony, které můžeme provozovat na celé síti a zároveň je potřebujeme oddělit od ostatních sítí.
- Snížení množství HW – tím, že mohou být na jednom přepínači různé podsítě, nemusíme pořizovat žádné speciální zařízení navíc.

4.2 Základní způsoby přiřazení hostů do VLAN

Zpravidla na přepínačích, které podporují VLAN, existuje jedna defaultní VLAN číslo 1, kterou není možné odstranit či vypnout. Z bezpečnostních důvodů se tato VLAN nedoporučuje používat.

Hosty můžeme přiřazovat podle:

- Podle portu – port přepínače je napevno nakonfigurován do určité sítě VLAN. Veškerá přicházející komunikace na tento port spadá do zadané sítě. Pokud do tohoto portu připojíme další přepínač, tak všechny zařízení připojená k němu budou patřit do stejné VLAN. Jedná se o nejpoužívanější řešení, jednoduše se spravuje a je přehledné a rychlé.
- Podle MAC adresy – pro každé zařízení se spravují tabulky se seznamem MAC adres a VLAN. Rámce se zařadí do VLAN podle zdrojové MAC adresy. Přepínač musí vyhledávat v tabulce MAC adres, pokud zařízení přepojíme do jiného portu, bude automaticky zařazeno do příslušné VLAN.
- Podle protokolu přenášeného paketu – v praxi se moc nepoužívá, protože se musí přepínač dívat do třetí vrstvy, což znamená zpomalení. Zařízení musí mít napevno definovanou IP adresu.

4.3 Nastavování VLAN

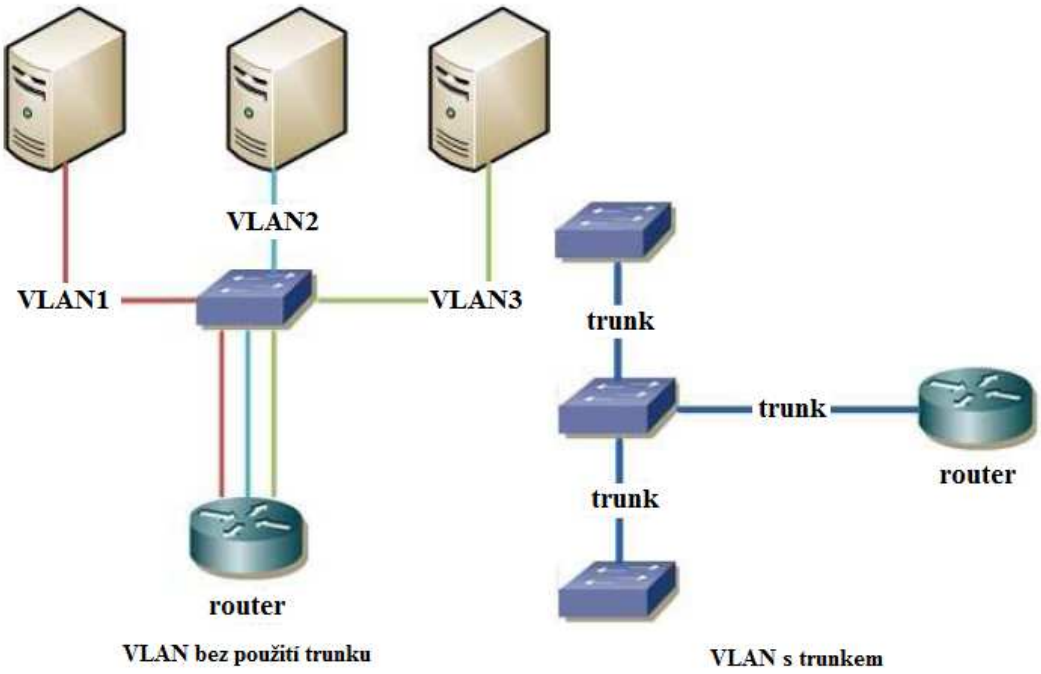
Identifikace VLAN je běžně pomocí čísla, pro jednodušší zapamatování a orientaci se k nim ještě přiřazují jména. Musí být pro správnou komunikaci na každém z přepínačů totožná. Možný číselný rozsah znázorňuje obrázek 15.

VLAN	popis
0 a 4095	reservované pro systémové použití
1	defaultní VLAN, standardně obsahuje všechny porty, nedá se smazat
2-1001	bežný rozsah pro ethernetové VLAN
1002-1005	speciální defaultní VLAN pro Token Ring a FDDI, nedají se smazat
1006-4094	rozšířené VLAN pro ethernet, nejsou vždy podporovány

Obr. 15 *Číselný rozsah VLAN*

Jednotlivé VLAN fungují naprosto odděleně, k propojení jednotlivých přepínačů je potřeba použít stejný počet kabelů, kolik je existujících VLAN. Při větším počtu VLAN přicházíme o volné porty na přepínači a zároveň u nízkého provozu používáme zbytečný

počet předimenzovaných kabelů. Z tohoto důvodu se dají propojit přepínače trunk kabelem a nastavit port jako trunk port, skrze něj pak probíhá veškerá komunikace VLAN do něj přiřazených. Při jeho použití ušetříme porty na přepínači, avšak probíhající komunikace všech VLAN na něj připojených se dělí o jeho datovou propustnost. Na obrázku 16 jsou znázorněny zmiňované propojení VLAN.



Obr. 16 *VLAN bez použití trunku a VLAN s trunkem*

4.4 VTP – VLAN Trunking Protocol

Většinou chceme, aby vytvořené VLAN existovaly ve více částech sítě (ne na jednom přepínači). Pro přenos informací o VLAN, se mezi přepínači využívá protokol VLAN Trunking Protokol (VTP) spravující přidávání, mazání a přejmenování VLAN uvnitř VTP domény. VTP doména je tvořena síťovými zařízeními se stejným jménem domény a jsou propojeny pomocí trunku. Každý přepínač ve VTP doméně má nastavený jeden ze tří těchto modů:

- Server – vytváří a maže VLAN, rozesílá informace o doméně – advertisements, udržuje inkrementální revizní číslo, které rozesílá z důvodu aktualizace.
- Klient – přijímá konfigurace ze serveru a udržuje lokální kopii (nelze měnit).
- Transparentní – ignoruje VTP, vytváří a maže lokálně VLAN, může přeposílat VTP advertisements (každých 5 minut server rozesílá, nebo při změně konfigurace).

4.5 Směrování mezi VLAN

VLAN se chovají jako klasické fyzické sítě, pro směrování mezi nimi potřebujeme mít každou síť zapojenou do směrovače. Směrovač si zapíše do směrovací tabulky informace o VLAN. Zde může nastat problém v případě zapojení trunk portu do směrovače, protože každá síť potřebuje výchozí bránu pro odesílání paketu. Protože se IP adresa nevyskytuje ve dvou

VLAN zároveň, máme možnost port rozdělit na takzvané subinterface a každé z nich nastavit příslušnou IP adresu. Ukázka nastavení je uvedena níže. [15]

```
ROUTER(config)#interface fastethernet 0/1.1 //port s indexem
ROUTER(config-if)#encapsulation dot1q 123 // přiřazení subinterface VLAN123
ROUTER(config-if)#ip address 192.168.20.1 255.255.255.0 // nastavení IP adresy
```

5. OPERAČNÍ SYSTÉMY

5.1 Operační systém MS Windows

Nejpoužívanější operační systém v domácnostech a firmách. Na začátku svého vzniku se proslavil špatnou bezpečností svých aplikací. Např. u verzí Windows 9x a Windows Me byl použit souborový systém FAT, který neumožňuje zabezpečení na úrovni souborů. Hesla jsou generována a uložena v souborech PWL, které jsou umístěny v adresáři C:\WINDOWS na které odkazuje soubor SYSTEM.INI. Tyto soubory PWL útočník zaměnil za své a díky svému heslu se přihlásil na konkrétní stanici. Tyto systémy jsou na svou dobu vynikající, ale z hlediska bezpečnosti v pozdější době jsou nahrazeny Windows XP. Za zmínku stojí verze Windows NT, systém s podporou počítačové sítě, kde slabina byla v programu Netmon, kde útočník mohl získat kontrolu nad serverem. Od Windows 2000 firma Microsoft začala brát větší zřetel na bezpečnost. Přináší novou adresářovou službu Active Directory, která tvoří jádro modelu zabezpečení operačního systému a poskytuje informace o objektech v síti. Tato služba slouží jako jediné místo, kde se nastavuje správa klientů, serverů, aplikací a uživatelských účtů. Od devadesátých let firma Microsoft slibovala verzi Windows, která bude bezpečnější, stabilní a hlavně kompatibilní. Tento slib se stal skutečností ve verzi Windows XP Home Edition a Windows XP Professional, ke které většina klientů přešla. O několik let později přišel Microsoft s Windows Wista (velké hardwarové nároky) a o něco později přišel s Windows 7 (v současné době novinkou na trhu, menší nároky na hardware). [5]

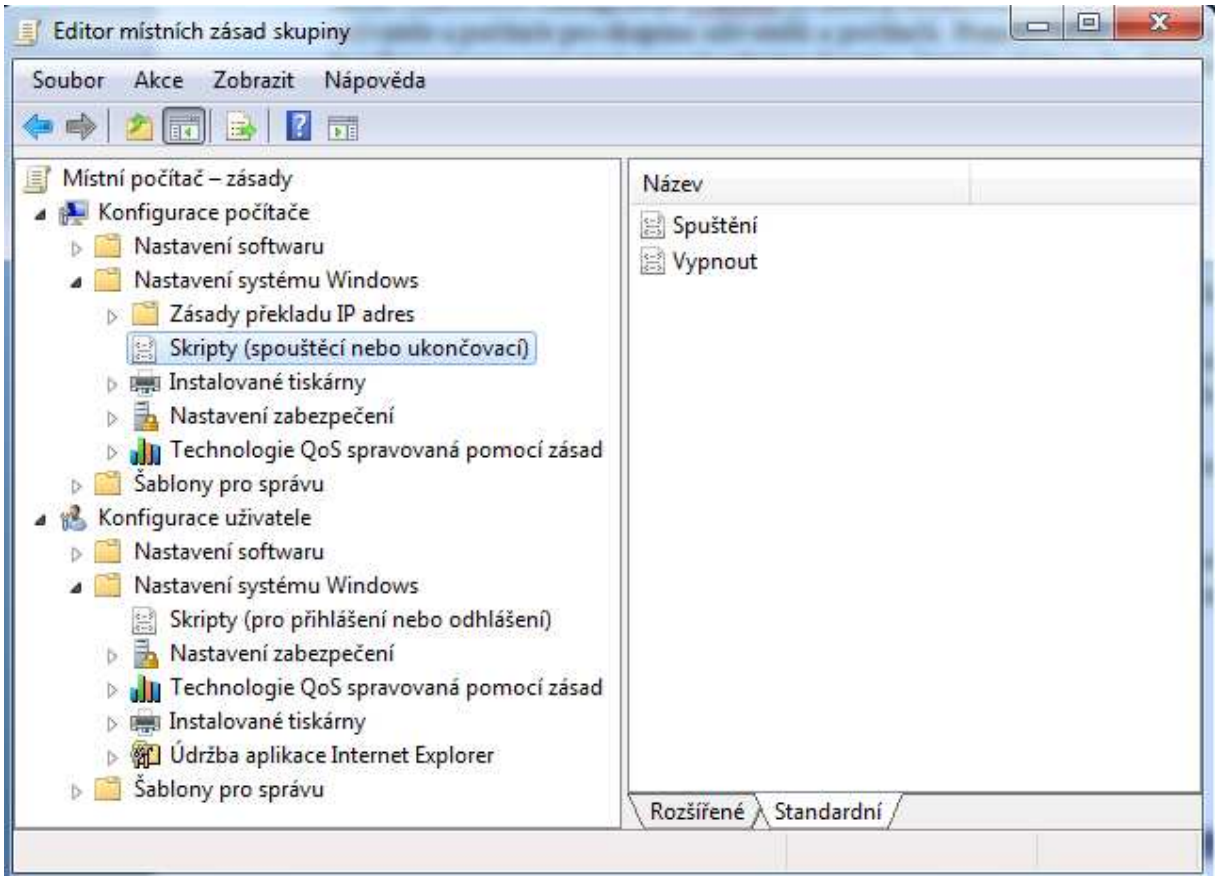
5.1.1 Local policy

MMC (Microsoft Management Console) je nástroj sloužící ke tvorbě zásad a definování konfigurace uživatele a počítače pro skupinu uživatelů a počítačů. Pomocí MMC můžeme vytvořit specifickou konfiguraci pracovní stanice pro konkrétní doménu, která je uložena do objektu a přidružena k službě Active Directory. Tyto zásady můžeme specifikovat:

- založené na registru – zásady pro operační systém a programy,
- možnosti zabezpečení – nastavení zabezpečení místního počítače, domény a sítě,
- možnosti instalace a údržby softwaru – centrální instalace, aktualizace a odebrání programu,
- možnosti skriptů – spouštěcí a ukončovací skripty pro počítač a uživatele,
- možnosti přesměrování složky – umožňuje přesměrovat složky do síťového umístění.

Zásady skupiny umožňují nastavit stav prostředí stanice uživatele, které systém aplikuje a vynutí. V MMC nástroji buď můžeme přidat modul snap-in zásady místního počítače, nebo můžeme jednotlivý snap-in modul spustit v příkazovém řádku, v našem případě napíšeme gpedit.msc a potvrdíme klávesou Enter. Moduly snap-in mají příponu souboru msc (viz obr. 17).

Na následujícím obrázku je zobrazen editor místních zásad skupiny, kde se definují a nastavují zásady pro místní počítač. Modul místního počítač obsahuje dvě hlavní větve. První slouží ke konfiguraci zásad vztahující se na počítač, a druhá se vztahuje k nastavení zásad pro uživatele přihlašujících se k počítači. [17]



Obr. 17 *Editor místních zásad skupiny*

5.1.2 Domain policy

V některých firmách se používá na stanicích operační systém Windows, stanice jsou přidány do domény, která je založena na serveru s Windows Server 2003 (v současné době jeho nástupce je Windows Server 2008). Z hlediska bezpečnosti představuje mocný nástroj zajištující bezpečnostní politiku firmy. Windows server může zajišťovat například služby DHCP, DNS, sdílení disků a tiskáren. Využívá také konzolu MMC pro správu jednotlivých komponent systému. Jeden z bezpečnostních nástrojů je adresářová služba Active Directory, umožňující nastavování doménové politiky, správu uživatelů a počítačových stanic, aktualizaci a instalaci software, které se replikují na jednotlivé stanice. [18]

5.1.3 Bezpečnostní rizika v aplikacích společnosti Microsoft

Některé nejběžnější používané aplikace pro operační systém Windows představují slabá místa v zabezpečení. Mezi tyto nejnebezpečnější aplikace například patří:

- Microsoft Internet Explorer (webový prohlížeč),
- Microsoft Exchange Server (správa elektronické pošty),
- Server IIS (Internet Information Server).

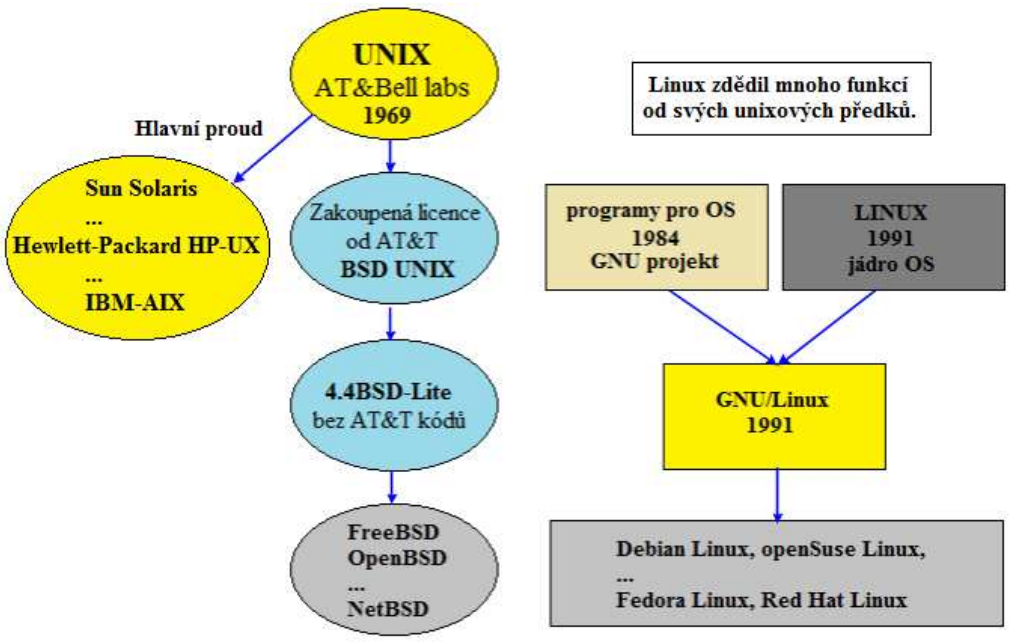
Je dobré si uvědomit, že existují hrozby nejen z operačního systému, ale také z jeho aplikací. Během roku vychází opravné balíčky pro systém a aplikace od společnosti Microsoft, které opravují jejich chyby. Pokud chceme, aby naše síť byla bezpečná, musíme tyto balíčky aplikovat.

5.2 Operační systém Linux

V roce 1984 byl Richardem Matthew Stallmanem založen projekt GNU. Cílem projektu bylo vytvořit svobodný operační systém, který v té době neexistoval. Veškeré důležité součásti operačního systému jsou navrženy, ale jádro systému není vytvořeno. V roce 1991 finský student Linuse Torvaldse vytvořil jádro operačního systému Linux. Vznikl GNU/Linux, který se skládá z programů pro operační systém z projektu GNU a linuxového jádra. Programy pro projekt GNU využívají licenci GPL (General Public License), neboli volně šiřitelný program.

Rok 1991 můžeme považovat za počátek Linuxové éry, ale z hlediska historie musíme jít do roku 1969, kdy vznikl operační systém UNIX, jako výzkumný projekt v AT&T Bell Labs. V roce 1976 je zdarma poskytnut americkým univerzitám, kde se stal základem kurzů o operačních systémech a akademických výzkumných projektech. V roce 1977 zakoupila Skupina pro výzkum počítačových systémů (Computer Systém Research Group, CSRG) v Berkeley na Kalifornské Univerzitě od firmy AT&T Bell Labs licenci na zdrojové kódy a začali vydávat vlastní verzi BSD (Berkeley Software Distribution) Unixu pro počítač PDP-11. V Berkeley byl stanoven dlouhodobý projekt k odstranění zdrojových kódů patřící AT&T Bell Labs z BSD, protože se Unix stal součástí komerčního prostředí a cena za licence rostla. Tento projekt se nepodařilo dokončit z finančního důvodu a CSRG byla zrušena. Před zánikem CSRG uvolnila svoji definitivní verzi kódu neobsahující kódy AT&T pod názvem 4.4BSD-Lite.

Aby vznikl plnohodnotný operační systém, tak potřebujeme k jádru Linuxu přidat další software, příkazy apod. V terminologii to nazýváme distribuce. Distribuce mají různá zaměření, podporu a různou oblibu. Historie Unixu a Linuxu je uvedena na následujícím obrázku, kde jsou také uvedeny nejznámější distribuce Linuxu (viz obr. 18).

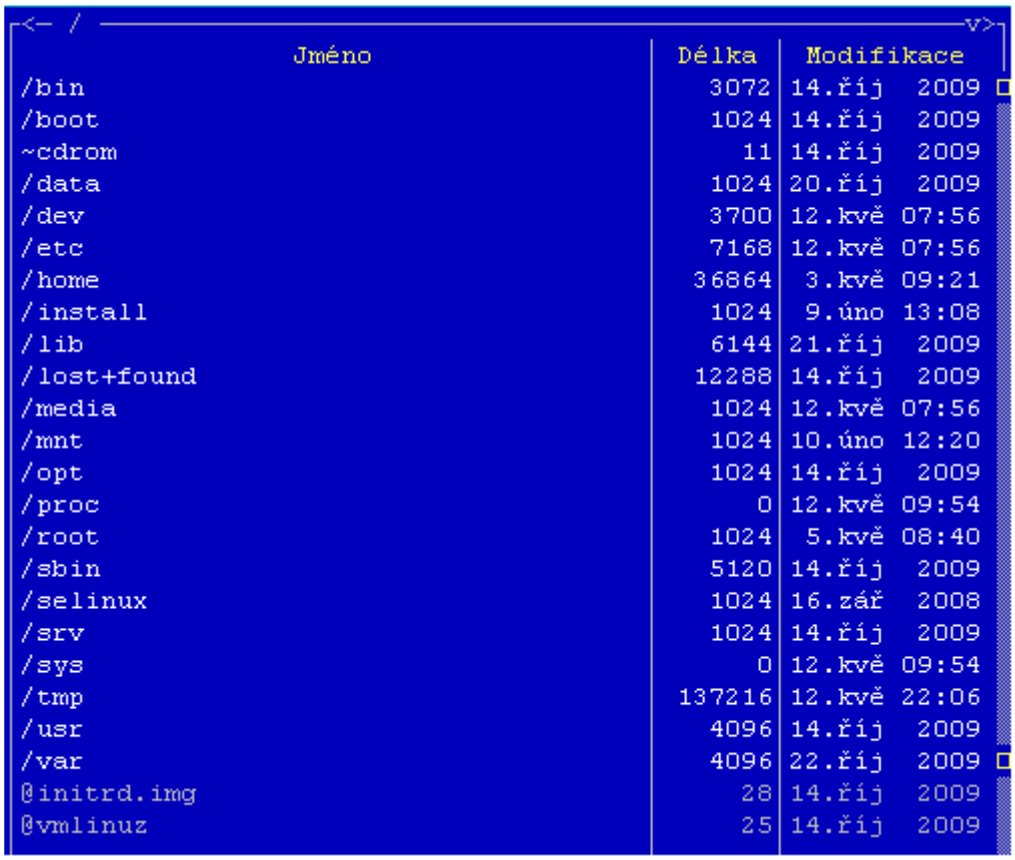


Obr. 18 *Historie UNIX a Linux*

Každá distribuce Linuxu má rozdilné kořenové adresáře, mezi standardy patří tyto:

- /bin – základní spustitelné soubory pro všechny uživatele,
- /boot – zde je uložen zavadeč Grub a jádro systému,
- /dev – obsahuje terminály zařízení ve formě souborů, umožňující komunikovat pomocí systémového volání,
- /etc – zde jsou textové konfigurační soubory, často se zde nastavují konfigurace nových balíčků a jejich závislosti, v adresáři /etc/init.d/ jsou spustitelné skripty služeb, např. příkazem v shellu se spustí Apache2 */etc/init.d/apache2 start*, můžeme použít ještě parametr stop a restart,
- /home – domovské adresáře uživatelů,
- /lib – sdílené knihovny systému, fonty a mapování klávesnice,
- /root – domovský adresář uživatele root,
- /tmp – dočasné soubory,
- /var – zde spuštěné aplikace zapisují své logy, nalezneme zde například chyby při spuštění aplikace, ověřování uživatelů a podobně. Bývá zde také standardní adresář www, kde jsou uloženy stránky pro webový server.

Na obrázku 19 je adresářová struktura Linuxu Debian Lenny.



Obr. 19 *Adresářová struktura Linuxu Debian Lenny*

V dalších kapitolách budou uvedeny programy a služby nejčastěji používané v bezpečnosti sítí LAN.

5.2.1 Samba

Je faktem, že Linux není u uživatelů tak rozšířen jako Windows, který jich má milióny. Na druhé straně Linux se stal spolehlivým a rozšířeným operačním systém pro servery. Ke spolupráci těchto systémů se využívá systém CIFS, který je založena protokolech SMB (Server Message Block).

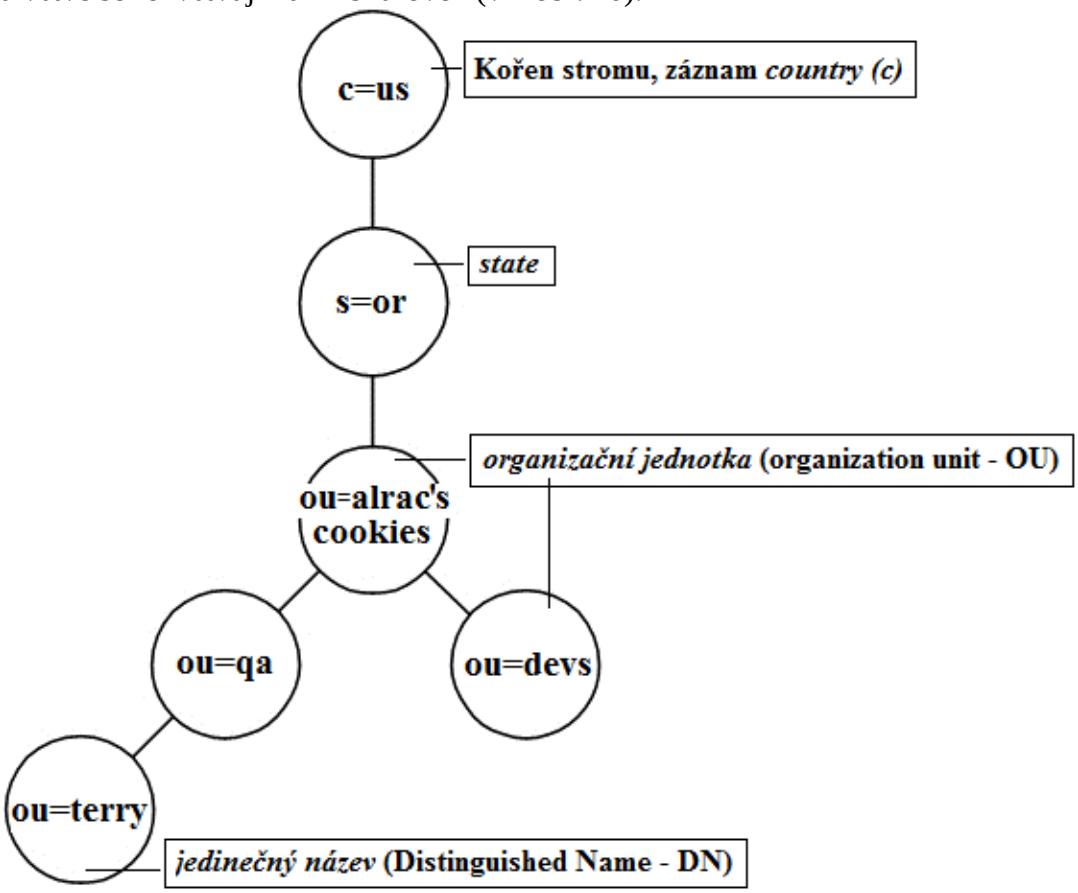
Samba je programový balík GNU, který implementuje svoji část protokolu CIFS na Linux server. Samba podporuje pokročilé vlastnosti, včetně přihlašování do domén Windows. Systém CIFS zde nabízí tyto služby:

- sdílení souborů,
- síťový tisk,
- autentizaci a autorizaci,
- vyhledávání jmen,
- oznamovaní služeb.

Každý uživatel, který chce přistupovat k sdíleným diskům pomocí SMB protokolu, musí mít založený uživatelský účet a přidělená práva k sdíleným diskům na serveru, kde běží Samba.

5.2.2 LDAP

Je odlehčený protokol pro ukládání a přístup k datům na adresářovém serveru. Na obrázku níže je znázornění stromové struktury adresáře LDAP, kde kořen je na nejvyšší úrovni a větve se rozvětvují na nižší úroveň (viz obr. 20).



Obr. 20 *Hierarchické uspořádání LDAP*

Na obrázku (viz obr. 20) je jedinečný název terry, tento název obsahuje také relativní jedinečný název (Relative Distinguidhed Name – RDN), což jsou záznamy všech jeho předchůdců, které tvoří UID (uid=terry, ou=qa,ou=alracʹs cookies, ou=or,c=us). Základní jednotkou je objekt adresáře (záznam). Záznam terry obsahuje atributy, kde každý atribut obsahuje typ a jeho hodnoutu. Atributy mohou mít několik hodnot a mohou vypadat následovně:

uid=terry
cn=T. Jones
gn=Terry
sn=Jones
telephonNumber=567 349 907
mail=tery@alrac.com

Vrcholem hierarchického uspořádání LDAP je na obrázku přípona c=us, tvoří tzv. sufix a názvový kontext (naming kontext). Nejčastěji se používá jako doménový název firmy, například dc=alrac, dc=com. [11] [19]

6. BEZDRÁTOVÉ SÍTĚ

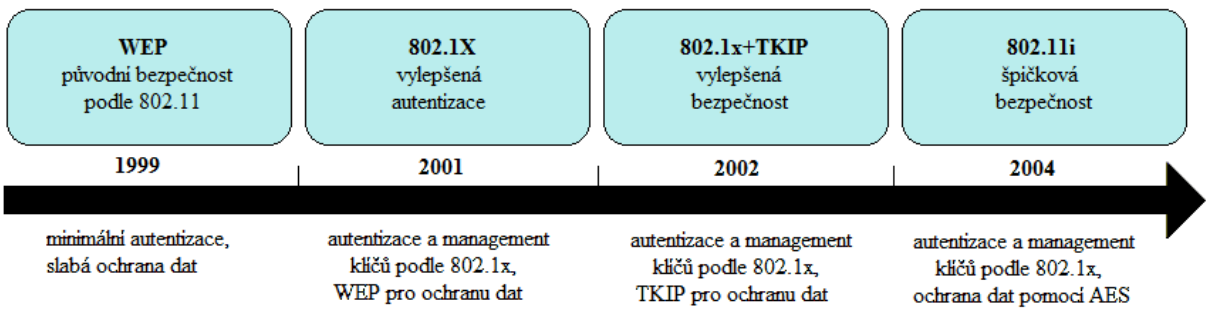
U bezdrátových sítí (WLAN) vzrostla popularita natolik, že se jejich podpora integruje přímo do nových notebooků, telefonů a podobných komunikačních zařízení. Bezdrátové sítě umožňují uživatelům pohodlný pohyb v areálu firmy, bez přerušení spojení a komunikovat s podnikovou sítí. Komunikovat s podnikovou sítí přes veřejný internet prostřednictvím veřejných bezdrátových sítí znamená pro firmu bezpečnostní problém. Veřejná bezdrátová síť je přístupná každému, tito lidé mohou odposlouchávat veškerou komunikaci a tím zneužít citlivá data. Musíme si uvědomit, že WLAN jako Internet nejsou důvěryhodné sítě a tak musíme při návrhu dohlížet také jak na to tuto, síť co nejlépe zabezpečit.

6.1 Zabezpečení bezdrátových sítí

Zabezpečení podle vrstev:

- na fyzické vrstvě – vymezení prostoru a průniku signálu (řešení rušení, modulací …), u antén využívat směrové a omezit použití všesměrových antén.
- na linkové vrstvě – CSMA/CA, šifrování. U MAC specifikovat seznamy povolených a zakázaných klientů podle MAC adres. Ověřování identity klienta je na druhé vrstvě buď otevřeně, nebo prostřednictvím sdíleného veřejného klíče – WEP. U 802.1x s serverem RADIUS (EAP , certifikáty serveru a uživatelů, přihlášení pomocí hesel). Filtrovat provoz promocí protokolů a silného šifrování (DES/3DES).
- na síťové vrstvě – filtrace IP adres a řízení přístupu pomocí jejich seznamů. Využití firewalu pokud je k dispozici. VPN (Virtual Private Network) – šifrování pomocí IPSec a tunelování prostřednictvím L2TP,PPTP.
- na aplikační vrstvě – monitorovací nástroje, autentizace klientů pomocí RADIUS serveru.

Vývoj zabezpečení WLAN je uveden na obrázku 21.



Obr. 21 *Vývoj zabezpečení WLAN*

6.2 Service Set IDentifier (SSID) a WEP

Základní mechanismy bezpečnosti v 802.11b. SSID reprezentuje konkrétní síť (označení dané sítě tvořené WLAN), klienti se připojují pouze k WLAN, jejíž SSID znají. Access point vyžaduje od klientů znalost SSID. Acces point vysílá v časových intervalech své

SSID tak, aby klient o něm věděl. V jiném případě musí klient vyslat zprávu k zjištění existence přístupového bodu. Z hlediska zabezpečení je dobré zakázat SSID, změnit implicitní nastavení na přístupovém bodu. Pravidelně měnit SSID a používat složité názvy (firma, majitel přístupového bodu) tak, aby je nebylo možné uhodnout. [9]

6.3 Wired Equivalent Privacy (WEP).

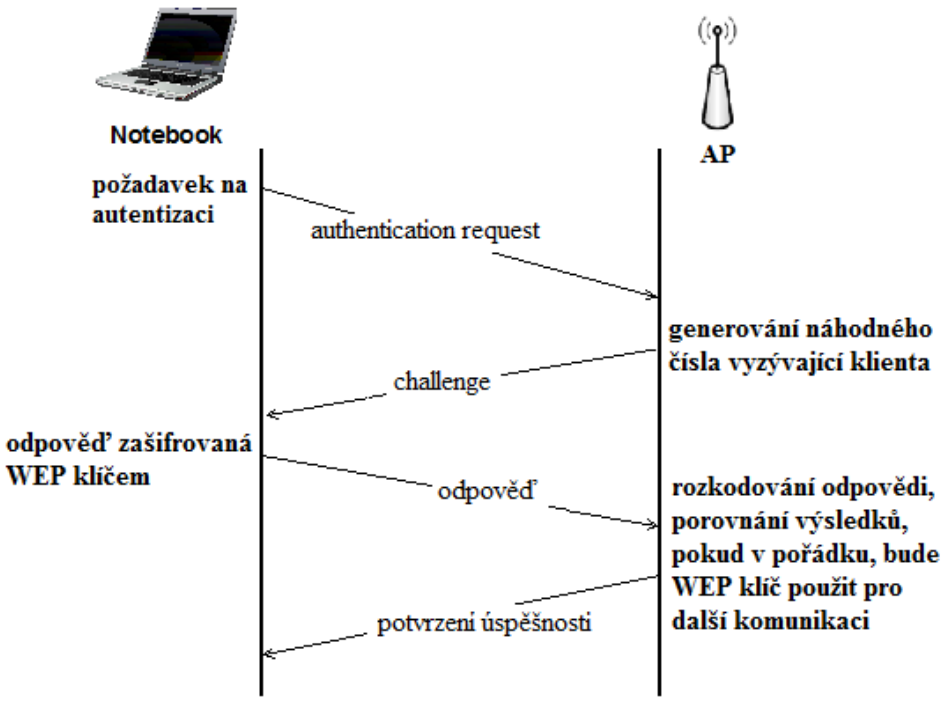
V sítích 802.11 je tento protokol zabudovaný jako standard pro zabezpečení rádiové části počítačové sítě, který využívá symetrický postup šifrování (pro šifrování a dešifrování se používá stejný 40 bitový klíč). Symetrický klíč je pro všechny uživatele stejný, u autentizace k přístupovému bodu ho klient používá se svou MAC adresou (ověřuje se totožnost síťové karty).

6.3.1 WEP autentizace

Může být jako open system (otevřená autentizace), nebo pomocí sdíleného klíče. Režim autentizace nemá přímou souvislost s šifrovaním dat. Při open systému lze použít WEP klíče, čímž získáme větší zabezpečení dat a jejich přenosu (viz obr. 22).

- U otevřené autentizace se může jakýkoliv klient připojit k přístupovému bodu bez zadání přihlašovacích údajů. Klient odešle identifikační údaje v autentizačním rámci. Acces point zkontroluje indetifikační údaje a zašle zpět rámec – authentication verification

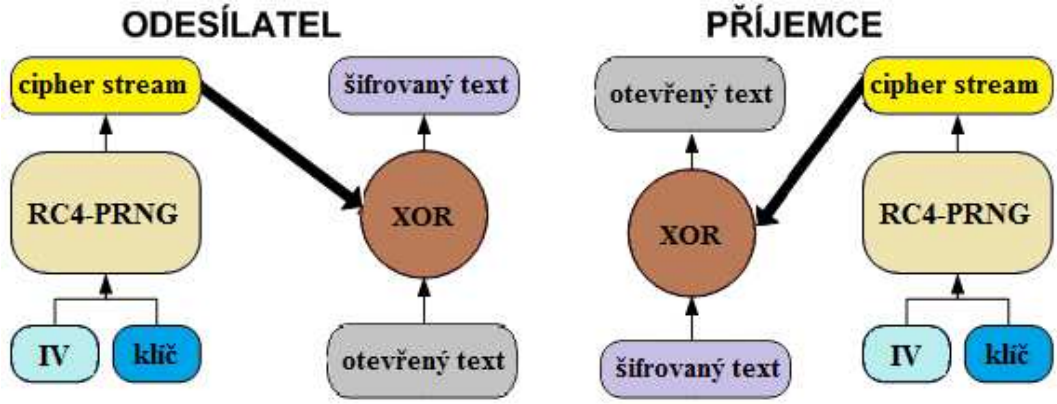
- Autentizace sdíleným klíčem probíhá tak, že po obdržení požadavku klienta je klientovi zasláno náhodné číslo, které klient zašifruje svým klíčem a odešle zpět. Acces point udělá to samé u sebe a pak obě hodnoty porovná. Pokud jsou shodné, je přístup povolen.



Obr. 22 *Autentizace sdíleným klíčem (shared key)*

6.3.2 WEP šifrování

Využívá se 64 bitový klíč, který je složen z uživatelského klíče a 24 bitový Initialization Vector (dynamicky měnící vektor). Vysílací strana vygeneruje vektor pro vytvoření šifry, který je následně zasílán v záhlaví každého paketu. Příjemce provede dešifrování dat pomocí sdíleného klíče a měnícího vektoru. WEP používá symetrickou proudovou šifru RC4 využívanou v SSL. Tento algoritmus generuje náhodná čísla a umožňuje šifrovat otevřené texty, kde jeden bit textu je roven jednomu bitu šifry a nazývá se šifrovací proud (cipher stream). Tajný klíč je stejný, dochází pouze k periodickému měnění vektoru. Výsledkem je náhodná posloupnost jedniček a nul spojená s daty pomocí logické funkce XOR je šifrována, dešifrována (viz obr. 23). [9]



Obr. 23 *Šifrování RC4*

6.3.3 Zabezpečení WEP

Nastavit nejvyšší úroveň šifrování a využívat směrové antény. K ověřování klientů instalovat RADIUS server a propojit s DHCP pro první autentizaci uživatele.

6.4 Filtrace MAC adres

Vytvořením přístupového seznamu ACL, ve kterém je seznam MAC adres s povoleným či zamítnutým přístupem. Nejlepší řešení je vytvořit seznam povolených MAC adres, protože MAC adresa se ukládá do firmware zařízení, které je možné změnit.

6.5 802.11x

Je nespecificky protokol pro bezdrátové sítě. IEEE 802.11x je bezpečnostní rámec zajišťující šifrování, distribuci klíčů a ověřování uživatelů. U ověřování bezdrátových sítí je realizováno pomocí access pointu WLAN.

Autentizace se provádí tak, že Access point zašle detekovanému klientovi zprávu EAP REQUEST-ID na kterou klient odpoví zasláním identifikačních údajů (EAP RESPONSE-ID). Tato data jsou zapouzdřena (EAPOL) a odeslána na RADIUS server, kde dochází k ověření uživatele a následně server zašle zprávu (ACCES_ACCEPT/DENY) obsahující zákaz nebo povolení přístupu do dané sítě, obsahující informaci pro klienta EAP SUCCESS/FAIIURE.

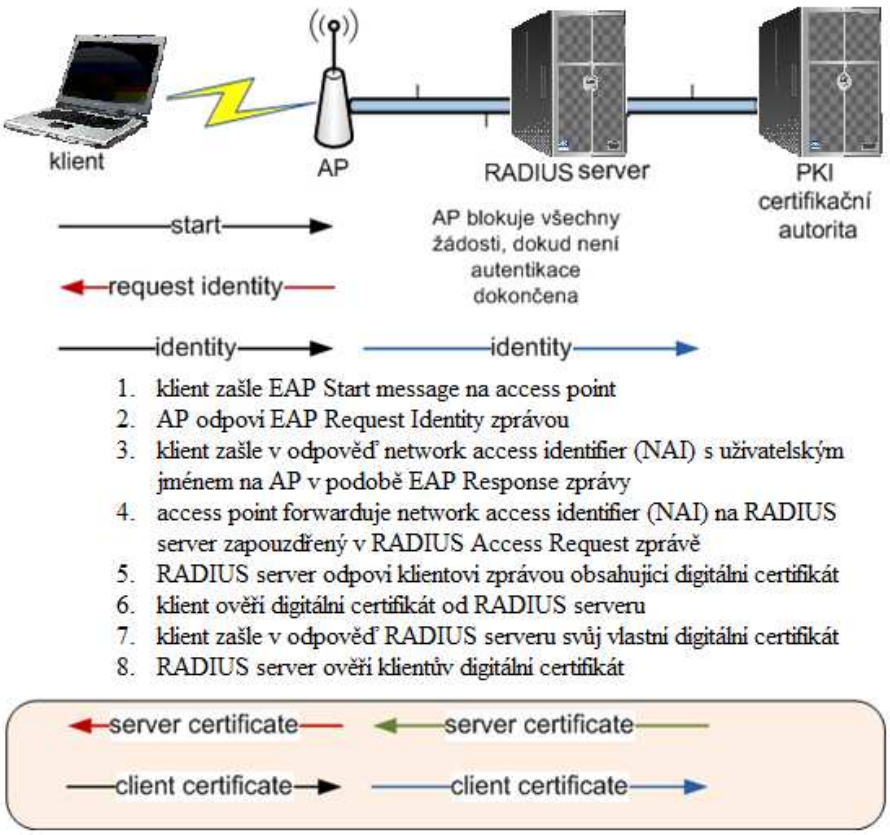
Pokud dojde k povolení přístupu, je pro daného uživatele povolen port pro přístup do sítě. [9]

6.6 WPA

Šifrování komunikace a přístup do bezdrátových sítí využívá mechanismy standardu 802.11i. Při šifrování se používá TKIP (Temporal Key Integrity Protokol), který používá 128 bitový klíč. TKIP pro každý paket mění dynamicky klíč. Integrita dat je kontrolována 64 bitovým klíčem.

WPA autentizace nabízí různé metody pro podniková prostředí a domácnosti:

- EAP-TLS a centralizovaného autentizačního serveru – klienti a server se navzájem identifikují pomocí digitálních certifikátů. Certifikáty musí být pro klienty a servery zakoupeny, nebo vyžít certifikační server (PKI). Certifikáty jsou chráněny TLS klíčem, který zabezpečuje kanál komunikace mezi Autentizační serverem (AS) a stanicí.
- PSK (Pre-Shared Key) – ověřování pomocí uživatelského hesla a login. Komunikace mezi RADIUS serverem a přístupovým bodem je šifrována pomocí sdíleného klíče. Komunikaci je možné chránit pomocí protokolu MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol) využívající jednosměrně zašifrované heslo, klient obdrží výzvu v podobě náhodně generovaného řetězce a id relace. Na výzvu klient odpoví identifikačními údaji, které jsou následně ověřeny RADIUS serverem. Pak server zašle zprávu o povolení či zamítnutí přístupu (viz obr. 24). Vytvoření a ochrana tunelu TLS pomocí PEAP. Možnost využití různých databází a distribučních seznamů.

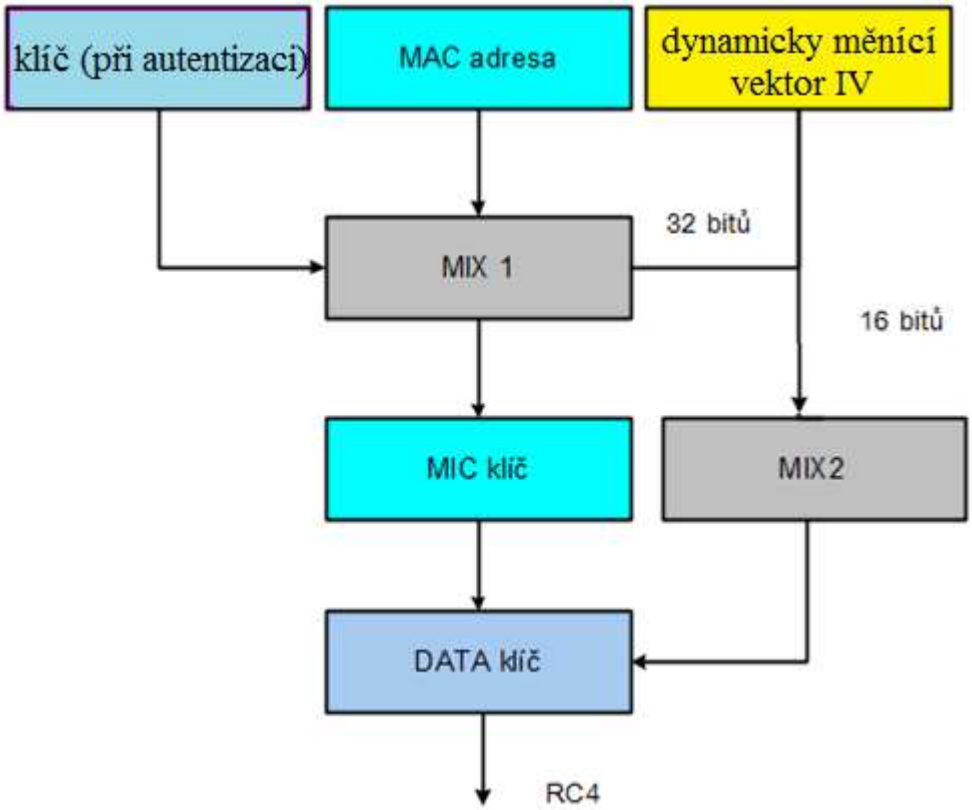


Obr. 24 *EAP-TLS autentizace*

6.6.1 WPA šifrování

48bitový Initialization Vector s TKIP vylepšuje zabezpečení. Vektor zde řeší dva úkoly (viz obr. 25):

- l6bitová hodnota se doplní do 24 bitů pro tradiční vektor
- 32bitová část se používá mixování klíčů jednotlivých paketů a tvoří pořadové číslo paketu. (PPK, Per Packet Keying).



Obr. 25 *princip WPA algoritmu*

WPA – MIC (metoda MICHAELS)

Každý rámec je vybaven kontrolním součtem (MIC), pokud se změní nebo poruší rámec, dojde k porušení jeho kontrolního součtu. Když tato situace nastane dvakrát do minuty, stanice bude odpojena a klíče se změní.

6.7 802.11i - WPA2

AES (Advanced Encryption Standard) představuje skupinu blokových šifer na kterých je založen protokol CCMP, zajištující ochranu přenášených dat.

7. REALIZACE ZABEZPEČENÍ LAN A WLAN

V předchozích kapitolách jsme se seznámili s problematikou bezpečnosti počítačových sítí. Byly zde představeny síťové protokoly, architektura sítí a bezpečnost bezdrátových sítí. Dále byly uvedeny operační systémy a jejich metody pro aplikování bezpečnosti.

Z výše uvedených znalostí je naším cílem vytvořit autorizaci bezdrátových klientů proti RADIUS serveru. Uživatelé se budou přihlašovat do bezdrátové sítě pomocí uživatelského jména a hesla, které bude uloženo v databázi MySQL. Dalším úkolem je nastavení limitu download a upload dat z internetu u bezdrátových klientů. Závěrem bude uvedena instalace a konfigurace doménového serveru pro stanice s operačním systémem Windows.

Dříve než se začneme věnovat konkrétními řešeními, je vhodné se seznámit s navrženými technologiemi.

7.1 Popis architektury

V této části jsou popsány základní informace o navržených technologiích.

7.1.1 Server RADIUS

Pro server byl vybrán operační systém GNU/Linux z důvodů stability a jeho ceny.

Jako distribuce GNU/Linux je použit Debian GNU/Linux 5.0.1. Tato distribuce obsahuje rozsáhlý repozitář instalačních balíčků a serverových aplikací svobodného software. Další výhodou je jeho stabilita a dostupnost pro mnoho platforem. Operační systém je možné stáhnout z oficiálních stránek *http://www.debian.org*. Instalace je přehledná a průběžně vedená nápovědou. Debian doporučuji nainstalovat bez grafického prostředí z důvodů větší bezpečnosti. Čím méně služeb běží na serveru, tím je potencionálně větší bezpečnost. V našem případě postačí vybrat dvě možnosti uvedené na obrázku 26.

Obr. 26 *Výběr programů*

7.1.2 Klienti RADIUS

Jsou zařízení pro bezdrátovou komunikaci sloužící jako přístupový bod, uživatelé se k němu připojí pomocí rádiového spojení. Uvedení klienti byli vybráni z důvodu jejich dřívějšího pořízení a jejich současnému využívaní v síti. Všechna tato zařízení je možné konfigurovat pomocí WWW rozhraní.

StraightCore WRT-312

Wifi router s 4-portovým přepínačem, podporující Wifi 802.11b/g. Přenosová rychlost je 100Mb/s, 54Mb/s. Podporuje šifrování 64 nebo 128-bitovým WEP kódem, WPA šifrování včetně TKIP a WPA2. Lze nastavit DHCP server, přístup podle MAC adres a adresní filtr.

Linksys WAP11 AP

Bezdrátový Access Point standardu 802.11b, pracující v pásmu 2,4 GHz s modulací DSSS a PBCC. Například podporuje 256 bitové WEP šifrování dat, filtrování připojených stanic na základě MAC adres.

WRT54G

Wifi router s 4-portovým přepínačem, umožnující připojení bezdrátových klientů. Komunikuje v pásmu 2,4 GHz, podporuje WLAN standardy 802.11b, 802.11g. Přenosová rychlost je 100Mb/s, 54Mb/s a podporuje protokoly TCP/IP, NetBEUI. Zabezpečení přístupu zvyšujeme funkcemi IP a Mac filtr, filtr portů, blokování www adres, omezením přístupu v daném čase, NAT technologií a podobně. Na obrázku níže je toto zařízení (viz obr. 27).

Obr. 27 *WRT54G*

V dalších kapitolách se budeme zabývat konkrétní konfigurací těchto zařízení.

7.2 Konfigurace serveru

V této kapitole se budeme zabývat instalací aplikace FreeRADIUS a následně její konfigurací pro použití MySQL databáze.

Jak již bylo uvedeno distribuce Debian Linux obsahuje v repozitáři mnoho aplikací, mezi nimi je také aplikace FreeRADIUS. Bohužel tato aplikace nemá zkompilovanou

podporu pro TLS. Proto doporučuji stáhnout zdrojové kódy z oficiálních stránek *http://freeradius.org*, kde nalezneme jeho nejnovější verzi. Současná verze kódů je uložena v komprimovaném archívu *freeradius-server-2.1.8.tar.gz*, tento archív je potřeba rozbalit a přeložit (kompilovat) do jádra operačního systému. Kompilace se provádí z důvodu správného chodu aplikace, která používá vlastní soubory knihoven. Tyto knihovny se po překladu nahrají do jádra operačního systému. Následující příkazy rozbalí archív zdrojových kódů a přeloží.

Stažený soubor nahrajte do /opt a tam jej rozbalte příkazem

`tar xzf` *freeradius-server-2.1.8.tar.gz*

V adresáři /opt vznikne nový adresář freeradius-server-2.1.8 do něj se přesuneme příkazem cd /opt/freerad* a zkompilujeme následující příkazy. Dodržujeme následující pořadí příkazů a vždy počkejme, než se příkaz provede celý.

./configurel
make
make install

Debian Linux používá balíčkovací systém APT, který usnadňuje instalaci aplikací. Aplikace se instalují z repositáře následujícím příkazem:

apt-get install xxx (xxx představuje jméno balíčku)

7.3 Instalace aplikace FreeRADIUS a databáze MySQL

Po instalaci aplikace FreeRADIUS je potřeba provést následující konfiguraci. Konfigurační soubory se nachází v adresáři */usr/local/etc/raddb.*

Konfigurační soubory:

- radius.conf – hlavní konfigurační soubor, zde se nastavují jednotlivé moduly. V našem případě zde povolíme modul pro databázi MySQL, kde budou informace o uživatelích uloženy. Povolíme následující řádek odstraněním znaku #.

  # $INCLUDE sql.conf

  FreeRADIUS 2 – od této verze byl konfigurační soubor rozdělen a další konfigurace se provádí v adresáři */sites-enabled* a */sites-available* konfigurací souboru *inner-tunnel.* V souboru ho povolíme odstraněním znaku # u *#sql v části authorize a authenticate.*

- eap.conf – zde se nastavuje metoda, jak budou uživatele ověřováni (certifikátem, heslem apod.) V našem případě zde bude nastavené:

  default_eap_type = md5
- clients.conf – zde se konfigurují všechna zařízení, která budou ověřovat proti freeradiusu, AP apod. Níže je uvedená ukázka nastavení klienta, kde se uvádí jeho IP

adresa, tajné heslo pro komunikaci, náš název zařízení pro jeho identifikaci a typ zařízení.

client 10.1.2.51 {
secret = 123456
shortname = WRT54G
nastype=other }

- user.conf - konfigurační soubor umožňující definovat lokální uživatele, definovat jeho přístup. V následující ukázce nastavení uživatele petr pro své přihlášení musí zadat své přihlašovací jméno a heslo. U uživatele tomas je přístup automaticky zakázán a u martina automaticky povolen.

```
petr  Cleartext-Password := „test“
tomas  Auth-Type := Reject
martin  Auth-Type := Accept
```

- *sql.conf* – konfigurační soubor pro provádění dotazů a připojení FreeRADIUS k databázi MySQL. Nastavení připojení k databázi je uvedeno níže. Uživatel radius přistupuje pod heslem radpass k databázi radius.

```
# Connection info:
server = "localhost"
#port = 3306
login = "radius"
password = "radpass"

# Database table configuration for everything except Oracle
radius_db = "radius"
```

Základní konfigurace je provedena, ještě musíme připravit databázi pro uživatele. V adresáři */usr/local/etc/raddb/sql/mysql* jsou předpřipravené tabulky pro databázi MySQL, které se nahrají do databáze raddb. Pomocí uvedených příkazů v shellu se připojíme do MySQL, vytvoříme databázi radius a odhlásíme se. Po té přejdeme do adresáře s tabulkami a nahrajeme soubory s příponou sql do databáze radius.

Vytvoření databáze:

mysql –uroot –pheslo (připojení do MySQL)
create database radius; (napíšme tento příkaz, vytvoří databázi radius)
\q (odhlášení z MySQL)

Nahrání tabulek do databáze:

*cd /usr/local/etc/raddb/sql/mysql (p*řejdeme k souborům obsahující tabulky)

mysql –uroot –pheslo radius < název souboru.sql (nahrání souborů do databáze radius, nahrajeme tyto soubory: *admin.sql, cui.sql, ippool.sql, nas.sql, schema.sql, wimax.sql*)

Zde je uveden výpis a popis tabulek databáze radius po nahrání všech souborů:

```
mysql> show tables;
+------------------------+
| Tables_in_radius       |
+------------------------+
| cui                    |
| nas                    |
| radacct                |
| radcheck               |
| radgroupcheck          |
| radgroupreply          |
| radippool              |
| radpostauth            |
| radreply               |
| radusergroup           |
| wimax                  |
+------------------------+
mysql>
```

Vytvořené tabulky v databázi radius jsou prázdné, pomocí SQL příkazů tyto tabulky naplníme daty.

- Nejprve se připojíme do MySQL a otevřeme databázi radius.

  mysql –uroot –pheslo (připojení do MySQL)
  \r radius (otevření databáze radius)

- Vytvoříme uživatele steve a přidělíme mu uživatelskou skupinu ekonomie. Vložíme tyto údaje do tabulky *radgroupreply* příkazem:

  mysql> INSERT INTO *radgroupreply* VALUES (0,'steve','ekonomie');

  Kontrolu vložených dat provedeme příkazem:

  mysql> select * from *radgroupreply*;

- Dalším krokem bude vložení údajů do tabulky radcheck, kde jsou informace k ověření uživatele. Zde hledá FreeRADIUS uživatele k autorizaci.

mysql> INSERT IN TO radcheck VALUES(0,'steve','Cleartext-Password',':=','heslo');

  Provedeme kontrolu vložených dat příkazem:

  mysql> select * from radcheck;

- Do tabulky radgroupcheck se nastavuje metoda ověření hesel uživatelů. Než se začne FreeRADIUS dívat do tabulky radcheck, podívá se do této tabulky a zjistí jak má hesla uživatelů porovnávat.

Metodu ověření hesel vložíme příkazem:

```
mysql>INSERT INTO radgroupcheck VALUES (0,'ekonomie','Auth-Type',':=','Local');
```

Provedeme kontrolu vložených dat příkazem:

```
mysql> select * from radgroupcheck;
```

- Pro lepší přehled nad databází doporučuji nainstalovat aplikaci phpmyadmin, která beží na webovém serveru. Následující příkaz nainstaluje phpmyadmin a automaticky server doinstaluje aplikaci Apache2, která z našeho serveru udělá webový server.

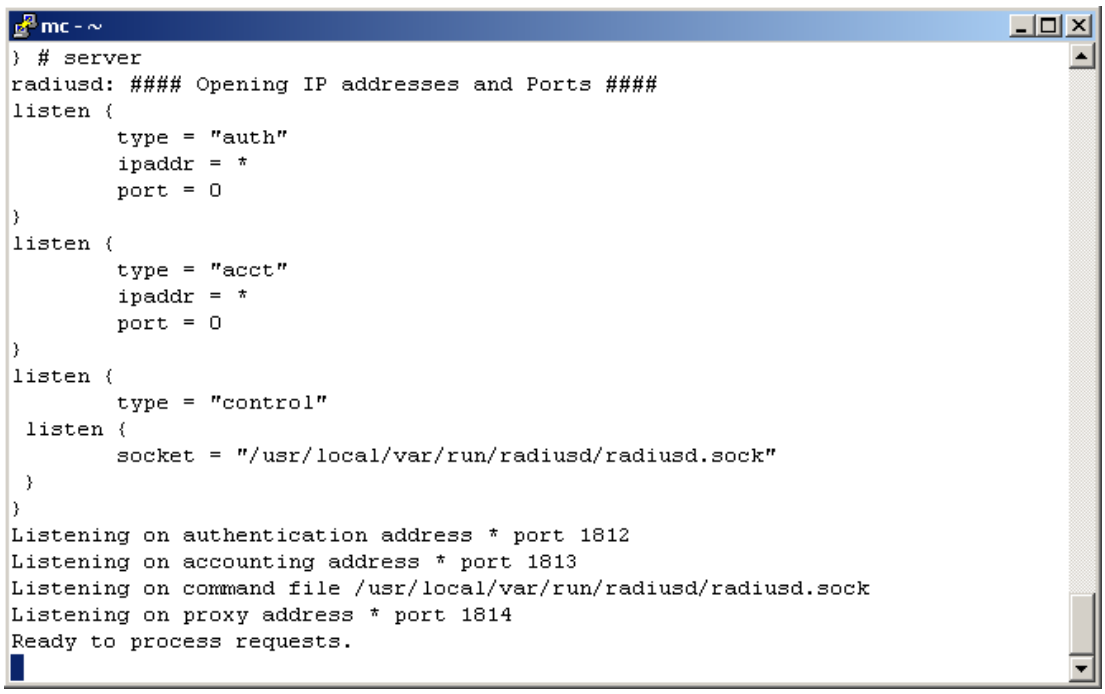
  apt-get install phpmyadmin

  Po instalaci zadejte na jiném počítači IP adresu RADIUS serveru do internetového prohlížeče, dle vzoru:

  http://IP adresa RADIUS serveru/phpmyadmin

A zadejte přihlašovací údaje pro připojení do MySQL, zde pak můžete lépe konfigurovat databázi a prohlížet v ní uložené data.

Nyní je vše nakonfigurováno a provedeme test FreeRadius příkazem *radiusd –X*, pokud je chyba v nastavení, tak se na obrazovce zobrazí chyby. Na následujícím obrázku 28 je výpis, že FreeRadius je správně nastaven a naslouchá na portech 1812,1813 a 1814.

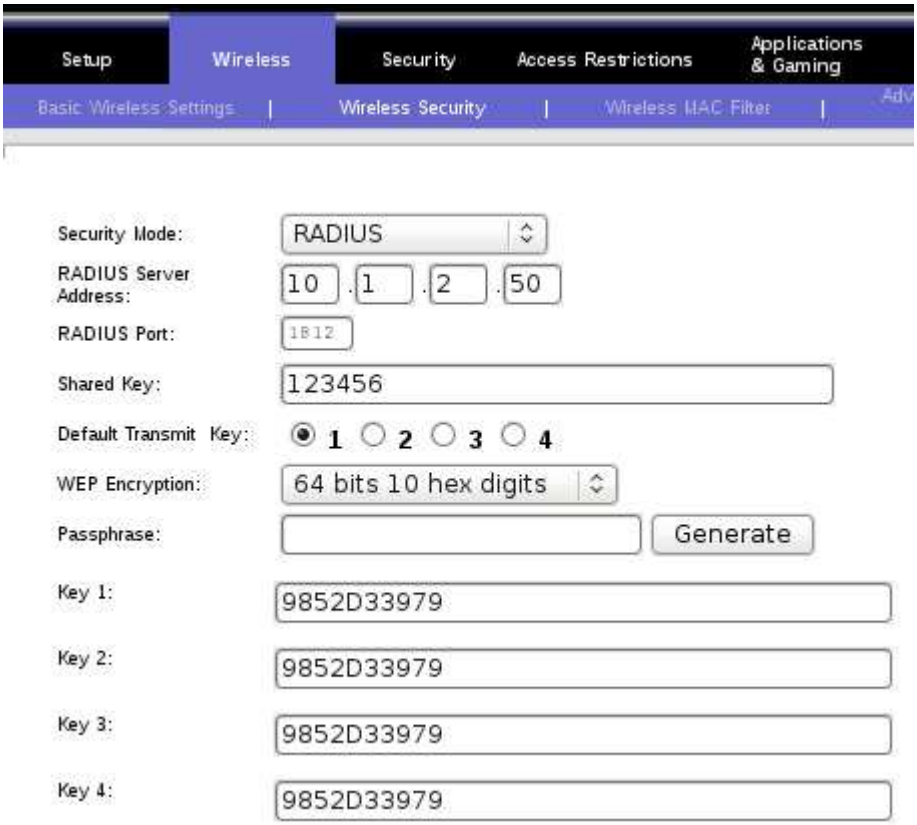


Obr. 28 *Výpis správné konfigurace serveru FreeRadius*

Server je nakonfigurován a nyní se musí nastavit zařízení, které bude ověřovat proti freeradiusu.

7.4 Nastavení klientů

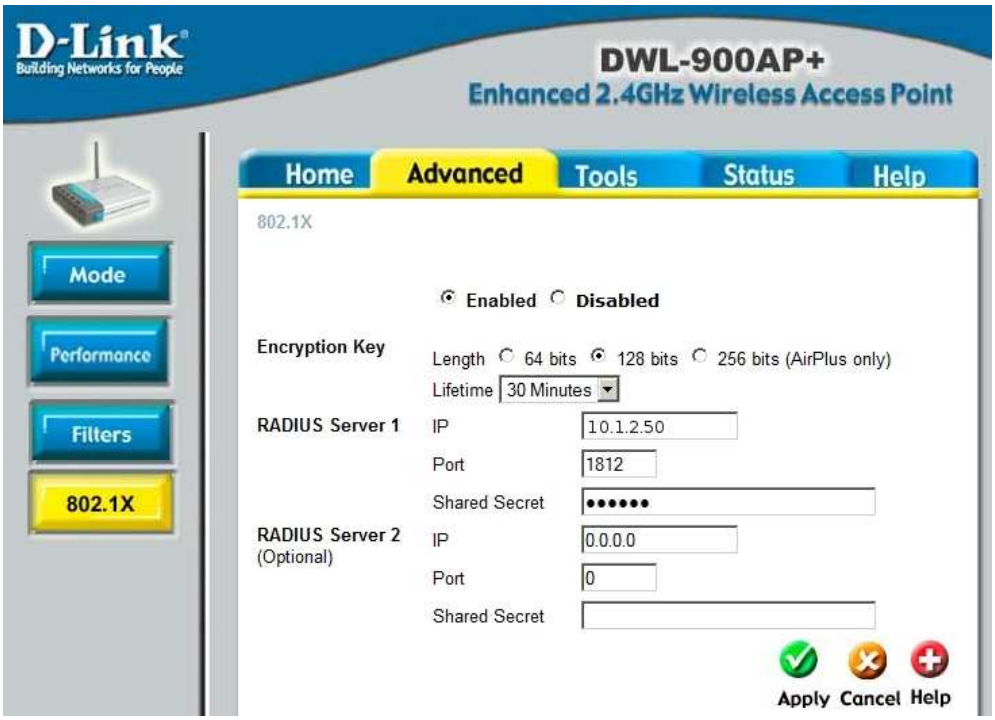
StraightCore WRT-312 a WRT54G je možné konfigurovat pomocí WWW rozhraní, kde je možné nastavit různé služby. Pro náš projekt nastavíme IP adresu pro FreeRadius server a nastavíme tajné heslo pro komunikaci (které bylo zadáno v souboru clients.conf). Následující obrázek 29 představuje nastavení na routeru WRT54G, které je podobné na routeru WRT-312.



Obr. 29 *Nastavení klienta pro ověřování proti serveru FreeRadus*

Linksys WAP11 AP

U tohoto Access Pointu nastal problém, že originální firmware od výrobce nepodporuje ověřování proti RADIUS serveru a navíc nelze zde například nastavit DHCP server. Jediným řešením bylo nalézt kompatibilní firmware od jiného výrobce, který bude na Liksys WAP11 AP správně fungovat. Po prohledání internetových stránek jsem našel vhodný firmware od firmy D-Link pro Access Point DWL-900AP+. Nahrání nového firmware je poměrně jednoduché, podle dokumentace od výrobce provedeme reset nastavení Acces Pointu na jeho původní nastavení. Počítač propojíme kříženým kabelem s Acces Pointem a nastavíme síť tak, aby bylo možné komunikovat s Acces Pointem pomocí WWW rozhraní. V internetovém prohlížeči počítače zadáme IP adresu přístupového bodu, kterou nalezneme v manuálu výrobce Liksys. V menu zvolíme nahrání nového firmware, který nahrajeme. Po asi minutě se provede restart přístupového bodu. Acces Point bude mít IP adresu podle manuálu výrobce D-Link. Výsledek nahrání nového firmware je vidět na obrázku 30. Nahráním nového firmware jsme získaly možnost autorizace proti RADIUS serveru.

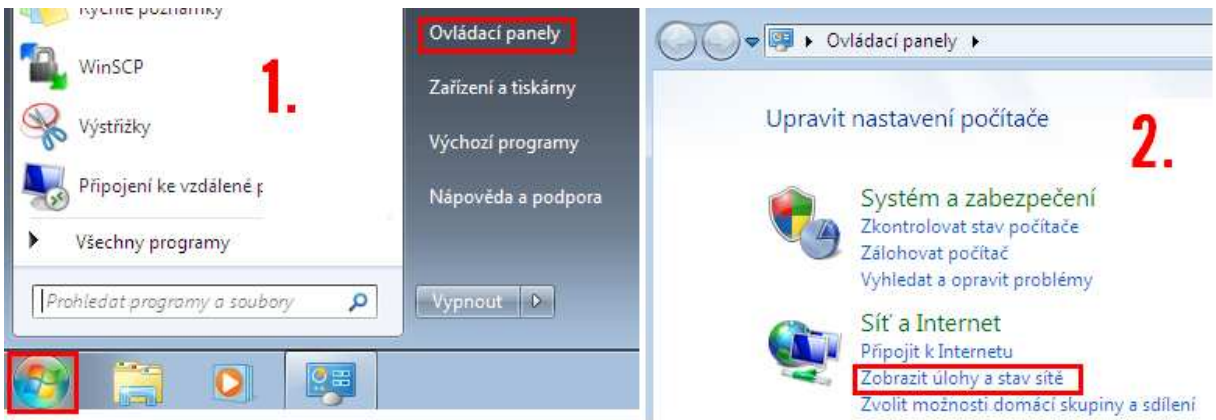


Obr. 30 *WWW rozhraní Acces Pointu po nahrání nového firmware*

7.4.1 Nastavení připojení do WLAN

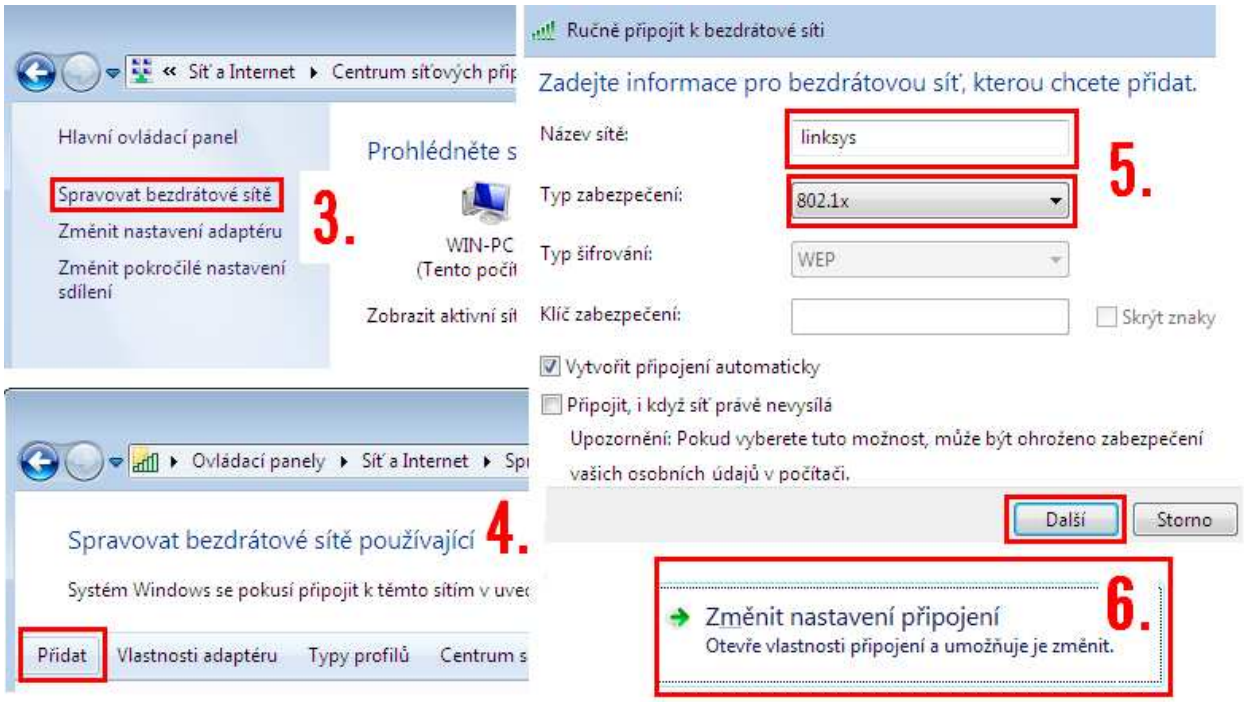
Následující návod stručně popisuje, jak nastavit přístup do bezdrátové sítě pomocí protokolu 802.1X ve Windows 7.

Zvolte ve spodním panelu tlačítko start a vyberte možnost *Ovládací panely*. Dalším krokem vyberte v ovládacím panelu *zobrazit úlohy a stav sítě.* Viz obrázek 31.



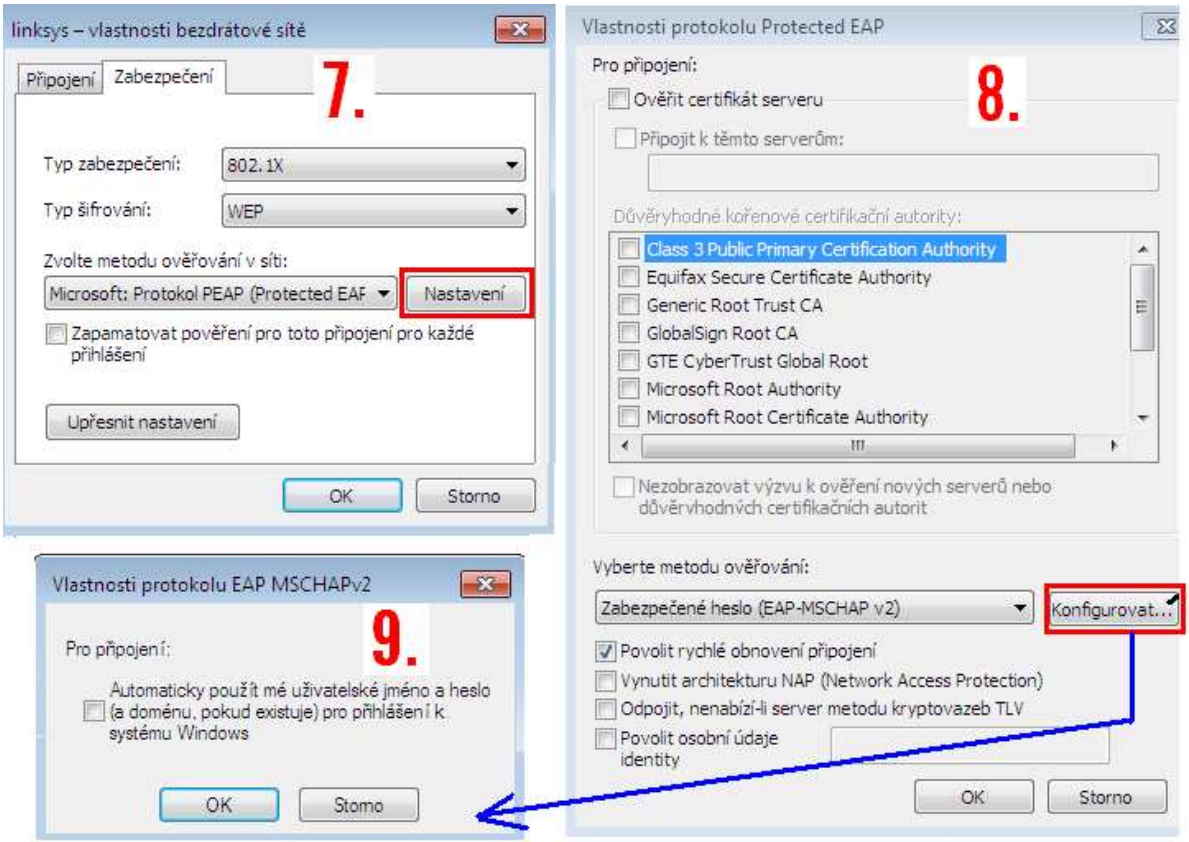
Obr. 31 *Nastavení připojení do WLAN - ovládací panel*

Zadejte s*pravovat bezdrátové sítě* a zvolte tlačítko přidat a v novém otevřeném okně nastavíme konfiguraci bezdrátového připojení. Zadejte název bezdrátové sítě, do které se budete připojovat. U položky *typ zabezpečení vyberte 802.1x* a zvolte tlačítko *další.* Potom vyberte možnost *změnit nastavení připojení.* Toto nastavení je zobrazeno na obrázku 32.



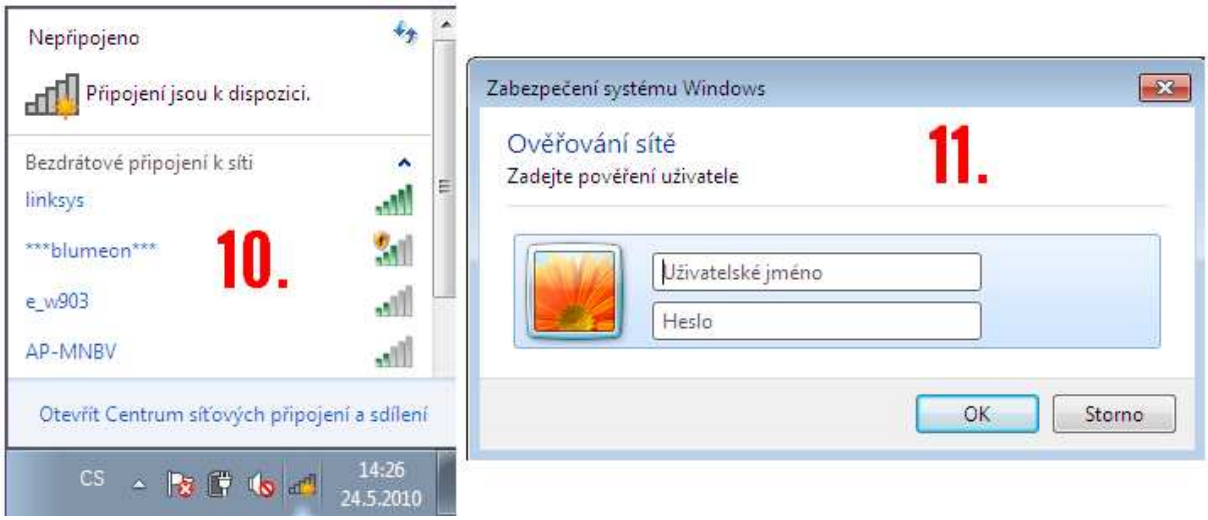
Obr. 32 *Přidání bezdrátové sítě*

V záložce zabezpečení vybereme možnost nastavení a nastavíme podle kroku osm a v možnosti konfigurovat nastavím podle kroku devět (viz obr. 33). Po dokončení tohoto nastavení se můžeme přihlásit do bezdrátové sítě.



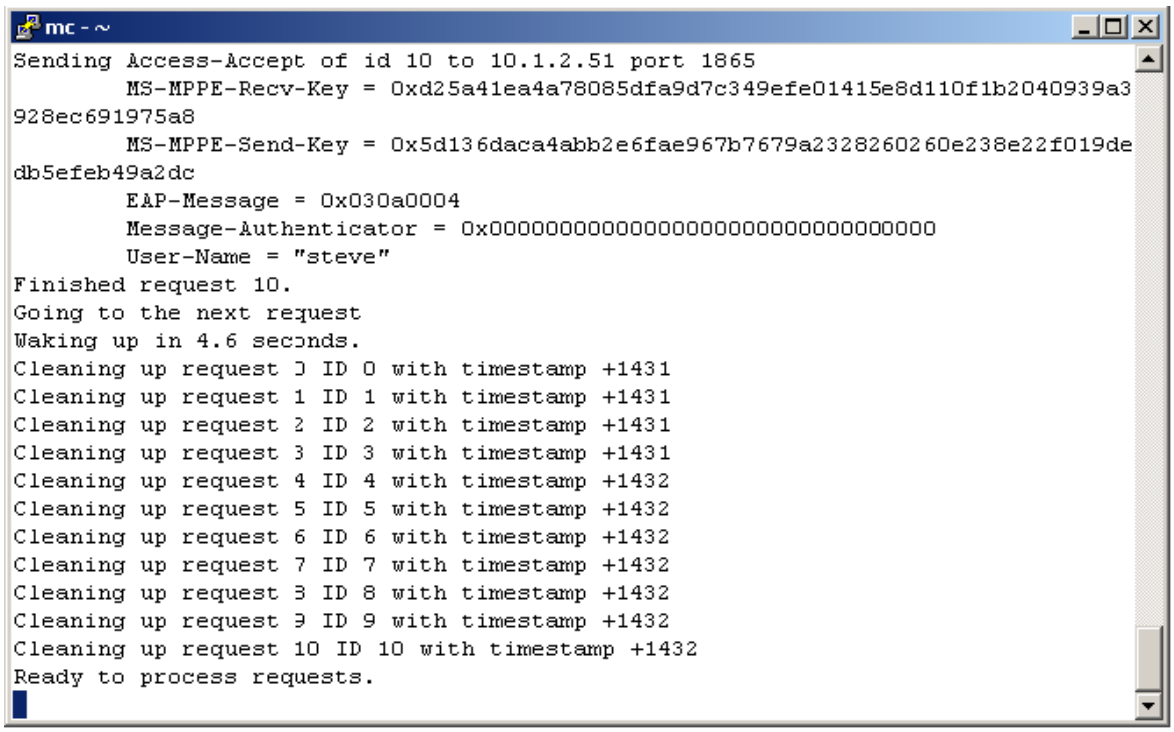
Obr. 33 *Úprava nastavení bezdrátové sítě*

Vybereme naši bezdrátovou sít *linksys a* pokusíme se připojit. Budeme vyzváni na zadání uživatelského jména a hesla (viz obr. 34). Zadáme našeho uživatele, který je uložen v databázi *radius*, nebo v konfiguračním souboru *user.conf*.



Obr. 34 *Připojení do bezdrátové sítě*

Na následujícím obrázku je potvrzující výpis FreeRADIUS serveru u uživatele *steve*, který žádal o ověření přístupu do bezdrátové sítě. Jeho přístup byl povolen, potvrzení na obrázku 35 je vidět v prvním řádku S*ending Acces-Accept*.



Obr. 35 *Potvrzující výpis FreeRADIUS u uživatele steve*

7.5 Řešení limitu download a upload dat z internetu

7.5.1 Konfigurace směrovače

Router Board 532 – směrovač s operačním systémem MikroTik je založen na bázi operačního systému GNU/Linux (kernel 2.4). Komunikace a konfigurace je možná například přes GUI Winbox, ssh, telnet, nebo sériovou konzoli. Router je na obrázku níže (viz obr. 36).

Obr. 36 *RouterBOARD 532*

Router slouží jako gateway, zajišuje tyto služby:

- DNS
- DHCP
- Firewall

Pro řešení nastavení limitu download a upload se musí nastavit ip accounting snapshot. Nastavením accountingu můžeme stahovat informace o komunikaci IP adres jednotlivých stanic, procházející pakety a jejich velikosti v bytech. K zabezpečení směrovače nastavte přístup k acconting z konkrétní IP adresy. Pomocí aplikace WGET můžeme tyto informace uložit na konkrétní stanici a dál je zpracovávat. Ukázkový příkaz pro stažení informací pomocí WGET (server Linux):

wget -q -nd http://IP_adresa_Mikrotiku/accounting/ip.cgi -O /tmp/prenos.tmp > /dev/null 2>/dev/null

Obsah staženého souboru *prenos.tmp*:

SRC-ADDRESS	DST-ADDRESS	BYTES	PACKETS	
10.1.2.7	*10.1.255.255*	*1963*	*9*	* *
82.59.12.29	*10.1.0.21*	*474*	*1*	* *
10.1.0.27	*89.29.170.89*	*168*	*1*	* *

7.5.2 Skript pro zpracování dat

Skript uvedený v této kapitole zpracovává soubor prenos.tmp a zapisuje získaná data do databáze. Skript je napsán v skriptovacím programovacím jazyku *ruby*, pokud není na serveru nainstalován, provedeme jeho instalaci s aplikací arping.

Příkazy pro instalaci programovacího jazyka ruby a potřebných programů:

apt-get install ruby rubygems libmysql-ruby libsequel-ruby

gem install sequel

apt-get instar arping

Skript pro zpracování souboru prenos.tmp:

```
#!/usr/bin/ruby
#
# Skript prochazi log s prenosy radek po radku, scita objem prenesenych
# dat pro jednotlive ip adresy a vysledek zapisuje do databaze. Skript
# zaroven kontroluje, zda uzivatel neprekrocil v aktualnim mesici zadanou
# kvotu a v pripade prekroceni kvoty uzivateli zablokuje pristup.
#
# Skript preskakuje prenosy uvnitr lokalni site, prenosy netykajici se
# lokalni site (napr. cizi broadcasty) a prenosy k nimz nelze dohledat
# zaznam hardwarove adresy. Plyne z toho, ze nemusi byt zaznamenany
# prenosy kratsi nez cca 5 minut.
#
# pouziti:
# watchlog.rb <log file>

require 'rubygems'
require 'sequel'

# kvota
MAX_DATA = 100000

# vypisovat informace?
DEBUG = true

# konfigurace pripojeni k databazi mysql
dbname = 'radius'
uname = 'radius'
passwd = 'radpass'
DB = Sequel.connect(:adapter => "mysql", :host => "localhost", :database =>
dbname,:user => uname, :password => passwd)

# jmeno souboru s logem
fname = ARGV.shift


# overi, ze se jedna o lokalni ip adresu
def is_local?(ip)
  ip =~ /^10\.\d+\.\d+\.\d+$/
end
```

```
# vytvori hash s ip jako klici, kde kazy zaznam obsahuje
# pocet stazenych a odeslanych dat v bytech
def spocti_prenos(fname)
  prenos = {}

  File.open(fname) do |f|
    f.each_line do |line|
      # rozparsujeme radek a pokud neodpovida vzoru, tak ho preskocime
      next unless line =~ /^(\d+\.\d+\.\d+\.\d+) (\d+\.\d+\.\d+\.\d+) (\d+) (\d+) \* \*/
      from, to, bytes, packets = $1, $2, $3, $4
      next unless is_local?(from) or is_local?(to) # nepocitej cizi prenosy
      next if is_local?(from) and is_local?(to) # nepocitej lokalni prenos

      if is_local?(from)
        # inicializuj data
        prenos[from] ||= {}
        prenos[from][:download] ||= 0
        prenos[from][:upload] ||= 0
        # pricti data
        prenos[from][:upload] += bytes.to_i
      else
        # inicializuj data
        prenos[to] ||= {}
        prenos[to][:upload] ||= 0
        prenos[to][:download] ||= 0
        # pricti data
        prenos[to][:download] += bytes.to_i
      end
    end
  end

  return prenos
end

# nastrojem arping vysle jeden dotaz na ip adresu
# najde => vrati mac adresu
# nenajde => vrati nil
def zjisti_mac(ip)
  #test = "ARPING 147.251.17.90 from 147.251.17.173 eth0
  #Unicast reply from 147.251.17.90 [00:1F:9E:BB:36:4A]  1.364ms
  #Sent 1 probes (1 broadcast(s))
  #Received 1 response(s)"

  cmd="arping -c 1 #{ip}"
`#{cmd}` =~ /from ([^ ]*) /m
  return $1
end

# secte prenesana data od zacatku mesice (Date.today - Time.now.day)
# a porovna s kvotou (MAX_DATA)
```

```
def prekrocil?(user)
  mesic = DB[:prenos].filter(:iduser => user).filter('datum > ?', Date.today - Time.now.day)
  download = mesic.sum(:download)
  upload = mesic.sum(:upload)
  (download + upload) > MAX_DATA
end

def zablokuj_uzivatele(user)
  u = DB[:user].filter(:id => user).first
  # nepridavat blokovaci radek, kdyz je uzivatel uz zablokovan
  return if DB[:radcheck].filter(:username => u[:username], :attribute => 'Auth-Type', :value => 'Reject', :op => ':=').sum(:id)
  DB[:radcheck].insert(:username => u[:username], :attribute => 'Auth-Type', :value =>'Reject', :op => ':=')
end

# **********************
# zacatek
# **********************
prenos = spocti_prenos(fname)
prenos.each do |ip, data|
  puts "%12s %9d %9d" % [ip, prenos[ip][:download], prenos[ip][:upload]] if DEBUG

  # zjisti MAC jinak preskoc
  mac = zjisti_mac(ip)
  unless mac
    puts "Nelze zjistit MAC" if DEBUG
    next
  end
  p mac if DEBUG

  # ziskej informace, kdo ma pocitac
  # pokud nenajde pro danou MAC adresu pocitac,
  # tak preskoc
  pc = DB[:pc].filter(:mac => mac).first
  unless pc
    puts "Pro MAC \"#{mac}\" nelze najit zaznam." if DEBUG
    next
  end

  # vytvor zaznam pro danou ip adresu a zjisteneho uzivatele (z pc)
  DB[:prenos].insert(:ip => ip, :iduser => pc[:iduser],
                     :download => data[:download], :upload => data[:upload],
                     :datum => Time.now)

  # zablokuj uzivatele, ktery prekrocil mesicni kvotu (MAX_DATA)
  zablokuj_uzivatele(pc[:iduser]) if prekrocil?(pc[:iduser])
end
```

Než se pustíme do spuštění skriptu, musíme upravit již nainstalovanou databázi radius. Následující strukturu tabulek nahrajeme do databáze *radius* pomocí souboru databaze.sql.

```
DROP TABLE IF EXISTS `pc`;
CREATE TABLE `pc` (
  `mac` varchar(253) NOT NULL,
  `iduser` int(10) unsigned NOT NULL,
  PRIMARY KEY (`mac`),
  INDEX (`iduser`)
) ENGINE=MyISAM;

DROP TABLE IF EXISTS `prenos`;
CREATE TABLE `prenos` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `ip` varchar(253) NOT NULL,
  `iduser` int(10) unsigned NOT NULL,
  `download` int(10) unsigned NOT NULL,
  `upload` int(10) unsigned NOT NULL,
  `datum` datetime NOT NULL,
  PRIMARY KEY (`id`),
  INDEX (`iduser`),
  INDEX (`ip`),
  INDEX (`datum`),
  INDEX (`iduser`,`ip`,`datum`)
) ENGINE=MyISAM;
```

Do tabulky pc se zapisuje identifikační číslo uživatele a MAC adresa jeho počítače. V tabulce přenos, jsou informace o download a upload uživatele (viz obr. 37).

Tabulky nahrajeme příkazem: *mysql –uroot –pheslo radius < název souboru.sql*

Skript se spouští příkazem:

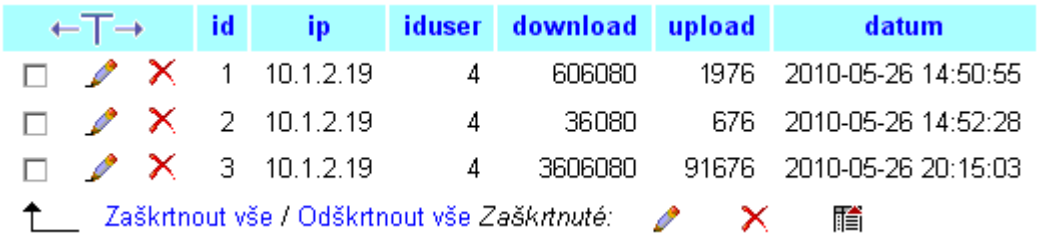
./configure watchlog.rb prenos.tmp

Ukázka zpracování dat skriptem je uvedena na obrázku 37:

```
"00:13:d4:12:96:50"
Pro MAC "00:13:d4:12:96:50" nelze najit zaznam.
   10.1.0.21    207970      8412
Nelze zjistit MAC
   10.1.0.10      2302      1886
"00:08:02:f7:41:62"
Pro MAC "00:08:02:f7:41:62" nelze najit zaznam.
  10.1.1.179       901       412
Nelze zjistit MAC
   10.1.0.99    102489      5557
Nelze zjistit MAC
   10.1.2.19   3606080     91676
"00:16:6f:81:d0:cc"
```

Obr. 37 *Běžící skript na serveru*

Skript zpracoval data v souboru prenos.tmp a uložil do databáze radius (viz obr. 38).



	id	ip	iduser	download	upload	datum
	1	10.1.2.19	4	606080	1976	2010-05-26 14:50:55
	2	10.1.2.19	4	36080	676	2010-05-26 14:52:28
	3	10.1.2.19	4	3606080	91676	2010-05-26 20:15:03

Zaškrtnout vše / Odškrtnout vše *Zaškrtnuté:*

Obr. 38 *Nahraná data v databázi radius, tabulka prenos*

Nyní je dokončena kompletní instalace RADIUS serveru s autorizací uživatelů a řešením přenosu dat z internetu.

7.6 Instalace doménového serveru

Jako operační systém pro server je vybrán Debian Linux. Tento server bude sloužit jako doménový řadič, zajišťující služby pro stanice s operačním systémem Windows XP Profesional Edition. Server bude poskytovat sdílení v síti SMB protokolem a autentizace uživatelů je ověřována v LDAP.

Operační systém doporučuji nainstalovat bez grafického prostředí z důvodů větší bezpečnosti. Čím méně služeb běží na serveru, tím je potencionálně větší bezpečnost.

Aplikace se instalují z repositáře následujícím příkazem:

apt-get install xxx (xxx představuje jméno balíčku)

Nainstalujete následující balíčky:

- openSSH-server – server slouží pro šifrování komunikace mezi klientem a serverem po síti. Často se používá ke vzdálené konfiguraci serveru program Putty a WinSCP.
- mc - Midnight Commander – souborový manažer.
- LDAP a schéma pro SMB. Instalaci provedeme následujícími příkazy:

  - příkaz nainstaluje LDAP a vyzve pro zadání uživatele admin LDAP

    apt-get install slapd ldap-utils

  - příkaz nakopíruje schéma SMB pro LDAP, které je potřeba rozbalit a přesunout do adresáře */etc/ldap/schema*.

    apt-get install samba-doc

    /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
    (adresář s uloženým schématem)

- konfigurace LDAP – následující příkaz vygeneruje SSHA klíč uživatele admin, který je potřeba zapsat do konfiguračního souboru */etc/ldap/slapd.conf*. Do souboru také vložte odkaz na schéma samby pro LDAP. Část souboru je uvedena zde:

  # Schema and objectClass definitions
  include /etc/ldap/schema/core.schema
  ...
  include /etc/ldap/schema/samba.schema

  # The base of your directory in database #1
  suffix "dc=nazev domeny,dc=cz"

  # rootdn directive for specifying a superuser on the database.
  # This is needed for syncrepl.
  rootdn "cn=admin,dc=nazev domeny,dc=cz"
  rootpw (zde se vloží SSHA klíč)

  V souboru */etc/ldap/ldapd.conf* upravte *BASE dc=nazev domeny,dc=cz*

- Nyní je nakonfigurován LDAP a následujícím příkazem se provedete jeho restart.

  /etc/init.d/slapd restart
  Stopping OpenLDAP: slapd.
  Starting OpenLDAP: slapd

  Test můžete provést příkazem:
  ldapsearch -xLLL -b "dc= nazev domeny,dc=cz"

- instalaci Samby provedeme následujícím příkazem

  apt-get install samba smbclient libpam-smbpass

  - Nastavíme práva pro příslušné adresáře:

    mkdir -v /home/profiles
    chmod 777 /home/profiles
    mkdir -v -p /home/netlogon

    V souboru */etc/samba/smb.conf* se konfiguruje nastavení Samby a sdílených adresářů, část nastavení sdílených disků a home adresářů jsou uvedeny zde:

    [homes]
    comment = Home Directories
    browseable = yes
    writable = yes
    create mask = 0644
    directory mask = 0755
    valid users = %S

[projekty]
comment = Projekty skoly
path = /home/projekty
browseable = yes
writable = yes
create mask = 0660
directory mask = 0770

- Příkaz k vytvoření souboru s aliasy uživatelů Samby:

  touch /etc/samba/smbusers

  Do souboru zapíšeme následující dva řádky:

  root = administrator admin
  nobody = guest pcguest smbguest

- Samba je nakonfigurována a můžeme provést její restart příkazem:

  /etc/init.d/samba restart

  Po restartu jako poslední krok vložíme admin uživatele LDAP do Samby příkazem *smbpasswd -W*

- Nastavení Samby můžeme zkontrolovat příkazem:

  smbclient -L bart -U anonymous%

  Po zadání příkazu se zobrazí výpis uvedený na obrázku 39.

```
bart:~# smbclient -L bart -U anonymous%
Anonymous login successful
Domain=[ domena.cz ] OS=[Unix] Server=[Samba 3.2.5]

        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      Home Directories
        netlogon        Disk      Network Logon Service
        projekty        Disk      Projekty
        skoleni         Disk      skoleni
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (bart server)
Anonymous login successful
Domain=[ZMVS.CZ] OS=[Unix] Server=[Samba 3.2.5]

        Server               Comment
        ---------            -------
        BART                 bart server

        Workgroup            Master
        ---------            -------
        domena.cz             BART
bart:~#
```

Obr. 39 *Výpis příkazu smbclient*

- instalace smbldap-tools – balík skriptů pro LDAP a Sambu. Skripty slouží k práci s uživateli, skupinami apod.

  apt-get install smbldap-tools

  Do adresáře */usr/share/doc/smbldap-tools* je uložen soubor *configure.pl.gz*, který je potřeba rozbalit a nastavit následující práva *chmod +x*. Po té spustit, soubor vytvoří adresář v adresáři */etc/smbldap-tools* soubory s konfigurací smbldap-tools.

- Příprava LDAP databáze pro Sambu – vytvoření základních nastavení, uživatelů a skupin pro Sambu v LDAP databázi se provede příkazem *smbldap-populate.* Budete vyzvání na zadání hesla, zadané heslo musí být uživatelem root.

- Name Service a PAM – zajistí podporu uložených uživatelů v LDAP, kteří jsou přihlášeni. Instalační příkaz je uveden níže.

  ```
  apt-get install libnss-ldap libpam-ldap
  ```

  Dalším krokem je editace a nastavení těchto souborů:

- /etc/pam.d/common-auth

  ```
  auth    sufficient      pam_ldap.so
  auth    required        pam_unix.so nullok_secure
  ```

- /etc/pam.d/common-password

  ```
  password   sufficient pam_ldap.so
  password   required   pam_unix.so nullok obscure md5
  ```

- edit /etc/pam.d/common-account

  ```
  account sufficient      pam_ldap.so
  account required        pam_unix.so

  session sufficient      pam_ldap.so
  session required        pam_unix.so
  ```

Doménový server je nakonfigurován, můžeme vytvářet uživatele a zařadit stanice s operačním systémem Windows XP do vytvořené domény.

Vytváření uživatelů a práce s uživateli se provádí pomocí skriptů, které byly již nainstalovány balíčkem *smbldap-tools*. Seznam nainstalovaných skriptů *smbldap-tools*: smbldap-groupadd, smbldap-groupdel, smbldap-groupmod, smbldap-groupshow, smbldap-passwd , smbldap-populate, smbldap-useradd , smbldap-userdel , smbldap-userlist , smbldap-usershow, smbldap-usermod,smbldap-userinfo.

Blíže si představíme pouze skript pro vytváření uživatelů, popis ostatních skriptů můžete najít v konfiguračním souboru Samby smb.conf (/etc/samba).

Vytvoření uživatele se provádí následujícími příkazy

- Vytvoření uživatele a domovského adresáře

  smbldap-useradd -a -m xxx *(xxx jméno uživatele, např. mkovar)*

- Nastavení hesla uživatele

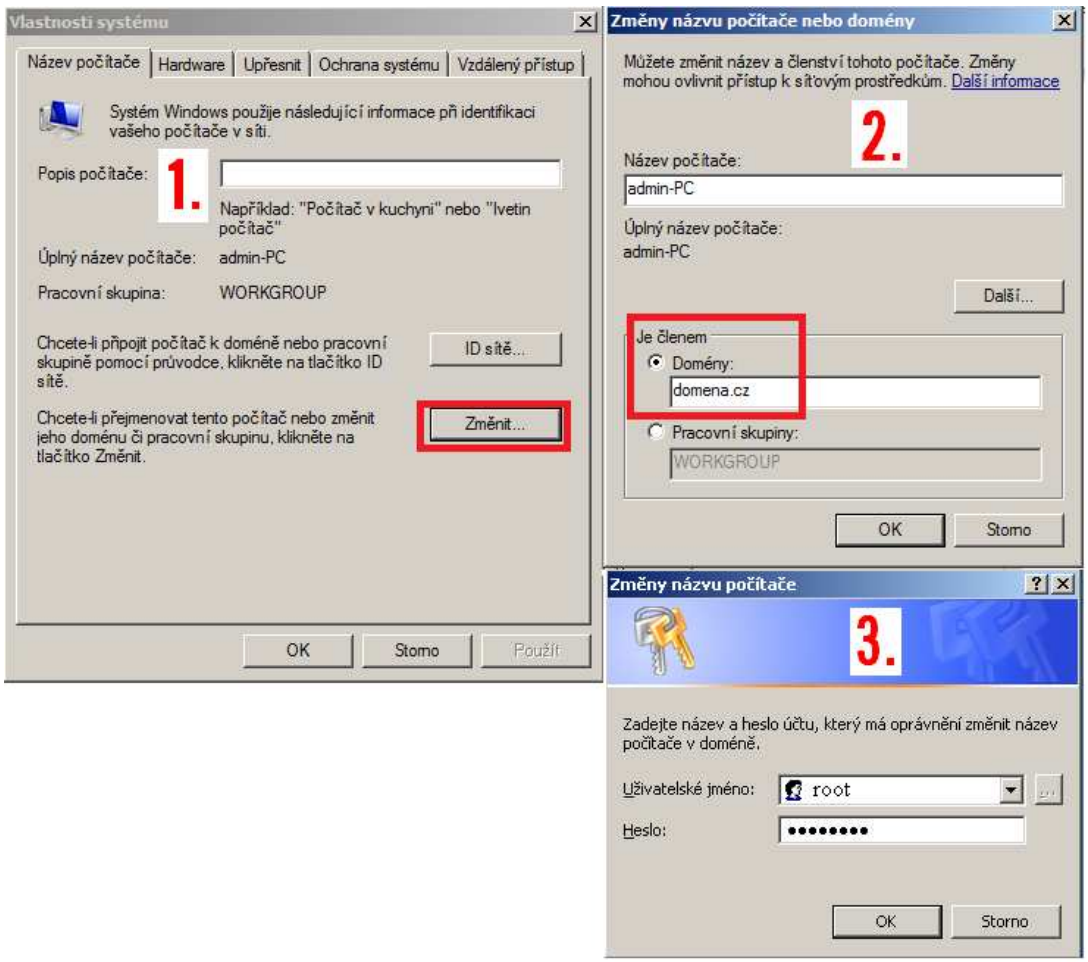
  smbldap-passwd xxx pass *(xxx jméno uživatele, pass – jeho heslo)*

- Přidání uživatele do skupiny

  smbldap-usermod - G skoleni xxx (skoleni je název skupiny, xxx jméno uživatele)

Nastaveni Windows klienta:

Po připojení stanice s Windows XP do vytvořené domény, se vytvoří v LDAP databázi účet stanice, který bude mít složený název s názvu stanice a znaku $ (např. M210-11$). Domovský adresář je připojen jako disk H:\. Následující obrázek 40 znázorňuje postup přidání stanice do vytvořené domény a obrázek 50 znázorňuje přihlášení uživatele do domény.



Obr. 40 *Přidání stanice do domény*

Obr. 41 *Přihlášení uživatele do domény*

7.7 Konfigurace stanic s operačním systémem Windows

V našem prostředí nemáme operační systém Windows Server 2003, který umí pomoci Group policy a Active directory replikovat bezpečnostní politiku na jednotlivé stanice v síti, včetně jejich nastavení. Proto musíme použít následující řešení.

Připravíme si jednu stanici a na ni nastavíme Local policy. Doporučiji na tuto stanici nainstalovat co nejvíce aplikací, které mohou být k dispozici uživatelům. Nastavíme spustitelné skripty pro uživatele a operační systém, které se budou aplikovat po přihlášení uživatele. Na stanici aktualizujeme bezpečnostní záplaty od firmy Microsoft pomocí Windows update. Na stanici nastavíme heslo uživatele administrator a ostatní uživatele zakážeme. Heslo uživatele administrator musí být složité, složené z velkých a malých písmen, čísel a speciálních znaků. Po dokončení těchto kroků bude stanice připravena k připojení do počítačové sítě. Než tak učiníme, využijeme programů, které mohou vytvořit tzv. image disku (nebo jeho části). Jedná se o záložní kopii disku, která je většinou uložena v jednom souboru. Ze záložní kopie disku můžeme obnovit systém na stanici, ale pro nás bude sloužit jako image, který nainstalujeme na ostatní stanice. Samozřejmě u tvorby image disku se můžeme setkat s několika problémy. Většinou v každé firmě existují různé druhy osobních počítačů, mají jiný hardware, což pro nás znamená další image disku z hlediska komptability ovladačů. Jedním řešení toho problému je nahrát univerzální ovladače na stanici, ze které bude vznikat image disku pro ostatní stanice. Dalším problémem mohou být licence operačního systému a instalovaných programů, zda se jedná o multilicenci (aplikace může být na více počítačích s jedním licenčním číslem) nebo běžnou licenci pro jednu stanici.

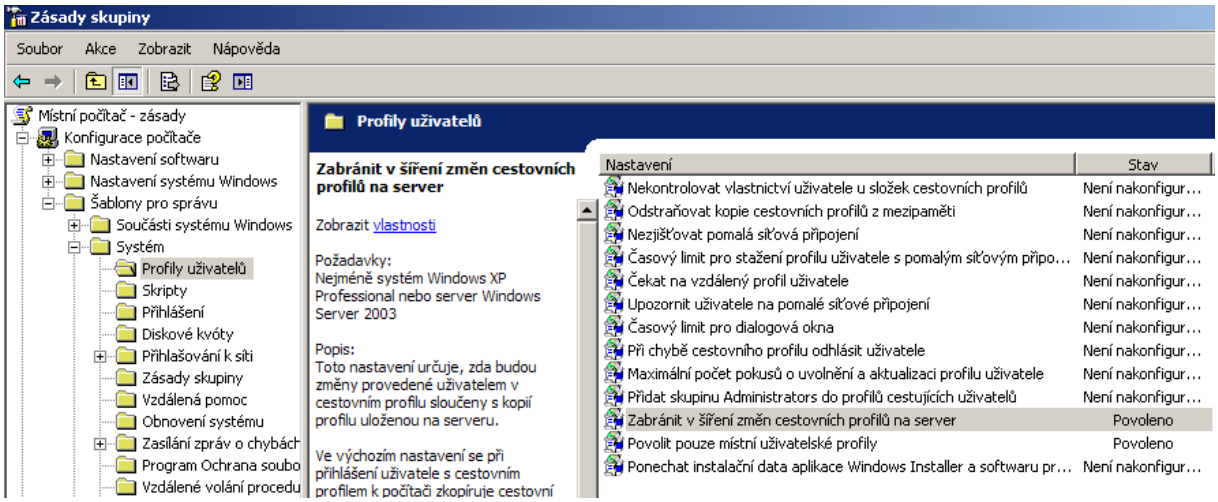
Při tvorbě image disku by mělo platit, aby byly nainstalovány aktuální verze software, včetně jejich záplat. Otestovat vytvořený image na jiné stanici a otestovat nainstalované aplikace, důvodem je že některé aplikace na jiné stanici nemusí fungovat správně.

Je samozřejmé, že s připraveným imagem nevydržíme delší čas, proto je dobré vést si evidenci nainstalovaných programů a jednou za čas vytvořit nový image disku.

V další části této kapitoly se seznámíme s konkrétním řešením nastavení stanic.

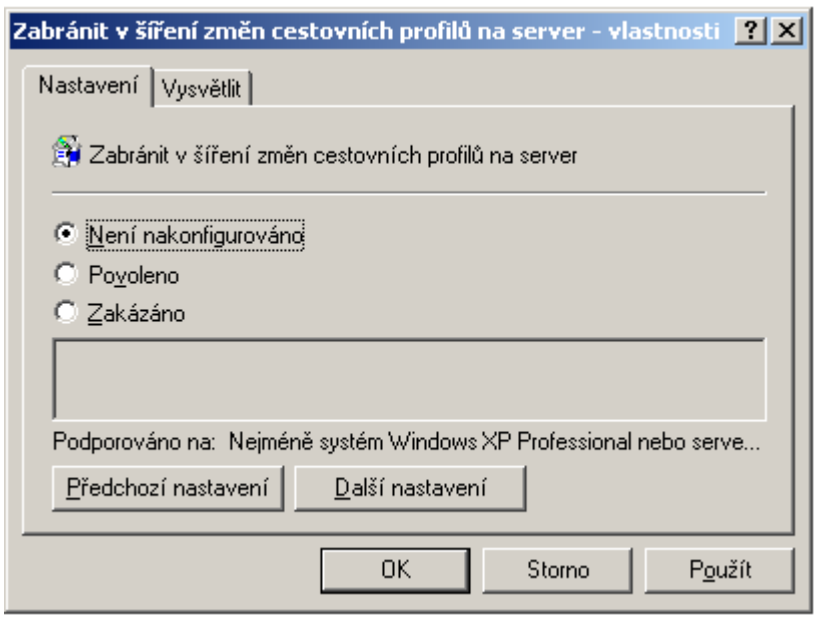
7.7.1 Nastavení Local policy

Nastavení lokální politiky se provádí pomocí zásad skupiny, které spustíme u Windows XP kliknutím na tlačítko start, vybereme možnost spustit a do okna napíšeme gpedit.msc a potvrdíme. Otevře se okno zásad skupiny (viz obr. 40).



Obr. 42 *Zásady skupiny*

U zásad skupiny můžeme nastavit tyto možnosti: není nakonfigurováno, povoleno, nebo zakázáno. Jak fungují tato nastavení, si popíšeme podle obrázku (viz obr. 41), kde vidíme možnost zabránit v šíření změn cestovních profilů na server. Pokud zde nastavíme není nakonfigurováno, bude zde platit defaultní nastavení od výrobce operačního systému (v dokumentaci výrobce zjistíme, zda je povoleno, nebo zakázáno šíření změn). Když nastavíme povoleno, zabráníme v šíření změn cestovního profilu na server. U možnosti zakázáno se bude cestovní profil šířit na server.



Obr. 43 *Zabránění v šíření cestovního profilu na server*

Zde uvedu několik nastavení lokální politiky u konfigurace počítače, které doporučuji nastavit, podle textu v závorkách.

Profily uživatelů

- Zabránit v šíření změn cestovních profilů na server. (povoleno)
- Povolit pouze místní uživatelské profily (povoleno)

Obnovení systému

- Vypnout nástroj Obnovení systému
- Vypnout konfiguraci

Zasílání správ o chybách

- Nastavení rozšířeného zasílání zpráv o chybách
  Výchozí nastavení oznamování chyb (zakázáno)
- Zobrazit oznamování chyb (zakázáno)

Program Ochrana souborů systému Windows

- Nastavit procházení pro program Ochrana souborů systému Windows (zakázáno)

Systémový čas

- Poskytovatelé času
  Povolit klienta Windows protokolu NTP

Správa internetové komunikace

- Vypnout hlášení chyb systému Windows (zakázáno)
- Vypnout automatické stahování kodeků Aplikace Windows Movie Maker (zakázáno)

Síť

Soubrory offline

- Povolit nebo zakázat použití funkce Soubory offline (zakázáno)
- Zakázat uživatelskou konfiguraci souborů offline (povoleno)
- Při přihlášení synchronizovat všechny soubory offline (zakázáno)
- Provést synchronizaci všech souborů offline před odhlášením (zakázáno)
- Před přechodem do režimu spánku synchronizovat soubory offline (zakázáno)
- Odebrat možnost Zpřístupnit offline (povoleno)
- Zabránit použití složky souborů offline (povoleno)
- Vypnout připomínání (povoleno)

Zde byla uvedená část nastavení lokální politiky stanice, která se používá na jednotlivých stanicích v počítačové síti.

7.8 Doporučující pravidla pro zajištění bezpečnosti v počítačové síti.

V této závěrečné kapitole bych uvedl několik pravidel a doporučení pro dodržování bezpečnosti, které používám v praxi.

- Používejte silná hesla u uživatelů a aplikací – složené z velkých a malých písmen, čísel a speciálních znaků. Administrátorská hesla používejte ve výjimečných případech a bezpečně. Používejte různá hesla k aplikacím, přístupů do počítačové sítě a také u uživatelských účtů.

- Pravidelně zálohuje důležitá data, například disky s uživatelskými daty, aby je bylo možné obnovit při jejich poškození a ztrátě.

- Zabezpečte fyzicky síťovou infrastrukturu, omezte přístup k serverům, zaměstnancům.

- Používejte na stanicích antivirové programy a dodržte, aby antivirový test na stanici a serverech proběhl celý.

- Pravidelně kontrolovat systémy a procedury, sledujte pravidelně logy souborů aplikací.

- Testujte bezpečnost proti průnikům a používejte systémy pro jejich detekci.

- Kontrolujte stav a servis hardware, záložních zařízení, přepěťových ochran a UPS.

- Se spoluprácí s vedením vaší firmy vytvořte vnitřní směrnice pro zajištění bezpečnosti informací.

8. ZÁVĚR

V rámci této práce mi bylo umožněno věnovat se problematice bezpečnosti lokálních počítačových sítí a bezdrátových sítí.

Teoretickým přínosem této práce je seznámení s analýzou současných mezinárodních norem a standardů v oblasti informačních technologií a jejich zavedení v bezpečnosti počítačových sítí.

Zaručení bezpečnosti dat v počítačových sítí by měla být základní povinností ve firmách a organizacích. Bezpečnost musí být zajištěna nejen informačními technologiemi, ale také vnitřními směrnicemi a standardy. Požadavky na bezpečnost by měli zahrnovat ochranu údajů ve všech formách, ochrany HW a SW komponent, ochrany budov a osob nacházejících se v prostorách podniku.

Praktickým přínosem této práce jsou praktické návrhy aplikování bezpečnosti pomocí hardware a software v lokálních a bezdrátových sítí.

V rámci bezpečnosti lokální počítačové sítě jsem uvedl softwarové řešení s operačním systémem GNU/Linux. Byl vytvořen doménový server, pro účel ověřování uživatelů klientských stanic, podpory sdílení složek a souborů v lokální síti pomocí systému Samba. Informace o uživatelích a stanicích jsou uloženy v databázi LDAP.

U řešení bezpečnosti bezdrátových sítí jsem navrhl řešení autorizace bezdrátových klientů proti RADIUS serveru. Pro tento účel je použita aplikace FreeRADIUS a databázový systém MySQL, kde jsou uloženy informace o uživatelích. FreeRADIUS je velice silný nástroj k zajištění bezpečnostní politiky s velkou škálou možností autorizace. Lze ho nakonfigurovat pro komunikaci s různými databázovými systémy. FreeRADIUS je napojen na MySQL databázi a dohromady slouží k autentizaci uživatelů připojující se do sítě.

Dalším úkolem bylo nastavení limitu download a upload dat z internetu u bezdrátových klientů. V navrhovaném řešení byl vytvořen skript v skriptovacím programovacím jazyku ruby, který zpracovává stažený soubor ze směrovače MikroTik na serveru. Soubor obsahuje informace o přenosech bytů mezi IP adresami síťových zařízení. Zpracovaná data jsou ukládána do upravené databáze FreeRADIUS serveru, kde jsou přiřazena k uživatelům podle jejich identifikačního klíče a fyzické adresy počítače. Hodnota nastavení limitu a download a upload je nastavena ve skriptu, který zjišťuje, zda připojený uživatel překročil stanovený limit. Při překročení limitu skript zapíše Acces-Reject do databáze FreeRadius a uživatel se již nepřihlásí.

Databázový systém MySQL byl vybrán, z důvodu jeho možnosti použití skriptovacích jazyků jako je perl a php. Tyto jazyky jsou v dnešní době používány pro tvorbu dynamických webových stránek. Za jejich pomoci je možné naprogramovat webovou administrační stránku databáze serveru RADIUS a tím ulehčit práci administrátorům sítě.

9. LITERATURA

[1] Dostálek L., Kabelová, A. a kol.: *Velký průvodce protokoly TCP/IP a systémem DNS.* Vydavatelství a nakladatelství Computer Press, Brno, 2002, ISBN 80-7226-675-6

[2] Odom, W.: *Počítačové sítě bez předchozích znalostí.* Vydavatelství a nakladatelství CP Books a.s., Brno, 2005, ISBN 80-251-0538-5

[3] Sportack, M. A.: *Směrování v sítích IP*. Vydavatelství a nakladatelství Computer Press, Brno, 2004, ISBN 80-251-0127-4

[4] Chapman, Jr. D. W., Fox A.: *Zabezpečení sítí pomocí Cisco PIX Firewall.* Vydavatelství a nakladatelství Computer Press, Brno, 2004, ISBN 80-722-6963-1

[5] Anonymous: *Maximální bezpečnost.* Nakladatelství Pearson Education Inc, Sams Publishing, 2003, ISBN 80-86497-65-8

[6] Smejkal, V., Rais, K.: *Řízení rizik.* Vydavatelství a nakladatelství Grada Publishing a.s., Praha, 2003, ISBN 80-247-0198-7

[7] Sedláček, V.: *Management systému informační bezpečnosti – ISMS.* Vivat Academia, Třebíč, 2010, ISBN 978-80-87385-05-0

[8] Zandl, P.: *Bezdrátové sítě WiFi – Praktický průvodce.* Vydavatelství a nakladatelství Computer Press, Brno, 2003, ISBN 80-7226-632-2

[9] Pužmanová, R.: *Bezpečnost bezdrátové komunikace – Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* Vydavatelství a nakladatelství Computer Press, Brno, 2003, ISBN 80-251-0791-4

[10] Pužmanová, R.: *Širokopásmový Internet, Přístupové a domácí sítě.* Vydavatelství a nakladatelství Computer Press, Brno, 2004, ISBN 80-251-0139-8

[11] Schroder, C.: *Linux Kuchařka administrátora sítě.* Vydavatelství a nakladatelství Computer Press, Brno, 2009, ISBN 978-80-251-2407-9

[12] *Raising awareness on information security across public and private organisations.* Luxembourg: Office for Official Publications of the European Communities, 2009, ISBN 978-92-9204-015-4

[13] Ludvík, M. - Štědroň, B.: *Teorie bezpečnosti počítačových sítí.* Vydavatelství a nakladatelství Computer Media, Praha, 2008, ISBN 978-80-86686-35-6

[14] Harper, A. - Harris, S. - Eagle, C. - Ness, J. - Lester, M.: *Hacking - manuál hackera.* Vydavatelství a nakladatelství Grada Publishing a.s., Praha, 2008, ISBN 978-80-247-1346-5

[15] Northcutt, S. - Zeltser, L. - Winters, S. - Kent Frederick, K. - Ritchey, R. W.: *Bezpečnost počítačových sítí.* Vydavatelství a nakladatelství Computer Press, Praha, 2005, ISBN 80-251-0697-7

[16] Osif, M.: *Microsoft Windows Server 2003.* Vydavatelství a nakladatelství Grada Publishing, a.s, Praha, 2003 ISBN 80-247-0395-5

[17] Osif, M.: *Microsoft Windows Server 2003 poradce experta.* Vydavatelství a nakladatelství Grada Publishing, a.s, Praha, 2003 ISBN 80-247-0396-3

[18] Toxen, B. C.: *Bezpečnost v Linuxu.* Vydavatelství a nakladatelství Computer Press Brno, 2003, ISBN 80-7226-716-7