Návody pro informační portál UTB ve Zlíně

Network instructions for information portal TBU in Zlin

Jan Strouhal

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan STROUHAL**
Osobní číslo:	**A06206**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Návody pro informační portál UTB ve Zlíně**

Zásady pro vypracování:

1. **Vytvořte podrobné návody podle požadavků centra výpočetní techniky. např. připojení k bezdrátové síti UTB ve Zlíně z různých operačních systémů, změna hesla na síti, konfigurace a použití e-mailu, atd..**
2. **Návody musí být zpracovány názorně, což vyžaduje projít všechny postupy, a následně je popsat i pro počítačově méně zdatné uživatele, včetně obrázků.**
3. **Pokud to bude situace vyžadovat, vytvořte požadované rozhraní.**
4. **Pokud bude potřeba, vytvořte návody pro následující operační systémy: Microsoft Windows XP, Vista a 7. Dále také obecný přístup pro GNU/Linux a pro jednu konkrétní distribuci, např. GNU Debian (ubuntu, ...).**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Wake on LAN - Wikipedie, otevřená enciklopedie [online]. 2007 , 12. 12. 2009 [cit. 2010-02-01]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Wake_on_LAN.**
2. **BOUŠKA, Petr. Wake on LAN - lokální i vzdálený subnet (články -) SAMURAJ-cz.com [online]. 2008 , 10.08.2008 [cit. 2010-02-01]. Dostupný z WWW: http://www.samuraj-cz.com/clanek/wake-on-lan-lokalni-i-vzdaleny-subnet/.**
3. **Vzdálená plocha ve Windows XP | Ovsem.net - software, hardware, online hry, webdesign, Windows 7 / Vista / XP [online]. 2005 , 7. December 2005 [cit. 2010-02-01]. Dostupný z WWW: http://www.ovsem.net/windows-xp/vzdalena-plocha-ve-windows-xp/.**
4. **Wi-Fi - Wikipedie, otevřená enciklopedie [online]. 2004 , 11. 12. 2009 v 08:02. [cit. 2010-02-01]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Wifi.**
5. **TYL, Lukáš. Jak nastavit e-mailový klient Outlook Express [online]. 2008 , 2008 [cit. 2010-02-01]. Dostupný z WWW: http://www.otazky-a-odpovedi.cz/Jak-nastavit-e-mailovy-klient-Outlook-Express/.**
6. **TYL, Lukáš. Jak nastavit e-mailový klient Microsoft Outlook 2007 [online]. 2008 , 2008 [cit. 2010-02-01]. Dostupný z WWW: http://www.otazky-a-odpovedi.cz/Jak-nastavit-e-mailovy-klient-Microsoft-Outlook-2007/.**
7. **Návody pro připojení k interní WiFi síti [online]. 2006 , 16. 5. 2006 [cit. 2010-02-01]. Dostupný z WWW: http://web.utb.cz/?id=0_8_13_0_0&iid=1&9001;=cs&type=0.**

Vedoucí bakalářské práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **5. března 2010**

Termín odevzdání bakalářské práce: **1. června 2010**

Ve Zlíně dne 5. března 2010

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Náplní bakalářské práce je vytvoření podrobných návodů pro studenty a zaměstnance UTB, které jsou zpracovány tak, aby podle nich byl schopen i počítačový začátečník dosáhnout kýženého výsledku. Prvním tématem v návodech je připojení k UTB Wi-Fi, a to pro operační systémy Microsoft Windows XP, Windows Vista a Windows 7. Dále pak pro OS Linux, a to jak přes grafické uživatelské rozhraní, tak pomocí textového souboru s konfigurací. Druhým tématem jsou e-maily. Zahrnuje návod, popisující webového klienta Webmail. Dále byly vytvořeny návody na konfiguraci nejpoužívanějších poštovních klientů MS Outlook Express, MS Live mail, MS Office Outlook 2007 a Mozzila Thunderbird 3. Třetím tématem je systém Novell. Tyto návody popisují, jak se přihlásit do systému Novell v učebnách a studovnách UTB, a jak se připojit k serverům Novell přes FTP. Posledním tématem, je návod na zprovoznění Wake on LAN. Tento systém slouží ke vzdálenému zapnutí počítače, odkudkoliv z internetu.

Klíčová slova:

Návody pro informační portál UTB ve Zlíně, Návody, Wi-Fi, eduroam, webmail, E-mail, Novell, FTP, Wake-on-LAN, WOL

ABSTRACT

The sense of this bachelor thesis is to create detailed manuals for computer beginners, to help them to acquire the coveted output. These manuals will help students and employees of Tomas Bata University in the main. The first topic is joining the UTB Wi-Fi net for operating systems Microsoft Windows XP, Windows Vista and Windows 7. Further the instruction for operating system Linux, describing the process using graphical interface, and using a text file with configuration too. The second topic is e-mails. It includes the instruction describing the web klient Webmail. Further, there are instructions to configurate the most widely used mailers: MS Outlook Express, MS Live mail, MS Office Outlook 2007 and Mozzila Thunderbird 3. Third topic describes joining the Novell system in school-rooms and study rooms, and how to join Novell system using FTP. The last topic is the instruction how to launch „Wake on LAN“ system. This system allows a computer to be turned on by a message sent from the Internet.

Keywords:

Network instructions for information portal TBU in Zlin, Wi-Fi, eduroam, webmail, E-mail, Novell, FTP, Wake-on-LAN, WOL

Poděkování:

Chtěl bych poděkovat v první řadě panu Syslovi, vedoucímu mé bakalářské práce, a také panu Vojtkovi, správci sítě UTB, se kterými jsem ve velké míře spolupracoval. Chtěl bych jim tímto moc poděkovat za pomoc, cenné podněty, ochotu a celkově za velmi dobrou spolupráci.

Dále bych chtěl poděkovat mojí rodině a přítelkyni za velkou podporu a obrovskou trpělivost.

Motto:

Když se chce, všechno jde.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Hlavní náplní bakalářské práce je vytvoření podrobných návodů pro studenty a zaměstnance UTB. Tyto návody jsou zpracovány tak, aby podle nich byl schopen i počítačový začátečník dosáhnout kýženého výsledku. Jsou napsány stylem „krok po kroku“, včetně názorných obrázků.

Prvním, a nejdůležitějším tématem v návodech je připojení k UTB Wi-Fi. Bezdrátová síť v UTB je napojena na mezinárodní síť eduroam. Byly vytvořeny návody na připojení k síti eduroam pro Microsoft Windows XP, Windows Vista a Windows 7. Dále pak pro operační systém Linux, a to jak přes grafické uživatelské rozhraní KDE, tak pomocí editace konfiguračních souborů.

Druhým tématem jsou e-maily. Byl vytvořen návod, popisující webového klienta Webmail, jak se ovládá, jaké jsou možnosti jeho nastavení, například filtrování spamu nebo přesměrování pošty do soukromé e-mailové schránky. Dále byly vytvořeny návody na konfiguraci nejpoužívanějších poštovních klientů. Mezi ně patří MS Outlook Express, MS Live mail, MS Office Outlook 2007 a Mozzila Thunderbird 3.

Třetím tématem je systém Novell. Byl vytvořen návod, který popisuje, jak se přihlásit do systému Novell v učebnách a studovnách UTB. Jelikož existuje možnost připojit se na UTB servery vzdáleně přes protokol FTP, a tím se dostat k síťovým diskům N:, O:, P: a Q:, byl také vytvořen návod k tomuto připojení.

Posledním tématem, je návod na zprovoznění Wake on LAN. Tento systém slouží ke vzdálenému zapnutí počítače, odkudkoliv z internetu. To znamená, že uživatel vypne standardním způsobem počítač, a pak si jej může z jiného zařízení, s přístupem na internet, zapnout. Poté se může k takto vzdáleně spuštěnému počítači připojit přes zabudovaný systém ve Windows – „Připojení ke vzdálené ploše“, nebo přes jiného terminálového klienta, např. VNC.

I. TEORETICKÁ ČÁST

1 WI-FI

1.1 Technické informace

1.1.1 Obecné informace

Wi-Fi je standard pro lokální bezdrátové sítě (*Wireless LAN, WLAN*) a vychází ze specifikace **IEEE 802.11**. Původním cílem Wi-Fi sítí bylo zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) sítě LAN. S postupem času začala být využívána i k **bezdrátovému připojení** do sítě Internet v rámci rozsáhlejších lokalit a tzv. hotspotů. Wi-Fi zařízení jsou dnes prakticky ve všech přenosných počítačích a i v některých mobilních telefonech. Úspěch Wi-Fi přineslo využívání bezlicenčního pásma, což má negativní důsledky ve formě silného zarušení příslušného frekvenčního spektra a dále častých bezpečnostních incidentů. [15]

1.1.2 Specifikace IEEE 802.11

Standard 802.11 **vznikl v roce 1997** a definoval bezdrátovou síť v pásmu 2,4 GHz o rychlostech 1 nebo 2 Mbit/s. Protože však postupem doby vznikaly další a další nároky na posun tohoto standardu, utvářely se v rámci této pracovní skupiny další pracovní podskupiny věnované rozšířením a změnám v tomto standardu. Tyto skupiny jsou označované písmeny, která se přidávají za číslo standardu 802.11. [17]

Přehled standardů IEEE 802.11:

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	OFDM a MIMO

Tabulka 1: Přehled standardů IEEE 802.11

1.1.2.1 IEEE 802.11a

Tento standard využívá WiFi v pásmu 5 GHz. Používá modulaci OFDM. Oproti standardu IEEE 802.11b/IEEE 802.11g je tento stabilnější a vyspělejší. Má větší povolený vyzařovací výkon oproti 802.11b/g, tím ho lze používat na delší vzdálenosti. [16]

1.1.2.2 IEEE 802.11b

Tento standard je jedním z doplňků norem IEEE 802.11 zabývajících se definicí bezdrátového komunikačního standardu známým pod komerčním názvem Wi-Fi. Byl schválen v roce 1999 a oproti původnímu standardu navyšuje přenosovou rychlost na 11 Mbit/s v přenosovém pásmu 2,4 GHz. Používá modulační schéma je DSSS pro rychlosti 1, 2, 5.5 a 11 Mbit/s. Dosah až 12km ve volném prostředí. [16]

Frekvenční rozsah je 2400 - 2485 MHz. Je rozdělen na 14 kanálů, které se vzájemně překrývají. V některých státech ovšem není povolené plné frekvenční spektrum, protože jeho části jsou již využívány pro jiné účely. V České Republice ČTÚ povoluje 13 kanálů, podobné to je ve většině Evropy, USA se používá pouze 11 kanálů. V pásmu 2,4GHz je povolen maximální výstupní výkon za anténou 100mW, což odpovídá hodnotě 20dB. [17]

1.1.2.3 IEEE 802.11g

IEEE 802.11g je WiFi standard rozšiřující IEEE 802.11b, se kterým je zpětně kompatibilní. Vysílá ve stejném frekvenčním pásmu 2400 - 2485 MHz, ale maximální nominální rychlost je 54 Mbit/s, což odpovídá reálným přenosovým rychlostem přibližně 25 Mbit/s.

Použité modulační schéma je OFDM pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s, přičemž pro rychlosti 1, 2, 5.5 a 11 Mbit/s je použito stejné schéma jako ve standardu IEEE 802.11b. [16]

1.1.2.4 IEEE 802.11n

IEEE 802.11n je WiFi standard, který si klade za cíl upravit fyzickou vrstvu a podčást linkové vrstvy, takzvanou *Media Access Control* (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100 Mbit/s. Maximální fyzická (L1) rychlost může být až 600 Mbit/s.

Zvýšení rychlosti se dosahuje použitím MIMO (multiple input multiple output) technologie, která využívá vícero vysílacích a přijímacích antén. [16]

1.1.3 Zabezpečení sítě

Problém bezpečnosti bezdrátových sítí vyplývá zejména z toho, že jejich signál se šíří i mimo zabezpečený prostor bez ohledu na zdi budov, což si mnoho uživatelů neuvědomuje. Nezvaný host se může snadno připojit i do velmi vzdálené bezdrátové sítě jen s pomocí směrové antény, i když druhá strana výkonnou anténu nemá. Navíc většina nejčastěji používaných zabezpečení bezdrátových sítí má jen omezenou účinnost a dá se snadno obejít. [15]

1.1.3.1 WEP

WEP (Wired Equivalent Privacy, česky soukromí ekvivalentní drátovým sítím) je původní zabezpečení Wi-Fi sítí a je součástí IEEE 802.11 standardu z roku 1997. Už z názvu je patrné, že cílem bylo poskytnout zabezpečení jaké je dostupné v drátových sítích. Používá šifrování komunikace pomocí statických WEP klíčů (Wired Equivalent Privacy) symetrické šifry, které jsou ručně nastaveny na obou stranách bezdrátového spojení.

Symetrická šifra je šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost.

Protože se ale veškeré informace v bezdrátových sítích přenášejí volným prostorem, je snadné je odposlouchávat. Pro získání klíčů existují specializované programy. Není totiž nutné se fyzicky drátem připojit k síti.

WEP používá proudovou šifrovací metodu RC4 pro utajení informaci a pro ověření jejich správnosti používá metodu CRC-32 kontrolního součtu. [14, 15, 18]

1.1.3.2 WPA

WPA (Wi-Fi Protected Access, česky Wi-Fi chráněný přístup) je druh zabezpečení bezdrátových počítačových sítí. Vznikl jako reakce na vážné bezpečnostní nedostatky objevené v systému WEP. Vznikl s cílem využít hardware podporující WEP, ale vhodnými doplňkovými mechanismy (především prací s klíči) eliminovat jeho slabá místa. Kvůli zpětné kompatibilitě využívá WPA klíče WEP, které jsou ale dynamicky bezpečným způsobem měněny. K tomu slouží speciální doprovodný program, který se nazývá suplikant. Z tohoto důvodu je možné i starší zařízení upgradovat pro podporu WPA.

WPA implementuje velkou část standardu IEEE 802.11i. Vznikl jako dočasná náhrada WEP do doby, dokud nebude dokončena specifikace 802.11i. Kompletní implementací

standardu IEEE 802.11i je WPA2, což je následník WPA, který ale není podporován některými staršími kartami.

Zásadní vylepšení oproti WEP zabezpečení spočívá v použití šifrování **TKIP** (Temporal Key Integrity Protocol), což je protokol dynamicky měnící klíče. Společně s mnohem delšími inicializačními vektory tak odolává útokům, jimiž je napadán WEP.

Další variantou je možnost použití šifrování AES, které se v současnosti považuje za nejbezpečnější.

Autentizace přístupu do WPA sítě je prováděno pomocí **PSK** (Pre-Shared Key – všichni uživatelé používají stejné přístupové heslo) nebo **RADIUS** server (ověřování přihlašovacím jménem a heslem). [15, 19]

1.1.3.3 WPA2

WPA2 implementuje povinné prvky standardu IEEE 802.11i. Konkrétně přidává k TKIP a algoritmu Michael nový algoritmus CCMP - (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) založený na AES, který je považován za zcela bezpečný. Od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, jež chtějí být certifikována jako Wi-Fi. [15, 19]

1.1.3.4 Autentizace přístupu do WPA sítě pomocí PSK

Režim s předsdíleným heslem - PSK pre-shared key (označovaný také jako *osobní* režim) je navržen pro sítě v domácnostech a malých kancelářích (tzv. SOHO segment), které si nemohou dovolit náklady a složitost autentizačního serveru pro IEEE 802.1X - např. RADIUS server. Každý uživatel musí před vstupem do sítě zadat heslo obsahující 8 až 63 tisknutelných ASCII znaků nebo 64 šestnáctkových číslic. Většina operačních systémů umožňuje uložení hesla na uživatelském počítači, aby nebylo nutné jej opakovaně zadávat. [15, 19]

1.1.3.5 Autentizace přístupu do WPA sítě pomocí protokolu IEEE 802.1X a RADIUS serveru

Přístupový bod vyžaduje autentizaci pomocí protokolu IEEE 802.1X. Pro ověření je používán na straně klienta program, který nazýváme *prosebník* (suplikant), kterému přístupový bod zprostředkuje komunikaci s třetí stranou, která ověření provede (například RADIUS server). [15]

1.1.3.5.1 RADIUS server

RADIUS (Remote Authentication Dial In User Service, česky uživatelská vytáčená služba pro vzdálenou autentizaci) je AAA protokol (authentication, authorization and accounting, česky autentizace, autorizace a správa účtů) používaný pro přístup k síti.

Při připojení do sítě je vyžadováno přihlašovací jméno a heslo. Tato informace je poslána přes RADIUS protokol do RADIUS serveru. Ten ověří pravost informace použitím autentizačních schémat jako PAP, CHAP nebo EAP. Pokud je uživatelské jméno a heslo přijato, server autorizuje přístup k poskytovateli internetu a vybere IP adresu (popřípadě rozsah adres) a další parametry spojení. [20]

1.2 Síť Eduroam

Eduroam je zkratka z Education Roaming. Jedná se o počítačovou infrastrukturu pro transparentní používání sítí univerzit a jiných vzdělávacích institucí. Myšlenka vznikla na půdě TERENA (Trans-European Research and Education Networking Association).

Cílem je takové propojení sítí všech účastníků, že uživatel jedné sítě se může pod svým účtem (udržovaným v domovské síti) připojit do libovolné z nich. Důsledkem pak je stejně jednoduché používání jako v případě mobilního roamingu.

Technicky je přihlašování účastníků řešeno pomocí RADIUS serverů.

Uživatel má pouze jedinou identitu (uživatelský účet vedený ve své domácí instituci) a s ní je schopen přihlášení do kterékoli spolupracující sítě. Celý systém je postaven tak, že na základě uživatelského jména jsou autentizační dotazy posílány do uživatelovy domovské sítě. Tam je rozhodnuto, zda je uživatel tím, za kterého se vydává, a zda má právo přístupu. Tato informace je přenesena zpět do navštívené sítě a přístupový mechanizmus se podle ní zařídí - buďto uživatele do sítě vpustí nebo jeho požadavek zamítne. Pro funkci takto nastíněného systému jsou nezbytné dvě věci. Uživatelské jméno, které v sobě nese informaci, odkud uživatel pochází, a autentizační infrastruktura, která je schopna přenášet autentizační data. Tvar uživatelského jména má proto následující syntaxi: "jmeno@realm". Jméno je běžné uživatelské jméno platné v rámci dané instituce a realm určuje, o jakou organizaci jde. Tento tvar je velmi podobný formátu adresy elektronické pošty a je podobný i významově. [24] Příklad uživatelského jména pro uživatele UTB může být např. „**j_novak@utb.cz**".

Např. student UTB se připojí do cizí sítě eduroam, jejich server pošle požadavek na ověření k RADIUS serveru UTB, který mu potvrdí přihlašovací údaje.

V České republice projekt zaštiťuje sdružení CESNET, z.s.p.o. které se v projektu angažuje od samého počátku jako koordinátor a propagátor aktivit související s počítačovým roamingem nejen u nás, ale i v ostatních evropských zemích. V současné době se vyskytují vysílače sítě eduroam ve většině zemí evropské unie. Kromě Evropy jsou vysílače eduroam také v Austrálii, Kanadě, Japonsku a Číně. [21, 22, 23]

1.3 Připojení k síti eduroam na UTB

Nejdříve je potřeba zaregistrovat se do školní sítě. To je možné provést na internetové adrese [27].

Po registraci je potřeba zkontrolovat, jestli je na bezdrátové síťové kartě nastaveno získávání IP adresy ze serveru DHCP a automatické získávání adresy serveru DNS.

Potom je potřeba zkontrolovat, zda se uživatel nachází na místě s dostatečným signálem sítě eduroam.

Pokud jsou tyto podmínky splněny, je potřeba vytvořit nové síťové připojení pro síť eduroam s následujícími parametry:

- Název sítě (SSID): eduroam
- Typ zabezpečení: WPA-podnikové
- Typ šifrování: TKIP
- Metoda ověřování v síti: Protokol PEAP (Protected EAP)
- Způsob ověření: EAP - MSCHAP v2
- Vypnout ověřování serverových certifikátů

Po vytvoření nového síťového připojení se zobrazí dotaz na uživatelské jmeno a heslo.

Uživatelské jméno je rozšířeno o doménu domácí organizace, podle níž je uživatel identifikován v rámci sítě eduroam.

Tvar uživatelského jména je **přihlašovací_jméno@utb.cz**

Bude tedy ve tvaru např. „**j_novak@utb.cz**“

„**Heslo**“ je heslo zvolené při registraci do WiFi sítě UTB.

V přílohách praktické části bakalářské práce jsou návody na připojení k síti eduroam pro Microsoft Windows XP, Windows Vista a Windows 7.

Dále pak pro operační systém Linux, a to jak přes grafické uživatelské rozhraní KDE, tak pomocí editace konfiguračních souborů.

2 E-MAIL

2.1 Technické informace

2.1.1 Obecné informace

Elektronická pošta, zkráceně **e-mail,** je způsob odesílání, doručování a přijímání zpráv přes elektronické komunikační systémy. [6] Technologie je definovaná normou RFC 5322.

2.1.1.1 E-mailová adresa

E-mailová adresa je údaj, který v e-mailové zprávě určuje adresáta zprávy (případně adresáta kopie zprávy) a také údaj o odesílateli zprávy. E-mailová adresa identifikuje elektronickou poštovní schránku uživatele e-mailu. [7]

E-mailová adresa je ve tvaru „**jméno@doména.doména_prvního_řádu**“.

Doména může mít více tvarů, buď bude obsahovat pouze doménu druhého řádu (např. „**jmeno@utb.cz**“), nebo mohou být před doménou druhého řádu ještě domény nižších řádů (např. „**jmeno@fai.utb.cz**“). Doména prvního řádu je např. „**.cz**“, „**.sk**“, „**.com**“ atd.

V e-mailové adrese platí stejná pravidla, jako pro tvorbu doménové adresy. Nesmí se používat mezery a některé speciální znaky.

2.2 Komunikační protokoly

Mezi počítači na internetu se vyměňují zprávy pomocí **SMTP** (Simple Mail Transfer Protocol). Uživatelé mají na svém počítači nainstalován program, který se nazývá e-mailový klient. Ten stahuje zprávy z poštovního serveru použitím protokolů **POP** (Post Office Protocol) nebo **IMAP** (Internet Message Access Protocol). Je možné ukládat e-maily buď na straně serveru, nebo na straně klienta.

Ke zprávám umístěným na poštovním serveru lze přistupovat také přes webové rozhraní. Není tedy potřeba e-mailový klient. Pro e-mailovou schránku UTB lze použít online klient Webmail, kterého je možné nalézt na internetové adrese <**http://webmail.utb.cz**>[8].

2.2.1 SMTP

Simple Mail Transfer Protocol (zkratka **SMTP**) je internetový protokol určený pro odesílání zpráv elektronické pošty. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem. SMTP funguje nad protokolem TCP, používá port TCP/25.[9]

Protokol SMTP předpokládá trvalou dostupnost příjemce i odesilatele - pokud se odesílajícímu poštovnímu serveru nepodaří zkontaktovat přijímající poštovní server, interpretuje to jako chybu a snaží se ji napravit opakováním pokusů o přenos. Kvůli této své vlastnosti protokol SMTP není použitelný pro přenos poštovních zpráv až ke koncovým poštovním klientům, kteří nemusí být trvale dostupní. Pro tyto účely musely být vyvinuty další protokoly, konkrétně protokoly POP3 (Post Office Protocol, verze 3) a IMAP (Internet Message Access Protocol). [10] Protokol IMAP pouze čte poštu ze serveru a při výběru ji ze serveru nemaže.

2.2.2 POP3

Post Office Protocol version 3 (zkratka **POP3**) je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru do e-mailového klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. Používá port TCP/110.

POP3 je následníkem protokolů POP1 a POP2 (označení POP už dnes téměř výhradně znamená POP3). [11]

Poštovní server UTB rezervuje určité místo pro každého majitele schránky. Tato kapacita je omezená, proto může dojít místo a nové e-maily nebude kam ukládat.

2.2.2.1 Výhody POP3

Veškerá pošta se stahuje do počítače, tudíž na serveru nemůže dojít místo pro novou poštu. Je zde možnost nastavení zanechávání kopie zpráv na serveru, tudíž místo dojít může.

2.2.2.2 Nevýhody POP3

Nefunguje synchronizace složek mezi poštovním klientem a serverem, veškerá stažená pošta zůstává v počítači a už k ní nelze přistupovat např. přes webového klienta (UTB Webmail) nebo jiného poštovního klienta.

2.2.3 IMAP

Internet Message Access Protocol (zkratka **IMAP**) je internetový protokol pro vzdálený přístup k e-mailové schránce. Na rozdíl od protokolu POP3 vyžaduje IMAP trvalé připojení (tzv. on-line), avšak nabízí pokročilé možnosti vzdálené správy (práce se složkami, přesouvání zpráv, prohledávání na straně serveru a podobně). Uživatel má však možnost pomocí e-mailového klienta stáhnout poštu včetně příloh do počítače a potom s ní pracovat i bez připojení k internetu (jako v případě POP3). Jakmile se pak uživatel připojí, e-mailový klient všechny operace synchronizuje se serverem.

V současné době se používá protokol **IMAP4** (IMAP version 4 revision 1 - IMAP4rev1), který je definován v RFC 3501.

[12]

Poštovní server UTB rezervuje určité místo pro každého majitele schránky. Tato kapacita je omezená, proto může dojít místo a nové e-maily nebude kam ukládat. Při používání protokolu IMAP toto může být problém. Pokud uživatel nepotřebuje mít některé zprávy na serveru (např. archivní zprávy), může si je přesunout do lokálních složek svého e-mailového klienta, podobně jako při použití protokolu POP3 a tím si uvolnit místo na serveru.

2.2.3.1 Výhody protokolu IMAP

- Protokol IMAP používá obousměrnou komunikaci mezi webmailem a jedním nebo několika e-mailovými klienty.
- Lze používat na více poštovních klientech najednou, pošta zůstává na serveru a stahuje se do poštovního klienta.
- Synchronizace složek mezi poštovním klientem a serverem.
- Uživatel nemusí stahovat celou zprávu, takže zprávy, které jsou velké, nebo je to spam, stahovat nemusí.

2.2.3.2 Nevýhody protokolu IMAP

Jelikož veškerá pošta zůstává na serveru, je možné, že na části disku vyhrazené pro uživatele dojde místo a nové e-maily nebude kam ukládat. Uživatel si však ve svém lokálním poštovním klientu může stáhnout přijatou poštu ze serveru přímo do počítače a ze serveru data smazat. Například si může na SMTP serveru nechávat důležitá data a archiv mít uložený v počítači.

2.3 Soukromí a šifrování

Bez osobních bezpečnostních opatření e-mail nezaručuje soukromí, protože:

- e-mailové zprávy všeobecně nejsou šifrované
- e-mailové zprávy musí projít cizími počítači v síti předtím, než dosáhnou cílový počítač, což znamená, že je relativně jednoduché je cestou zachytit a přečíst si cizí zprávu
- většina poskytovatelů internetového připojení ukládá na své servery kopie e-mailových zpráv předtím, než je doručí. Tyto zálohy můžou zůstat na serveru až několik měsíců, a to i v případě, že si je ve své schránce majitel schránky vymaže.

Existují šifrovací aplikace, které mohou tyto nedostatky řešit, jako např. virtuální privátní sítě, šifrování zpráv pomocí PGP nebo GNU Privacy Guard.

Kromě šifrování zpráv můžeme šifrovat také samotný přenos. Používá se šifrovaná komunikace s e-mailovým serverem pomocí **Transport Layer Security** (**TLS**) nebo **Secure Sockets Layer** (**SSL**).

[6, 13]

Poštovní server UTB používá šifrování SSL. V praktické části je v návodech na nastavení jednotlivých klientů popsáno, jak aktivovat SSL šifrování. Pro protokol **IMAP** se používá port **993**, pro **POP3** je to pak port **995**. Uživatelé mohou také narazit na dotaz pro schválení certifikátu u poštovního klienta Mozzila Thunderbird 3, který nemá zabudovanou důvěryhodnou certifikační autoritu, kterou používá poštovní server UTB.

2.3.1 Princip fungování SSL

Ustavení SSL spojení funguje na principu asymetrické šifry, kdy každá z komunikujících stran má dvojici šifrovacích klíčů – veřejný a soukromý. Veřejný klíč je možné zveřejnit, a pokud tímto klíčem kdokoliv zašifruje nějakou zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem.

Ustavení SSL spojení (*SSL handshake*, tedy „potřásání rukou“) pak probíhá následovně:

1. Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
2. Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.
3. Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.

4. Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
5. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
6. Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
7. Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
8. Aplikace od teď dál komunikují přes šifrované spojení.

Během první fáze ustanovení bezpečného spojení si klient a server dohodnou kryptografické algoritmy, které budou použity.

[13]

2.3.2 Spam

Spam je nevyžádaná reklamní pošta. Nízké náklady na odeslání zprávy umožňují spammerům pomocí internetového připojení odeslat stovky miliónů elektronických zpráv denně. Obrovské množství aktivních spammerů způsobuje přetížení počítačů v internetu, které takto dostávají desítky či stovky nevyžádaných e-mailů denně. [6]

Antispamové filtry na poštovním serveru UTB kontroluji všechny příchozí zprávy, a nevyžádanou poštu označují textem „[SPAM]“ na začátku předmětu e-mailu. Uživatel si ve svém klientovi může nastavit automatické přesouvání těchto zpráv do určené složky s nevyžádanou poštou. Tuto složku je někdy potřeba zkontrolovat, jestli tam není nějaká zpráva omylem označená za spam. K přesměrování spamu ve Webmailu slouží filtry. V návodu pro online klienta Webmail je popsán postup, jak tento filtr vytvořit.

2.4 Praktické používání e-mailu

Uživatelé mohou přistupovat ke své schránce buď pomocí některého z e-mailových klientů, nebo přes webové rozhraní. V případě přístupu z e-mailového klienta je potřeba zvolit protokol pro příchozí poštu. Lze použít buď POP3 nebo IMAP.

V případě přístupu k poštovnímu serveru UTB lze používat:

- webový klient Webmail,
- některý e-mailový klient

E-mailová adresa je ve tvaru: „**uživatelské_jméno@fakulta.utb.cz**“
Např. student FAI má e-mailovou adresu „**j_novak@fai.utb.cz“**

2.4.1 Webmail

Je možné jej nalézt na internetové adrese <**http://webmail.utb.cz**>[8].

Pro přihlášení je potřeba zadat:

- Uživatelské jméno, které je stejné jako při přihlašování do školní sítě, (např. Novell) Bude tedy např. „**j_novak**“
- Heslo, které je taktéž stejné jako při přihlašování do školní sítě

2.4.2 Některý z e-mailových klientů

V případě přístupu ke schránce z poštovního klienta je potřeba nastavit tyto parametry:

Do kolonky	**Vyplnit**
Jméno	jméno a příjmení
E-mailová adresa	e-mailovou adresu (např. **j_novak@fai.utb.cz**)
Typ účtu	zvolit POP3 nebo IMAP
Server příchozí pošty	**imap.utb.cz** (jak pro protokol POP3, tak pro IMAP)
Server pro odchozí poštu	**smtp.utb.cz*** (při připojení ze sítě UTB)
Uživatelské jméno	přihlašovací jméno do školní sítě, např. **j_novak**
Heslo	heslo (je stejné jako při přihlašování do školní sítě, např. Novell)
Šifrování	Pro server příchozí pošty nastavit šifrované připojení SSL (pro **POP3** je to port **995**, pro **IMAP** je to port **993**)

Tabulka 2: Parametry konfigurace e-mailového klienta

*2.4.2.1 *SMTP server*

Pokud je uživatel připojen k internetu ze sítě UTB, použije server **smtp.utb.cz**. Jestliže je připojen z jiné sítě (mimo UTB), pravděpodobně server smtp.utb.cz nebude fungovat. Musí tedy používat SMTP server, který provozuje poskytovatel jeho internetového připojení.

Praktická část této bakalářské práce se zabývá popisem webového klienta Webmail, a dále obsahuje návody na konfiguraci e-mailových klientů MS Outlook Express, MS Live mail, MS Office Outlook 2007 a Mozzila Thunderbird 3

3 PROTOKOL FTP

3.1 Technické informace

3.1.1 Obecné informace

FTP (anglicky **File Transfer Protocol**) patří do aplikační vrstvy rodiny protokolů TCP/IP a je jeden z nejstarších. Od začátku byl směřován jako protokol pro rychlé datové přenosy souborů. Na počítačích, které uskutečňují datový přenos, mohou být rozdílné operační systémy, FTP protokol je nezávislý na platformě. Jeho stáří je mu výhodou, ale zároveň i slabinou. Je definován normou RFC 959 a posléze rozšířen normou RFC 2228. Jeho podporu obsahuje většina webových prohlížečů nebo specializované programy.[1,2]

3.1.2 Historie

Původně byl protokol FTP navržen v podobě, kterou dnes známe jako „**aktivní**“. V průběhu času se internet začal vyvíjet a velmi rozšiřovat, což způsobilo nedostatek adresového prostoru IPv4. Začala se používat technologie NAT, která pracuje na principu překladu adres. Bylo potřeba protokol FTP upravit tak, aby fungoval i s počítači, které byly připojeny za NATem, tudíž nebyly dostupné napřímo z internetu. Byl tedy implementován tzv. „**pasivní**“ režim, který do značné míry zjednodušil práci lidem za NATem.[2]

3.2 Základní informace o spojení

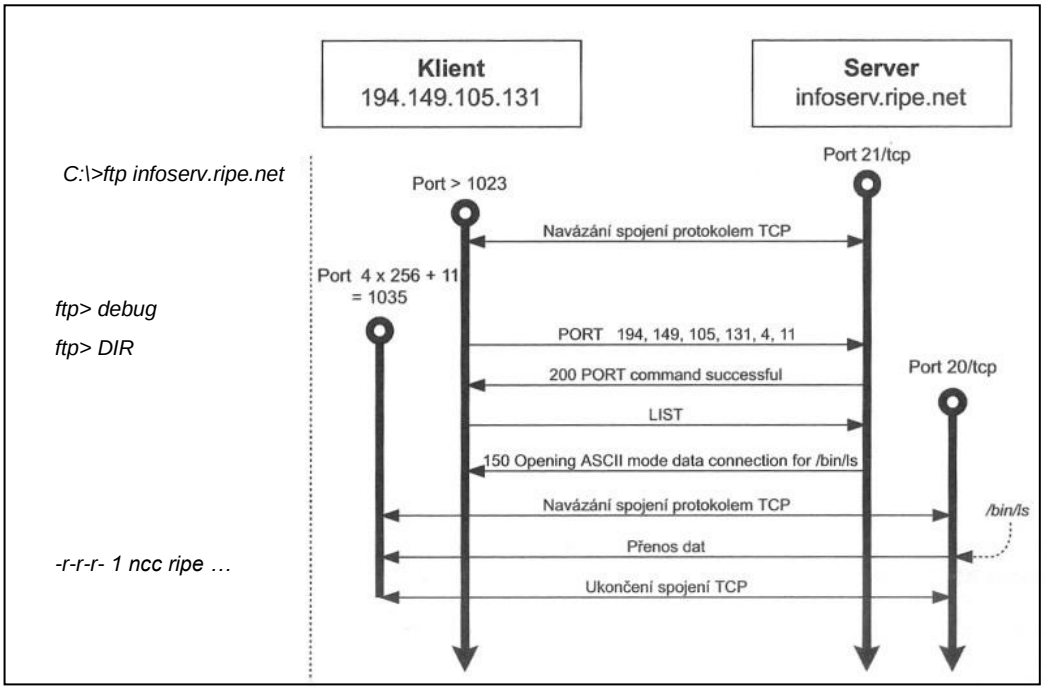
Spojení se vždy navazuje mezi klientem (program, který vystavuje požadavky) a serverem (server je program, který umí tyto požadavky splnit). Server tzv. naslouchá na určeném portu na veškeré požadavky, tj. program serveru je neustále spuštěn, ať již provádí nějakou činnost či nikoliv.[2]

Portu může mít přiřazeno číslo od 1 do 65535. Je definován ve vysílaných a příchozích IP paketech. Operační systém pak podle čísla portu směřuje pakety jednotlivým programům. Prvních 1024 portů je definováno normou RFC. Říká se jim „**přiřazené**“. Každá z nich má oficiálně definovanou službu nebo protokol serveru. [2]

Protokol FTP má definovaný port 21 pro příchozí spojení (naslouchání). Na portu číslo 20 pak probíhá samotný přenos dat. Správce serveru však může tyto čísla portů změnit. [1]

3.2.1 Aktivní FTP spojení

Jak již bylo řečeno, aktivní spojení je původní verze FPT protokolu. Pro řízení spojení se používá port 21, pro přenos dat port 20. Klient odešle z jednoho ze svých vyšších portů (nad 1024) příkaz na server, který naslouchá na portu 21. Takto probíhá řídící spojení, pomocí něhož klient ovládá FTP server. Klient se autentizuje a pak může zadávat serveru různé příkazy. Server potom tyto příkazy plní a jejich výstup (ať už výpis adresáře, či samotná up/down-loadovaná data) vysílá ze svého portu 20 na port nad 1024 klienta, který komunikující program zvolí. [1,2]



Obrázek 1: Aktivní FTP spojení [5]

3.2.1.1 Výhody aktivního spojení:

Velkou výhodou protokolu FTP je oddělení řídícího spojení a datového spojení. Snižuje se režie spojení, není tedy potřeba složitě odlišovat řízení a data. Další výhodou je možnost odesílat data úplně jinam, než je klient. To znamená např., že správce má možnost z pomalé linky odesílat data po páteřní lince z jednoho serveru na druhý. Tato možnost je ovšem

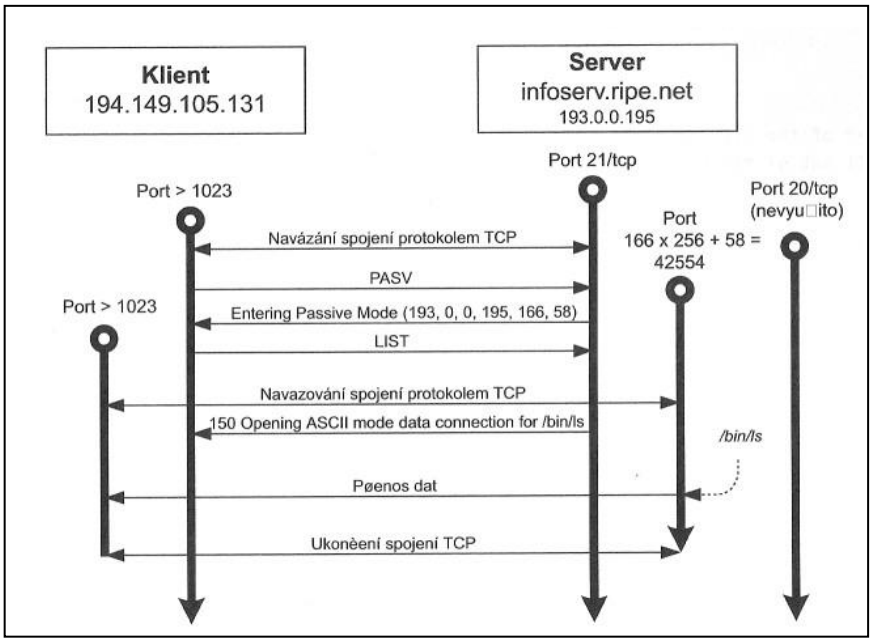
z bezpečnostních důvodů standardně vypnuta. Dále může být takto nakonfigurovaný server umístěn za NATem, pouze musí být přesměrovaný port 21. [1,2]

3.2.1.2 Nevýhody aktivního spojení:

Největší nevýhodou, a zároveň důvodem vzniku pasivního módu je nemožnost navázání spojení s klientem za NATem. Tento problém lze vyřešit vhodným nastavením routeru, přesměrováním portu 20. [2]

3.2.2 Pasivní FTP spojení

Pasivní režim byl vytvořen, aby bylo možné připojit se na server i z klientů za NATem. U pasivního spojení se obě spojení vystavují směrem k FTP serveru.



Obrázek 2: Pasivní FTP připojení [5]

Přepnutí se provádí v textově ovládaném klientu pomocí příkazu **PASV**. Ve speciálních programech je většinou tato volba uvedená v nastavení. [2]

V pasivním režimu však nastává problém, jak odlišit jednotlivé datové porty jednotlivých klientů. Tento problém řeší FTP server tak, že otevírá pro každý požadavek na datové spojení dedikovaný dočasný server na náhodném portu z rozsahu portů nad 1024/TCP (tento rozsah jde u většiny server nastavit). Tento port sdělí server klientovi textovou odezvou v řídícím spojení: [2]

```
PASV
227 Entering Passive Mode (123,213,231,123,234,100).
```

-klient zadá příkaz PASV

-server odpoví, že má klient vystavit nové datové spojení na určenou adresu a port. Tato informace je v závorce. První 4 oktety (oktet = číslo oddělené čárkou) odpovídají IP adrese FTP serveru, a poslední dva označují port. Ten se čte následujícím způsobem: pátý oktet se vynásobí číslem 256 a k tomuto číslu se přičte šestý oktet. V případě uvedeného příkladu 123,213,231,123,234,100 je to 234*256=59904, 59904+100=60004. Adresa je tedy 123,213,231,123 a port 60004. [2]

3.2.2.1 Výhody pasivního spojení:

Klient za NATem nemusí nijak přesměrovávat porty.

3.2.2.2 Nevýhody pasivního spojení:

Server nemůže být za NATem, tento problém lze vyřešit speciálními moduly pro NAT.

3.2.3 Nejčastější použití FTP

- sdílení dat (hudba, videa, vlastní tvorba, data…)
- správa webových stránek
- vzdálený přístup k datům na serveru (školní disky)

[1]

3.3 Příkazy pro řízení

Dělí se do tří skupin:

1. Access Control Commands (příkazy řízení přístupu)
2. Transfer Parameter Commands (příkazy nastavující parametry přenosu)
3. FTP Service Commands (obsluhující příkazy)

1. Access Control Commands

- USER - zadání uživatelského jména
- PASS - zadání uživatelského hesla
- ACCT - zadání uživatelského účtu (téměř se nepoužívá)
- CWD - změna aktuálního adresáře
- CDUP - změna aktuálního adresáře na nadřazený adresář
- QUIT - ukončení spojení

2. Transfer Parameter Commands

- PORT - specifikuje počítač a port pro datové spojení. Klient pošle tento příkaz a bude na daném portu čekat na datové spojení.
- PASV - žádá server o pasivní mód, tzn., že server bude poslouchat a klient bude iniciovat datové spojení.
- TYPE - určuje typ reprezentace dat, např. text nebo binární

3. FTP Service Commands

- RETR - slouží k přenosu souboru ze serveru
  - GET - přenos jednoho souboru ze serveru (příkaz klientského software ftp)
  - MGET - přenos více souborů ze serveru (příkaz klientského software ftp)
- STOR - přenos souboru na server
  - PUT - přenos jednoho souboru na server (příkaz klientského software ftp)
  - MPUT - přenos více souborů na server (příkaz klientského software ftp)
- RNFR, RNTO - přejmenování souboru
- DELE - smazání souboru
- MKD - vytvoření nového adresáře
- RMD - smazání adresáře (adresář musí být prázdný)
- ABOR - zrušení předchozího příkazu
- PWD - zjištění aktuálního pracovního adresáře
- LIST - získání seznamu souborů. K získání tohoto seznamu se musí otevřít datové spojení. Pokud parametr tohoto příkazu je adresář, získá se výpis tohoto adresáře, pokud je to soubor, získají se informace o tomto souboru a pokud příkaz nemá parametr, je vrácen výpis aktuálního adresáře. Výpis příkazu list však závisí na systému a je určen především pro člověka.
- NLST - podobný příkazu LIST, jen s tím rozdílem, že seznam vrací na každém řádku jen jméno souboru (adresáře) a žádné další informace.
- SYST - slouží k zjištění typu systému, na kterém běží FTP server.

[1]

3.4 Nevýhody FTP

Přenášené informace nejsou ve standardním protokolu šifrované, což snižuje bezpečnost (ohrožuje jméno, heslo, ale i přenášená data).

Je-li použit firewall, u aktivního přenosu protokol vyžaduje jeho speciální podporu. Dále aktivní přenos nepodporuje šifrované řídících spojení. Je tedy nutné používat pasivní přenos. FTP server má delší odezvy.

[1,2]

3.5 Zabezpečení FTP

Jelikož jsou při běžném přihlašování pomocí FTP protokolu přihlašovací údaje přenášeny pouze v textové podobě, je technicky možné je zachytit. Tyto problémy jsou řešeny různými nadstavbami FTP jako je „**FTPS**“ nebo „**FTP přes SSH**“. [1]

3.5.1 FTPS

Tato nadstavba je zpětně kompatibilní s běžným FTP a využívá technologie SSL/TLS. Zajišťuje zabezpečený přenos citlivých informací, jako je přihlašovací jméno, heslo nebo i vlastní přenášená data). [3]

3.5.2 FTP přes SSH (SFTP)

FTP přes SSH je někdy označováno jako “bezpečné FTP” (Secure FTP, neboli SFTP). Používá tunelování FTP skrz spojení navázaného pomocí SSH protokolu. [4]

3.6 Praktické používání FTP

Přistupovat na FTP lze několika způsoby.

- z konzoly, FTP se ovládá přímo pomocí příkazů
- z operačního systému nebo webového prohlížeče
- ze specializovaného programu (např. Total Commander)

Praktická část této bakalářské práce se zabývá popisem přístupu na FTP pomocí operačního systému a programu Total Commander.

3.6.1 Důležité údaje k připojení k UTB FTP serverům:

Název relace:	Vyplňuje se u programů typu Total Commander. Zde se napíše uživatelem zvolený název, např. central
Hostitel (adresa FTP)**:**	**nw-central.utb.cz** pro server nw-central (disk P) **nw-orion.utb.cz** pro server nw-orion (disk O) **nw-fame.utb.cz** pro server nw-fame (disk O pro FAME)
Jméno uživatele:	Zde se vyplní přihlašovací jméno jako do školní sítě, to je ve formátu: první písmeno jména_příjmení, např. **j_novak**
Heslo:	Zde uživatel zadá heslo (je stejné jako při přihlašování do školní sítě, např. Novellu)

3.6.2 Připojení z konzoly

Pomocí konzoly operačního systému Microsoft Windows se jde připojit k ftp a ovládat server pomocí textových příkazů. Připojení se provádí v příkazové řádce spuštěním programu CMD.exe. Druhým krokem je přepnutí do režimu ftp napsáním příkazu „FTP“. Poté už je možné zadat adresu konkrétního FTP serveru. Po připojení se server ovládá textovými příkazy, nápovědu je možné vyvolat napsáním znaku „**?**“ nebo „**help**“ a potvrzením tlačítkem Enter.

3.6.3 Připojení z operačního systému nebo webového prohlížeče

Další možností k připojení na FTP server je použití grafického prostředí Windows. Buď pomocí průzkumníka, nebo webového prohlížeče. Postup je velice podobný.

3.6.4 Připojení ze specializovaného programu

Nejvhodnější způsob připojení k FTP serveru je použití specializovaného programu. Těch je celá řada. Nejpoužívanějším programem je asi **Total Commander**.

Nejrozšířenější program specializující se přímo na FTP je freewarový program **FileZilla**. Ten je multiplatformní (podporuje operační systémy Microsoft Windows, Linux a MAC OS X). Existuje ve verzích **FileZilla Client** a **FileZilla Server**.

V praktické části této bakalářské práce je popis přístupu na FTP pomocí programu Total Commander.

4 WAKE ON LAN

4.1 Obecné informace

Wake on LAN (zkratka **WOL**, **WoL**) je technologie, umožňující zapnutí vypnutého počítače přes počítačovou síť. Byla vyvinuta firmou IBM v roce 1997, později tento standard podpořila firma Intel. [25]

4.2 Základní požadavky na probouzený počítač

Je nutná podpora u **základní desky** a u **síťové karty**. Funguje to tak, že i když je počítač vypnutý, síťová karta je stále napájena a poslouchá komunikaci, zda nepřišel speciální rámec (frame), který se jmenuje **Magic Packet**. Síťová karta pracuje ve speciálním režimu Magic Packet Mode. Ve chvíli, kdy zachytí Magic Packet, který je určen pro ni, pošle signál základní desce, aby zapnula počítač. [26]

Dříve se pro externí síťové karty používal speciální kabel, který je spojoval se základní deskou. Později se tento budící signál začal posílat po PCI sběrnici (od verze PCI 2.2). Dnes je síťová karta většinou integrovaná na základní desce, takže je vše jednodušší (ale ve skutečnosti je přesto připojena přes PCI či PCIe). [26]

Funkce Wake on LAN funguje pouze po korektním vypnutí počítače. WOL nebude fungovat například při přerušení dodávky elektrické energie nebo při vypnutí počítače dlouhým podržením spouštěcího tlačítka PC.

4.2.1 Magic Packet

Magic Packet je standardní rámec, který obsahuje **zdrojovou adresu**, **cílovou adresu**, která může být adresou cílové stanice nebo multicastovou (tzn. i broadcast) adresou. Datový obsah paketu musí kdekoliv uvnitř (ale většinou zde jiný obsah není) obsahovat synhronizační stream, což je 6 bytů o hodnotě FF. Následovaný 16 krát zopakovanou MAC adresou cílové stanice (bez oddělovače).

Rámec se odesílá jako UDP a doporučuje se použít port 9 (discard) nebo 7 (echo). Zdrojový port je dynamický. [26]

4.3 Konfigurace probouzeného systému

V praktické části této bakalářské práce je podrobný návod na konfiguraci.

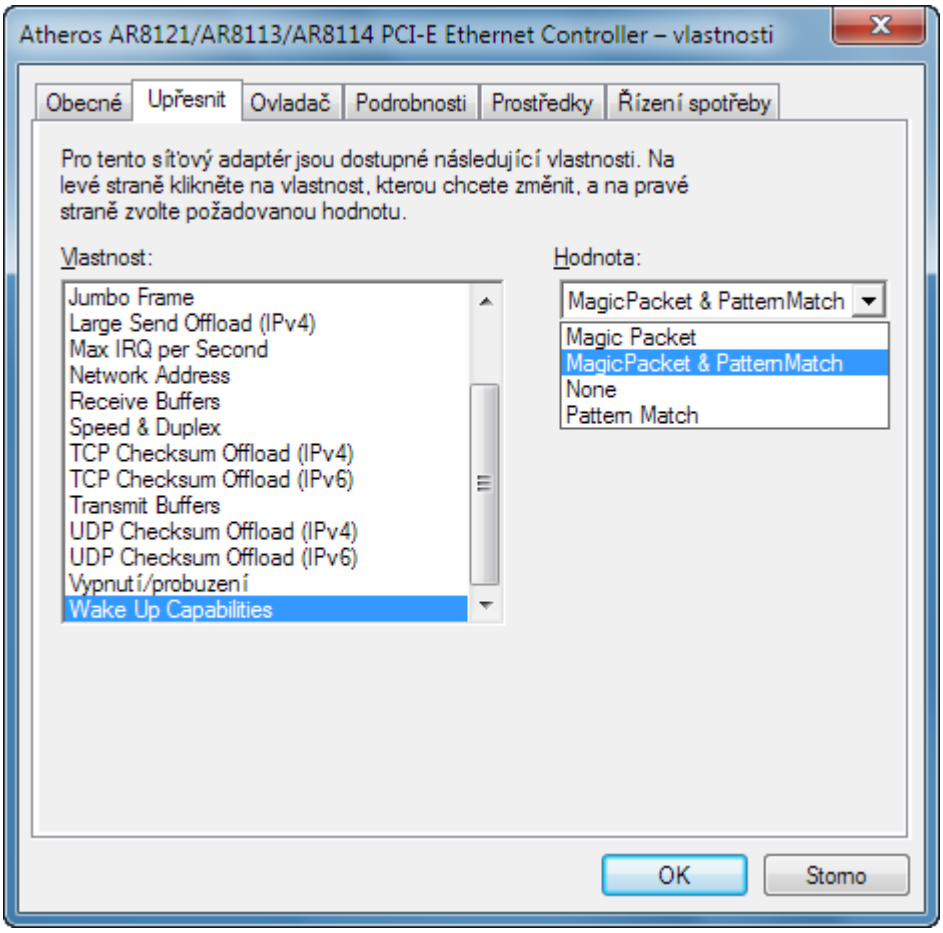
4.3.1 Operační systém

V operačním systému MS Windows je potřeba aktivovat technologii WOL, aby Windows při vypínání přepnuly síťovou kartu do speciálního režimu „**Magic Packet Mode**“, ve kterém je síťová karta stále napájena, naslouchá síťovou komunikaci a čeká na Magic Packet.

Tuto funkci je možné aktivovat ve Správci zařízení, ve vlastnostech síťové karty.

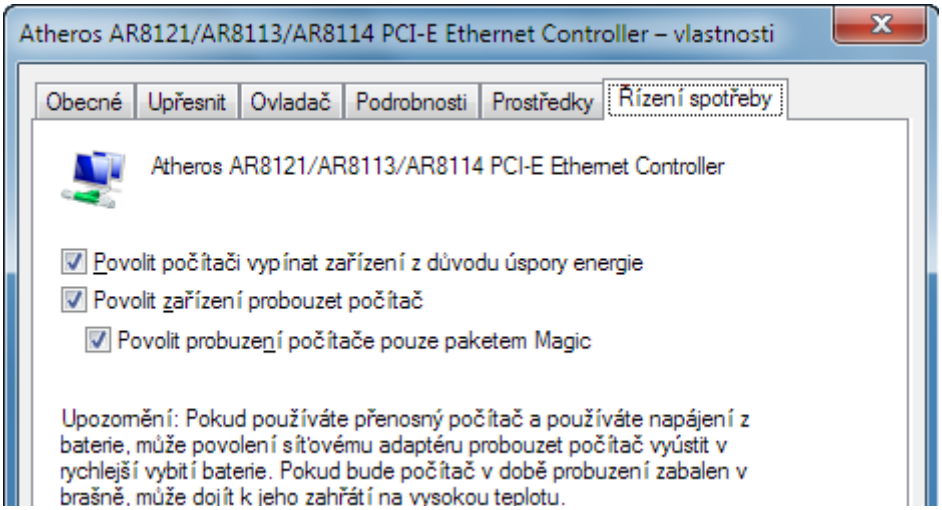
V kartě „**Upřesnit**“ je potřeba vyhledat položku s názvem „**Vypnutí/probuzení**“ a přepnout na „**Povoleno**“. Podle typu síťové karty se mohou tyto položky lišit.

Může tam také být např.: „**Shutdown Wake-On-LAN**“, „**Wake on Magic Packet**“, „**Wake From Shutdown**” a podobně. Všechny položky, které obsahují formulaci „**Wake on LAN**” nebo „**WOL**” je potřeba přepnout na „**Povoleno**”, popřípadě anglicky „**Enabled**“. Pokud je v seznamu položka „**Wake Up Capabilities**”, zvolí se „**Magic packet & PatternMatch**“.



Obrázek 3: Konfigurace síťové karty, záložka „Upřesnit“

Poté je potřeba v kartě „**Řízení spotřeby**“ povolit všechny tři zobrazené možnosti zaškrtnutím.



Obrázek 4: Konfigurace síťové karty, záložka „Řízení spotřeby“

4.3.2 BIOS

Povolení v programu SETUP BIOSu se provádí u každé základní desky jinak. Může to být přímo položka „**Wake on LAN**“, nebo jiné formulace. Síťovou kartu může reprezentovat také obecné „**Power On By PCIE Device**” nebo „**Power On By PCI Device**“, podle toho v jakém typu slotu je síťová karta připojena (může být buď starší PCI nebo novější PCI express, zkráceně PCIe), v případě integrované karty na jaké sběrnici je karta připojena (většinou jsou připojené napřímo do PCI nebo PCIe).

4.3.3 Test správné funkčnosti WOL

Správné nastavení zapínaného počítače je nejlepší otestovat z jiného počítače, připojeného ve stejné sítě, nejlépe spojeného napřímo se zapínaným počítačem. Existuje mnoho programů vytvořených pro funkci WOL v praktické části je popis programu „**Magic Packet Utility**“ od firmy AMD.

4.3.4 Router

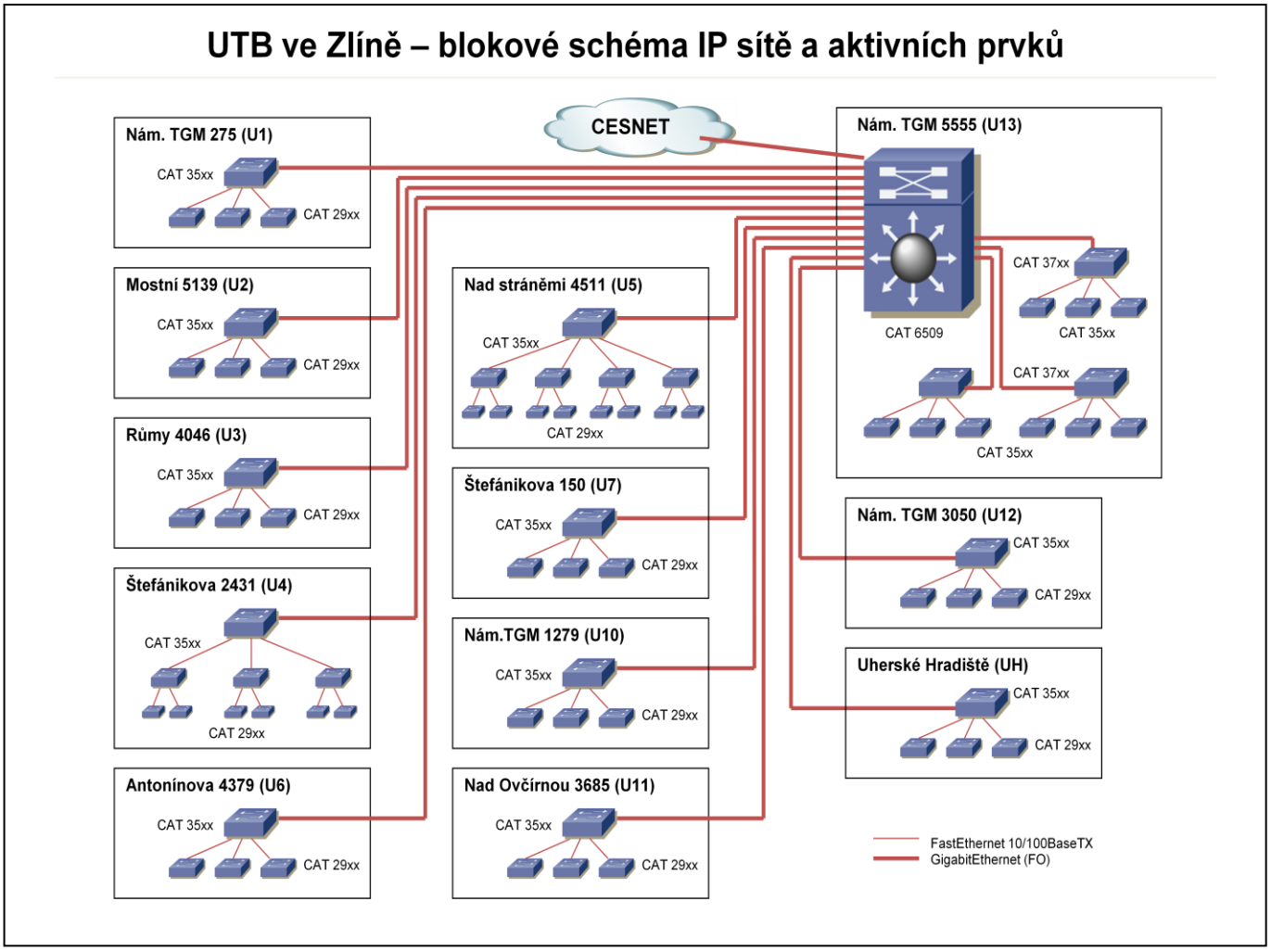
Pokud chce uživatel zapínat počítač z Internetu, a jestliže je zapínaný počítač připojen za routerem a nemá pevnou IP adresu, je potřeba router nastavit tak, aby příchozí Magic Packet (který přijde z internetu) přesměroval na síťovou kartu zapínaného počítače (naslouchá většinou na portu 9 nebo 7).

II. PRAKTICKÁ ČÁST

5 INFORMAČNÍ TECHNOLOGIE NA UTB

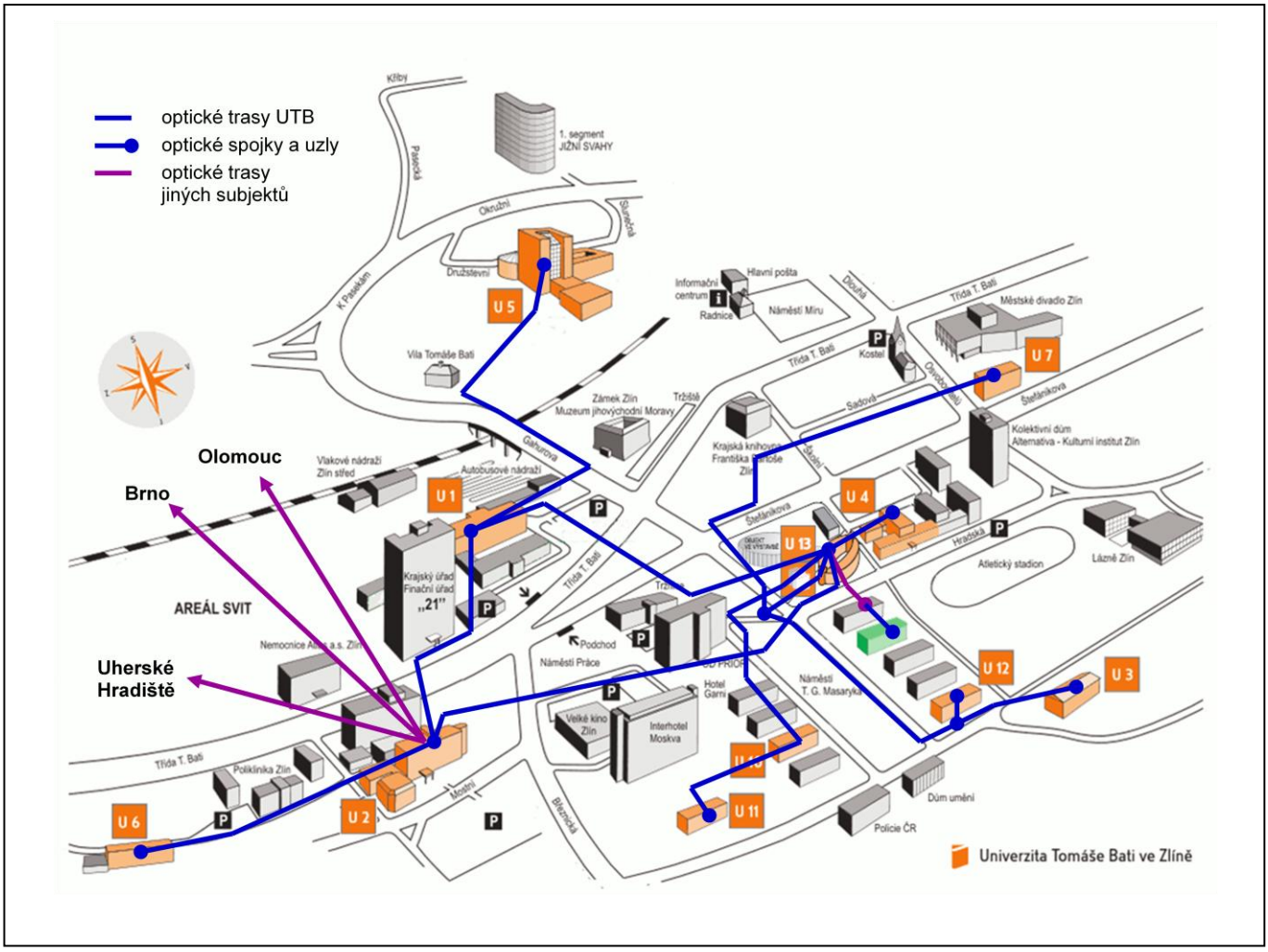
5.1 Páteřní síť UTB

Hlavní internetová páteřní konektivita z CESNETu vede na U13 do centrálního routeru Cisco Catalyst 6509. Odtud jsou připojeny pomocí páteřní optické sítě ostatní páteřní switche na dalších budovách UTB. V každé budově je umístěn centrální switch Cisco Catalyst řady 35xx, odkud vede konektivita do dalších tzv. workgroup switchů Cisco Catalyst řady 29xx.



Obrázek 5: UTB ve Zlíně - Blokové schéma IP sítě a aktivních prvků

Z budovy U13 vedou optické linky do ostatních budov UTB. Budovy U13, U2 a U1 jsou propojeny navzájem (v kruhu). Z budovy U2 vede optická linka do budovy U6 (kolej) a dále potom další páteřní linky směr Uherské Hradiště, Brno a Olomouc. Tyto meziměstské trasy nejsou majetkem UTB. Z budovy U1 vede páteřní spoj do budovy U5. Všechny ostatní páteřní spoje mezi budovami vedou z U13.



Obrázek 6: UTB ve Zlíně - Schéma optických obvodů

5.2 Systém Novell

Uživatelské účty pro přístup uživatelů do sítě UTB jsou spravovány na serverech Novell NetWare. Tyto servery slouží jako tzv. fileservery, uživatelé zde mají své domovské adresáře a jsou zde sdílené adresáře pro různé skupiny uživatelů. V současnosti jsou na UTB 3 servery Novell: **nw-central**, **nw-orion** a **nw-fame**. Uživatelé se k těmto serverům připojují prostřednictvím Novell klienta nainstalovaného na počítačích v učebnách, studovnách a dalších pracovištích.

Po připojení přes Novell client se uživatelům mapují pracovní síťové disky pod písmeny N:, O:, P: a domovský adresář Q:

Další možností je připojení přes FTP rozhraní.

5.3 Poštovní servery

V současnosti se pro správu elektronické na UTB pošty používají dva servery:

- SMTP.UTB.CZ
- IMAP.UTB.CZ

5.3.1 SMTP.UTB.CZ

Tento server přijímá a odesílá veškerou příchozí a odchozí poštu z a do internetu.

Příchozí pošta prochází antivirovým a antispamovým filtrem a následně je předána na další servery, kde jsou uloženy e-mailové schránky uživatelů.

5.3.2 IMAP.UTB.CZ

Na tomto serveru jsou uloženy e-mailové schránky všech uživatelů UTB. K e-mailovým schránkám je možný přístup prostřednictvím protokolu IMAP nebo POP3. Kromě těchto protokolů je možné použít webový klient webmail, což je vlastně ve skutečnosti webový IMAP klient.

5.4 WiFi

WiFi síť UTB je připojena do mezinárodní sítě eduroam, do které jsou připojeny všechny vysoké školy v ČR a velké množství vysokých škol v Evropě.

Přístupové body jsou rozmístěny ve všech budovách UTB, kde probíhá výuka. Signál je dostupný převážně ve větších prostorách s volným pohybem studentů, typu foyer, vestibuly, prostornější chodby, případně v některých posluchárnách apod. Studenti tak mají možnost v době mezi výukou využívat internetového připojení.

ZÁVĚR

Byly vypracovány podrobné návody pro připojení k Wi-Fi, pro e-mail, pro Wake On LAN a pro přihlášení do systému Novell a FTP připojení na Novell servery. Tyto návody jsou vytvořeny stylem „krok po kroku“ včetně názorných obrázků. Dohromady bylo vytvořeno 13 návodů, uložených ve formátu .PDF. Všechny návody mají dohromady 103 stran. V současné době jsou již k dispozici studentům a zaměstnancům UTB na webových stránkách Centra výpočetní techniky UTB na adrese „**http://cvt.utb.cz**“.

Do budoucna bude potřeba tyto návody aktualizovat pro nové operační systémy a programy. V červnu letošního roku vyšla nová verze kancelářského balíku MS Office 2010, na podzim by měl být aktualizován program MS Live Mail a příští rok by měl vyjít nástupce Windows 7. Bude tedy potřeba vytvořit další návody pro tyto novinky.

Návody poslouží hlavně novým studentům prvních ročníků, ale také stávajícím studentům, a usnadní jim přístup k informačním technologiím dostupným na UTB.

ZÁVĚR V ANGLIČTINĚ

Detailed instructions for joining the Wi-Fi net, e-mail, Wake On LAN system and joining the Novell system have been worked up. These manuals are created „step by step“, including supporting pictures. 13 instruction manuals were created here in PDF. Together, it is 103 pages. Currently, students and employees of UTB can use it, it‘s on their disposal on the Centre of Computer Technology‘s web page: „**http://cvt.utb.cz**“.

Into the future, manuals will be needed to update, depending up a new systems and programs. A new version of office suite „MS Office 2010“ came out in June this year, program MS Live Mail would have been upgraded in the autumn and next year the successor of Windows 7 would came out. It’ll be needed to create another instruction manuals for these news.

These instructions will be mainly used by first year students, but it can help other students too. These manuals will make Information Technology on UTB more accessible for everyone.

SEZNAM POUŽITÉ LITERATURY

[1] File Transfer Protocol. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 23. 9. 2004, last modified on 19.4.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/File_Transfer_Protocol>.

[2] Uživatel TOUCHWOOD, *Poradna.net* [online]. 30.09.2006 [cit. 2010-05-21]. Jak funguje FTP. Dostupné z WWW: <http://pc.poradna.net/a/view/307878-jak-funguje-ftp>.

[3] FTPS. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 3.12.2006, last modified on 17.3.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/FTPS>.

[4] SSH file transfer protocol. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 10.10.2007, last modified on 28.3.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/SSH_file_transfer_protocol>.

[5] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP : Bezpečnost*. Vydání první. Praha : Computer Press, 2001. 565 s. ISBN 80-7226-513-X.

[6] E-mail. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 23.9.2004, last modified on 18.4.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/E-mail>.

[7] E-mailov%C3%A1 adresa. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 22.12.2007, last modified on 28.4.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/E-mailov%C3%A1_adresa>.

[8] Univerzita Tomáše Bati ve Zlíně. *Webmail* [online]. 2010 [cit. 2010-05-21]. UTB Přihlásit. Dostupné z WWW: <https://webmail.utb.cz/src/login.php>.

[9] Simple Mail Transfer Protocol. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 23.9.2004, last modified on 4.5.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol>.

[10] PETERKA, Jiří. Aplikační protokoly TCP/IP. *CHIPweek* [online]. 5. května 1998 , 1998, 19/98, [cit. 2010-05-21]. Dostupný z WWW: <http://www.earchiv.cz/a98/a819k180.php3>.

[11] Post Office Protocol version 3. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 26.9.2005, last modified on 1.5.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Post_Office_Protocol_version_3>.

[12] Internet Message Access Protocol. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 26.9.2005, last modified on 20.4.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Internet_Message_Access_Protocol>.

[13] Secure Sockets Layer. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 14.2.2004, last modified on 26.6.2009 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Secure_Sockets_Layer>.

[15] Wi-Fi. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 9.1.2004, last modified on 13.4.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Wi-Fi>.

[16] IEEE 802.11. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 17.8.2006, last modified on 21.5.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/IEEE_802.11>.

[17] *Lupa.cz* [online]. 2007 [cit. 2010-05-21]. Začínáme s WiFi. Dostupné z WWW: <http://tutorialy.lupa.cz/jak-na-wifi/zaciname-s-wifi/>.

[18] Wired Equivalent Privacy. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 20.9.2006, last modified on 18.5.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy>.

[19] Wi-Fi Protected Access. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 23.9.2006, last modified on 25.2.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access>.

[20] RADIUS. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 30.8.2006, last modified on 11.4.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/RADIUS>.

[21] Eduroam. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 14.9.2008, last modified on 31.10.2009 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Eduroam>.

[22] Eduroam. *Eduroam* [online]. 2010 [cit. 2010-05-21]. What is eduroam?. Dostupné z WWW: <http://www.eduroam.org>.

[23] AARNet Pty Ltd. *AARNET* [online]. 2010 [cit. 2010-05-21]. Eduroam in Asia Pacific. Dostupné z WWW: <http://www.aarnet.edu.au/Content.aspx?p=137>.

[24] ING. TOMÁŠEK, Jan. *Csuzivatelfungovani_roamingu [eduroam_cz]* [online]. 24.09.2006 [cit. 2010-05-21]. Jednoduchý popis fungování roamingu a mobility pro uživatele. Dostupné z WWW: <http://www.eduroam.cz/doku.php?id=cs:uzivatel:fungovani_roamingu>.

[25] Wake on LAN. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 19.1.2007, last modified on 5.5.2010 [cit. 2010-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Wake_on_LAN>.

[26] BOUŠKA, Petr. *Wake on LAN - lokální i vzdálený subnet články - SAMURAJ-cz_com* [online]. 10.08.2008 [cit. 2010-05-21]. Wake on LAN - lokální i vzdálený subnet. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/wake-on-lan-lokalni-i-vzdaleny-subnet/>.

[27] *UTB Interní informace Informace CVT WiFi síť* [online]. 9. 11. 2006 [cit. 2010-05-26]. Žádost o registraci do WiFi sítě na UTB. Dostupné z WWW: <http://web.utb.cz/?id=0_8_13_0&iid=5⟨=cs&type=0>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	authentication, authorization and accounting - je autentizační, autorizační a účtovací protokol
AES	Advanced Encryption Standard – standard pro symetrickou blokovou šifru
AMD	Advanced Micro Devices - je přední světová společnost v oboru informačních technologií.
ASCII	American Standard Code for Information Interchange – je kódová tabulka, definující znaky anglické abecedy
BIOS	Basic Input-Output System - implementuje základní vstupně–výstupní funkce pro počítače IBM PC kompatibilní
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – je protokol založený na AES, který je považován za zcela bezpečný
CESNET	CESNET z. s. p. o. – sdružení vysokých škol
ČTÚ	Český telekomunikační úřad
DHCP	Dynamic Host Configuration Protocol - aplikační protokol z rodiny TCP/IP
DNS	Domain Name Systém - je hierarchický systém doménových jmen
DSSS	Direct Sequence Spread Spectrum - technika přímého rozprostřeného spektra. Je jednou z metod pro rozšíření spektra při bezdrátovém přenosu dat.
EAP	Extensible Authentication Protocol – je autentifikační protokol
eduroam	Education Roaming - počítačová infrastruktura pro transparentní používání sítí univerzit a jiných vzdělávacích institucí
FHSS	frequency hopping spread spektrum - je jedna z metod přenosu v rozprostřeném spektru. Její princip spočívá v přeskakování mezi několika frekvencemi při přenosu bitu nebo bitů.
FTP	File Transfer Protocol – protokol pro přenos souborů
FTPS	File Transfer Protocol Secure – FTP zabezpečené pomocí SSL nebo TLS
GNU	GNU's Not Unix - je projekt zaměřený na svobodný software
CHAP	Challenge Handshake Authentication Protocol - slouží k prokazování totožnosti
IBM	International Business Machines Corporation - je přední světová společnost v oboru informačních technologií.
IEEE	Institute of Electrical and Electronics Engineers (česky „Institut pro elektrotechnické a elektronické inženýrství“) je mezinárodní nezisková profesionální organizace usilující o vzestup technologie související s elektrotechnikou.
IMAP	Internet Message Access Protocol - protokol pro odesílání e-mailů
IP adresa	Internet Protocol adress – síťová adresa

KDE	K Desktop Environment – grafické prostředí OS linux
MAC	Media Access Control - je jedinečný identifikátor síťového zařízení
MAC OS	Macintosh Operating System – operační systém od firmy Macintosh
MIMO	Multiple-input multiple-output (MIMO), česky více vstupů více výstupů, je abstraktní matematický model pro multi-anténní komunikační systémy
MS	Microsoft
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol – je verze protokolu CHAP od firmy Microsoftu
NAT	Network Address Translation – překlad síťových adres
OFDM	Orthogonal Frequency Division Multiplexing, česky ortogonální multiplex s kmitočtovým dělením. Jedná se o přenosovou techniku pracující s tzv. rozprostřeným spektrem, kdy je signál vysílán na více nezávislých frekvencích, což zvyšuje odolnost vůči interferenci.
OS	Operační systém
PAP	Password Authentication Protocol - je jednoduchý ověřovací protokol
PC	Personal Computer – osobní počítač
PCI	Peripheral Component Interconnect - je počítačová sběrnice pro připojení periferií k základní desce
PCIe	PCI-Express - je počítačová sběrnice pro připojení periferií k základní desce
PDF	Portable Document Format - je souborový formát pro ukládání dokumentů
PEAP	Protected EAP
PGP	Pretty Good Privacy - je počítačový program, umožňující šifrování a podepisování
POP	Post Office Protocol - protokol pro odesílání e-mailů
PSK	Pre-Shared Key - je druh zabezpečení bezdrátových počítačových sítí
RADIUS	Remote Authentication Dial In User Service – je protokol, používaný pro přístup k síti nebo pro IP mobilitu
RFC	request for comments - řada standardů a dalších dokumentů popisujících Internetové protokoly
SFTP	Secure FTP - tunelování FTP skrz spojení navázaného pomocí SSH protokolu
SMTP	Simple Mail Transfer Protocol - protokol pro odesílání e-mailů
SOHO	Small Office, Home Office – segment domácností a malých kanceláří
SSID	Service Set Identifier - je jedinečný identifikátor bezdrátové počítačové sítě

SSL	Secure Sockets Layer - je kryptografický protokol, poskytující možnost zabezpečené komunikace na Internetu
TCP	Transmission Control Protocol - je jednen ze základních protokolů sady protokolů Internetu, konkrétně představuje transportní vrstvu.
TCP/IP	Transmission Control Protocol/Internet Protocol – je sada protokolů pro komunikaci v počítačové síti
TERENA	Trans-European Research and Education Networking Association – mezinárodní nezisková organizace
TKIP	Temporal Key Integrity Protocol - je protokol dynamicky měnící klíče
TLS	Transport Layer Security - je kryptografický protokol, poskytující možnost zabezpečené komunikace na Internetu
UDP	User Datagram Protocol - je jedním ze sady protokolů internetu
VNC	Virtual Network Computing
WEP	Wired Equivalent Privacy - je druh zabezpečení bezdrátových počítačových sítí
Wi-Fi	Wireless LAN - je standard pro lokální bezdrátové sítě
WOL	Wake on LAN – je technologie, umožňující zapnutí vypnutého počítače přes počítačovou síť.
WPA	Wi-Fi Protected Access - je druh zabezpečení bezdrátových počítačových sítí

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Návod 1 01 FTP.pdf

Návod 2 02 Novell.pdf

Návod 3 03 MS_Outlook_Express.pdf

Návod 4 04 MS_Win_Live_Mail.pdf

Návod 5 05 Mozilla_Thunderbird_3.pdf

Návod 6 06 MS_Office_Outlook_2007.pdf

Návod 7 07 Webmail.pdf

Návod 8 08 WiFi_Win_XP.pdf

Návod 9 09 WiFi_Win_Vista.pdf

Návod 10 10 WiFi_Win_7.pdf

Návod 11 11 WiFi_Linux_KDE.pdf

Návod 12 12 WiFi_Linux_příkazový_řádek.pdf

Návod 13 13 Wake_on_LAN.pdf

PŘÍLOHA P I: NÁZEV PŘÍLOHY