UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

VYUŽITÍ SÍTĚ INTERNET PRO PŘENOSY DATOVÝCH PAKETŮ V RÁMCI DÁLKOVÉ DIAGNOSTIKY TISKAŘSKÝCH STROJŮ

BAKALÁŘSKÁ PRÁCE

2007 **MILOŠ FALTA**

UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

VYUŽITÍ SÍTĚ INTERNET PRO PŘENOSY DATOVÝCH PAKETŮ V RÁMCI DÁLKOVÉ DIAGNOSTIKY TISKAŘSKÝCH STROJŮ

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Miloš Falta
VEDOUCÍ PRÁCE: Ing. Milan Maršík

2007

UNIVERSITY OF PARDUBICE
INSTITUTE OF ELECTRICAL ENGINEERING AND INFORMATICS

USING THE INTERNET FOR DATA PACKET TRANSMISSION WITHIN REMOTE PRINTING MACHINES DIAGNOSTICS

BACHELOR WORK

AUTHOR: Miloš Falta
SUPERVISOR Ing. Milan Maršík

2007

Vysokoškolský ústav: Ústav elektrotechniky a informatiky
Katedra/Ústav: Ústav elektrotechniky a informatiky
Akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pro: Falta Miloš

Studijní program: Informační technologie

Studijní obor: Informační technologie

Název tématu: Využití sítě Internet pro přenosy datových paketů v rámci dálkové diagnostiky tiskových strojů

Zásady pro zpracování:

Cílem bakalářské práce je prokázat schopnost posluchače analyzovat konkrétní problém v oblasti přenosu dat se zaměřením na dálkovou diagnostiku, problém teoreticky popsat a analyzovat, využít dostupné informace a odbornou literaturu a provést praktické ověření získaných poznatků. Práce bude vycházet ze studia konkrétního problému a odborné literatury.

Předpokládaný rozsah diplomové práce:

- popis fungování globální sítě Internet, způsoby propojení lokálních sítí se sítí Internet
- problematika přenosu TCP/IP paketů z prostředí lokální sítě na platformě Ethernet do globální sítě a zpět
- zprovoznění přenosu dat mezi dvěma uzly v různých lokálních sítích
- odzkoušení přenosu dat s PLC automatem B&R
- problematika zabezpečení propojených lokálních sítí
- související problémy nad rámec rozsahu diplomové práce

Seznam odborné literatury:

- HORÁK, J. *Hardware: učebnice pro pokročilé.* Praha: Computer Press, 2000. ISBN 80-7226-553-9.
- HORÁK, J. a KEŠLÁGER, M. *Počítačové sítě pro začínající správce: funkce sítí a síťových zařízení, konfigurace, účty, protokoly, tisk v sítích, přístup k datům, archivace, Windows, Netware, Linux.* Brno: Computer Press, 2003. ISBN 80-7226-876-7.

Rozsah: 30 - 50 stran včetně potřebných příloh

Vedoucí práce: KBA - Grafitec Dobruška

Vedoucí katedry (ústavu): prof. Ing. Pavel Bezoušek, CSc.

Datum zadání práce: 30.11.2006

Termín odevzdání práce: 3.9.2007

Prohlašuji

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 29. 8. 2007 Miloš Falta

(vlastnoruční podpis)

Poděkování

Rád bych poděkoval vedoucímu bakalářské práce Ing. Milanovi Maršíkovi a Ing. Jiřímu Kápičkovi za odborné vedení a cenné rady při zpracování bakalářské práce.

Poděkování patří také mým rodičům, kteří mi umožnili studovat tuto školu a všem, kteří mě podporovali během studia.

ABSTRAKT

Tato práce se zabývá problematikou přenosu dat pro dálkové diagnostiky tiskových strojů Performa 66/74.

Práce charakterizuje problémy s přenosem datových paketů mezi dvěma LAN sítěmi spojenými přes Internet. Je navrženo několik řešení, cílem práce je tyto možnosti popsat a zhodnotit, zda jsou použitelné pro řešení stanoveného problému. Důrazy jsou kladeny na co nejvyšší zabezpečení lokálních sítí a současně s tím minimální nároky na potřebnou rekonstrukci sítě. Na základě svých znalostí a zkušeností jsem navrhl vlastní řešení, které podle mě nejlépe vyhovuje všem stanoveným cílům a nárokům.

Obsah

1 Úvod

Světová síť Internet skýtá mnohé možnosti. Rozšířením vysokorychlostních linek se rozvíjí i možnosti vzdálené komunikace a diagnostiky strojů. Pro jejich provoz se hledá takové spojení, které v sobě komponuje maximální využití přenosových kapacit, minimálních nákladů na realizaci a samozřejmě zabezpečení před zneužitím této komunikace třetí stranou.

Tato práce má za cíl shromáždit teoretická data pro případnou realizaci propojení tiskového stroje s počítačem ve vzdálené lokální síti. Úkolem je na základě požadavků společnosti KBA – Grafitec navrhnout propojení mezi počítači ve firemní síti s tiskovými stroji propojenými k síti Internet. Práce má následující strukturu. V úvodní části práce popisuji historii a připojení k Internetu. Jako další následuje přiblížení protokolů TCP/IP.

Dále jsou popsány jednotlivé možnosti připojení tiskového stroje. Ke každé možnosti jsem uvedl své vyjádření k aspektům, které byly sledovány. Závěr shrnuje dosažené výsledky a nabízí možnost dalšího rozšíření. Práce končí seznamem použité literatury a seznamem obrázků.

2 Analýza zadání

2.1.1 Možnosti tiskového stroje

Tiskový stroj Performa je offsetový tiskový stroj (obrázek 1), který se vyrábí ve dvou až šestibarevném provedení pro formát 52x74 cm. Stroj umožňuje tisk až 13 000 archů za hodinu, nezávislé nastavení zón tisku. Každá barva má 23 těchto zón, ty lze ovládat z řídícího počítače na vykladači stroje, nebo dálkově z pultu GrafiControl.

Obrázek 1 - Performa 74

Počítač je tvořen PLC Automatem B&R s dotykovým displejem (obrázek 2). Umožňuje běžná nastavení stroje od celkových otáček stroje po nastavení otáček jednotlivých ventilátorů na vykladači pro nastavení optimálního přítlaku papíru.

Obrázek 2 - Ovládací jednotka

Tiskový stroj neumožňuje tisk dokumentů jako klasická tiskárna připojená k počítači nebo do počítačové sítě. Tiskový stroj funguje na principu obtisku dané barvy na papír tak rychle, aby se jednotlivé barvy stačily slít a vytvořit tak požadovaný odstín. Co a jakou barvou se má obarvit, určuje formátový válec, na který se upevní výměnná deska.

2.1.2 Fyzická rozhraní

Pro potřeby dálkové diagnostiky jsou k dispozici dva druhy rozhraní, sériové RS232 a Ethernet.

Sériové rozhraní slouží k lokálnímu připojení počítače pomocí sériové linky k automatům nebo k připojení vzdáleného počítače přes modem za použití telefonní linky. Při lokálním připojení je komunikační rychlost 57 600 b/s, při použití analogového modemu se jedná o typickou rychlost 28 800 b/s. Dále je možné připojení GSM modemu s technologií CSD, ale zde se dosahovalo rychlosti maximálně 9600 b/s.

V případě použití modemů pro dálkovou diagnostiku se projevuje vliv poruch na přenosové trase a tím dochází k častějšímu opakování přenášených dat a snížení reálné přenosové rychlosti.

Rozhraní Ethernet slouží k připojení blízkého počítače k automatu buď přímým spojením přes ethernetový kabel, nebo spojením přes lokální počítačovou síť. V praxi toto připojení používají programátoři k nahrávání nebo ladění řídícího software přímo u stroje. Do budoucna se pro potřeby dálkové diagnostiky předpokládá použití sítě Internet ke spojení vzdáleného počítače s automaty tiskového stroje. Toto řešení je předmětem bakalářské práce „Využití sítě Internet pro přenosy datových paketů v rámci dálkové diagnostiky tiskových strojů.“

2.1.3 Softwareové prostředky

Na základě licenční smlouvy poskytuje firma B&R softwarové aplikace Automation Studio a PVI Transfer. Tyto aplikace jsou určeny především vývojářům software, servisní pracovníci je využívají jen vyjímečně.

Pro potřeby servisu je vytvářena vlastní aplikace, která není vázána licenční smlouvou s firmou B&R a zohledňuje požadavky servisních pracovníků.

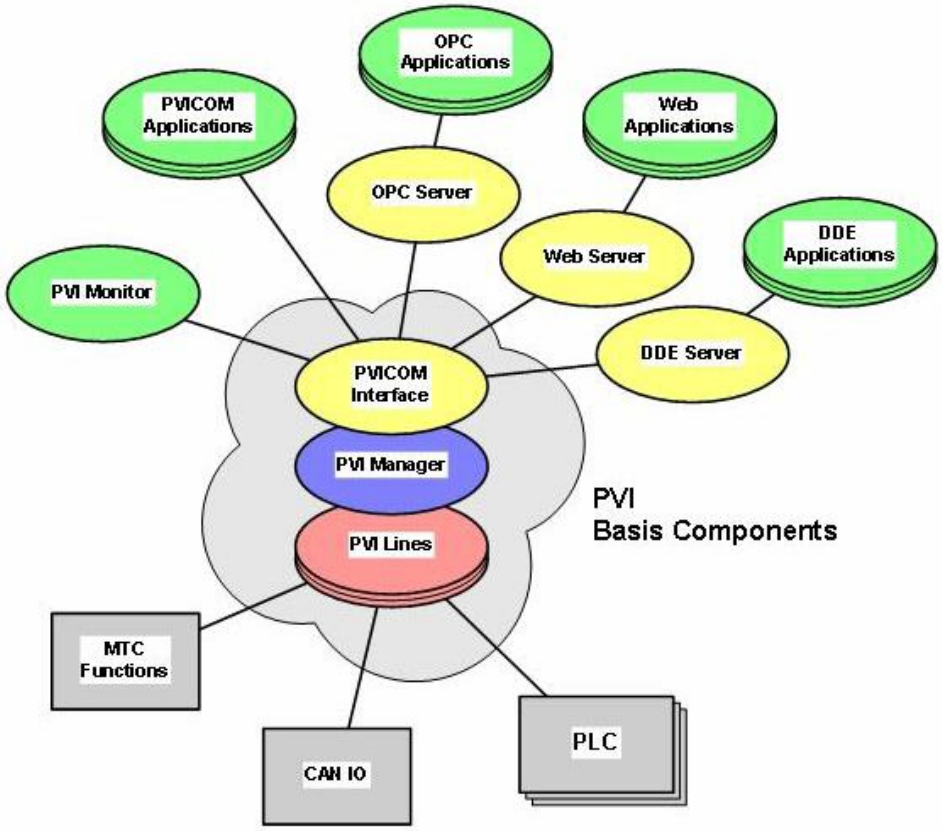
Centrálním prostředkem komunikace s PLC systémy B&R je PVI (Process Visualisation Interface) base systém (obrázky 3,4). Hlavní části PVI base system tvoří PVI Manager, PVI Monitor, PVICOM Interface a PVI lines.

PVI Manager je ústřední částí PVI. Zodpovídá za řízení všech přenosů dat od přenosů jednoduchých proměnných po seznamy programových či datových objektů. PVI Manager organizuje přenosy dat se zřetelem jak na časování, tak i na jejich určení.

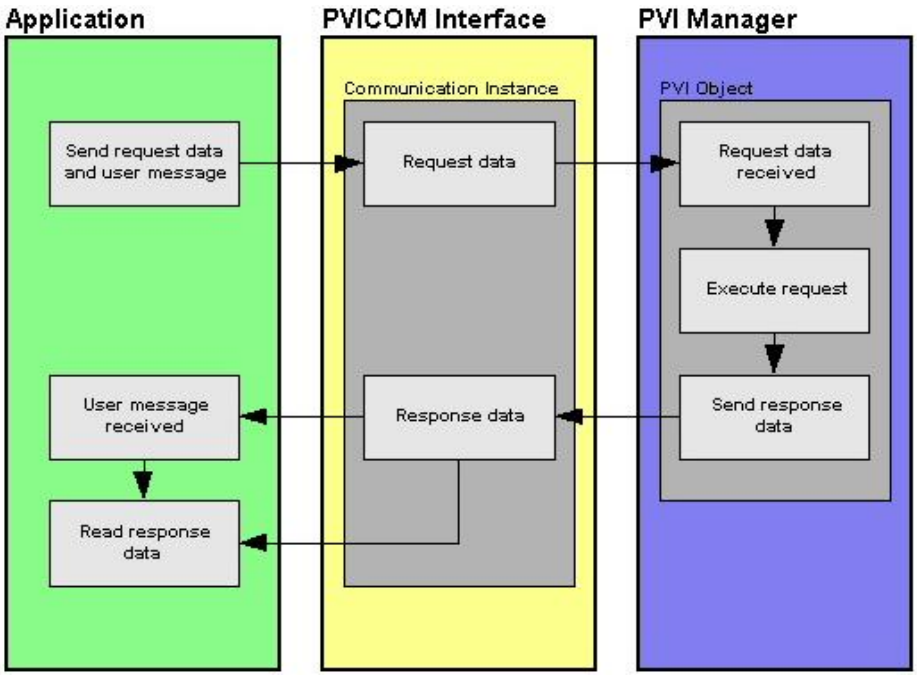
PVI Monitor je pomocný nástroj pro zobrazení stavu operací, verzí PVI částí a operačních systémů PLC.

PVICOM Interface (client interface) zajišťuje přístup k PVI na nejnižší úrovni. Reprezentuje nejtěsnější a z hlediska výkonnosti nejoptimálnější PVI interface.

Základní úloha PVI line je propojení PVI objektů s objekty vně PVI. PVI line je také odpovědný za komunikaci s B&R řídícími obvody.



Obrázek 3 - Přehled o nejdůležitějších PVI částech



Obrázek 4 - Sekvence spolupráce aplikace s PVI Managerem prostřednictvím PVICOM Interface

2.1.4 Využití sítě Internet pro přenosy datových paketů v rámci dálkové diagnostiky tiskových strojů.

Dálková diagnostika tiskových strojů funguje tak, že položím dotaz automatu tiskového stroje, ten dotaz zpracuje a následně odešle odpověď. To zabezpečuje balík RPC, který zavolá na PLC Automatu B&R příslušnou proceduru, která vrátí odpověď.

Přenos datových paketů by neměl být problém, jelikož tiskový stroj komunikuje pomocí dvou portů FTP nebo RPC. Protože oba jsou v balíku protokolů TCP/IP, stačí odzkoušet komunikaci pomocí příkazu ping, který využívá protokolu IP a jeho ICMP zpráv. Díky tomu máme zajištěnou komunikaci mezi tiskovým strojem a počítačem určeným pro diagnostiku.

Využití sítě Internet umožní přechod paketů TCP/IP. Pakety posílány jen po firemní lokální síti, ale mohou se šířit po Internetu. Tato komunikace by měla být šifrovaná, jelikož se budeme pohybovat v cizím prostředí, myšleno v prostředí, kde kdokoli na komunikační cestě může naši komunikaci monitorovat.

3 Historie Internetu

3.1 Co je to vlastně Internet?

Internet je počítačová „supersíť“, ve které jsou počítače vzájemně propojeny a za pomoci toho spolu mohou komunikovat, předávat si informace nebo je dokonce sdílet a poskytovat. Každý počítač může komunikovat s libovolným jiným počítačem zapojeným do stejné sítě.

Internet je spojení sítí, které mají určitou strukturu a vnitřní rozdělení. Tím je umožněna komunikace mezi jednotlivými počítači zapojenými do sítě Internet, které jsou trvale propojeny datovými spoji s možností průchodu velkého objemu dat.

Internet je síť typu WAN (Wide Area Network), je tvořená propojením lokálních sítí LAN (Local Area Network) po celém světě. Sítě pracují na stejném základě, kterým je sada protokolů TCP/IP (Transmision Control Protocol / Internet Protocol), ta je v současné době nejpoužívanější sadou protokolů, uznanou jako norma.

3.1.1 Jak požadované informace získáme?

Internet je skupina počítačů obsahující informace, jež nám dovolují k nim pomocí sítě přistupovat. Tyto počítače jsou zdrojem informací, které jsou dostupné uživatelům. Počítače na Internetu pracují ve dvou stavech. Jako klienti a zároveň také jako servery. Servery poskytují své internetové služby, klienti pak služby daného serveru využívají.

Službami Internetu je zasílání dat ze serveru klientovi na jeho žádost. Většinou jsou to data, která jsou umístěna na pevném disku serveru jako třeba WWW stránky, které jsou za chodu na serveru dynamicky vytvořeny a odeslány klientovi jako třeba počet aktuálně přihlášených uživatelů.

Internet nabízí spoustu adres obsahujících materiály od osobních stránek, firemních prezentací, obrazových galerií, přes specializované informační stránky až po literární tvorbu.

3.1.2 Jak Internet funguje?

Internet funguje pomocí přenášení souborů. Způsob jejich uveřejňování nebo poskytování jednotlivým uživatelům je umožněn využitím jednotlivých služeb. Výměna dat mezi serverem a klientem je ve skutečnosti zajišťována pomocí určitého množství dalších počítačů, které jsou mezi koncovými počítači.

Většina služeb poskytovaných serverem má pasivní charakter, jenž v praxi znamená, že zařízení zajišťující určitou službu čeká na konkrétní

požadavky od klienta a na jejich základě potom zašlou danému klientovi soubory s požadovanými informacemi.

3.2 Komunikace mezi uzly, přenos dat

3.3 Specifická IP adresa

Počítače připojené k síti Internet mezi sebou komunikují pomocí protokolů TCP/IP. Pro veškerou komunikaci počítačů mezi sebou byla zavedena jednotná adresace počítačů, pomocí tzv. IP adres. Tato adresa se skládá ze čtyř dekadických čísel vzájemně oddělených tečkou (např.: 192.168.0.32), a proto se stává každý počítač jedinečným pro svou síť.

Protože snadnější a zapamatovatelnější je používat jména než čísla, byl v roce 1984 zaveden systém pojmenování počítačů tzv. DNS (Domain Name System), který umožňuje převod IP adresy na symbolické jméno a zpět.

3.3.1 Dělení na pakety

Jedním z počítačů je klient neboli uživatelský počítač, druhým je server, na kterém jsou přístupné požadované informace. Pro propojení těchto dvou počítačů může existovat více tras. Jejich počet se dynamicky mění dle vytíženosti a průchodnosti jednotlivých sítí.

Kvůli častým změnám v datové síti jsou před odesláním informace rozděleny na tzv. pakety. Každý paket je po síti přenášen samostatně, nezávisle na ostatních. Routery nebo další síťové prvky, které jsou mezi koncovými počítači, rozhodují, kterou cestou jsou jednotlivé pakety posílány.

Pro rychlejší přenos dat existuje vzájemné propojení většiny českých poskytovatelů Internetu nazvané PEERING. Toto propojení zajistí, že v případě požadování dat od serveru, který se nachází v síti těchto po-

skytovatelů, bude přenosová rychlost podstatně větší, protože paketům bude znemožněno putování mimo Českou republiku.

3.4 Myšlenka vzniku Internetu

Nutnost dokonalejšího spojení se projevila v době studené války, kdy Spojené státy americké potřebovaly fungující systém pro zajištění řízení a velení, který by dokázal udržet spojení mezi akademickými, vládními a strategickými počítači (města, státy, vojenské základny atd.). Nejdůležitějším požadavkem bylo vytvoření odolné sítě, která zajistí spojení mezi nepoškozenými uzly při absenci některých uzlů.

Dosavadní komunikace byla pouze centralizována. Centrální uzel zajišťoval veškerou komunikaci s okolím. K rozpadu celé sítě stačilo vyřadit pouze řídící uzel.

Na počátku 60. let dostala firma RAND Corporation zakázku jak vyřešit problém, aby mohly počítače i po jaderné válce spolehlivě komunikovat. RAND Corporation přišla v roce 1964 s řešením založeným na dvou principech:

1. Síť neobsahuje centrální složku
2. Síť bude fungovat, i když budou některé její části vyřazeny

3.5 Vývoj Internetu

3.5.1 Zcela na počátku

Firma RAND Corporation navrhla síť, ve které všechny její uzly měly rovnocenné postavení. Firma počítala s tím, že přenosy mezi jednotlivými uzly nemusejí být spolehlivé. V roce 1961 se zrodila myšlenka, že přenášená data budou rozdělena na části, které se budou přenášet jako samostatné celky (pakety).

Každá taková část bude opatřena adresou svého příjemce. Každý paket má cestu zvolenou nezávisle na ostatních, s ohledem na vytíženost sítě. Různé pakety se mohou po síti ubírat různými cestami. To z důvodu, kdyby jedna z možných cest byla náhle zničena, další pakety se automaticky přenesou jinou cestou. Tato metoda je ve studijních materiálech označována jako přeposílání paketů.

3.5.2 Stručný přehled vývoje

Ministerstvo obrany USA začalo pracovat v roce 1968 na vzniku sítě ARPANET a také ji financovalo. V roce 1983 se od původní sítě oddělily všechny uzly spojené s vojenstvím a vytvořily tak samostatnou síť MILNET. Avšak i tato síť byla schopná komunikovat s původním ARPANETem.

ARPANET tím získal mnohem citlivější náplň práce, ale stále byl financován ministerstvem obrany Spojených států amerických. I další ministerstva financovala budování svých sítí založených na protokolu TCP/IP vzhledem k jeho kvalitám protokolu. Po roce 1983 se TCP/IP stal nejznámějším a nejpopulárnějším protokolem pro sítě LAN. Dochází tak k hromadnému rozvoji lokálních sítí s protokoly TCP/IP, které umožňovaly připojení k rozšiřující se soustavě vzájemně propojených sítí na bázi stejných protokolů.

Původní ARPANET se stal páteřní sítí, která zabezpečovala komunikaci mezi klienty a servery. Připojováním dalších a dalších sítí vzniká směs vzájemně propojených sítí, která se nazývá Internetem.

3.6 Nultá fáze

V dobách studené války měly Spojené státy americké požadavek vytvořit odolnou síť spojující instituce vlády, takovou síť, která bude funkční i po výpadku některých uzlů a bude tak zajištěna komunikace mezi neporušenými uzly.

Vojenští plánovači přemýšleli, jak zajistit komunikaci mezi vládními složkami v případě, že by mělo dojít k jadrné válce. Během 60. let organizace RAND připravila koncepce decentralizované odolné paketově orientované sítě.

Kolem roku 1968 byl v USA vyvinut samostatný zárodek Internetu. Ministerské úřady obrany USA, resp. grantová agentura ARPA (Advanced Research Project Agency), začala vyvíjet síť ARPANET a právě ta řídila jeho vývoj i financování.

3.7 První fáze

Národní fyzikální laboratoří ve Velké Británii byla vyvinuta síť postavená na těchto principech a díky tomuto nápadu se ARPA rozhodla vyvíjet podobný projekt. A právě podle této agentury dostala síť svůj název ARPANET. Samostatná agentura ARPA se poté přejmenovala na DARPA (Defense Advanced Research Project Agency).

3.7.1 Připojení prvních uzlů

V průběhu první fáze měla síť na dálku umožnit přístup k tehdejším nejvýkonnějším superpočítačům nejvýznamnějších univerzit v USA. První uzly sítě byly nainstalovány na podzim roku 1969 na univerzitách – UCLA (University of California Los Angeles), UCSB (University of California Santa Barbara), SRI (Stanford Research Institute) a na univerzitě v Utahu.

Vlastní uzel byl realizován univerzitním počítačem Honeywell DDP516, který byl naprogramován tak, aby pracoval jako tzv. Interface Message Procesor (IMP). Pro vzájemnou komunikaci se používaly uzly IMP, pevné disky, okruhy, které mají přenosovou rychlost 50 kbps a které používají přenosový protokol NCP (Network Control Protocol).

Roku 1969 napsal Steven Rocker první materiál RFC (Request For Comment) řešící témata spjatá s problematikou sítí, které využívají uzlové počítače a jejich programové vybavení. Časem se ukázalo, že tento postup není vždy tím nejlepším. Existují totiž takové aplikace, kterým nevadí ani případná ztráta 20% dat, špatně získaná data se zahazují, protože následně získaná bezchybná data stejně nemohou použít. Tento protokol je nazývám UDP a používá se hlavně u přenosu hlasu, který upřednostňoval rychlost přenosu před kvalitou dat.

3.7.2 Rozvoj počítačových sítí

Lidé používající Internet nechtěli mít připojeno pouze několik vybraných počítačů, ale celou místní síť, tedy veškeré počítače v organizaci. A tak se v nejrůznějších firmách a na univerzitách staly velice dostupnou záležitostí lokální počítačové sítě.

V 70. letech a na počátku 80. let se ARPANET stále rozvíjel, oblast počítačových sítí a Internetu se stále rozšiřovala. Díky tomuto prvotnímu impulzu začaly vznikat další nové sítě (jako Usenet a Bitnet). A tak se k této síti začaly postupně připojovat i další organizace. Díky kvalitám a přístupnosti protokolů TCP/IP byly tyto sítě stále častěji budovány právě na jejich základě.

Výhoda byla na obou stranách. Jak pro uživatele, tak pro provozovatele bylo jednoznačně výhodné a žádoucí se s ARPANETem propojit. ARPANET využívá paketového přenosu. pakety jsou přesměrovány do cílových sítí, ve kterých si je přebírají adresované počítače a tak se na všechny sítě pohlíží jako na sobě rovné.

Propojování sítí zajišťují:

1. počítače se speciálním vybavením
2. směrovač (router)
3. brána (getaway)

3.7.3 Rozvoj dalších počítačových sítí

1. 1970 – ALOHANET, bylo objeveno využití způsobů přepínání paketů a také bezdrátového připojení
2. 1979 – USENET
3. 1986 – NSFNET (National Science Foundation Network)

ARPANET se rychle rozšiřuje, první zahraniční uzly se připojují ve Velké Británii a v Norsku, přesně tedy roku 1973.

3.7.4 Tabulka připojených uzlů k ARPANETU

Tabulka 1 - Počet připojených uzlů

rok	počet uzlů	rok	Počet uzlů
1969	4	1991	500 000
1971	15	1992	více než 1 000 000
1972	37	1994	3 000 000
1984	1 000	1996	15 000 000
1986	5 000	1999	50 000 000
1987	více než 10 000	2001	100 000 000
1989	100 000	2002	150 000 000

3.7.5 Rozvoj síťových služeb

V 70. letech dochází k velkému rozvoji síťových služeb, především se naskýtá možnost pracovat na vzdálených počítačích (prostřednictvím tzv. vzdáleného přihlašování, remote login). 1. 10. 1969 byla po síti mezi počítačem ve SRI a UCLA poslána první zpráva.

V červenci 1972 byl vymyšlen program umožňující posílání zpráv a vzniká elektronická pošta, ve které byl poprvé použit znak „@“. Uživa-

telé začali využívat přenosové možnosti elektronické pošty pro diskuze v rámci elektronických konferencí.

Nedlouho poté byl objeven „mailing-list“. Jde o ARPANETovou komunikační metodu pro automatické rozesílání identické zprávy velkému počtu uživatelů. Více adresátů znamenalo větší objemy dat a tím nastala nutnost realizovat lepší možnosti připojení.

1. 1971 vynalezen mail
2. 1972 telnet
3. 1974 specifikován TCP, v roce 1978 rozdělen na TCP/IP
4. 1983 vynalezeno pojmenování serverů DNS
5. 1984 start DNS, NCP/TCP

3.7.6 ARPANET páteřní sítí

V 80. letech se ARPANET stal páteřní sítí. Pentagon se v roce 1980 rozhodl, že preferovaným protokolem pro ministerstvo obrany bude TCP/IP.

V roce 1982 musely všechny počítače přejít na tento protokol, pokud si chtěly udržet spojení s ARPANETem, protože od začátku roku 1983 přestala být síť ARPANET průchozí pro protokol NCP.

TCP/IP se stává nejpoužívanějším protokolem pro lokální sítě, které se dále připojovaly na ARPANET. Díky propojení těchto sítí se ARPANET stal zárodečnou sítí. Vzájemné propojení těchto sítí se označilo jako Internet.

3.8 Druhá fáze Internetu

V roce 1983 bylo připojeno k Internetu několik tisícovek počítačů, do roku 1992 jich bylo už víc než milion, hlavně díky rozšíření i mimo americký kontinent a napojením dalších velkých sítí jako NSFNET,

EUNET (European Unix Network), EARN (European Academic and Research Network), japonské sítě JUNET (Japan Unix Network) a britské JANET (Join Academic Network).

3.8.1 DNS

Proč přidělovat jména? Pro člověka je jednodušší pamatovat si název, slovo než čtveřici čísel. Ale důvod byl ještě jeden, a to geografické umístění serveru.

DNS je systém hierarchického řazení jednotlivých doménových jmen. Pro fungování systému je používán protokol DNS, který vzájemně převádí IP adresu na doménové jméno a zpět. Protokol využívá pro svou funkci port 53 jak s protokolem TCP také i s UDP. Hierarchie DNS je shodná s hierarchií sítě. DNS server České republiky má DNS jméno „cz“, ten má dále právo přidělovat jména v rámci republiky.

Společnost O2 dostala jméno „o2“ od nadřazeného serveru. Jako příklad zadám do vyhledávače adresu www.cz.o2.com vyhledávač vyšle dotaz na kořenový name server, který mu zašle IP adresu serveru s názvem „com“, jeho se dotazuje na adresu serveru s názvem „o2“, jeho zase na adresu serveru „cz“ a mám IP adresu požadovaného serveru, ovšem neplést si server „cz“ pod doménou „o2“ se serverem „cz“ přímo podřízenému kořenovému serveru.

Zde je zřetelně vidět hierarchická struktura, kterou si můžeme přiblížit i takto:

1. com
    a. o2
        1. cz
        2. de
        3. sk
    b. google
    c. dalas

2. org
3. cz
    a. o2
    b. seznam
    c. atlas

Zde je vidět, že doménové jméno nemusí být celosvětově unikátní, ale musí být unikátní v rámci své nadřazené domény. V implementaci se však jako prvního nedotazujeme kořenového name serveru, ale nejbližšího nadřazeného a pokud ten neví, ptá se zase svého nadřazeného.

3.8.2 Použití TCP/IP

K velkému rozmachu protokolů TCP/IP došlo v letech 1983 a 1986. Největší zásluhu na tom měla politika agentury DARPA, který nechala vyvinout implementaci TCP/IP do Unixu prostřednictvím firmy BSD (Berkeley Software Distribution) a jejich BSD Unixu.

V této době se vysokoškolská střediska vybavovala systémem BSD Unix a tím se protokoly TCP/IP rychle rozšířily po celých Spojených státech amerických. Za pomocí IP-adres jsou automaticky vybudovány první vrcholné domény.

3.8.3 Ukončení činnosti ARPANETu

Systém ARPANET skončil v březnu roku 1990 a páteřní sítí Internetu se tak stala NSFNET.

3.8.4 WWW

V roce 1989 byl vynalezen WWW (World Wide Web). Zkratka WWW představuje soustavu propojených hypertextových dokumentů, z toho český překlad zní „celosvětová pavučina“.

Roku 1991 byl na minnesotské univerzitě představen vyhledávací systém Gopher, to byl jeden z posledních kroků k rozmachu služby WWW. Tato služba se tak stala nedílnou součástí Internetu a tím se tento systém přiblížil dnešní podobě Internetu. Univerzita v Nevadě poté uvedla jeho nástupce systém Veronica.

3.9 Připojení ČR k Internetu

Internet byl do roku 1993 doménou vědeckých nebo vysokoškolských pracovišť, i když zde fungoval od roku 1991. Současní uživatelé se bránili příchodu komerčních aktivit na Internet. Po roce 1993 se k síti dostaly komerční organizace i firmy ze všech možných odvětví lidské činnosti.

3.9.1 Internet u nás

Až roku 1989 byly v listopadových dnech odstraněny politické bariéry, které bránily připojení do celosvětové sítě. Byly zde ale problémy technologického charakteru, jelikož naše komunikační infrastruktura nebyla připravena na větší rozvoj.

První sítě měly nízké požadavky a vystačily s vytáčeným spojením po veřejné telefonní sítí. Síť FIDO se sem dostává v březnu 1990 a dva měsíce nato i síť EUNET propojující převážně unixové počítače.

3.9.2 EARN

Evropská část sítě Bitnet se do Československa dostává v roce 1990 jako síť EARN. Jelikož síť EARN poskytovala pouze elektronickou poštu a přenos souborů, vystačila tak i s pomalými pevnými okruhy.

Prvním uzlem této sítě u nás se stal počítač IBM 4381 v Oblastním výpočetním středisku Českého vysokého učení technického v Praze (dále pod novějším názvem VC ČVUT), který byl naším prvním národním uz-

lem sítě EARN. Ten měl spojení s Lincem linkou o rychlosti 9600 bps. Plánem bylo vybudovat páteřní síť přes celé Československo, která by poskytovala spojení všech tuzemských vysokých škol s Internetem. Na tuto síť by se pak napojovaly sítě MAN (Metropolitan Area Network), které se svou rychlostí přibližují spíše síti LAN.

Československé federální orgány se k myšlence stavěly negativně, a proto plány o vybudování těchto páteřních sítí poskytly oběma ministerstvům školství. Nutné propojení Brna a Bratislavy bylo začleněno do českého projektu a uskutečnilo se za podpory Slovenska. Návrh do parlamentu byl dán v prosinci 1991, v červnu byl projekt schválen, na jeho uskutečnění se uvolněno 20 milionů korun a budování páteřní sítě bylo započato.

3.9.3 CESNET

Pro připojení na Internet se nejčastěji používala síť CESNET (Czech Education and Scientific Network). U nás to byl projekt FERNET (Federal Education and Research Network), který se musel přejmenovat na FESNET (Federal Education and Scientific Network). Roku 1992 se z FESNETu stal CESNET.

CESNET realizoval připojení vysokoškolských středisek, připojení celých měst však měly za úkol projekty na vybudování metropolitních sítí. První univerzity se k evropskému Internetu připojily v listopadu roku 1991 a od této doby se datuje historie Internetu v České republice, tenkrát ještě v Československé republice. Jednalo se o vytáčené spojení mezi Výpočetním centrem ČVUT a Lincem. Formálně bylo Československo k síti Internet připojeno 13. února 1992.

3.10 Topologie Internetu

3.10.1 Topologické změny v CESNETu

Uvnitř struktury CESNETu dochází postupem času k výrazným změnám. Všechny významnější uzly by měly být připojeny minimálně dvěma nezávislými přípojkami.

Tato struktura umožňuje rovnoměrně využívat všechny části CESNETu a zachovávat rychlost připojení i při výpadku některých částí sítě.

Ke změnám rychlosti připojení dochází i na spojích se zahraničím kde se původní přípojka do Lince přepojila na Vídeň a přibyla přípojka i do Amsterdamu s rychlostí přenosu 64 kbps, který byla díky konferenci INET´94/JENZ zvýšena na 512 kbps.

Po rozpadu Československa na Česko a Slovensko byla ještě vybudována přípojka z Brna do Banské Bystřice.

3.10.2 Struktura sítě

Pro českou CESNETovskou páteřní síť byla zvolena hvězdicová struktura se dvěma hlavními uzly Prahou a Brnem. V listopadu 1992 byly navzájem propojeny linkou 64 kbps. Začátkem roku 1993 se připojil Liberec, Hradec Králové, Pardubice a další vysokoškolská města. Na konci roku byl CESNET rozšířen již v 11 městech. Tyto spoje začínaly na rychlosti 19,2 kbps, brzy tato rychlost nevyhovovala, a tak byly spoje vylepšeny.

3.10.3 Komerční služby Internetu

Roku 1995 se Internet rozšířil i mezi veřejnost. CESNET nebyl jen jako pomyslný tunel, ale jako páteřní síť, která umožňuje připojení i ji-

ným uživatelům. Český telekomunikační úřad udělil povolení poskytovateli CESNETu k poskytování Internetu.

Následný vývoj se dal předpokládat, jedná se o zvýšení rychlosti, vyšší spolehlivost a optimalizaci. V roce 1999 prošel český Internet další výraznou změnou, a to digitalizací telefonní sítě. Díky tomuto kroku mohli poskytovatelé připojení zlevnit tarify pro připojení.

Větší rozvoj Internetu pak způsobilo i to, že klesly ceny za pořízení osobních počítačů a na trh služeb přišli i konkurenční poskytovatelé internetového připojení.

3.10.4 Způsoby připojení k síti Internet

1. Vytáčené spojení po telefonní lince – dříve nejrozšířenější připojení k Internetu. Jednalo se o vytočení spojení ke svému poskytovateli Internetového připojení (ISP), kde se místo zvuku přenášela data. Rychlost přenosu záležela na rychlosti modemu, nejčastěji to byl 56kbps. Tento typ připojení se nazývá PPP (Point-To-Point Protocol).
2. ISDN (Integrated Services Digital Network) – jedná se o pokročilejší technologii, která využívá dva komunikační kanály. Jeden pro přenos hlasu a druhý pro datový přenos. Oba kanály mají přenosovou rychlost 64kb/s. Pro stahování je možné využít i přepnutí první linky pro datový přenos, tím se rychlost zdvojnásobí. Toto připojení je výrazně dražší, ale spolehlivější než vytáčené spojní.
3. ADSL (Asymetric Digital Subscriber Line) – rychlost tohoto připojení je asymetrická, což znamená, že pro stahování má vyšší rychlost než pro odesílání dat. Ze současné nabídky je tu rychlost 2048 kb/s pro stahování a 128 kb/s pro odesílání dat.

4. Pevná linka – Speciální datová linka pro ty, kteří potřebují být nepřetržitě připojeni k Internetu, např. servery. Pronájem linky je dražší a odvozený od rychlosti. Toto připojení je nevhodné pro domácí použití.
5. Wi-Fi (Wireless Fidelity) – Standard bezdrátové sítě (IEEE 802.11a, b, g). Tato technologie používá pro komunikaci mikrovlnné spojení. Nejčastěji pracuje na frekvencích 2,4 a 5 GHz. Tato technologie se v České republice rychle rozšířila, jelikož poskytovateli stačí umístit na vyvýšené místo vysílač (AP – Access point) a klienti v okolí se mohou připojit do sítě a využívat tak služeb daného poskytovatele. Nutnou podmínkou je přímá viditelnost na vysílač a dostatečně kvalitní signál, pokud signál není kvalitní, lze použít mikrovlnnou anténu.
6. Síť mobilních telefonů – I po mobilní síti GSM lze přenášet data a díky tomu lze i takto poskytovat Internet uživatelům. Poskytovatel připojení do GSM sítě se tak stává i poskytovatelem připojení. Rychlost takové sítě je teoreticky okolo 170 kb/s, v ČR prakticky 50 kb/s (zhruba rychlost vytáčeného spojení), záleží však na kvalitě signálu. Nebo lze použít modernějších technologií jako jsou GPRS, EDGE a CDMA. GPRS má maximální rychlost 80kb/s při konfiguraci přijímače 4+1(4 sloty pro download a jeden pro upload). EDGE při stejné konfiguraci přijímače poskytuje 236,8 kb/s, v praxi však okolo 200 kb/s. Při použití technologie multislot class 32 je pak rychlost GPRS 100 kb/s a EDGE 296 kb/s. Tato spojení se vyznačují několikanásobnou odezvou na rozdíl od ADSL. Službu CDMA nabídl tehdejší Eurotel s rychlostí okolo 300 kb/s. V praxi na Praze 1 s CDMA se stahovalo okolo 100 kBps s dobou průměrné odezvy 130 ms, oproti EDGE, které mělo rychlost 15 kBps a odezvou 600 ms.

7. Kabelová televize a satelitní přijímač – Pokud máte v bytě kabelovou televizi od poskytovatele, který souběžně nabízí i připojení k Internetu, lze se pomocí modemu připojovat k Internetu přes kabelovou televizi, stejně tak je na tom satelit. Toto připojení přes kabelovou televizi bývá rychlé a příplatek za Internet nebývá tak vysoký.

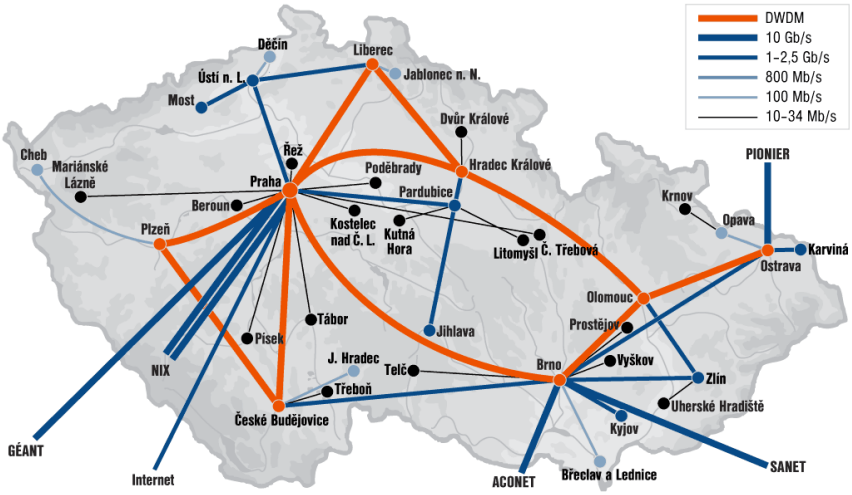
3.10.5 Rychlost připojení

Uživatelé si nejčastěji stěžují, že Internet je pomalý, když chtějí zobrazit WWW stránku http://www.stranka.com, ale problém není v Internetu jako takovém, ale pouze u jejich poskytovatele připojení, neboli rychlosti mezi ISP a uživatelem.

Internet je velice rychlý (obrázek 5) , Internet zajišťuje přenos souborů z místa na místo. Třeba zmiňovaná WWW stránka je na serveru uložena v podobě souborů. Při zobrazení takovéto stránky se přenáší soubor, ten vytvoří server klientovi, který pak jeho prohlížeč dokáže dekódovat a zobrazit tak požadovaný obsah. Přenos takovéhoto souboru je velmi rychlý, jelikož velikost souboru je minimální.

Chceme-li ale stáhnout multimediální soubor, který může být i několikanásobně větší, je už rozdíl v rychlosti znatelný. Soubor je umístěn na serveru vzdáleném i několik tisíc kilometrů od místa, kde je sídlo uživatele.

Po vyslání požadavku o přenos souboru se tento soubor během několika vteřin přes vysokorychlostní linky Internetu přesune k vašemu ISP. Od něj musí být ještě přenesen až k vám, a to přenosovou rychlostí definovanou ISP. Máme-li zakoupenu pouze pomalou linku, může přenos souboru trvat minuty, než se objeví na vašem PC.



Obrázek 5 - Rychlosti připojení uzlů
zdroj: http://www-hep2.fzu.cz/~nemecek/
AtlasFZU2000_soubory/v3_document.htm

3.10.6 Přehled služeb Internetu

Nejčastější služba poskytovaná servery je WWW server, který byl v roce 1989 vynalezen a stal se tak nedílnou součástí Internetu. Výpis standardních služeb.

1. WWW - prohlížení Internetových stránek
2. E-mail (Electronic Mail) – Posílání elektronických dopisů a správa vlastní elektronické schránky
3. FTP (File Transfer Protocol) – přenos souborů sítí

Mimo tyto základní služby jsou zde i další ICQ, IRC, Chat, IP Telefonie, Napster, SSH, WAP, Net Meeting.

3.10.7 Historie Internetu a TCP/IP shrnutí

Shrnutí změn ve vybraných letech:

1. 1962 – Vzniká projekt počítačového výzkumu agentury DARPA.

2. 1969 – Vytvořena experimentální síť ARPANET, první pokusy s připojením uzlů (4 uzly).
3. 1972 – ARPANET rozšířena na cca 20 směrovačů a 50 počítačů, použit protokol NCP (Network Control Protocol).
4. 1972 – Ray Tomlinson vyvíjí první e-mailový program.
5. 1973 – Zveřejněn TCP (Transmision Control Protocol).
6. 1976 – První kniha o ARPANET.
7. 1980 – Experimentální provoz TCP/IP v síti ARPANET, adresace IPv4, protokol DNS, směrovací protokoly.
8. 1983 – Rozdělení ARPANET na ARPANET (výzkum) a MILNET (Military network, provoz). TCP/IP přeneseny do komerční sféry.
9. 1984 – Vyvinut DNS (Domain Name System).
10. 1985 – Zahájen program NSFNET, sponzoruje rozvoj sítě ve výši 200 miliónů dolarů, první komerční služby.
11. 1987 – Vzniká pojem „Internet“.
12. 1987 – V síti je propojeno 27 000 počítačů.
13. 1989 – Tim Berners-Lee publikuje návrh vývoje WWW (Information Management: a Proposal).
14. 1990 – Tim Berners-Lee a Robert Cailliau publikují koncept hypertextu.
15. 1990 – končí ARPANET.
16. 1991 – Nasazení WWW v evropské laboratoři CERN.
17. 1993 – Marc Andreessen vyvíjí Mosaic, první WWW prohlížeč, a dává ho zadarmo k dispozici.
18. 1994 – Vyvinut prohlížeč Netscape Navigátor
19. 1994 – Internet se komercionalizuje.
20. 1996 – 55 milionů uživatelů
21. 1999 – Rozšiřuje se Napster
22. 2000 – 250 milionů uživatelů
23. 2003 - 600 milionů uživatelů
24. 2005 - 900 milionů uživatelů
25. 2006 – více jak miliarda uživatelů

4 Protokol TCP/IP

4.1.1 Popis vrstev TCP/IP

Tento protokol má pouze 4 vrstvy na rozdíl od modelu ISO/OSI, který jich má 7. Jedná se o vrstvy aplikační, transportní, síťovou a vrstvu síťového rozhraní. S těmito vrstvami se následně blíže seznámíme.

1. Aplikační vrstva je určena pro napojení aplikace k síťovému rozhraní.
2. Transportní vrstva zajišťuje spolehlivost přenosu. Jsou aplikace, které se bez spolehlivosti neobejdou, ale existují i přenosy, které zajištění spolehlivosti nepotřebují. Pokud posílám e-mail, požaduji, aby bylo vše bez sebemenší chybičky, zde se využívá protokol TCP. Oproti tomu například při telefonování požaduji rychlejší přenos a pokud je paket poškozen, nepotřebuji ho poslat znovu, protože mě už nezajímá, co někdo řekl před vteřinou, ale zajímá mě, co říká zrovna teď a veškeré chybné pakety se zahazují, což umožňuje protokol UDP.
3. Síťová vrstva slouží pro maximální využití přenosové rychlosti. Snaží se pakety ať TCP nebo UDP co nejrychleji přesunout po síti. Data posílá po blocích nezávisle na sobě, pokud by se část přenosové cesty zahltila, pakety si samy najdou jinou příznivou cestu jak se dostat k cíli.
4. Vrstva síťového rozhraní je univerzální mezičlánek mezi síťovými vrstvami a libovolnou síťovou kartou. Zda se jedná o chybový přenos nebo relativně spolehlivých cestách.

4.1.2 Porovnání vrstev ISO/OSI a TCP/IP

Tabulka 2 - Vrstvy ISO/OSI a TCP/IP

ISO/OSI	TCP/IP	protokoly
Aplikační vrstva	Aplikační vrstva	Aplikační protokoly
Prezentační vrstva		
Relační vrstva		
Transportní vrstva	Transportní vrstva	TCP, UDP
Síťová vrstva	Síťová vrstva	IP, PPP
Linková vrstva	Vrstva síťového rozhraní	Ethernet, Token Ring
Fyzický vrstva		

4.1.3 Internetové protokoly

Tabulka 3 - Protokoly jednotlivých vrstev

Aplikační vrstva	Bit Torrent, DNS, DHCP, FTP, http, HTTPS, IMAP, IRC, NNTP, NTP, POP3, RTP, SIP, SMTP, SNMP, SSH, Telnet
Transportní vrstva	DCCP, SCTP, TCP, UDP
Síťová vrstva	ARP, IPv4, IPv6, RARP

4.1.4 Problematika přenosu

V prostředí protokolů TCP/IP operují dva protokoly TCP a UDP. TCP se vyznačuje tím, že před posíláním informací je nejdříve navázáno spojení a po přenosu dat je opět spojení zrušeno.

Protokol TCP přijímá informace po jednotlivých bitech, které mu přijdou z vyšší vrstvy. Ty shromažďuje ve vyrovnávacím bufferu, nejčastěji do velikosti 64 kb, které pak pošle celé najednou.

Vyrovnávací buffer není pokaždé vhodné použít, třeba pro zjištění stavu klienta apod. Pro tyto případy existuje mechanizmus zvaný „push“, který odeslání vynutí i při neúplném bufferu.

Přenos dat pomocí TCP používá kladné potvrzování (positive acknowledgement), úspěšně přijatá data se potvrdí a na nekompletní se nereaguje. Očekává se jejich opětovné zaslání, které proběhne až po čase, aby nedocházelo k zahlcení sítě, tomuto času se říká „time out“.

Řešit posílání dat přímo tímto způsobem by bylo zdlouhavé, proto se používá kontinuální potvrzování (continuous acknowledgement). Toto potvrzování funguje tak, že se odešle několik bloků dat ještě předtím, než byla přijata první potvrzovací informace, tyto potvrzovací informace jsou přijímány dodatečně.

UDP – nenavazuje spojení s druhou stranou při posílání informací. Sám nepoužívá buffer, dostane blok dat už z vyšší vrstvy a celý tento blok odešle jako celek (datagram).

4.1.5 Bezpečnost protokolu TCP/IP

Protokol TCP/IP nebyl vyvíjen pro řešení bezpečnosti. Zadání bylo specifikováno tak, aby protokol co nejefektivněji a nejpřizpůsobivěji využíval přenosovou cestu. Proto veškeré komunikace pomocí TCP/IP nejsou nijak zabezpečeny. Bezpečnost se týká v podstatě dvou věcí.

Data do úrovně síťové vrstvy nejsou zabezpečena a zároveň nejsou data zabezpečena ani proti odposlechu na přenášené lince. Zde jsou možná řešení bezpečnosti. O opakování přenosu se stará Transportní vrstva protokolu TCP. Nejjednodušeji se pak data zašifrují už v aplikační vrstvě v samotné aplikaci, které může obsahovat specifické šifry.

Nevýhodou TCP/IP je, že aplikační úroveň neověřuje správnost dat, toho lze využít a poslat někomu e-mail pod smyšlenou adresou odesílatele.

4.2 Popis IPv6

Novou generaci protokolu IP představuje protokol IPv6, který odstraňuje některé negativní vlastnosti původního protokolu IPv4. Pod označením IPnG (IP next Generation) byl protokol vyvíjen od roku 1991 s důrazem na problém adresace uzlů, dynamické konfigurace, podpory multimediálních aplikací a bezpečnostních procedur. Nasazování tohoto protokolu se plánuje překryvným způsobem a díky tomu souběžným během obou verzí protokolu.

4.2.1 Záhlaví protokolu

Nové specifikace protokolu způsobily změnu řídících polí v záhlaví IP paketu, byly odstraněny přebytečné položky a zřetězení základních i volitelných položek záhlaví. Základní záhlaví je možné rozšířit o Hop-by-Hop, Option, Routing, Fragment, Destination Options, Authentication, Encapsulating Security Payload, které se používají pouze v případě požadavku na danou funkci..

4.2.2 Rozšíření adresovatelného prostoru IP adres

Díky obrovskému rozvoji Internetu se blíží doba, kdy budou veškeré IP adresy vyčerpány, tedy všech 4 294 967 296 adres. Na počátku vývoje se počítalo s adresováním pomocí 32 bitů, což pro tehdejší možnosti bylo nepřekonatelné množství připojitelných bodů.

Jak se dá tento problém řešit? Dnes je už připraven novější protokol označován IPv6, který má šířku adresy 128 bitů. Tento protokol se zavádí do praxe.

4.2.3 Automatická konfigurace uzlů

V protokolu jsou mechanizmy pro automatické přidělování konfiguračních údajů sítě jednotlivým uzlům.

4.2.4 Bezpečnostní procedury

Bezpečnostní procedury ověřování přístupu a kódování jsou již do protokolu zabudovány na úrovní IP komunikace. Nový protokol umožňuje volitelný výběr bezpečnostních metod, standardně však používá metodu autorizace přístupu MD5 a kódování dat podle DES (Data Encryption Standard).

Tyto bezpečnostní vlastnosti jsou implementovány pomocí volitelného podzáhlaví. Vzhledem k faktu, že se procedury implementují přímo v základním protokolu IP, označujeme tento způsob za zabezpečení na úrovni jádra TCP/IP (kornel level security). Jednotlivé aplikace pak využívají už existující procedury a nemusí je implementovat samostatně.

4.2.5 Podpora multimediálních aplikací

S narůstajícím počtem aplikací požadujících komunikaci v reálném čase v síti Internet bylo počítáno, a proto byla přidána podpora i pro komunikace tohoto typu. Pro tento účel se používá metoda označení toku návěstím (Flow label). Tokem rozumíme IP pakety posílané mezi zdrojem a cílem s požadavky specifikovanými na přenos.

Přiřazením číselného návěští danému toku pomocí protokolu RSVP (Resource Reservation Protocol) mohou směrovače obsluhovat přenosy paketů různých toků odlišným způsobem.

Tím však problém vzrůstajícího počtu uživatelů není vyřešen. Se zvyšujícím se počtem uživatelů stoupá také rychlost, kterou musí servery mezi sebou komunikovat. Protokol TCP už také nebude stačit, proto se vyvíjí jeho nástupci. Jde o protokol RTP (Real-Time transport Protokol) Díky těmto protokolům dokážeme rychleji a plynuleji přenášet data.

4.2.6 Souhrn o protokolu IPv6

Nejmarkantnější rozdíl oproti klasickému protokolu IPv4 je v systému adres. Jak již bylo uvedeno, systém používá namísto 32 bitových adres nově 128 bitové adresy, které jsou symbolicky vyjádřeny novým způsobem. Adresy se zapisují v hexadecimálním formátu (osm 16 bitových polí) přičemž jednotlivá pole jsou oddělena oddělovačem „:“ namísto „.“. Je to z důvodu univerzálního vyjádření adresných schémat.

FEA1:122B:0000:0000:0000:0000:4A51:1022 - FEA1:122B::4A51:1022

0000:0000:0000:0000:0000:0000:172.16.45.6 - ::172.16.45.6

4.3 Lokální síť

4.3.1 Dělení počítačů v síti

1. Pracovní stanice je počítač připojený do sítě, pracuje s ním běžný uživatel. Od osobního počítače se liší tím, že může využívat služeb nabízených sítí.
2. Server je počítač, ke kterému přistupuje pouze správce sítě, nikoli běžný uživatel. Server poskytuje pracovním stanicím služby pomocí sítě, souborový server, tiskový server, mail server a další.

4.3.2 Dělení lokálních sítí

1. Klient - server – Jde o typ připojení, kde jeden počítač (většinou ten nejvýkonnější) slouží jako server a ostatní počítače v síti slouží jako pracovní stanice, které se k serveru připojují. Typickým propojením klient - server je síť Novell Netvare.
2. Peer-to-peer má opačné chování. Všechny počítače si jsou rovny v tom smyslu, že kterýkoli počítač se může stát serverem i klientem. K libovolnému počítači připojíme tiskárnu a do

jiného dáme velký disk, pokud počítač s tiskárnou potřebuje data z disku, je klientem a počítač s diskem je v tuto chvíli server, ovšem potřebuje-li počítač s diskem tisknout, postavení se otočí. Tento druh spojení umožňuje systém Artisoft LAN static nebo Microsoft Windows for Workgroups.

Obě struktury lokálních sítí mají výhody i nevýhody. V síti typu klient - server je už z principu snadná správa síťových dat, která jsou soustředěna na serveru. Za nespornou nevýhodu se dá označit situace, kdy se vyskytne závada na serveru, neboť to znamená ochromení celé sítě.

Za podstatnou výhodu peer-to-peer se dá označit to, že lze s výhodou použít všechny počítače, které předtím pracovaly samostatně. I pořizovací cena této sítě je rapidně nižší, jelikož se ušetří za nákup serverů. Rychlost takto postaveného systému sítě je nižší než u systému klient - server. Bezpečnost celého systému sítě je však se stoupajícím počtem počítačů výrazně náročnější. V tomto typu je zvýšená pravděpodobnost výskytu „děr“ v zabezpečení.

Největším nebezpečím je, když se počítač zvaný server využívá jako pracovní stanice. Při zkoušení nového programového vybavení může tento software způsobit výpadek počítače na předem nespecifikovanou dobu. Po dobu výpadku je síť nepoužitelná a může dojít i ke ztrátě toho nejdůležitějšího, dat.

4.3.3 Služby poskytované lokální sítí

1. Poskytování diskového prostoru – každý server zapojený do sítě může nabízet okolním počítačům své disky (celé nebo jen jejich části). Dá se určit disk nebo adresář, kam bude mít daný uživatel přístup. Přes tuto službu nabízí uživatelům využívání velkokapacitních disků serverů a manipulaci se soubory, které uživatel nemůže mít na svém lokálním počítači. To umožňuje,

aby se soubory pracovalo více uživatelů najednou. Umístíme-li na sdílenou jednotku databázové soubory, umožníme tím více uživatelům s nimi pracovat. S ohledem na oprávnění jednotlivých uživatelů budou někteří z nich moci databáze pouze prohlížet, jiní budou jejich obsah měnit.

2. Sdílení tiskáren – bylo nejpodstatnější příčinou rozvoje lokálních sítí. V lokální počítačové síti stačí, vybavíme-li tiskárnou nejméně jeden server. Všichni uživatelé tak mohou tisknout na této tiskárně, stejně jako kdyby byla připojena přímo k jejich počítači.
3. Sdílení dalších periferních zařízení – mezi které patří např. CD-ROM disky a plottery.
4. Elektronická pošta – uživatelé mají na serveru vyhrazeny své e-mailové schránky, kde mají uloženou svou e-mailovou komunikaci. Využívání elektronické pošty umožňuje zasílat i celé soubory v podobě příloh dokumentu. Uživatel je o příchodu pošty upozorněn hned po jejím přijetí na svůj poštovní server.
5. Chat mezi uživateli sítě – Jde o obousměrnou komunikaci v reálném čase. Zprávy jsou po odeslání zobrazeny na obou monitorech zároveň. Tato komunikace bývá nazývána On-Line Chat. Pokud tímto způsobem komunikuje více uživatelů najednou, pak se jedná o NetMeeting.

4.4 Zabezpečení počítačové sítě

4.4.1 Ochrana dat a zvýšení bezpečnosti provozu.

Je velmi nebezpečné, jestliže získá přístup na některý z našich počítačů nepovolaná nebo nepoučená osoba. I v dobrém úmyslu může napáchat značné škody na datech nebo instalovaném programovém vybavení.

Takovým událostem se dá zabránit několika způsoby. Od fyzického uzamčení počítačů až po nákup speciálního softwarového vybavení pro každý z počítačů. Většina lokálních sítí nám umožní zajistit bezpečnost sítě hned na třech úrovních:

1. První úroveň je zajištěna vyžádáním hesla při přihlašování uživatele k síti. U každého uživatele můžeme rovněž určit, ve kterých dnech v týdnu a ve kterých hodinách či u kterého počítače je oprávněn v síti pracovat.
2. Druhá úroveň je zajištěna tzv. seznamem přístupových práv. Mezi přístupová práva patří např. právo otevírat soubory ke čtení nebo k editaci, vytváření nových a mazání již existujících. Takto lze jemně „vyladit“ práva jednotlivých uživatelů.
3. Třetí úroveň je tvořena atributy souborů a adresářů, které omezují uživateli přístup k jednotlivým částem systému. Atributy umožňují zakázat kopírování, prohlížení, mazání, apod.

4.4.2 Pracovní bezdiskové stanice

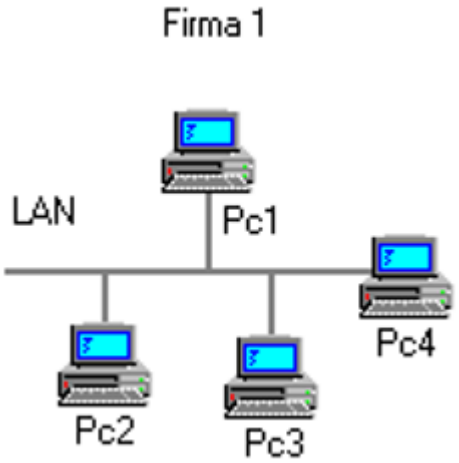
Vzdálené zavádění operačního systému umožňuje pracovat v síti na počítačích, které nejsou vybaveny žádnou disketovou nebo diskovou mechanikou. Systém je nutné zavádět ze serveru. Právě tyto jednotky jsou totiž nejčastěji „vstupní branou“, kterou se dostanou viry do našeho systému. Správce sítě je člověk, který se stará o správu a bezpečnost sítě. Může získat veškeré informace o dění v síti. Mezi sledované činnosti patří i úspěšné či neúspěšné přihlášení do sítě, manipulace se soubory, pokusy o přístup do adresářů, apod. Sledovat lze i délku připojení, počet vytisknutých znaků.

Důležité jsou i prostředky zajišťující ochranu dat před náhlým zničením (např. výpadek elektrického proudu). Sem patří např. UPS (Uninterruptible Power Supply – nepřerušitelný zdroj napájení), které při výpadku nebo poklesu napětí upozorní operátora na možnost předčasného vypnutí serveru a začne server napájet ze záložních akumulátorů.

4.5 Přenos dat mezi dvěma uzly v různých lokálních sítích

4.5.1 Popis funkce lokální sítě

Základem tohoto procesu je přenos dat mezi počítači v rámci firmy (např.: sdílení dokumentů) a jedná se zde tedy o LAN sít (obrázek 6).

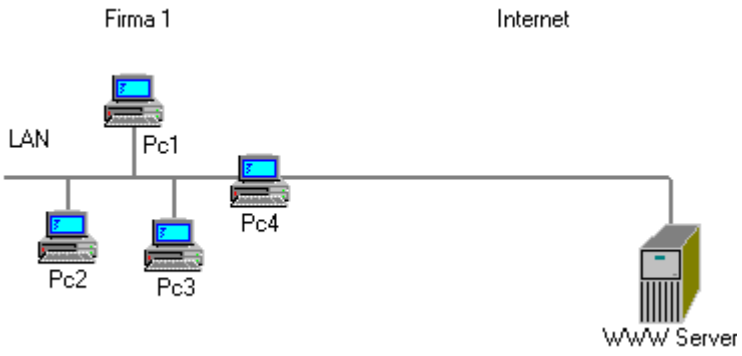


Obrázek 6 - Základní LAN síť

Pro představu počítač 4 umožňuje sdílení svých souborů ostatním počítačům ve své síti. Pokud se počítač 1 připojí k počítači 4, ve své podstatě se jedná o komunikaci mezi dvěma uzly, mezi kterými dochází k přenosu dat.

4.5.2 Data v podobě WWW stránky

Pokud se však chceme podívat na www stránky, nehovoříme už o síti LAN ale o WAN komunikaci. Tato WAN komunikace probíhá mezi počítačem, kde se data zobrazují a serverem, na kterém jsou stránky uloženy. Zjednodušeně si jej lze představit takto:



Obrázek 7 - Propojení s WWW serverem

Přistupuje-li k WWW obsahu tohoto serveru na síti Internet jakýkoli počítač z firmy, pokud se jedná o počítač 4, který je přímo připojen k Internetu jde v tomto zjednodušeném modelu o stejný případ, který je uveden výš. Pokud se chce připojit počítač 2, jde už o složitější případ.

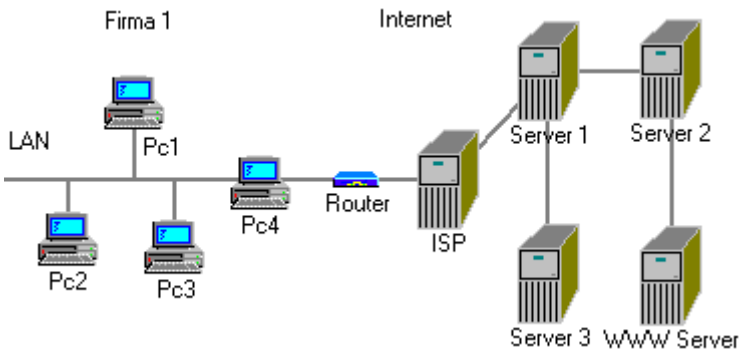
4.5.3 Základní připojení k serveru na Internetu

Počítač 2 chce komunikovat s počítačem v síti Internet, pro tento případ má ve svém nastavení uloženo, že komunikace musí jít před počítač 4, kam počítač 2 vyšle požadavek, počítač 4 pošle požadavek na WWW server.

Počítač 4 si pamatuje, že počítač 2 komunikuje s WWW serverem, a tak mezi nimi vytvoří pomyslný tunel, data z obou stran projdou k tomu druhému a zpět. V tomto modelu jsem vysvětlil zjednodušeně, jak komunikace funguje, je-li v komunikační cestě zapojen aktivní prvek jako je server.

4.5.4 Rozšíření o IPS

Samozřejmě v reálném životě je v cestě prvků několik. Přenos dat zprostředkovávají další servery, síťové prvky, jako je server, router, switch a hub.



Obrázek 8 - Propojení s ISP

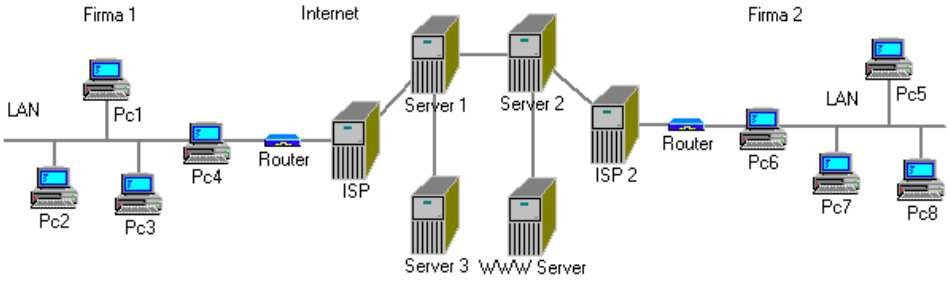
Z obrázku 8 lze vyčíst, že poskytovatel Internetu nemusí mít k Internetu připojovat pouze jednu firmu, ale uživatelů může být několik, proto je zde uveden Router, ale může to být i jiný síťový prvek.

Poskytovatel je zase připojen k Internetu třeba od CESNETu. Ten opět nabízí připojení i dalším poskytovatelům, tím vzniká struktura pyramidová. Jako je ISP jedním z koncových prvků pyramidy, může se zase on stát dalším středovým prvkem a síť dále štěpit.

Pokud se chce nyní opět počítač 2 připojit k WWW, vyšle požadavek počítači 4, ten zase dál routeru a tak to jde dál, než se propojování dostane k WWW serveru.

Počítač 2 s WWW serverem spolu mohou komunikovat stejně, jako by byly na lokální síti. Nyní máme komunikaci mezi LAN sítí a Internetem, nyní toto schéma rozšíříme ještě o druhou lokální síť.

Z obrázku se dá vyčíst, že na pravé straně přibyla firma 2, která je jako první firma tvořená svou lokální sítí a serverem připojeným k Internetu. Jelikož firma 2 má pouze jednu veřejnou IP adresu, počítač 2 se může v tomto momentu připojit nejdále na počítač 6, který tvoří server pro tamní lokální síť, chceme-li se dostat dále na lokální síť musíme na serveru použít překladač adres který si vysvětlíme dále.



Obrázek 9 - Propojení LAN - LAN

Z tohoto příkladu (obrázek 9) je zřejmé, že se nejedná o propojení dvou sítí LAN, kde bychom se museli potýkat s problémy typu duplicita sítí a IP adres. Proto se nepokouším propojit dvě sítě doslova, ale propojit jednotlivé dva počítače. Spíše tedy libovolný počítač z firmy s automatem B&R.

5 Vlastní řešení

5.1 Odzkoušení přenosu dat s automat B&R po síti

Komunikaci jsem odzkoušel na lokální síti. Po připojení do sítě jsem nejprve otestoval, zda vůbec mohu komunikovat s automatem B&R.

K tomu mi posloužil příkaz ping na IP adresu automatu, ten standardně odpověděl, čímž bylo spojení prokázáno. Poté jsem pustil program pro zjištění portů, na kterých daný stroj poslouchá. Zjistil jsem, že automat používá dva porty:

1. port 21, který je určen pro přenos souborů pomocí protokolu FTP
2. port 111, přes který se komunikuje se serverem RPC

5.2 RPC

Balík RPC (Remote Procedure Call) neboli Vzdálené volání procedur poskytuje velmi obecný mechanismus pro aplikace typu klient-server. Balík RPC vyvinula firma Sun Microsystems a v podstatě se jedná o souhrn funkcí potřebných pro komunikaci. Důležitou aplikací postavenou na balíku RPC je systém NFS, síťový souborový systém, a systém NIS, síťový informační systém. Oba tyto systémy budou probírány v následujících kapitolách.

Server RPC se skládá ze sady procedur, které klient může volat tím způsobem, že pošle serveru požadavek RPC společně s parametry procedury. Server spustí jménem klienta požadovanou proceduru a existuje-li návratová hodnota, pošle ji zpět klientovi.

Aby mohl být balík RPC nezávislý na typu hardwaru, jsou všechna data předávaná mezi klientem a serverem převedena vysílajícím počítačem do tzv. formátu externího vyjádření dat XDR (External Data Representation) a přijímající počítač je převede zpět do místního vyjádření dat.

5.2.1 Nekompatibilita verzí

Někdy způsobí zdokonalení RPC aplikace nekompatibilní změny v rozhraní volání procedur. Samozřejmě, že prostá výměna serveru může způsobit havárii všech aplikací, které stále očekávají původní chování. Proto mají programy RPC přiděleny číslo své verze, obvykle se začíná hodnotou 1 a při každé nové verzi rozhraní RPC je tato hodnota zvýšena.

Server může často současně nabízet několik verzí RPC. V takovém případě označí klient ve svém požadavku číslo verze, kterou chce ve své implementaci dané služby používat. Vlastní síťová komunikace probíhá mezi servery RPC a jejich klienty. Server RPC nabízí jednu nebo více skupin procedur, každá množina procedur se nazývá program a je jednoznačně určena číslem programu.

5.3 Postup komunikace

1. Jednoduché zabalení všech parametrů a identifikátorů procedury do formy vhodné k přenosu po sít
2. Zaslání upravených dat
3. Rozbalení dat na vzdáleném místě
4. Zavolání správné procedury s právě jedním parametrem
5. Převedení výsledku do zmiňované formy
6. Odeslání zpět odesílateli požadavku
7. Rozbalení dat
8. Předání požadovaného výsledku komunikačnímu programu

Nevýhodou pro programátora je, že nelze předávat ukazatele, protože v druhé proceduře nemají žádný smysl.

5.3.1 Konkrétní způsob obecného schématu

Aplikace, která daný požadavek vznáší, si nemusí uvědomovat komunikaci po síti díky transparentnímu sdílení. Formulace požadavku je naprosto stejná. Síťovou komunikaci si musí uvědomovat až programová část, která příslušný požadavek vyřizuje, jelikož si musí být vědoma existence síťových uzlů a komunikovat s nimi. Tato programová část bude nejspíše realizována jako samostatný proces, který sestaví příslušný požadavek a formou zprávy ho odešle na server, poté bude čekat na jeho odpověď. Během čekání bude proces uveden do stavu „čekající“ s požadavkem na aktivování po příchodu požadované informace ze serveru.

Tento postup bude v praxi používán, ale je v rozporu se zásadami strukturovaného programování. Proto je lepší se na tento problém dívat jako na proceduru, která se zavolá v okamžiku požadavku na odesílání zprávy. Ukončí se po příchodu odpovědi návratem za místo jejího volání a pokračování v programu. Program zavolá lokální proceduru, která je součástí implementace RPC jako spojka. Ta zajistí vše potřebné včetně čekání a poté se řádným způsobem ukončí. Parametry, které spojka klien-

ta dostala při svém volání, patří vzdálené proceduře. Proto spojka klienta parametry převede do tvaru vhodného pro přenos (tzv. marshalling) a připojí je ke zprávě odesílané serveru. Data projdou sítí a na serveru se opět rozbalí, provede se procedura, odpověď se opět převede a přenese po síti zpět, kde se rozbalí a výsledek se dále zpracuje.

Pokud jsou předávané parametry hodnotou, je vše v pořádku, chceme-li ale zavolat proceduru s referencí, dostává pouze ukazatel na objekt, který je skutečným parametrem. Objekt ale existuje pouze na straně klienta, a proto není možné použít tentýž ukazatel na straně serveru. Možným řešením je, že ještě před zavoláním procedury na serveru lze tento objekt zkopírovat na server a poté procedura dostane referenci na tento zkopírovaný objekt, který pak může modifikovat. Jakmile procedura skončí, objekt se zase zkopíruje zpátky ke klientovi.

Pro správné pochopení způsobu, jakým je mechanizmus RPC implementován, je dobré začít s představou, že každá procedura má přidělený číselný identifikátor. Tento identifikátor musí být pro každou proceduru specifický, to požadovalo jediný centrální subjekt, který by identifikátory vhodně koordinoval a přidělоval. Tohoto úkolu se zhostila firma Sun Microsystems. Aby nemusela přidělovat jednoznačný identifikátor pro každou proceduru, rozhodli se identifikátor skládat ze tří složek:

1. číslo programu, které identifikuje skupinu procedur pro určitou službu. Například skupina procedur pro protokol NFS má přidělené číslo 10003.
2. číslo procedury, které identifikuje proceduru v rámci skupiny
3. číslo verze

Firmě Sun stačí pečovat pouze o jednoznačnost první složky. Kdokoli se rozhodne pomocí RPC implementovat novou službu, může si vyžádat jednoznačné číslo programu. Druhé číslo jednotlivým procedurám si pak může přidělit sám, dle své libosti. Třetí složka vychází vstříc po-

stupnému vývoji, diky ní lze implementovat novější verze, ale současně s tím zabezpečit zpětnou kompatibilitu s předchozími verzemi.

5.3.2 Jeden parametr postačí

Pro snadnější implementaci stanovila firma Sun, že každá procedura bude mít pouze jeden vstupní parametr a jeden výstupní. Tato podmínka není nijak omezující.

V případě potřeby použití více parametrů, je možné vytvořit strukturu, kde budou tyto údaje uvedeny a proceduře zadat ukazatel na tuto strukturu, která bude při volání příslušné procedury odeslaná na server. Ke správnému využití musí být obě strany předem dohodnuty na formátu předávané datové struktury a významu jednotlivých položek.

XDR je zde pro to, aby obě strany správně interpretovaly každou část vstupních a výstupních dat. Jsou dva principy řešení. První je založen na tom, že každá zúčastněná strana bude předem znát konverze, které používá kterákoli druhá strana. Pak je možné při přenosu provést potřebné konverze pouze jednou, nebo vůbec, používají-li obě strany stejnou konverzi.

Alternativním řešením je zavést společný mezitvar a veškerá data přenášet v něm. Tím se sice musí konverze provádět vždy dvakrát, ale každá strana si vystačí s jednou sadou konverzních prostředků a nemusí se přizpůsobovat novým konverzím druhých stran.

Právě druhé řešení zvolila firma Sun pro implementaci svého RPC. Konkrétní realizací je standard XDR, který byl zveřejněn a je používán v rodině protokolů TCP/IP. Standard XDR tedy definuje jednotný způsob převádění přenášených dat, je nezávislý na architektuře odesílatele i příjemce.

5.3.3 Strana klienta

Jakmile dokážeme proceduru jednoznačně identifikovat pomocí vhodného identifikátoru, může nám k volání procedur stačit jediný prostředek, systémová rutina pojmenovaná **callrpc**, který má osm parametrů:

1. identifikace uzlu, kde má být vzdálená procedura provedena
2. číslo programu vzdálené procedury
3. číslo verze
4. číslo vzdálené procedury v rámci skupiny
5. vstupní parametr
6. XDR filtr vstupního parametru
7. výstupní parametr vzdálené procedury
8. XDR filtr výstupního parametru

5.3.4 Registrace procedur

Na serveru musí existovat někdo, kdo ví o službách poskytovaných formou vzdálených procedur. Má je na starosti RPC dispečer (RPC library dispatcher), který je příjemcem žádostí o volání procedur a také následně volá jednotlivé rutiny.

Každá procedura, která je implementována, se musí před voláním registrovat. Musí sdělit, o jakou proceduru se jedná, konkrétní způsob volání, konverze svých vstupně-výstupních parametrů. Pro registraci se používá rutina registerrpc s těmito parametry:

1. číslo programu
2. číslo verze
3. číslo procedury v rámci skupiny
4. vstupní bod lokální procedury, která implementuje vzdálenou proceduru
5. vstupní parametr
6. XDR filtr vstupního parametru

7. výstupní parametr vzdálené procedury
8. XDR filtr výstupního parametru

5.3.5 Tři úrovně RPC

Výše naznačený mechanizmus RPC není jediný možný. RPC lze využít ve třech úrovních, ta doposud předpokládaná je ta prostřední. Je charakteristická tím, že na této úrovni je nutné si uvědomovat existenci vzdálených uzlů a znalost konkrétních vzdálených procedur.

Při seriózní tvorbě aplikací je nevýhodou, že není možné nijak ovlivnit transportní mechanismus pro skutečný přenos v síti (UDP/TCP), časové limity, chybové hlášky a přístupová práva.

Transportní přenos a ostatní problémy si musí vyřešit aplikace, ta si musí uvědomovat, který mechanismus použít a jaké důsledky z toho vyvodit. Pokud potřebuje zasáhnout do způsobů komunikace, musí použít nejnižší úroveň práce s RPC a realizovat požadavek pomocí callrpc.

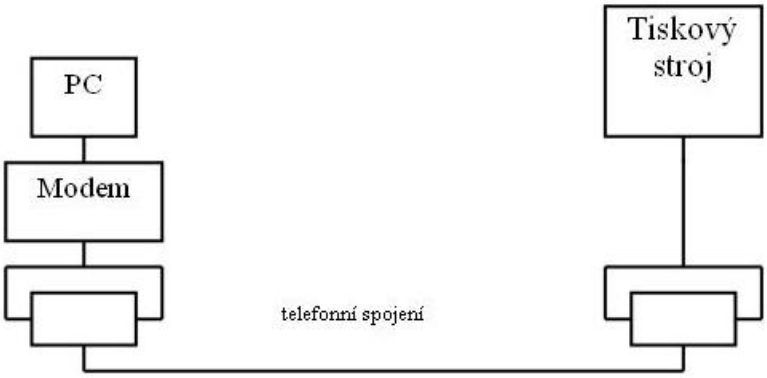
6 Možnosti propojení pro dálkovou diagnostiku

6.1.1 Propojení telefonní linkou

Toto propojení v praxi už funguje a je plně a úspěšně využíváno (obrázek 10). Nutnou podmínkou na straně zákazníka je vlastnictví telefonní linky a propojení tiskového stroje k této lince.

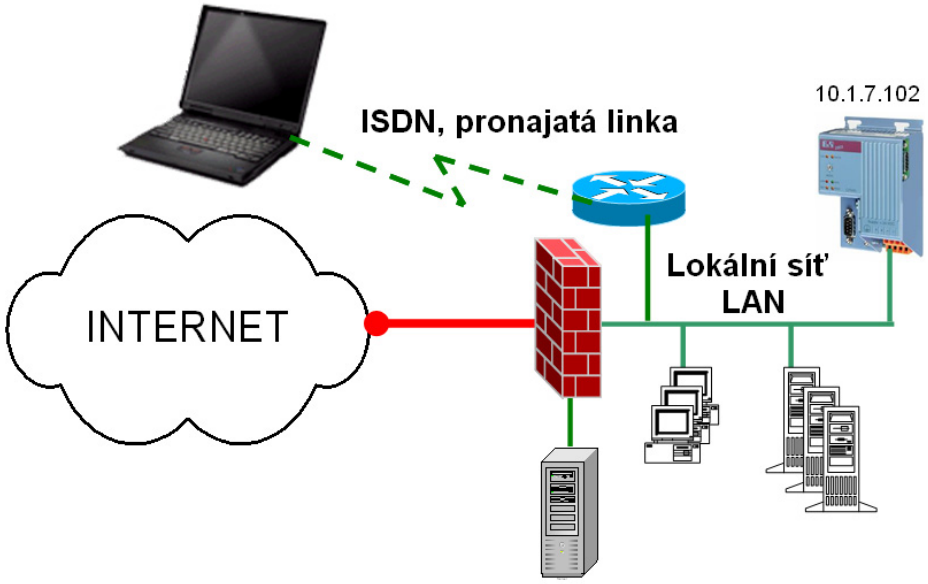
Počítač vytočí na modemu číslo, na které je připojen tiskový stroj. Na straně zákazníka modem není potřeba, jelikož je integrován přímo v automatu B&R. Tiskový stroj příchozí hovor přijme a je navázaná datová komunikace mezi počítačem a automatem B&R.

Můžeme provádět dálkovou diagnostiku dle libosti. Omezením tohoto spojení je rychlost, která je 57 600 b/s, ta je však v současné době nepostačuje.



Obrázek 10 - Propojení pomocí modemu

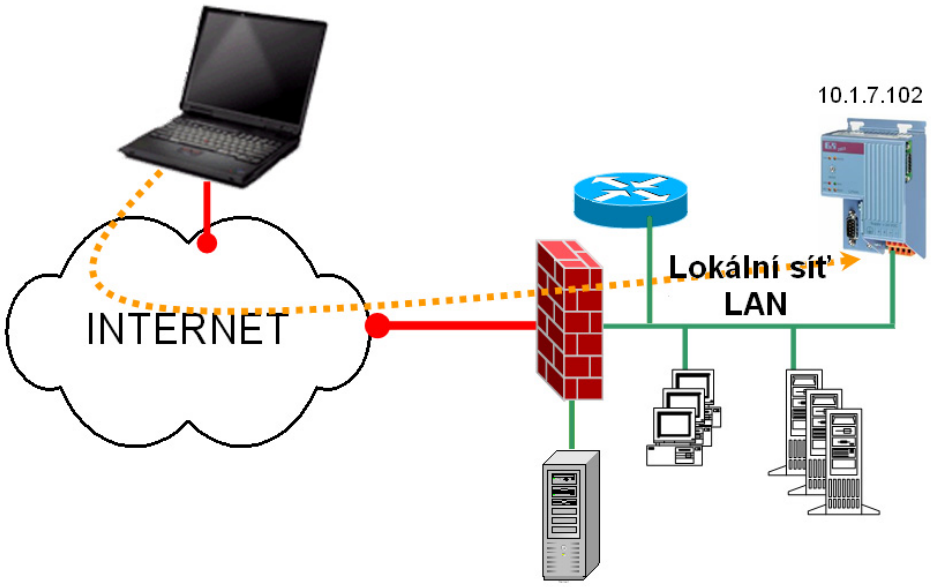
Proto se budeme zabývat spíše druhým rozhraním tiskového stroje, a to rozhraním Ethernet. Toto rozhraní má mnohem větší datovou prostupnost.



Obrázek 11 - Propojení v rámci LAN sítě
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

Na tomto obrázku 11 je vidět, jak vypadá ideální situace. Počítač, který komunikuje s PLC automatem B&R, není připojen přes síť Internet, ale je připojen pomocí speciální přípojky určené pouze pro něj, což

je možné třeba v rámci jedné firmy nikoli na velké vzdálenosti, proto tento návrh neodpovídá situaci, kterou jsem se rozhodl řešit v tomto materiálu. Tímto tuto možnost zavrhuji a trochu ji poupravíme pro naše využití.



Obrázek 12 - Propojení s využitím Internetu
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

Zde na obrázku 12 je vidět, že komunikace prochází již Internetem a díky tomu se může uskutečnit přenos informací i na velké vzdálenosti s využitím komunikačních cest Internetu.

6.2 Firewally

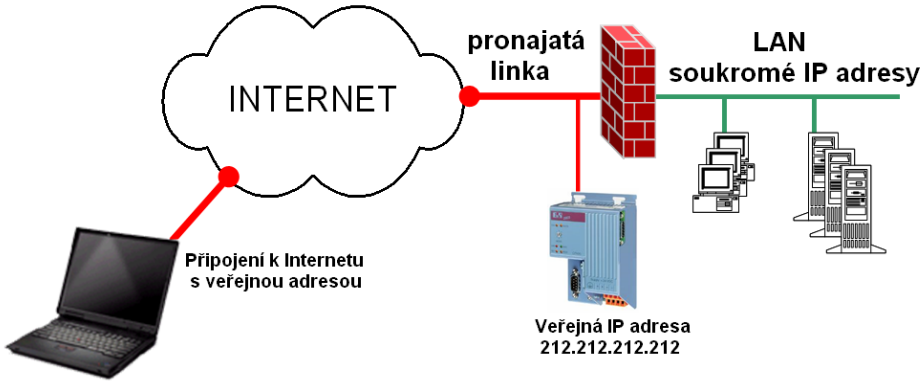
Je to ve své podstatě soupis pravidel, podle kterých se má postupovat, pokud jde o síťovou komunikaci. Firewally jsou buď hardwarové nebo softwarové. Hardwarové firewally jsou umisťovány mezi server a poskytovatele Internetu. Kdybychom Firewally umístili až za server, internetoví útočníci zvenku by se na server mohli dostat. Zato softwarový Firewally je nainstalován přímo na serveru.

Pravidla se píší pomocí jednoduché logiky. Vyhovuje paket první podmínce? Pokud ano, je určen i postup, jak s ním naložit. Když nevyhovuje, porovnáme ho s dalším pravidlem. Nastane-li situace, že paket nenajde podmínku, je zahozen. Pokud je seznam pravidel prázdný, máme 100% jistotu, že se k nám na server nikdo nedostane, ale problém je v tom, že se nikdo nedostane ani na Internet.

6.2.1 Možnosti propojení uzlů za pomocí Internetu

Další řešení nabízí možnost připojení automatu přímo do sítě Internet s veřejnou adresou (obrázek 13). Problém je v tom, že by se poskytovatel musel přizpůsobit IP adrese automatu, jelikož automat má několik předem nastavených adres.

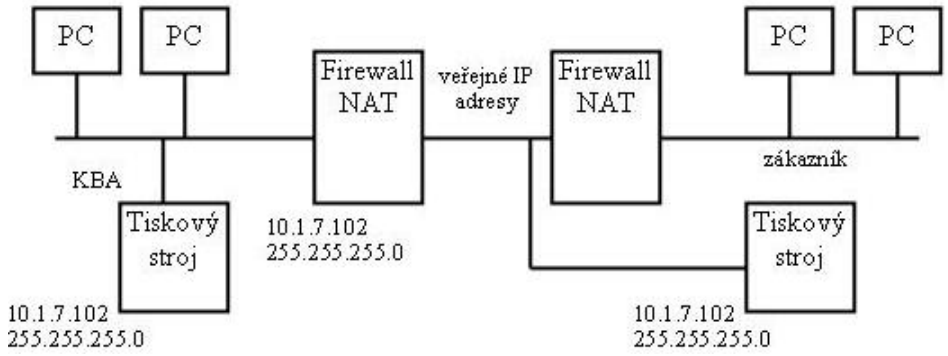
Druhým problémem je, že s automatem by mohl komunikovat kdokoli, kdo by znal jeho IP adresu, proto je zde nepřípustné bezpečnostní riziko.



Obrázek 13 - Nezabezpečené připojení
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

Obrázek 13 ukazuje možnost připojení tiskového stroje přímo do Internetu. Tato možnost je jednoduchá, ale jako taková nemá využití, protože data procházející Internetem nejsou nijak zabezpečena a hrozil by tak útok z Internetu. Detailní popis je na obrázku 15. Podmínkou je,

že nám poskytovatel musí přidělit jednu z určených IP automatu B&R, protože IP adresy na tiskovém stroji jsou hardwarově nastavitelné.



Obrázek 14 - Nezabezpečené připojení k Internetu

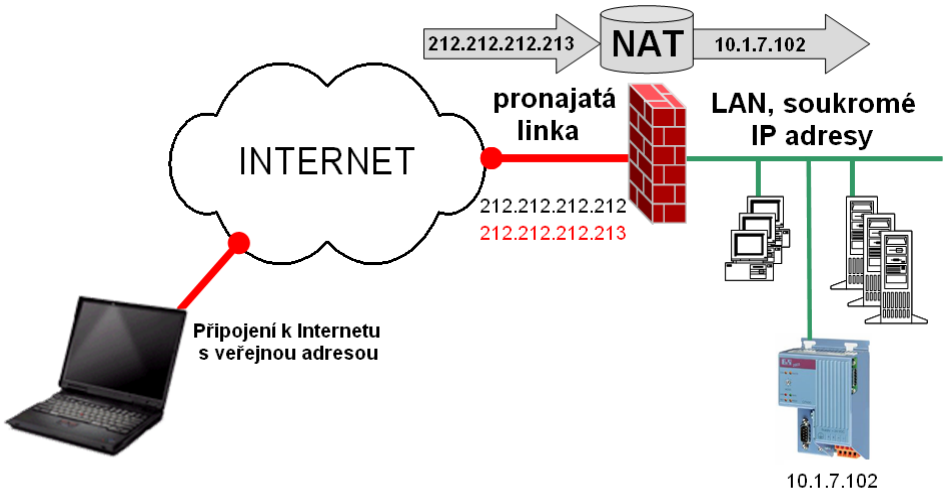
Tento způsob nepožaduje po zákazníkovi žádné speciální nastavení. Jeho server ani lokální síť se nezmění (obrázek 14), na serveru v KBA je pouze potřeba povolit porty pro FTP (20, 21) a RPC (111) a ICMP.

6.2.2 NAT překladač adres

Představme si, že máme poskytovatele připojení, který nám přidělil jednu veřejnou IP adresu, ale potřebujeme připojit větší množství počítačů. Veřejnou adresu přidělíme routeru a všem počítačům přidělíme lokální IP adresy. NAT (Network address translation) překladač na routeru způsobí, že všechny pakety putující do Internetu budou mít IP adresu routeru a všechna komunikace bude zpátky směřovat na router, který podle NAT tabulky jistí, který počítač ze sítě vyslal požadavek a kam má tudíž přeposlat odpověď.

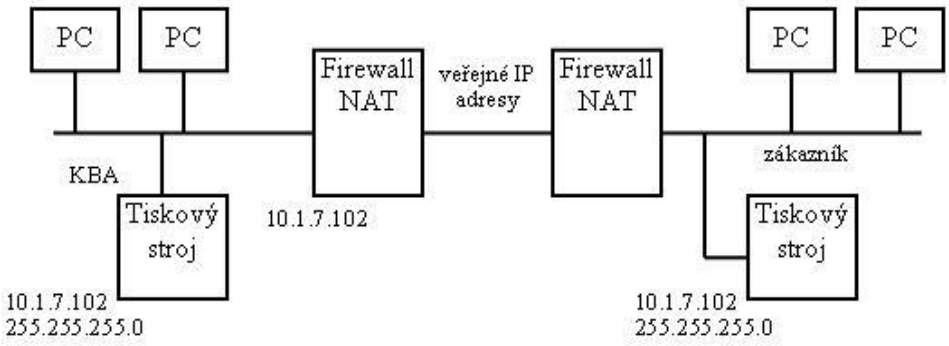
6.2.3 Použití NAT

Zde je vidět možnost připojení automatu za firewallem (obrázek 15), který má k dispozici dvě veřejné IP adresy. První z nich funguje pro běžnou práci celé lokální sítě pro přístup k Internetu a přístup například z Internetu k webovému serveru.



Obrázek 15 - Překládání druhé IP adresy
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

Druhá funguje výhradně pro potřeby automatu a komunikaci s ním. Překladač NAT přeloží druhou adresu na adresu automatu a ten pak může bez problémů komunikovat. Problém je v tom, že zřízení další veřejné adresy je neekonomické a v dalších variantách se objeví lepší možnost.



Obrázek 16 - Propojení se stávající LAN sítí

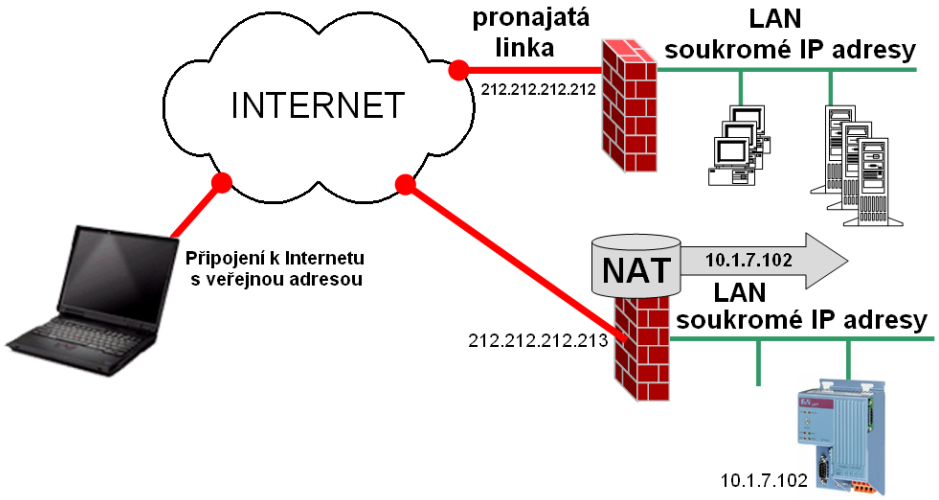
V této variantě je tiskový stroj připojen už na straně serveru, je umístěný za server (obrázek 16), to stroj chrání proti přímému napadení. Poněvadž ale požadujeme komunikaci tiskového stroje s Internetem, musíme na firewallu a překladači adres nastavit příslušné podmínky.

Firewall nastavíme tak, aby propustil pakety směřující na tiskový stroj, jde-li o porty ICMP, FTP a RPC. Překladač adres zůstane stejný pro

firemní účely, takže rozsah adres 192.168.1.1 až 192.168.1.254 bude překládat směrem do Internetu a zpět. Pokud ale přijde paket s IP adresou na druhou veřejnou IP adresu, přeloží ji na adresu automatu B&R a zpět.

6.2.4 Dvě nezávislé sítě

Opět použití dvou IP adres, kde ovšem nedochází k překladu adresy na jednom firewallu, ale obě veřejné IP adresy mají svůj vlastní firewall, a díky tomu je zaručeno, že jakákoli komunikace s automatem nebude nijak rušit lokální síť ani nezpůsobí sebemenší bezpečnostní mezeru ve stávající lokální síti, protože ta zůstane stejná (obrázek 17).



Obrázek 17 - Nezávislá síť
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

Pouze vedle ní vznikne další lokální síť, ve které bude kromě routeru připojen pouze automat nebo automaty, pokud jde o vlastníka více těchto zařízení. Nákladné, ale optimální řešení v rámci bezpečnosti sítě.

6.2.5 Virtuální počítačové sítě VLAN

V devadesátých letech nastává výrazný přesun od sdílených technologií LAN k přepínaným řešením na bázi přepínačů. Použití přepínačů umožňovalo pružnější segmentaci a dělení LAN do samotných segmentů.

Takto koncipované sítě mají vyšší datovou propustnost a umožňují filtraci provozu na mikrosegmenty sítě.

Při rozsáhlých sítích (nad 200 počítačů) dochází při intenzivním vysílání broadcast ze strany protokolů vyšších vrstev, k zahlcení sítě neboli tzv. broadcast bouřím (broadcast storm). Na jejich eliminaci byly původně používány routery propojující segmenty na úrovni síťové vrstvy.

Navrhovaným řešením pro eliminaci těchto nedostatků přepínaných sítí je technologie virtuálních počítačových sítí VLAN (Virtual Local Area Network). Virtuální počítačová síť je chápána jako samotná skupina počítačů logicky definovaná v rámci přepínané sítě nezávisle na jejich fyzickém uspořádání.

Dominantní vlastností virtuálních sítí je, že každá má svou samostatnou broadcast doménu. V síti s režimem VLAN mohou přímo komunikovat jen počítače ve stejné virtuální síti. Při filtraci broadcast provozu jsou virtuální sítě navrhované i za účelem:

1. zvýšení bezpečnosti komunikace
2. vyšší propustnosti
3. propojení počítačů nezávislé na fyzickém umístění v síti
4. jednodušší změny v rámci infrastruktury sítě při pohybu uživatelů

6.2.6 Vytváření VLAN

Virtuální počítačovou síť definujeme jako samostatnou logickou skupinu počítačů, které tvoří broadcast doménu. Podle způsobu definice počítače k síti rozdělujeme přiřazení prostřednictvím:

1. Portů přepínačů – na každém z portů přepínačů definujeme jeho příslušnost k určité virtuální síti. Nevýhodou je, že daný port může patřit pouze jedné virtuální síti, pokud se za tento port vloží hub, jsou všechny jeho počítače ve stejné VLAN.
2. MAC adres – virtuální síť je definovaná pomocí logické skupiny zvolených MAC adres. Nevýhodou takovýchto sítí je degregace datové propustnosti na portech s opakovači, nepříjemné je i používání různých síťových adaptérů s různými MAC adresami.
3. Síťové vrstvy – tato síť je tvořena pomocí identifikátorů vyšších vrstev, resp. síťové adresy vybraného síťového protokolu. Přepínače musí identifikovat příslušné informace již na úrovni síťové vrstvy, přičemž však nezabezpečují plnohodnotně směrování jako směrovače.
4. Skupinových (multicast) adres – přiřazením skupinových adres definovaným virtuálním sítem. I zde se jedná o použití vyšší vrstvy, proto takto definované sítě VLAN jsou protokolově závislé. Na vytváření virtuálních sítí se aplikuje zejména standard IEEE 802.1q.

6.2.7 Standardizace sítí VLAN

Virtuální počítačové sítě byly původně vytvářeny firemním způsobem, který byl implementován na přepínačích daného výrobce. Snaha o vytvoření otevřených komplexních řešení si později vyžádala standardizaci virtuálních sítí, aby mohly být vytvářeny VLAN i na přepínačích různých výrobců. Postupem času byly vyvinuty dva standardy.

IEEE 802.10 je standard řešící problematiku bezpečnosti komunikace v sítích LAN / MAN, který později pro potřeby virtuálních sítí upravila firma Cisco. Řešení vychází z protokolu ISL (Inter Switch Link Protocol), který vkládá dodatečné informační záhlaví do paketů posílaných mezi Cisco přepínači. Z identifikace záhlaví přepínač určí, ke které VLAN paket patří, z paketu odstraní část záhlaví a původní rámec odešle

na porty příslušející k identifikované virtuální síti. Z důvodů otevřenosti a akceptace ze stran ostatních výrobců byl systém firmy Cisco uveden do standardu IEEE 802.10.

IEEE 802.1q – představuje plnohodnotný standard pro vytváření VLAN, který vypracovala komice IEEE 802.1 (Internetworking Sub-committee) podobně jako standard pro transparentní bridging IEEE 802.1d.

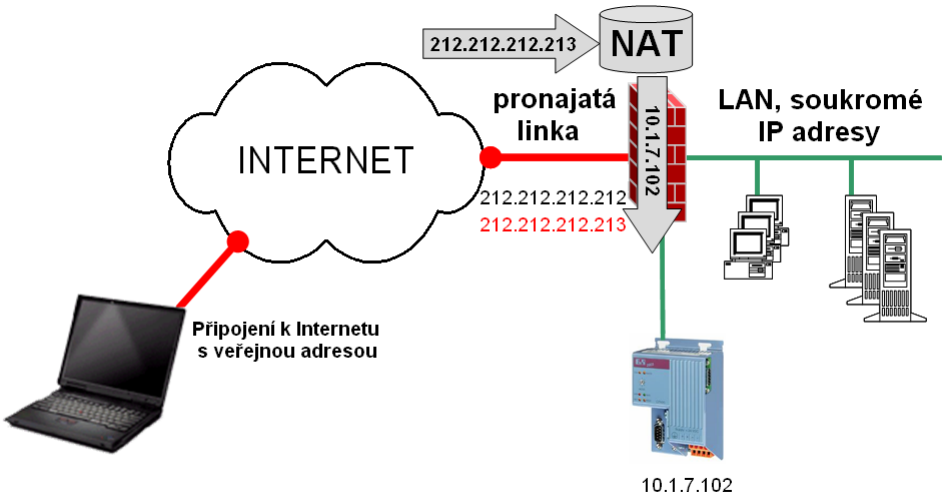
Na rozdíl od IEEE 802.10 byl vypracován za účelem identifikaci sítě VLAN v přenášených paketech, ale také definuje celkovou architekturu virtuálních sítí. Předpokládalo se, že tento standard bude dominantní pro implementaci VLAN.

6.2.8 Komunikace v prostředí VLAN

Z vlastnosti VLAN vyplývá, že přímá komunikace mezi počítači rozdílných virtuálních sítí není možná. Na její zabezpečení jsou potřeba doplňkové mechanismy. V praxi jsou problémové komunikace:

1. peer-to-peer
2. ve vztahu k celopodnikovým centrálním serverům a službám

Zde je požadována konektivita všech počítačů v rámci sítě. Na jejich zabezpečení jsou využity funkce síťové vrstvy a směrování na základě přiřazených síťových adres. Komunikaci potom zabezpečuje vyhrazený směrovač, který je připojen na každou z definovaných VLAN. Virtuální sítě jsou efektivní, pokud 80% komunikace je v rámci sítě.



Obrázek 18 - Překladač druhé adresy bez přístupu z LAN
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

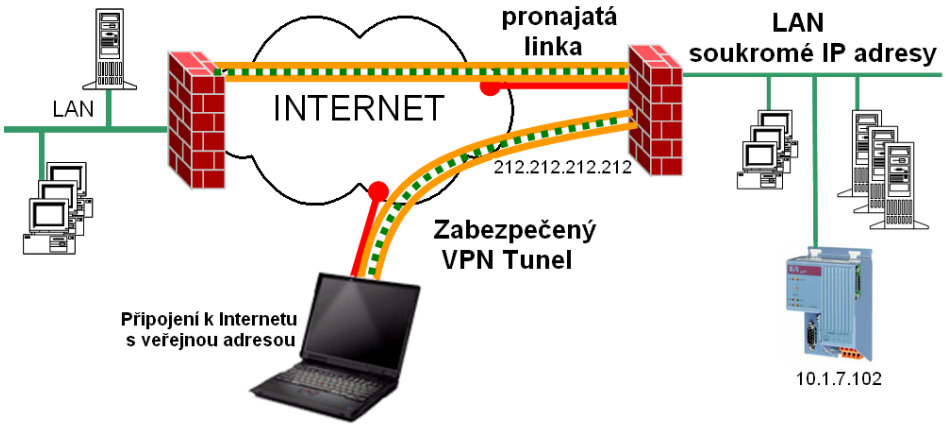
Na obrázku 18 je vidět použití dvou IP adres, ale automat je připojen přímo na firewall. To způsobí, že komunikace s automatem nebude brzdit místní lokální síť, ale LAN síť nebude mít přístup k automatu B&R.

Ale při ohledu na to, že po lokální síti se komunikuje rychle a propojení tak bude brzdit připojení od firewallu k ISP, je tato možnost zbytečná, v ničem nám výrazně nepomůže, spíše uškodí.

Z obrázku je patrné, že tiskový stroj je připojen přímo na další síťové rozhraní serveru. V praxi lze tuto situaci realizovat za pomocí VLAN. První skupinu VLAN budou tvořit firemní počítače. Druhou sítí bude automat B&R, protože jednotlivé sítě o sobě nevědí.

6.2.9 Použití VPN tunelu

Toto je nejbezpečnější propojení, které lze v daném okamžiku navrhnout. Oba servery společností mezi sebou vytvoří síť VPN (Virtual Private Network), která je sama o sobě zabezpečenou sítí, takže je obtížná infiltrace zvenčí (obrázek 19).

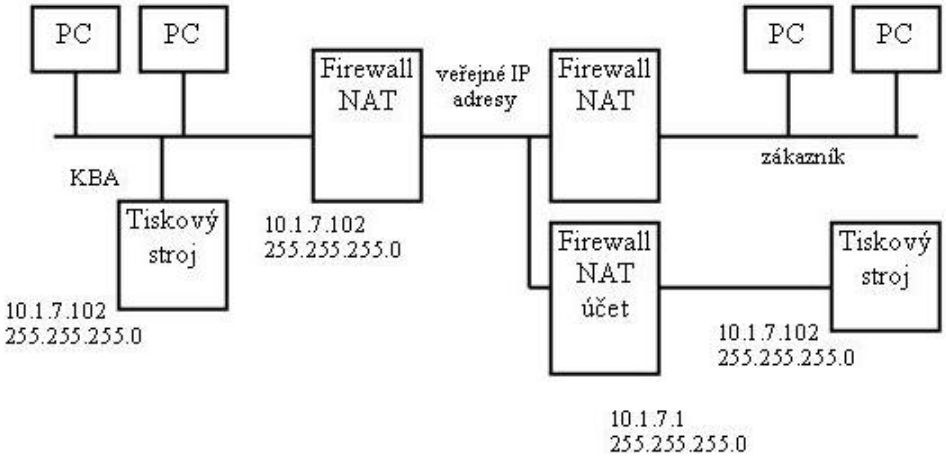


Obrázek 19 - Použití VPN tunelů
zdroj: "Údržba přes veřejnou síť" na Workshop B&R 2006

Toto spojení vytvoří šifrovaný tunel přímo mezi těmito počítači. To znamená, že data mohou jít po síti LAN nezabezpečena, jelikož se nepředpokládá napadení z vlastní sítě. Přechod přes Internet bude zabezpečen šifrovaným VPN tunelem a na druhé straně mohou být data opět nezabezpečena. Toto zabezpečení záleží na povaze aplikace a jejím návrhu a na možnostech automatu B&R.

Na straně vlastníka automatu se vytvoří na serveru účet s omezenými právy. Vytvoříme zabezpečený tunel například protokolem SSH nebo programem OpenVPN. Přihlásíme se k vytvořenému účtu a díky tunelu bude komunikace šifrovaná. Můžeme poté spustit aplikaci, která je nainstalována na serveru, třeba Firefox, který se k Internetu připojuje přes poskytovatele Internetu serverového počítače a také vidí danou lokální síť.

Pro jistotu můžeme vyzkoušet příkaz ping na náš automat B&R. Tímto připojením k serveru je zabezpečena komunikace s automatem, můžeme s ním začít komunikovat.

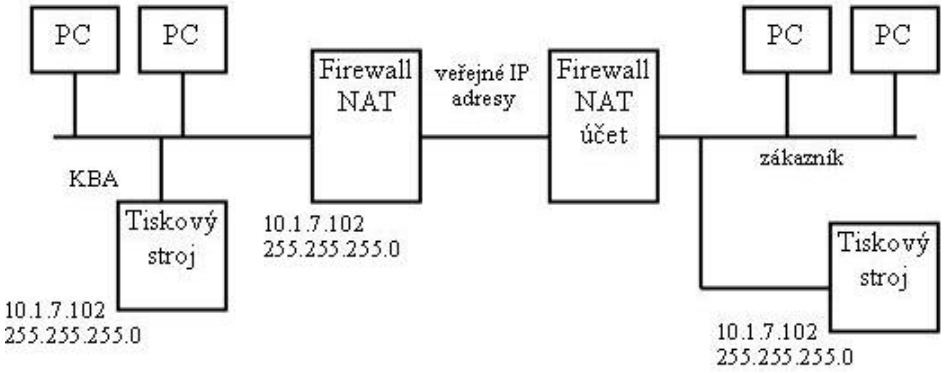


Obrázek 20 - Dvě IP adresy, 2 servery

Obrázek 20 ukazuje předchozí variantu nezabezpečeného připojení k Internetu rozšířenou o server, který bude obsahovat firewall, NAT a účet. Firewall a překladač adres budou opět propouštět protokoly ICMP, FTP, RPC, ale také v tomto případě port 22 pro SSH komunikaci, popřípadě ještě další pro správu PC.

Podstatou této možnosti je fakt, že se na účet s omezenými právy lze přihlásit šifrovanou službou (SSH) a tím bude komunikace zabezpečená proti napadení. Účet musí splňovat pouze podmínku, že po jeho přihlášení bude tiskový stroj dostupný.

Obrovskou výhodou je fakt, že se nijak nezasahuje do zákazníkovy lokální sítě. Nevýhodou však je pořízení druhé veřejné IP adresy a potřeba každému zákazníkovi instalovat server.



Obrázek 21 - Použití zákazníkova serveru

Tato varianta využívá opět zabezpečené připojení na účet, změnou je, že účet je vytvořen na serveru zákazníka (obrázek 21). Účet nám umožňuje pouze vzdálené přihlášení a přístup na tiskový stroj. Nastavení Firewallu zůstává stejné, jaké měl správce, je pouze rozšířeno o požadavky na přihlášení k účtu z Internetu, protokoly ICMP, FTP, RPC, SSH. Překladač adres přeloží adresu na adresu automatu. Popřípadě vytvoří tunel mezi specifickým portem serveru na tiskový stroj. Překlad ostatních firemních PC pro přístup k datům mezi sebou a Internetem zůstane zachován.

Tato varianta má výhody, že není potřeba druhá veřejná IP adresa a ani nutnost pořizovat k tiskovému stroji počítač. Nutnou podmínkou ale je možnost a ochota správce sítě vytvořit na serveru účet s danými právy.

6.3 První pokusy o přenos

Jelikož mám doma domácí počítačovou síť a potřeboval jsem být k ní připojen i z jiných míst, například ze školy, byl jsem nucen použít nějaký software, který by umožňoval přistupovat k počítači připojenému k Internetu stejně, jak kdyby byl na lokální síti. S veřejnou IP adresou by s tím nebyl sebemenší problém, ale rozhodl jsme se, že nebudu svému poskytovateli platit za nadstandardní službu, a tak jsem objevil program Hamachi. Po přečtení recenzí jsem jej odzkoušel a byl jsem mile překvapen. Tento program propojí počítače tak, že se chovají jako na lokální sí-

ti, rozdíl je pouze v omezení rychlost komunikace, která je odvislá od nejpomalejší části komunikační cesty nejčastěji mezi koncovým počítačem a poskytovatelem Internetu.

Program Hamachi vytvoří po nainstalování další virtuální rozhraní, přes které komunikuje za pomocí klientského programu. Jeho IP adresa je 5.x.x.x a díky této specifické IP adrese se může připojit k Proxy serveru, díky tomu je zabezpečena komunikační cesta mezi počítačem a sítí Internet. Chci-li se pak připojit na tento počítač, stačí mi připojit se na tento vzdálený Proxy server s dostatečným oprávněním. Toto oprávnění nám zajistí klient, po jeho spuštění se vytvoří popsaná komunikační cesta. V klientu nastavíme, ke které síti se chceme přihlásit a heslo sítě.

Veškeré sítě zde fungují jako VLAN a oddělují tak jednotlivé uživatele od sebe v rámci jedné lokální sítě. Každý z klientů může být zařazen současně i do více lokálních sítí. Komunikace mezi klientem a serverem je řešena zabezpečením RSA. Můžeme vytvořit vlastní novou síť, nebo použít již stávající. Princip je stejný jako virtuální sítě řešené pomocí routerů na lokální síti. Pokud se připojí současně minimálně dva počítače ze stejné sítě, mohou spolu komunikovat jejich běžící procesy a aplikace.

Toto řešení by bylo jednoduché a účinné, problém je v tom, že lze komunikovat pouze s počítačem, na kterém je klient nainstalován. Pro náš účel je ale potřeba komunikovat s automatem B&R. Aby byl automat přístupný, musel by se tento klient instalovat přímo na server. To by jeden problém vyřešilo, ale další je na snadě. Jelikož bychom chtěli instalovat cizí program na server, který je neustále připojen k Internetu, nemůžeme mít jistotu, že si výrobce nenechal nějaká „zadní vrátka“. Tím by se do systému dostal i někdo cizí bez znalosti hesla pro vstup a mohl tak narušovat bezpečnost. Proto jsem tuto možnost po dlouhodobém zkoumání vypustil.

7 Závěr

V úvodu popisuji vývoj Internetu, aby se dalo lépe pochopit propojení jednotlivých počítačů v různých lokálních sítích. Dále popisuji skupinu protokolů TCP/IP s ohledem na problematiku přenosu a jejich bezpečnost.

Samotný návrh začíná vysvětlením problematiky propojení dvou uzlů od prostého propojení v rámci sítě LAN po propojení pomocí Internetu. Pokračuji v popisu automatu B&R připojeného v lokální síti. Dále uvádím porty a protokoly automatu B&R používající mechanismu RPC. Následuje vysvětlení virtuálních sítí a Firewallu braného za nejdůležitější ochranu proti útokům z Internetu. V práci dále najdete některé možnosti připojení tiskového stroje k Internetu pro využití dálkové diagnostiky. K jednotlivým možnostem je uveden můj komentář a poté jsou uvedena dle mého názoru dvě nejlepší řešení.

Domnívám se, že propojení tiskového stroje Performa přes Internet pro účely dálkové diagnostiky je možné a výhodné. Proto doporučuji společnosti KBA - Grafitec, aby se této myšlenky nevzdávala.

Seznam použité literatury

[1]. HULÁN, Radek. *T-Mobile EDGE : průměrná rychlost, katastrofální ping* [online]. 22.2.2005 , 22.2.2005 [cit. 2007-05-01]. Dostupný z WWW: <http://radekhulan.cz/item/t-mobile-edge-prumerna-rychlost-katastrofalni-ping>.

[2]. *Bezpečně OnLine : Jak zločinci využívají Internet* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://www.bezpecneonline.cz/sekce1/s1026.htm>.

[3]. *CESNET2 : Topologie a technické řešení* [online]. [cit. 2007-05-01]. Dostupný z WWW: <http://www.cesnet.cz/provoz/technika.html>.

[4]. *Druhy počítačových sítí* [online]. 2.8.2005 [cit. 2007-04-08]. Dostupný z WWW: <http://referaty-seminarky.cz/druhy-pocitacovych-siti-isdn-lan-wan/>. ISSN 1802-422X.

[5]. EStránky.cz. *Internet a vše ostatní* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://www.internet.estranky.cz/stranka/pravidla-site>.

[6]. HÁDLIK, Marcel. *Jak funguje Internet : Protokoly TCP/IP a ISO OSI* [online]. 22.10.2006 [cit. 2007-04-07]. Dostupný z WWW: <http://www.pripojtese.cz/art_doc-B0FEA1D23FDA15BBC125720B0047BA3A.html>.

[7]. *Historie sítě ARPANET/Internet* [online]. 11 [cit. 2007-04-15]. Dostupný z WWW: <http://www.kyberpunk.org/historie_site_arpanet_internet>.

[8]. HLADÍK, Radek. *OpenVPN : VPN jednoduše* [online]. 11.10.2004 [cit. 2007-05-14]. Dostupný z WWW: <http://www.root.cz/clanky/openvpn-vpn-jednoduse/?SID=B2C8610523B5A570BFE833E72DC715F1>. ISSN 1212-8309.

[9]. HLADÍK, Radek. *OpenVPN : VPN jednoduše* [online]. 18.10.2004 [cit. 2007-05-14]. Dostupný z WWW: <http://www.root.cz/clanky/openvpn-vpn-jednoduse-2/>. ISSN 1212-8309.

[10]. Internet pro všechny. *Internet, připojení k němu a možný rozvoj : Historie a vývoj internetu* [online]. 22.3.2006 [cit. 2007-04-14]. Dostupný z WWW: <http://www.internetprovsechny.cz/clanek.php?cid=163>. ISSN 1801-1160.

[11]. Internet pro všechny. *Internet, připojení k němu a možný rozvoj : Internet a počítačové sítě* [online]. 13.3.2006 [cit. 2007-04-14]. Dostupný z WWW: <http://www.internetprovsechny.cz/clanek.php?cid=161>. ISSN 1801-1160.

[12]. KODÝTEK, Pavel. *Historie Internetu* [online]. 31.1.2006 [cit. 2007-04-15]. Dostupný z WWW: <file:///c:/+Skola/Bakal%C3%A1%C5%99ka/Historie%20Internetu.htm>.

[13]. *M. Bartošek. Krátce z historie Internetu. Zpravodaj ÚVT MU. ISSN 1212-0901, 1995, roč. V, č. 3, s. 10-13.*

[14]. MACNAR, Tomáš. *Sítový protokol TCP/IP* [online]. [cit. 2007-04-14]. Dostupný z WWW: <http://maturita.cz/referaty/informatika/tcp_ip.htm>.

[15]. MaR. *IP adresa* [online]. 15.8.2006 [cit. 2007-04-07]. Dostupný z WWW: <http://www.pripojtese.cz/art_doc-EBCC0973C740F991C12571CA0032AD14.html>.

[16]. MERUNKA, Mirek. *Jak funguje Internet po kabelovce* [online]. 18.6.2001 [cit. 2007-04-07]. Dostupný z WWW: <http://www.isdn.cz/clanek.php?cid=2982>. ISSN 1213-077X.

[17]. MUSIL, Marek. *Co je Internet* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/coToje.php>.

[18]. MUSIL, Marek. Druha faze *Internetu* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/2faze.php>.

[19]. MUSIL, Marek. *Funkcionalita Internetu* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/princip.php>.

[20]. MUSIL, Marek. Internet u nás [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/cr.php>.

[21]. MUSIL, Marek. Nulta faze *Internetu* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/0faze.php>.

[22]. MUSIL, Marek. Provoz Internetu [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/provozInternetu.php>.

[23]. MUSIL, Marek. Prvni faze *Internetu* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/1faze.php>.

[24]. MUSIL, Marek. Sluzby Internetu [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/sluzbyInternetu.php>.

[25]. MUSIL, Marek. *Vyvoj Internetu* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/myslenka.php>.

[26]. MUSIL, Marek. *Vyvoj site Internet* [online]. [cit. 2007-04-07]. Dostupný z WWW: <http://ihistory.webzdarma.cz/chap/vyvoj.php>.

[27]. NATURA. *Historie sítě ARPANET/Internet* [online]. 6.12.2004 [cit. 2007-04-14]. Dostupný z WWW: <http://cyberpunk.wz.cz/data/index2.php?second=historie/arpanet>.

[28]. PETERKA, Jiří. *Na počátku byl ARPANET* [online]. [cit. 2007-04-14]. Dostupný z WWW: <http://www.earchiv.cz/a95/a504c502.php3>.

[29]. PETERS, Guy. *Komunikace* [online]. 8.1.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://artax.karlin.mff.cuni.cz/~peters/konf.html#Bitnet>.

[30]. PETŘÍČEK, Miroslav. Stavíme firewall. Root.cz [online]. 18.12.2001 [cit. 2007-04-14]. Dostupný z WWW: <http://www.root.cz/clanky/stavime-firewall-1/>. ISSN 1212-8309.

[31]. PETŘÍČEK, Miroslav. Stavíme firewall. *Root.cz* [online]. 2.1.2002 [cit. 2007-04-14]. Dostupný z WWW: <http://www.root.cz/clanky/stavime-firewall-2/>. ISSN 1212-8309.

[32]. PETŘÍČEK, Miroslav. Stavíme firewall. *Root.cz* [online]. 8.1.2002 [cit. 2007-04-14]. Dostupný z WWW: <http://www.root.cz/clanky/stavime-firewall-3/>. ISSN 1212-8309.

[33]. *Počítačové sítě* [online]. [cit. 2007-04-14]. Dostupný z WWW: <http://maturita.cz/referaty/referat.asp?id=739>.

[34]. *Příručka správce sítě* [online]. [cit. 2007-05-01]. Dostupný z WWW: <http://www.nuc.elf.stuba.sk/lit/ldp/03/030-09.htm>.

[35]. Rave. *História siete Arpanet* [online]. 3.7.2006 [cit. 2007-04-08]. Dostupný z WWW: <http://cyberpunk.blog.cz/0607/historia-siete-arpanet-internet-cz>.

[36]. SOCHOREK, Radim. *GSM-slovník* [online]. 29.12.2006 [cit. 2007-05-02]. Dostupný z WWW: <http://www.sochorek.cz/archiv/slovniky/gsm.htm>.

[37]. ŠEVELOVÁ, Irena. *Využití internetu* [online]. 8.11.2006 [cit. 2007-04-07]. Dostupný z WWW: <http://www.pripojtese.cz/art_doc-A4C8E73E1F15F107C125721F0053232E.html>.

[38]. ViZ. *Jak funguje Internet?* [online]. 15.8.2006 [cit. 2007-04-07]. Dostupný z WWW: <http://www.pripojtese.cz/art_doc-F4872A028FAB492EC12571CA002D4D93.html>.

[39]. VOPAT, Vladimír. *IPv6* [online]. [cit. 2007-04-08]. Dostupný z WWW: <http://atm.felk.cvut.cz/mps/referaty/IPv6/VO/index.html>.

[40]. VRABEC, Vladimír. *Co bylo, než vznikl český Internet?* [online]. 13.8.2002 [cit. 2007-05-01]. Dostupný z WWW: <http://www.lupa.cz/clanky/co-bylo-nez-vznikl-cesky-internet/>. ISSN 1213-0702.

[41]. VRABEC, Vladimír. *Časová mapa českého Internetu* [online]. 13.2.1998 , 16.10.2002 [cit. 2007-05-01]. Dostupný z WWW: <http://www.lupa.cz/clanky/casova-mapa-ceskeho-internetu/>. ISSN 1213-0702.

[42]. VRABEC, Vladimír. *Pionýrské začátky českého Internetu* [online]. 10.9.2002 [cit. 2007-05-01]. Dostupný z WWW: <http://www.lupa.cz/clanky/pionyrske-zacatky-ceskeho-internetu/>. ISSN 1213-0702.

[43]. VRABEC, Vladimír. *Vítězná cesta TCP/IP* [online]. 27.8.2002 [cit. 2007-05-01]. Dostupný z WWW: <http://www.lupa.cz/clanky/vitezna-cesta-tcpip/>. ISSN 1213-0702.

[44]. Wikipedia. *Aloha* [online]. 16.5.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Aloha>.

[45]. Wikipedia. *ARPANET* [online]. 11.4.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/ARPANET>.

[46]. Wikipedia. *Asymetric Digital Subscriber Line* [online]. 20.5.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/ADSL>.

[47]. Wikipedia. *CESNET* [online]. 30.1.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/CESNET>.

[48]. Wikipedia. *E-mail* [online]. 24.2.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Elektronick%C3%A1_po%C5%A1ta>.

[49]. Wikipedia. *Enhanced Data Rates for GSM Evolution* [online]. 8.5.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/EDGE>.

[50]. Wikipedia. *Firewall* [online]. 24.4.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Firewall>.

[51]. Wikipedia. *General Packet Radio Service* [online]. 8.5.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/GPRS>.

[52]. Wikipedia. *Internet* [online]. 15.5.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Internet>.

[53]. Wikipedia. *Internet service provider* [online]. 14.4.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/ISP>.

[54]. Wikipedia. *IP adresa* [online]. 17.5.2007 [cit. 2007-05-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IP_adresa>.

[55]. Wikipedia. *ISDN* [online]. 15.4.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/ISDN>.

[56]. Wikipedia. *Kódový multiplex* [online]. 10.5.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/CDMA>.

[57]. Wikipedia. *Modem* [online]. 18.5.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Modem>.

[58]. Wikipedia. *Paket* [online]. 6.4.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Paket>.

[59]. Wikipedia. *Peering* [online]. 12.3.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Peering>.

[60]. Wikipedia. *Počítačová síť* [online]. 8.5.2007 [cit. 2007-05-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5#MAN>.

[61]. Wikipedia. *Relační vrstva* [online]. 11.5.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Rela%C4%8Dn%C3%AD_vrstva>.

[62]. Wikipedia. *RFC* [online]. 10.3.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/RFC>.

[63]. Wikipedia. *Sada protokolů Internetu* [online]. 18.5.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Sada_protokol%C5%AF_Internetu>.

[64]. Wikipedia. *Seznam čísel portů TCP a UDP* [online]. 6.4.2007 [cit. 2007-05-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Seznam_%C4%8D%C3%ADsel_port%C5%AF_TCP_a_UDP>.

[65]. Wikipedia. *Token ring* [online]. 25.3.2007 [cit. 2007-05-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Token_Ring >.

[66]. Wikipedia. *Unix* [online]. 8.5.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Unix>.

[67]. Wikipedia. *Usenet* [online]. 1.1.2007 [cit. 2007-05-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Usenet>.

[68]. ŽÍDEK, Lukáš. *Co je DNS a princip využití na Internetu* [online]. 4.10.2006 [cit. 2007-04-07]. Dostupný z WWW: <http://www.pripojtese.cz/art_doc-19D3C2A5C24AA842C12571FC004E8D7A.html>.

Seznam obrázků

Seznam tabulek

Seznam zkratek

ADSL	**A**symetric **D**igital **S**ubscriber **L**ine	je asymetrické připojení k Internetu, kdy rychlost pro stahování je vyšší než pro odesílání.
ALOHANET		je radiová síť ve které uzel odešle informaci, bez ohledu na stav sítě
ARPA	**A**dvanced **R**esearch **P**rojects **A**gency	společnost která vytvořila síť založenou na přepojování paketů bez centrální složky
ARPANET	**A**dvanced **R**esearch **P**rojects **A**gency **Net**work	síť ARPANET byla zárodkem dnešního Internetu, která byla spuštěna roku 1969 a odpojena v roce 1990.
B&R	**B**ernecker & **R**ainer	multinacionální podnik působící v automatizačním průmyslu
BITNET		je Evropská obdoba EARN, jedná se o mailovou konferenci neboli posílání totožného mailu více lidem
BSD	**B**erkeley **S**oftware **D**istribution	Společnost vytvářející distribuci Unixu označovanou BSD Unix
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess	je metoda digitálního multiplexování, příjmu více digitálních signálu v jednom zařízení
CESNET	**C**zech **E**ducation and **S**cientific **Net**work	Poskytovatel připojení i Internetu převážně pro akademická pracoviště
DARPA	**D**efense **A**dvanced **R**esearch **P**rojects **A**gency	Nový název společnosti ARPA

DNS	**D**omain **N**ame **S**ystem	umožňuje přidělovat jména počítačům, roku 1983 uveden do praxe. Převádí jméno na IP adresu a zpět.
EARN	**E**uropean **A**cademic and **R**esearch **N**etwork	síť která poskytovala pouze elektronickou poštu a přenos souborů
EDGE	**E**nhanced **D**ata rates for **G**SM **E**volution	další stupeň datové komunikace prostřednictvím GSM sítě
elektronická pošta	e-mail	je způsob pro odesílání a přijímání zpráv
firewall	český překlad "zeď "	je bezpečnostní síťový prvek zkoumající příchozí i odchozí pakety
Gopher		vyhledávací systém představen minnesotskou univerzitou
GPRS	**G**eneral **P**acket **R**adio **S**ervice	datový služba pro uživatele GSM telefonů
GSM	**G**lobal **S**ystem for **M**obile Communication	globální systém mobilní komunikace
IMP	**I**nterface **M**essage **P**rocessor	propojení počítačů různých typů s nekompatibilním hardwarem a softwarem
IP adresa		je adresou konkrétního zařízení v síti. V dané síti se nesmí objevit dvě shodné adresy.
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork	nabízí připojení k Internetu plně digitálním přenosem dat.

ISP	**I**nternet **S**ervice **P**rovider	je firma nebo organizace prodávající nebo poskytující přístup do Internetu a příbuzné služby. Někdy se používá termínu Internet access provider.
kladné potvrzování	positive acknowledgement	znamená že správně přijatá data se potvrdí a na chybná se nereaguje a tím se v zápětí vyšlou znovu
komutované spojení		vytáčené připojení po standardní telefonní lince
kontinuální potvrzování	continuous acknowledgement	je zde pro urychlení, pošle se několik paketů a mezitím přijdou odpovědi zda jsou v pořádku či nikoli
LAN	**L**ocal **A**rea **N**etwork	je síť propojující uzly v rámci jedné místnosti až několika budov
MAC adresa	**M**edia **A**ccess **C**ontrol	jedinečná adresa síťového prvku
mailing-list		je soupis všech adres na které má být odeslána zpráva
MAN	**M**etropolitan **A**rea **N**etwork	je síť spojující městské části, o rozlohách jednotek kilometrů
MD5	**M**essage-**D**igest algorithm **5**	hašovací funkce o velikosti 128 bitů
MILNET		síť propojující vojenská střediska oddělená od původního ARPANETu
NCP	**N**etWare **C**ore **P**rotocol	Předchůdce protokolů TCP/IP
NFS	**N**etwork **F**ile **S**ystem	internetový protokol pro vzdálený přístup k souborům
NSFNET	**N**ational **S**cience **F**oundation **Net**work	ARPANET byl vytlačen do pozice pouze páteřní sítě a roku 1990 byl plně zastoupen NSFNETem.

paket		je základní jednotkou přenosu informací v počítačových sítích.
páteřní síť		páteřní síť je velice rychlé propojení mezi nejdůležitějšími uzly hvězdicové struktury
PEERING		propojení několika poskytovatelů internetu kteří propojením získají razantní zrychlení v rámci jejich sítě
PLC	**P**rogrammable **L**ogic **C**ontroller	programovatelný logický automat
RFC	**r**equest **f**or **c**omments	je označení pro standardy popisující internetové protokoly
RPC	**R**emote **P**rocedure **C**all	vzdálené volání procedur
RSA	iniciály autorů **R**ivest, **S**hamir, **A**dleman	šifra s veřejným klíčem
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol	je sada protokolů sloužících k komunikaci v počítačových sítích. Protokol je soupis pravidel, určujících syntaxi a význam jednotlivých hesel při komunikaci
Time out		je čas po kterém se pakety prohlašují za ztracené
topologie		stavba sítě
UNIX	**U**nary **I**nformation and **C**omputing **S**ervice	jedná se o operační systém, který dokáže zpracovávat úlohy nezávisle a umožňuje přihlášení více uživatelů na jeden počítač
USENET		je síť která vytváří diskusní skupiny a umožňuje celosvětově nalézt uživatele se společnými zájmy

VPN	**V**irtual **P**rivate **N**etwork	virtuální linka mezi počítači
WAN	**W**ide **A**rea **N**etwork	je rozsáhlá síť spojující LAN a MAN sítě s působností po celé zemi nebo kontinentu o libovolné vzdálenosti
Wi-Fi	**Wi**reless **Fi**delity	Bezdrátové spojení pracující se standardy IEEE 802.11a, b, g
XDR	E**x**ternal **D**ata **R**epresentation	formátu externího vyjádření dat

ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	Využití sítě Internet pro přenosy datových paketů v rámci dálkové diagnostiky tiskových strojů
Autor práce	Miloš Falta
Obor	Informační technologie
Rok obhajoby	2007
Vedoucí práce	KBA - Grafitec Dobruška
Anotace	Cílem bakalářské práce je návrh síťového řešení propojení dvou sítí pro použití vzdálené diagnostiky tiskařských strojů s minimálními náklady a určitou mírou bezpečnosti
Klíčová slova	Historie Internetu, TCP/IP, Firewall, RPC, B&R, automat, PLC