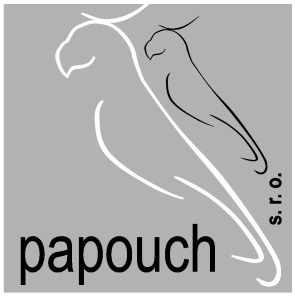
PAPOUCH s.r.o.

Datové komunikace, inteligentní měřící systémy
Soběslavská 15, PRAHA 3, tel: 267 314 268-9, 602 379 954



Důležité pojmy z oblasti počítačové sítě

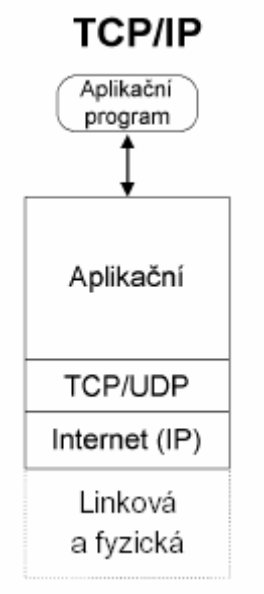
7.1.2003

ÚVOD

Tento práce vznikla na základě potřeby popsat některé důležité pojmy z oblasti počítačových sítí. Vzhledem k tomu, že naše firma má v sortimentu celou řadu zařízení právě určených k použití na Ethernet, je sepsání tohoto dokumentu více než vhodné. V dokumentu se nachází celá řada příkladů, které jsou aplikovány právě na našich výrobcích. Tato práce je určena jako vhodný doplněk k manuálům k našim výrobkům. V žádném případě nemá sloužit jako učební materiál, ale spíše jako dokument vysvětlující některé pojmy a postupy popsané v manuálech k našim zařízením.

1. Síťové protokoly

Síťový protokol je norma popsaná na papíře. V internetu se používají normy nazývané Request For Comments – zkratkou RFC: tyto dokumenty se číslují postupně od jedničky. V současné době jich je několik tisíc, ale mnohé postupem času již zastaraly. Problematika komunikace mezi počítači je rozdělena do více protokolů a do několika pomyslných vrstev síťového modelu TCP/IP (Obr.1). Každé této vrstvě odpovídají určité komunikační protokoly.



Obrázek 1 Síťový model TCP/IP

1.1. Jednotlivé vrstvy TCP/IP

1.1.1. Fyzická vrstva

Fyzická vrstva popisuje elektrické a optické signály, popřípadě bezdrátový přenos. Na fyzické vrstvě je vytvořen tzv. fyzický okruh. Na fyzický okruh mezi dvěma a více počítači mohou být dávána další zařízeni jako jsou modemy, směrovače, opakovače a mnoho jiných zařízení.

1.1.2. Linková vrstva

Linková vrstva zajišťuje v případě lokálních sítí výměnu dat v rámci lokální sítě. Základní jednotkou pro přenos dat je na linkové vrstvě datový rámec. Datový rámec se skládá ze záhlaví, přenášených dat a zápatí. V záhlaví nese linkovou adresu příjemce, linkovou adresu odesílatele, a další řídící informace. V zápatí nese obvykle kontrolní součet přenášených dat.

1.1.3. Internet protokol

IP protokol přenáší tzv. IP-datagramy mezi vzdálenými počítači. Každý IP-datagram ve svém záhlaví nese adresu příjemce (úplná směrovací informace pro dopravu datagramů k adresátovi). Síť může každý IP datagram Přenášet samostatně. Datagramy mohou k adresátovi dorazit v jiném pořadí než byly odeslány. Síťové rozhraní v síti Internet má svou celosvětově jednoznačnou IP-adresu. Jedno síťové rozhraní může mít více IP-adres, ale nesmí být dvě stejné IP-adresy pro různá síťová rozhraní.

Protokoly TCP a UDP

Protokol TCP dopravuje data pomocí TCP segmentů, které jsou adresovány jednotlivým aplikacím. Protokol UDP rozděluje data na tzv. datagramy. Protokoly TCP a UDP zajišťují spojení mezi aplikacemi, které jsou spuštěny na vzdálených počítačích.

TCP protokol je tzv. spojová služba (příjemce potvrzuje přijímaná data). Zajišťuje obousměrnou komunikační rouru (skládající se z páru socketů) mezi procesy, které běží na vzdálených počítacích.

Poznámka: Pár je tvořen adresou protokolu IP klienta, číslem portu klienta, adresou protokolu IP serveru a číslem portu serveru. Pojmy klient server jsou upřesněny v kapitole 2.

V případě ztráty si příjemce vyžádá zaslání ztraceného segmentu. Při použití tohoto protokolu je zapotřebí počítat s určitou režií, která je spojená s navázáním relace, bezpečným přenosem dat a ukončením relace mezi koncovými zařízeními. Přijatý proud dat rozdělí na segmenty ty očísluje kopii segmentu udržuje ve speciálním bufferu a pokud neobdrží potvrzení přijetí vyslaného segmentu vyšle tento segment znovu. Použitím tohoto protokolu pro přenos dat se stává tento přenos vysoce bezpečným, ovšem vzhledem k potvrzováním přijatých dat také podstatně pomalejším než je tomu u protokolu UDP.

UDP protokol obdobně jako TCP protokol přijímá proud dat od aplikací které jsou identifikovány svým číslem portu předá je nižší vrstvě kde je protokol IP převede na datagramy. Protokol UDP nepoužívá relace, je to nespojitý protokol, data nečísluje ani nijak nepotvrzuje jejich doručení. Kontrolu nad přijatými daty nechává převážně na uživatelských aplikacích. Odpadá tu také nutnost udržovat spojení v době, kdy nejsou přenášena data. UDP protokol není tak bezpečný jako TCP protokol, o to rychlejší.

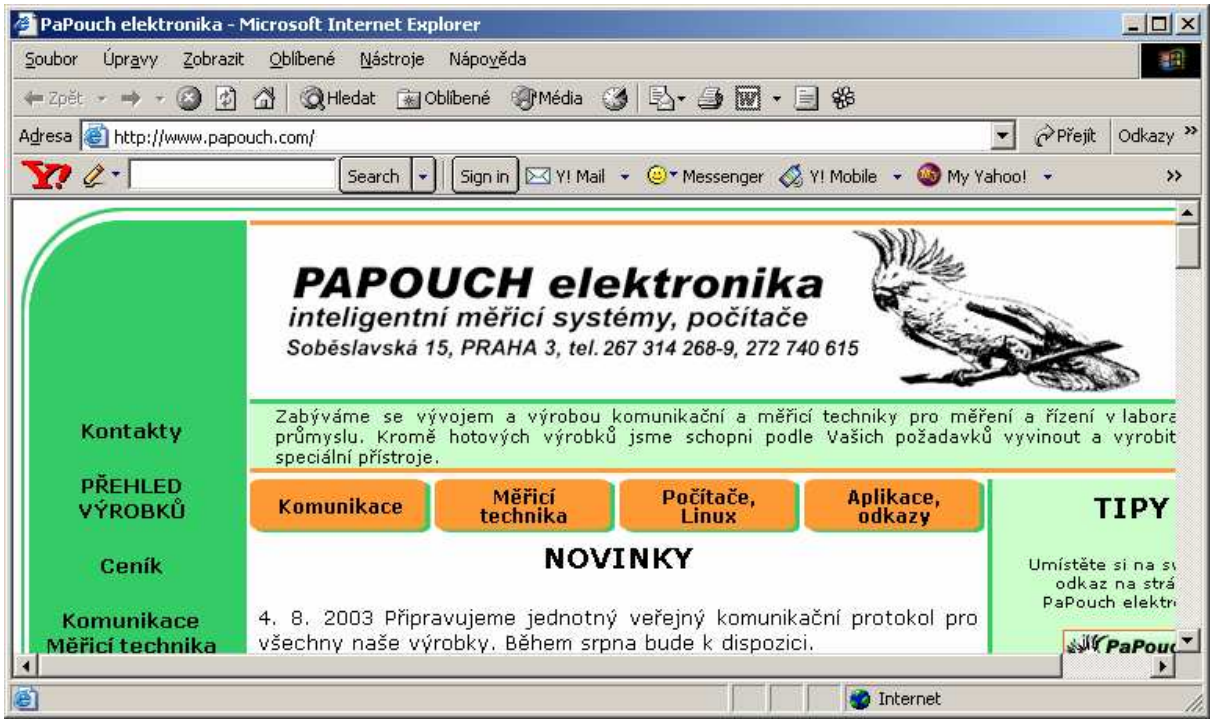
1.1.4. Aplikační vrstva

Aplikačních protokolů je velké množství. Jmenujme si aspoň některé. HTTP,Telnet a v neposlední řadě SNMP protokol.

Protokol HTTP

HTTP protokol pracuje většinou s portem 80. Pro komunikaci se používá tzv. URL adresa (cesta ke zdroji informací).

Příklad: www.papouch.com



HTTP zajišťuje komunikaci mezi prohlížečem a webovým serverem.Přenos HTTP je obousměrný, server může odeslat prohlížeči kopii vybrané stránky a prohlížeč může zase odeslat data na server. Prohlížeč a server si mohou spolu dohodnout určité technické údaje týkající se parametrů přenosu. HTTP podporuje také prostředníky. Počítač ležící mezi prohlížečem a webovým serverem může plnit roly proxy serveru.

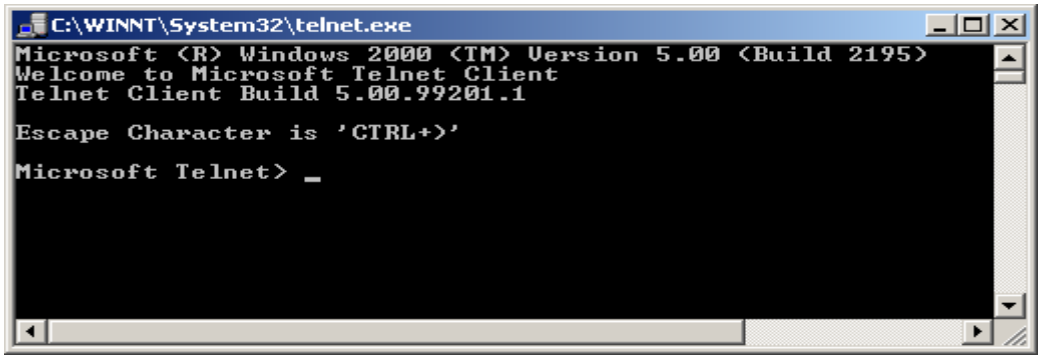
Proxy server umožňuje výměnu dat mezi uživatelskými agenty a originálními servery. Agent požaduje zaslání dokumentů uložených na originálním serveru. Relace HTTP je spuštěna při odesílání žádosti v prohlížeči. Spolehlivé doručení dat zajišťuje protokol TCP.

Telnet

Protokol Telnet dovoluje uživateli klientského terminálu terminálu připojit se k vzdálenému síťovému uzlu (nebo serveru Telnetu) prostřednictvím TCP/IP. Telnet pracuje se spojeními TCP (port serveru 23) a přenáší mezi terminálem a koncovým počítačem osmibitové znaky. Je navržen tak, aby mohl pracovat s libovolným počítačem a terminálem. Relace klient/server Telnetu je pro uživatele transparentní, takže uživatel má dojem, že pracuje přímo se vzdáleným počítačem. Výhodou implementace této služby je dostupnost klienta Telnetu takřka na každém počítači, takže odpadá shánění vhodného terminálu například pro nastavováni zařízení.

Příklad spuštění Telnetu a navázání spojení v operačním systému Windows

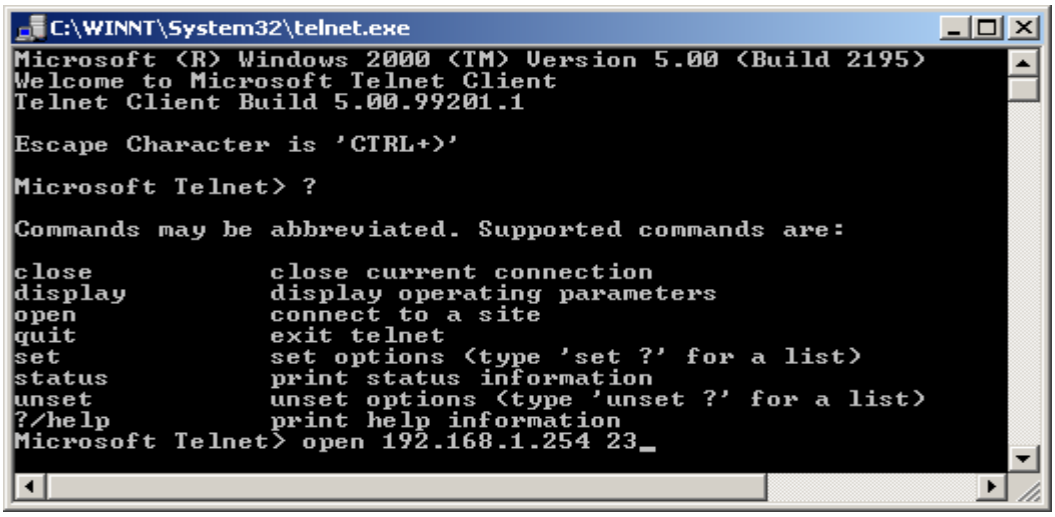
Příklad bude popsán na jednom našem zařízení které, má v sobě implementován Telnet server. Jestliže chce uživatel nastavovat přes Telnet, tak v nabídce start vybere položku spustit a do příkazového řádku zapíše Telnet a potvrdí enterem. Otevře se mu okno s Telnetem (Obrázek.3).



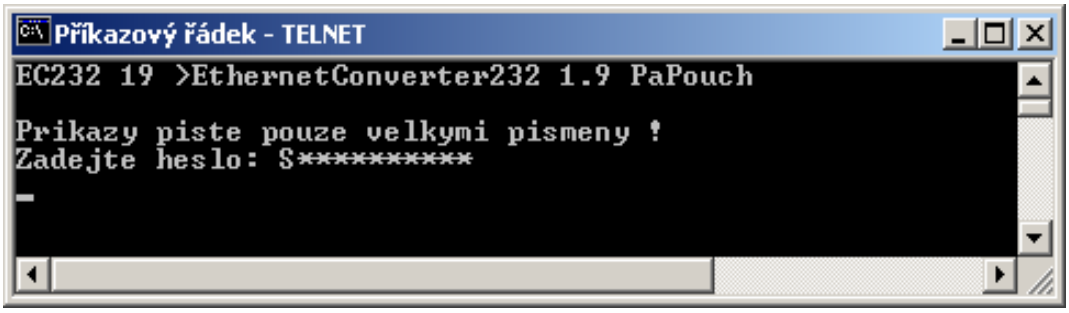
Obrázek 3. Otevření Telnetu z Windows

Nastavení Telnetu a navázání spojení s EC232

Nápovědu Telnetu uživatel vyvolá zapsáním otazníku a potvrzením enterem (Obrázek 4). Dále je potřeba zjistit zda má Telnet zapnuto zobrazování uživatelem psaných znaků tzv. LOCAL_ECHO. Jestliže ne tak je zapotřebí tuto funkci zapnout. Navázání spojení s převodníkem EC232 se provede tak, že do příkazového řádku za Microsoft Telnet> napíše uživatel „open mezera ip adresa převodníku mezera port 23 a potvrdí enterem" (Obrázek 4). Navázání spojení je vidět na obrázku 5. Po zadání hesla bude moci uživatel provádět veškerá nastavení EC232 pomocí instrukcí které jsou popsány v manuálu k EC232.



Obrázek 4. Nápověda Telnetu a způsob přihlášení



Obrázek 5. Okno Telnetu po navázání spojení

Bližší informace o možnostech nastaveni Telnetu jsou popsány v nápovědě k aplikaci Telnet.

Protokol SNMP

Jedná se o protokol určený pro správu sítě. Definice správy sítě není tak jednoduchá. Jedná se o monitoring stavu sítě v určitých bodech a vzdálenou správou těchto bodů předcházení, popřípadě eliminaci potíží vzniklých v síti.

Protokol SNMP se dá ovšem využít i jiným způsobem, například v automatizaci. Představme si tedy zařízení, který je připojeno (např. přes sériový port) k systému nebo zařízení, které má přístup do počítačové sítě s protokolem TCP/IP. Systém pak může prostřednictvím nějakého protokolu poskytovat systémům v počítačové síti informace o stavu snímané veličiny. A proč tedy nepoužít existující a v praxi používané prostředky pro síťový management včetně používaného protokolu SNMP (Simple Network Management Protocol)? Výhodné také je, že lze pro monitoring použít stávající systémy pro management sítě, které umí s pomocí protokolu SNMP realizovat sběr hodnot a reagovat na ně podle námi definovaných pravidel.

Protokol SNMP pracuje nad protokolem UDP a zajišťuje rychlé doručení řídících požadavků a odpovědí mezi počítači na kterých běží aplikace SNMP. Protokol SNMP má tři hlavní entity dovolující vzdálenou zprávu sítí:

Správce: Správce tvoří řídící software pro vzdálenou zprávu a monitorování agentů SNMP.Správce tvoří centrální bod zprávy mající uživatelské rozhraní, ze kterého jsou prostřednictvím SNMP doručovány příkazy agentům. Správci směrují požadavky na port UDP 161 agenta a naslouchají na portu UDP 162

Agenti: Agenti naslouchají požadavkům správců a odpovídají jim na požadavky.Mezi požadavky převážně patří údaje které mají agenti uloženy v místí databázi MIB. Agenti udržují databázi MIB, jejíž struktura je tvořena hierarchickým stromem všech spravovaných a monitorovaných objektů. Kromě reakce na dotazy lze agenta nastavit taky do stavu aby sami správce informovali o nastalých skutečnostech například chybových stavech. Agent zasílá tzv. Trapy.Trapy jsou nevyžádané informace zasílané agentem správci, který po jejich vyhodnocení provádí předem definované operace.

Proxy: Proxy SNMP zajišťuje předávání zpráv mezi agenty a správci, nebo jako prostředník mezi agenty, kteří využívají různé verze protokolu.

Databáze MIB

Každý agent má zřízenou databázi MIB. Jedná se o databázi objektů které, agent řídí popřípadě v kterých shromažďuje data. Název objektu, udávající umístění objektu, je vyjádřen jako série kladných celých čísel, popisujících cestu k objektu v rámci stromu MIB.

2. Důležité pojmy Ethernetu

Pojem TCP server TCP klient

TCP server: Jedná se o program kdy je v takzvaném pasivním režimu je sestaven socket, ale není inicializováno spojení s druhou stranou. Server naslouchá na určitém portu. Pokusí-li se klient přistoupit na daný port tak v tu chvíli dojde k inicializaci spojení. Proběhne-li inicializace úspěšně, otevře se tzv. roura (dojde k spárování socketu serveru a klienta) a může probíhat přenos dat.

TCP klient: Jedná se o program kdy je v takzvaném aktivním režimu. Je sestaven socket a TCP klient se pokouší sám iniciovat spojení s TCP serverem na portu na kterém server naslouchá. Proběhne-li inicializace s protější stanou v pořádku, dojde k navázání spojení, vytvoří se takzvaná roura a může dojít k přenosu dat.

Pojem Lokální IP adresa

32-bitové číslo jednoznačně určující počítač v lokální síti. Zapisuje v desítkové soustavě jako čtveřice bytů (0-255) oddělených tečkami (např. 192.168.1.254). Každý paket obsahuje informaci, odkud byl vyslán (zdrojová IP adresa) a kam má být doručen (cílová IP adresa).

Poznámka: Lokální IP adresa nemůže být viditelná z internetu je vždy za firevallem popřípadě za proxy serverem.

Pojem maska lokální sítě

Maska lokální sítě rozděluje IP adresu na dvě části: adresu sítě a adresu počítače v této síti. Maska se zapisuje stejně jako IP adresa (např. 255.255.255.0), ale je třeba ji vidět jako 32-bitové číslo mající zleva určitý počet jedniček a zbytek nul (maska tedy nemůže mít libovolnou hodnotu). Jednička v masce lokální sítě označuje bit adresy sítě a nula bit adresy počítače. Všechny počítače v jedné lokální síti musejí mít stejnou masku lokální sítě a stejnou síťovou část IP adresy.

Proxy server

Velmi rozšířený způsob sdílení internetového připojení. Proxy server představuje prostředníka mezi klientem a cílovým serverem.

Pojem firewall

Software nebo hardwarové zařízení, které chrání počítač nebo počítačovou síť před průnikem zvenčí (typicky z Internetu).

3. Ověření dostupnosti zařízení

Příklad dostupnosti zařízení je popisován na jednom našem z našich výrobku (EC232). Dostupnost zařízení je možné ověřit příkazem "PING". Spusťte okno konzoly a napište "PING x.x.x.x", kde x.x.x.x je IP adresa modulu EC232. Výchozí adresa převodníku je 192.168.1.254 . Příkaz PING odešle několik malých paketů na zadanou adresu a očekává jejich návrat od protějšího systému. Pokud druhá strana tuto komunikaci zachytí, pošle data zpět a tím potvrdí svou dostupnost. Na Obrázek6 je vystup příkazu PING při správné odpovědi od protějšího systému. Vidíte na něm čtyři téměř stejné po sobě jdoucí řádky které vypisuji údaje o správné odpovědi. Z řádků lze vyčíst čas, za který se každý z paketů dokázal vrátit od testovaného systému zpět. Čím je tento čas kratší, tím je přenos dat mezi systémy rychlejší, resp. pohotovější. Tato doba je závislá na rychlosti odezvy mezi jednotlivými prvky sítě na cestě mezi naším a vzdáleným systémem. Na době této odezvy také závisí i zpoždění dat mezi řídícím systémem a sériovou linkou RS232 na převodníku EC232. Na Obrázek 7. je výstup ("Vypršel časový limit žádosti.") stejného příkazu PING při odpojeném, tj. nedostupném zařízení.

Obrázek 6. Výsledek správně provedeného příkazu PING na IP adrese 192.168.1.254

Obrázek 7. Výsledek příkazu PING na IP adrese 192.168.1.254 bez odezvy od převodníku

4. Šifrování přenášených dat

Vzhledem k tomu, že se internet a počítačové sítě za posledních 10 let u nás staly fenoménem, který je nedílnou součástí takřka všech odvětvích činnosti lidského života. Často dochází k přenosu velmi důvěrných dat. Proto také vzniklo odvětví nazývané kryptografie(šifrování dat). Tento obor se zabývá konstrukcí šifrovacích algoritmů díky nimž se data stávají nedostupná pro ty kteří k nim nemají oprávněný přístup. Jsou vyvíjeny stále dokonalejší algoritmy pro zašifrování dat, kdy jejich dešifrování bez správného algoritmu je zhola nemožné, popřípadě velmi nákladné, kdy se tento proces nevyplatí. V dnešní době rozeznáváme: Symetrické šifry a kryptografické systémy s veřejným klíčem. Pokusím se velmi zjednodušeně vysvětlit rozdíl mezi těmito dvěma způsoby šifrování.

Symetrické šifry:

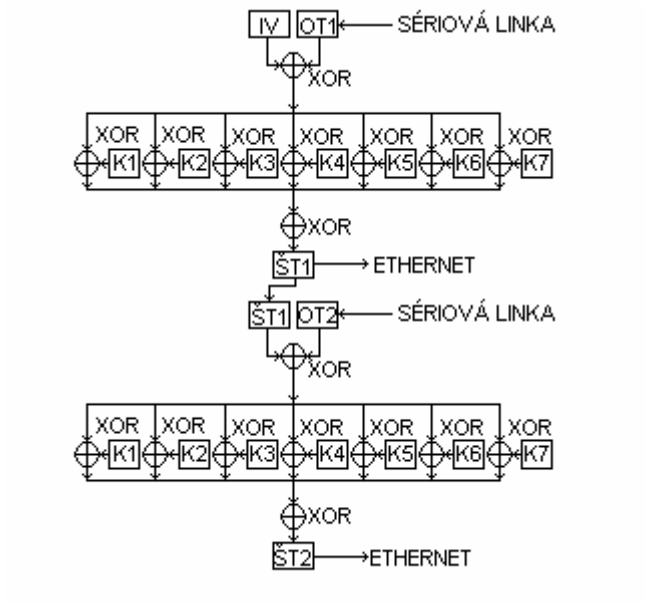
Jde o techniku šifrování, která pracuje se dvěma identickými klíči. Každý z nich lze využít jak pro zašifrování, tak i pro odšifrování. Pokud se zajistí, aby odesilatel a příjemce byli vybaveni těmito klíči (a neměl je nikdo jiný), lze symetrické šifrování využít zejména k zajištění důvěrnosti dat (bez potřebného klíče je nikdo třetí "neodemkne").

Kryptografické systémy s veřejným klíčem:

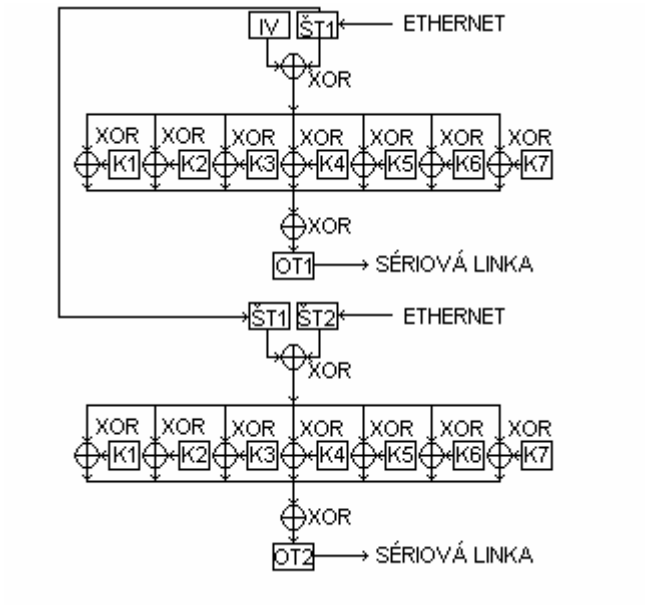
Jedná se o takzvané asymetrické šifry. Tyto šifry pracují se dvěma klíči: privátním klíčem a s klíčem veřejným. Obě strany, které spolu komunikují si navzájem vymění veřejné klíče těmi pak data šifrují. K dešifrování dat používají svůj soukromí klíč.

Způsob šifrování

Příklad způsobu šifrování je popsán na jednom z našich výrobků (EC232). Data modulu EC232 jsou šifrována symetrickou šifrou, která se řadí do skupiny blokových šifer. Jako předloha pro tvorbu šifrovacího algoritmu je použito blokové šifrování v módu CFB. Šifrování zprávy se provádí tak, že při otevření datového socketu převodníku se vyšle náhodně generovaný blok dat (inicializační vektor). Velikost inicializačního vektoru je dána velikostí šifrovaných bloků dat otevřeného textu. U převodníku EC232 se velikost bloku rovná jednomu znaku. Inicializační vektor se použije k zašifrování (XOR) prvního bloku dat otevřeného textu směřujícího do Ethernetu. Výsledek tohoto šifrování se dále šifruje (XOR) s jednotlivými znaky klíče. Tím vznikne sedm různých mezivýsledků, které se šifrují (XOR) v jeden jediný. Výsledek se použije jako šifrovaná data pro Ethernet a také k šifrování dalšího otevřeného textu. Blokové schéma algoritmu šifrování je na obrázku 19. Blokové schéma algoritmu dešifrování je na obrázku 20. ***IV*** je inicializační vektor, ***OT1*** a ***OT2*** jsou první a druhý blok otevřeného textu, ***ŠT1*** a ***ŠT2*** jsou dva bloky šifrovaného textu, ***K1*** – ***K7*** jsou jednotlivé znaky klíče zadaného uživatelem.



Obrázek 8. Algoritmus šifrování dvou bloků otevřeného textu



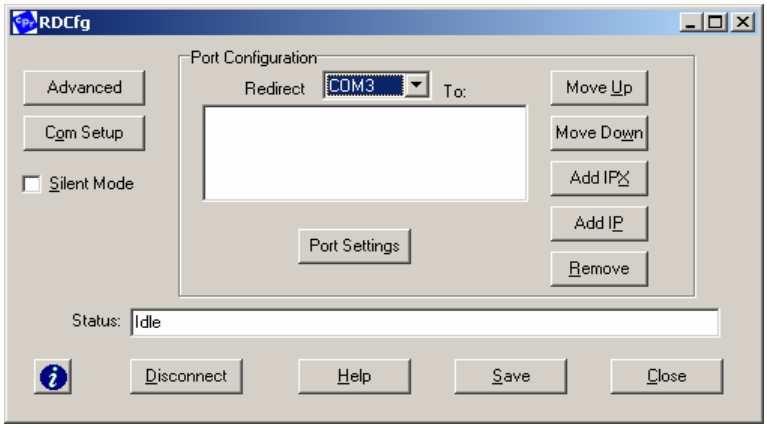
Obrázek 9. Algoritmus dešifrování dvou bloků šifrovaného textu

5. Virtuální COM

Jedná se o program, který přidá do operačního systému zdánlivý sériový port. Data, která byla na tento virtuální port zaslána z aplikace využívající tento port, jsou přesměrována na jiné hardwarová rozhraní (USB,Ethernet a jiné). Z pohledu aplikace se jedná o klasickou sériovou linku. Zde bych chtěl uvést jako příklad virtuální COM firmy lantronix. Jedná se o program který se z pohledu uživatele chová jako sériový COM a přitom data zasílá na Ethernet na předem zadanou IP adresu a port, ovšem pouze přes TCP. UDP tento program nepodporuje. Program se jmenuje Comport Redirector a stáhnout si ho můžete z adresy: ftp://ftp.lantronix.com/pub/redirector/ . Tento program také funguje s našimi Převodníky EC232 a EC485.

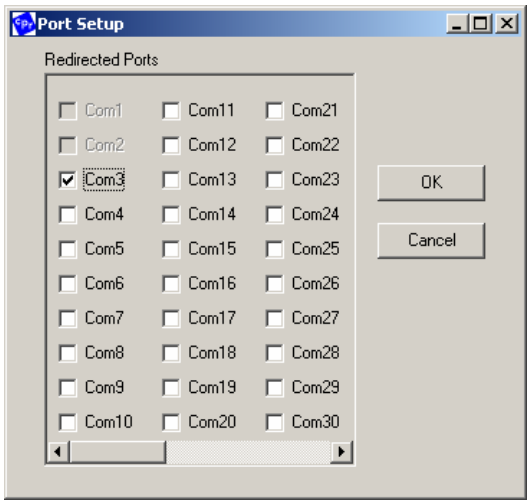
5.1. Instalace a nastavení Comport Redirectoru

Po stažení redirectoru a úspěšném nainstalování je zapotřebí restartovat počítač. K tomu vás ostatně vyzve i instalátor redirektoru. Po restartu počítače v nabídce Start\Programy\Lantronix Redirector je položka Configuration. Po spuštění této položky se otevře aplikační prostředí pro konfiguraci Comport Redirectoru (Obrázek 10).



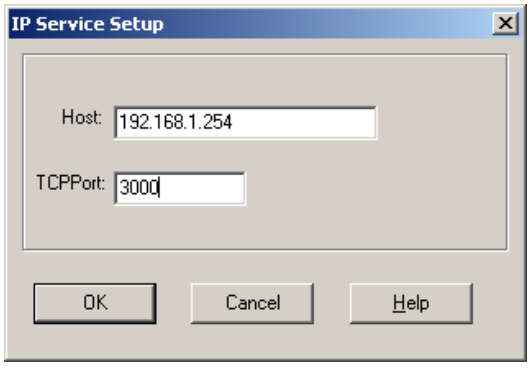
Obrázek 10 Konfigurační okno Comport Redirectoru

Stisknutím „Com Setup" otevřete okno, ve kterém vyberete jeden volný COM, ke kterému budete přistupovat při posílání dat z aplikace na Ethernet (Obrázek 11).



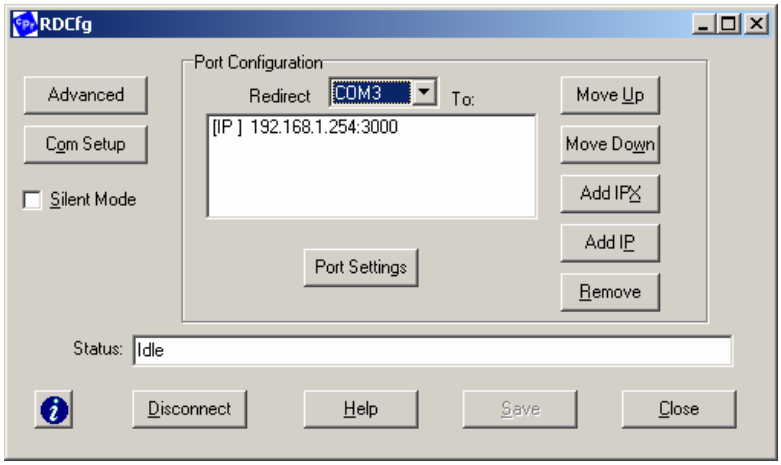
Obrázek 11 Okno pro volbu virtuálního COMu

Po potvrzení vybraného COMu se vrátíte do hlavního konfiguračního okna, ujistíte se, že v položce redirect je vybrán správný COM (Obrázek 10) a stisknutím „Add IP" nastavíte IP adresu a port zařízení, na které bude redirector data přesměrovávat (Obrázek 12). **Tento prográmek má ovšem malou záludnost a to tu, že přidává k zadanému portu u IP 11000. To znamená, že jestliže jsem nyní zadal, aby data byla posílána na IP 192.168.1.254 a port 3000, tak jsou ve skutečnosti odeslána na adresu IP 192.168.1.254 a na port 14000.** A proto, při konfiguraci je potřeba dávat pozor na jaký port ve skutečnosti jsou data posílána.



Obrázek 12 Okno pro nastavení IP adresy a portu

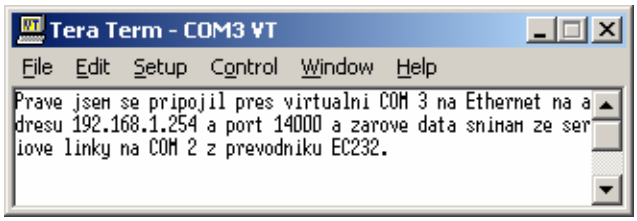
Po zadání IP adresy a portu a po návratu do hlavního okna by toto okno mělo vypadat tak, že by měl být zobrazen virtuální COM a IP adresa s portem na který virtuální COM směřuje data (Obrázek 13). Nastavení potvrdíte „Save".



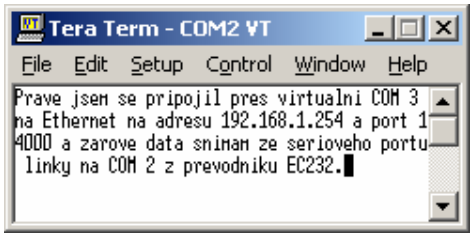
Obrázek 13 Okno s nastaveným virtuálním COMem

5.2. Spuštění aplikace

Po úspěšném nastavení virtuálního COMu si ukážeme jak tento COM funguje. Pro ukázku použiji jeden z našich výrobku (převodník EC232 dále popsán v manuálu k EC232 ver. 19). Převodník EC232 je modul přes který je možné posílat data ze sériové linky na Ethetnet a obráceně. Comport Redirector je podporován až od verze firmware 19 u EC232 a 15 u EC485. Máme–li převodník nastaven tak aby byla možná data přenášet pomocí virtuálního COMu (popis nastavení v manuálu k EC232 ver. 19) můžeme přejít k samotné komunikaci. Pro komunikaci jsem si vybral terminál Tera Term ke stažení na adrese: http://hp.vector.co.jp/authors/VA002416/teraterm.html. Otevřu si virtuální COM3 a druhé okno jako sériový port na COM2. V cestě mezi aplikaci s COM3 a COM2 je převodník EC232 . Po připojení (otevření virtuálního COMu) mohu posílat data z jedné strany na druhou (Obrázek 14,15).



Obrázek 14 Otevřená aplikace využívající virtuální COM



Obrázek 15 Aplikace přijímající data ze sériové linky