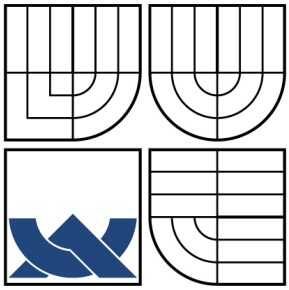
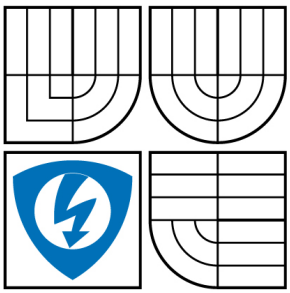


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ODOLNOST KOMUNIKAČNÍ JEDNOTKY LAN PROTI ÚTOKŮM Z INTERNETU

LAN COMMUNICATION UNIT RESISTIVITY AGAINST INTERNET ORIGINATION ATTACKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

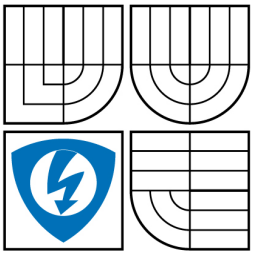
AUTOR PRÁCE — Bc. MICHAL VALACH

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. JIŘÍ MIŠUREC, CSc.

SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Michal Valach	***ID:***	83171
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Odolnost komunikační jednotky LAN proti útokům z Internetu

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s realizací komunikační jednotky pro dálkový sběr dat z elektroměru. Vytvořte programové nástroje pro testování odolnosti komunikační jednotky LAN vůči útokům ze sítě Internet. Proveďte sadu testů na odolnost útoků na komunikační jednotku. Vyhodnoťte dosažené výsledky. Navrhněte možnosti k zodolnění jednotky vůči útokům.

DOPORUČENÁ LITERATURA:

[1] Koutný, M.: Komunikační jednotka LAN. Diplomová práce VUT v Brně, FEKT, Ústav telekomunikací, 2006.
[2] Stuart McClure, Joel Scambray, George Kurtz: Hacking bez záhad. Grada, Praha 2007.

Termín zadání:	9.2.2009	***Termín odevzdání:***	26.5.2009

Vedoucí práce: doc. Ing. Jiří Mišurec, CSc.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ANOTÁCIA

Táto práca sa zaoberá kryptografickým modulom RCM 3700, ktorý slúži na prenos zašifrovaných dát. Rozoberám základné protokoly siete, typy útokov v sieti Ethernet, ktoré zisťujú informácie o danom zariadení, podporovaných službách a analýzujú prenášané dáta, následne sú prevádzané útoky na vyradenie prevádzky a snaha zneužitia dát. Ďalej je v práci zrealizovaná VLAN konfiguráciou smerovača CISCO 2801 na zvýšenie bezpečnosti v LAN. Pre kryptografický modul RCM 3700, ktorý pracuje na vývojovej doske, bola navrhnutá doska plošného spoja s resetom, napájacím obvodom a rozhraním pre RS 232 a celý modul je umiestnený do krabičky.

Kľúčové slová: DoS, DDoS, útoky v sieti Ethernet, TCP/IP, DHCP, SYN flood, RCM3700, RCM3000, RS 232, ARP

ABSTRACT

This thesis is focused on crypto-module RCM 3700, which is used for encrypted data transmission. Following work analyses basic network protocols and some sort of attacks in Ethernet network. The main goal of these attacks is to collect information and services about the device and to analyze transmitted data. Based on these information attacks can be done more precisely than without them. The main target of these attacks is the denial of particulary service or data abuse.

Furthermore, in the diploma thesis configuration of router CISCO 2801 is applied in order to improve the LAN security. The deveploment board, which includes reset function, supplied circuit and interface for RS 232, was designed for crypto-module RCM 3700.

Keywords: DoS, DDoS, attacks in Ethernet, TCP/IP, DHCP, SYN flood, RCM3700, RCM3000, RS 232, ARP

Bibliografická citácia mojej práce:

VALACH, M. *Odolnost komunikačni jednotky LAN proti útokům z Internetu* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 84 s. Vedúci diplomovej práce doc.Ing. Jiří Mišurec, CSc.

Prehlásenie

Prehlasujem, že svoju diplomovú prácu na téma " Odolnost komunikační jednotky LAN proti útokům z Internetu " som vypracoval samostatne pod vedením vedúceho diplomovej práce a s použitím odbornej literatúry a ďaľších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, a nezasiahol som nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomý následkov porušenia ustanovenia § 11 a následujúceho autorského zákona č. 121/2000 Sb., s možnými trestneprávných dôsledkov vyplývajúcích z ustanovenia § 152 trestného zákona č. 140/1961 Sb.“

V Brně dne …..…… ……..

(podpis autora)

Poďakovanie

Ďakujem vedúcemu diplomovej práce doc. Ing. Jiřímu Mišurcovi, CSc., za jeho užitočnú metodickú pomoc, cenné rady pri spracovaní mojej práce a za to, že mi umožnil sa na tak zajímavom projekte podielať. Rád by som tiež poďakoval svojej manželke a rodičom za podporu, ktorú mi dávali po celú dobu mojeho štúdia.

V Brně dne .....…… ……..

(podpis autora)

Obsah

Zoznam obrázkov

Zoznam tabuliek

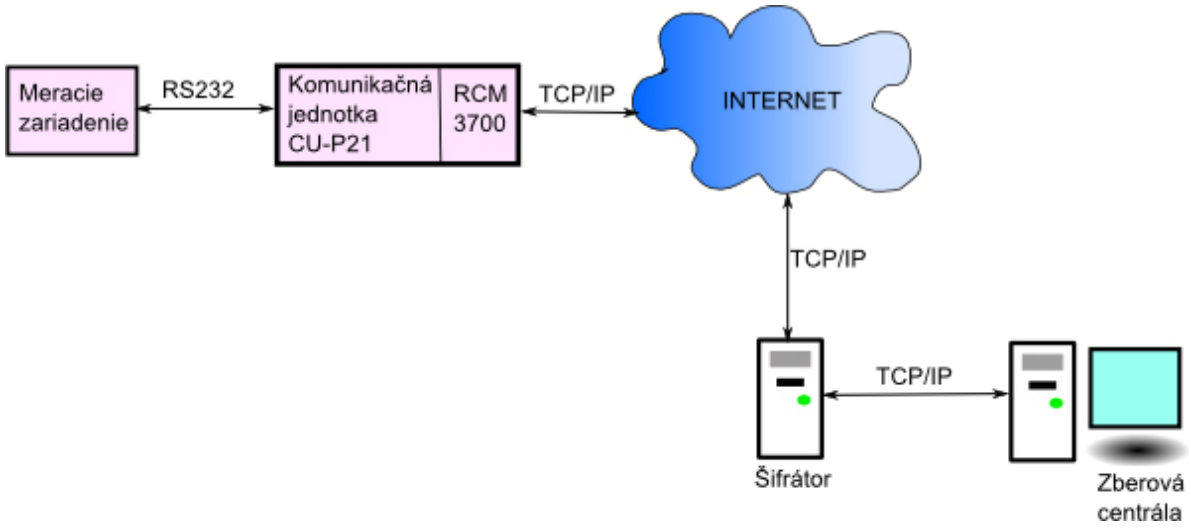
ÚVOD

V sústavách pre distribúciu tepla, vody, plynu alebo elektrickej energie je pre distribučnú spoločnosť dôležité poznať údaje o odberoch každého spotrebiteľa a o vlastných nákladoch. Vzhľadom k tomu že z pravidla ide o rozľahlé sústavy, sú odpočty z jednotlivých miest prevádzané poverenými pracovníkmi osobnou obchádzkou. To je časovo aj finančne náročné. Preto sa hľadajú možnosti ako odpočty zautomatizovať a zefektívniť. Jednou z možností je použitie komunikačnej jednotky s Ethernetovým prenosom dát. Každodenná realita dnešných komunikačných sieti spočíva v tom že sa prenášajú dôležite a verejnosti neprístupné informácie. Neautorizovaná prevádzka otvára dvere pre stratu dát alebo ich zneužitie. Pre zabezpečenie dát je nutné poznať ich cenu, dokázať ohodnotiť riziká a mať ochotu investovať do protiopatreniam. Bezpečnosť sa dá definovať ako zaistenie proti hrozbám, minimalizáciou rizík a komplex administratívnych, technických, logických a fyzických opatrení pre prevenciu a detekciu neautorizovaného využitia dát. Táto práca sa zaoberá základnými typmi útokov v sieti Ethernet ktoré zisťujú informácie o danom zariadení, podporovaných službách a analýzou prenášaných dát. Po zistení informácii sú prevádzané útoky na vyradenie prevádzky daného zariadenia.Virtuálne LAN sa realizujú aj koli bezpečnostnému hľadisku, preto som nakonfiguroval smerovač CISCO 2801 s podporou VLAN. VLAN zabraňuje útokom v rámci lokálnej siete. Kryptografický modul je programovateľný a realizuje svoju funkciu vďaka vývojovej doske, ktorá bola zakúpená s modulom, preto navrhujem v dalšej časti dosku plošného spoja pre RCM 3700 a pre vizuálny a ochraný charakter bude doska umiestnená do hliníkovej krabičky.

1 CIEĽ PRÁCE

RCM 3700 je kryptografický modul určený na prenos dát po sieti Ethernet. V laboratórii sa tento modul využíva na prenos zašifrovaných dát medzi elektromerom a zberovou centralou, ktorú tvorí PC s príslušným softwarom. Program pre modul je napísaný v jazyku dynamic C. Modul poskytuje zabezpečený prístup na web server pomocou SSL. Server slúži na základnú konfiguráciu modulu. Cieľom práce je zoznámiť sa s komunikačným modulom RCM 3700, na ktorom beží HTTPs server, komunikácia je šifrovaná pomocou šifry AES a je zapojený do vývojovej dosky, previesť sadu útokov z lokálnej siete, navrhnúť vhodné protiopatrenie a navrhnúť dosku plošného spoja pre daný modul a umiestniť do krabičky. V druhej kapitole podrobne rozoberám protokol TCP/IP, ktorý využíva aj modul RCM 3700 a znalosť TCP/IP je dôležitá na prevedenie niektorých útokov. V kapitole 3 sa zaoberám protokolom ARP, ktorý sa využíva na adresovanie v LAN na druhej OSI vrstve. Je nezabezpečený a dá sa zneužiť na odpočúvanie komunikácie. V ďaľších kapitolách sú realizované jednotlivé typy útokov. Kapitola 11 je o relizácii VLAN, ktorá je nakonfigurovaná z bezpečnostného hladiska a zabraňuje útokom z lokálnej siete. Od kapitoly 15 sa zaoberám modulom RCM 3700, Rabbit 3000 a samotným návrhom dosky plošného spoja

2 KOMUNIKAČNÁ JEDNOTKA



OBR.1 ZAPOJENIE KOMUNIKAČNEJ JEDNOTKY

Meracie zariadenie - predstavuje elektromer, ktorý meria odber a dodávku elektrickej energie.

CU-P21 - je komunikačná jednotka meracieho zariadenia predstavuje rozhranie medzi kryptografickým modulom a meracím zariadeniam. Rozhranie RS232 je využite na prepojenie zdroja dát s kryptografickým modulom, ktorý je pripojený do siete.

RCM3700 - kryptografický modul, ktorý prevádza rôzne zabezpečovacie techniky ako je šifrovanie AES alebo SSL.

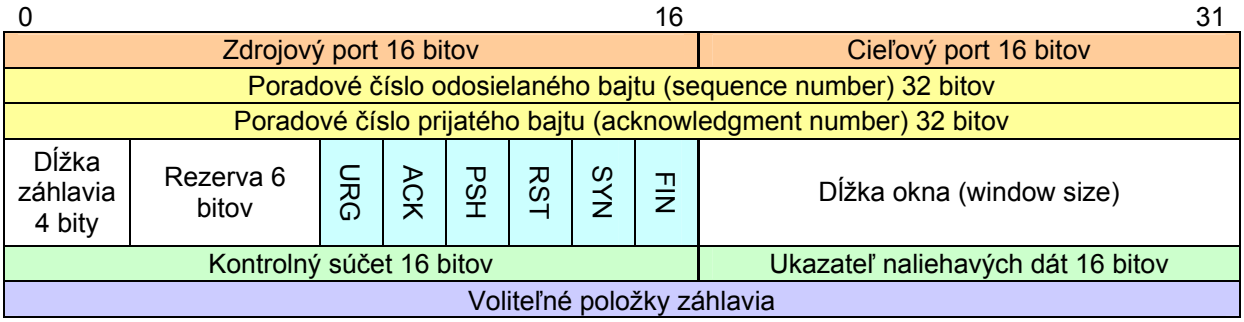
Šifrátor - zaisťuje kryptografické operácie na strane zberovej centrály, obojstrannou autentizáciou, šifrovanie a dešifrovanie dátového toku.

Zberová centrála - centrálny bod siete zaisťujúci zber dát. Zberová centrála môže pracovať v móde aktívnom, alebo pasívnom.

V pasívnom móde sa k centrále prihlasujú elektromery. V aktívnom móde centrála inicializuje spojenie a žiada elektromery o posielanie dát.[8]

3 TCP PROTOKOL

Protokol TCP zaisťuje spoľahlivé, spojovo orientované, plno duplexné spojenie. Tcp garantuje, že odoslané dáta sú protistranou kompletne prečítané a v rovnakom poradí ako boli vyslané tzn. že sú ošetrené chyby typu stratenia paketu, duplicitného paketu alebo v príchode paketu v nesprávnom poradí. Dátovej jednotke a úrovni transportnej vrstvy sa hovorí segment. Každý segment dát ma priradené svoje číslo seqencie (sequence number), ktoré protistrana potvrdzuje paketom ACK. Pokiaľ dôjde k strate paketu a vysielacia strana neobdrží potvrdenie o prijatí paketu, odošle data s príslušným číslom seqencie znovu.



OBR. 2 HLAVIČKA TCP PAKETU

Zdrovojvý port (source port)- 16 bitov, port odosielateľa TCP segmentu.

Cieľový port (destination port)- 16 bitov, port adresáta TCP segmentu.

Poradové číslo odosielaného bajtu (sequence numer-SEQ)- 32 bitov, odosielane bajty sa číslujú, pole obsahuje poradové číslo prvého z odosielaných v segmente.

Poradové číslo prijatého bajtu (acknowledgment number- ACK)- 32 bitov, pri obojstrannej komunikácii strana ktorá odosiela data, má možnosť v rámci hlavičky týchto dát potvrdiť prijatie dát od protistrany. Uvedie sa hodnota ďalšieho očakávaného bajtu, tj. napr. kde posledný správne prijatý bajt je číslovaný ako 200, pole obsahuje 201.

Dĺžka záhlavia (header length)- 4 bity, dĺžka záhlavia v bajtoch

Príznakové bity (flags)- 6 bitov, nastavených na „1“:

URG (urgent)- segment nesie naliehavé data, pre prednostné doručenie v rámci daného spojenia

ACK (acknowledgemnt)- indikuje, že hodnota uvedená v poli potvrdzovaného bajtu je platná

PSH (posh function)- signalizácia, že data majú byt ihneď po prijatí predané aplikácii a nemá sa čakať na prijatie ďalších segmentov

RST (reset the conection)- požaduje okamžité ukončenie spojenia

SYN (synchronize sequence number)- odosielateľ začína novu sequenciu číslovania bajtov, využíva sa pri nadväzovaní spojenia (segment neobsahuje data)

FIN (no more data from sender)- odosielateľ ukončil prenos dát, využíva sa pri uzatváraní spojenia

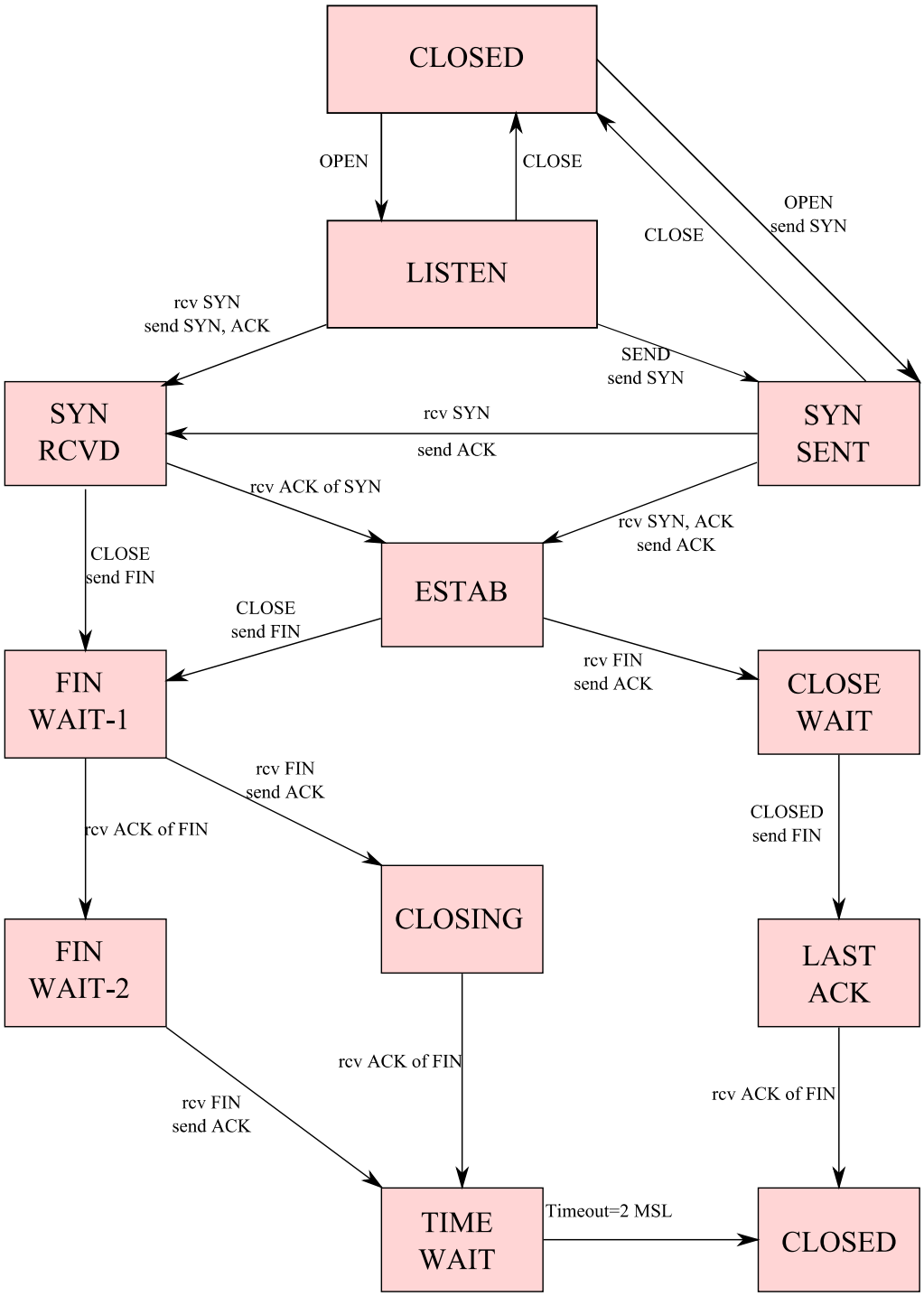
Dĺžka okna (Windows size)- 16 bitov, vyjadruje maximálny počet bajtov, ktoré môže vysielač odoslať, bez čakania na potvrdzovanie od prijímača

Kontrolný súčet (TCP checksum)- 16 bitov, počíta sa nie len zo samotného TCP segmentu, ale aj z niektorých položiek IP záhlavia. Kontrolný súčet vyžaduje párny počet bajtov, preto v prípade nepárneho počtu sa data fiktívne doplnia jedným bajtom na konci

Ukazateľ naliehavých dát (urgent pointer)- 16 bitov, pole je vyplnené len ak je nastavený príznakový bit URG na „1“.

Voliteľné položky záhlavia (options)- pole nemusí byt prítomné, jeho dĺžku je možné odvodiť z celkovej dĺžky záhlavia uvedené v príslušnej pozícii.[3][10]

3.1 Stavový diagram



OBR. 3 STAVOVÝ DIAGRAM

CLOSED- spojenie nie je naviazané.

LISTEN –čaká na prichádzajúce spojenie.

SYN_SENT- prebieha nadväzovanie nového spojenia (klient vyšle SYN paket, protistrana potvrdenie SYN-ACK).

ESTABLISHED- spojenie je naviazane a plne funkcie(pripravene k prenosu alebo už prenos prebieha).

FIN_WAIT1- ukončenie spojenia na nasej strane (poslali sme paket FIN a čakáme na potvrdenie).

FIN_WAIT2- pokračuje ukončenie inicializované našou stranou (prijali sme paket potvrdzovania a očakávame FIN paket protistrany).

TIME_WAIT –posledná fáza inicializovaného ukončenia (prijali sme FIN paket a potvrdili jeho prijatie, až po ukončení prodlevy, ktorá je v RFC definovaná ako dvojnásobok hodnoty MSL-Maximum Segment Life, prejde do stavu CLOSED).

CLOSING- ukončenie spojenia inicializovane našou stranou (poslali sme FIN a čakáme na potvrdenie, v medzičase sme prijali FIN paket, potvrdíme jeho prijatie a čakáme na prijatie nášho FIN paketu).

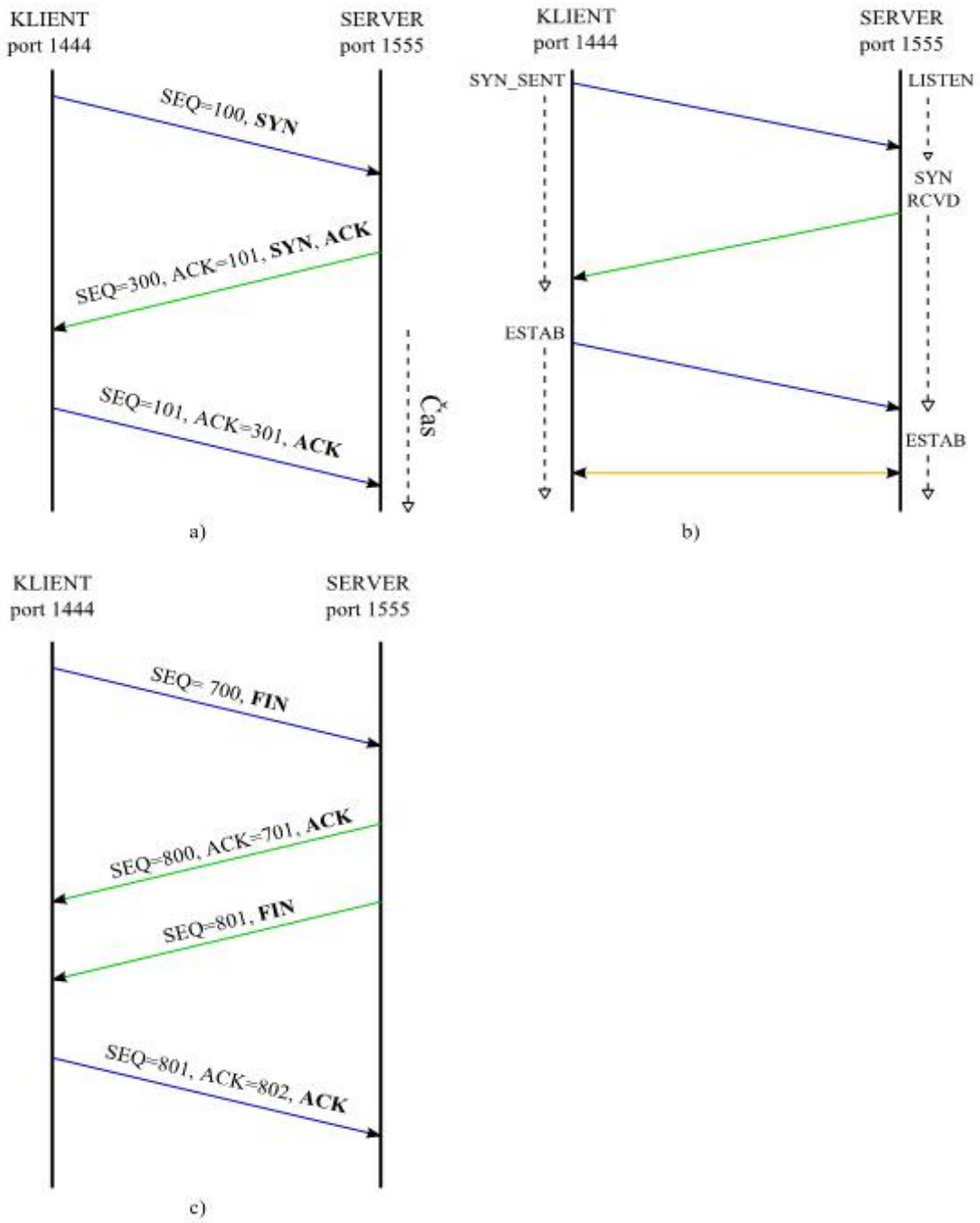
CLOSE_WAIT- ukončenie spojenia inicializovane protistranu (prijali sme FIN a potvrdili prijatie).

LAST_ACK- pokračuje ukončenie protistranou (poslali sme FIN čakáme na potvrdenie a potom prejde do stavu CLOSED). [3]

3.2 Naviazanie a ukončenie spojenia

Naviazanie spojenia začína tak, že strana klienta inicializuje spojenie, pošle SYN a v poly SEQ nastaví číslo. Druhá strana odpovie nastavením príznaku ACK a zároveň chce synchronizovať, nastaví číslovanie pre prenos dát v spätnom smere, prvotne číslo do SEQ. Potvrdí prijatie bajtu očíslovaného ako 100, tak že do potvrdzovaného bajtu (ACK) zapíše 101. Celé sa to odošle v jednom segmente. Klient nastaví príznak ACK, potvrdí prijem bajtu 300 tým, že do ACK zápise 301. Číslo SEQ narastá na základe počtu prenesených bajtov. Segment sa odošle a spojenie je nastavené (established). Tomuto spôsobu sa hovorí trojcestne podanie si rukou (three-hand shake). Skrátený zápis: [SYN] > [SYN, ACK] > [ACK]. [3][1]

Ukončenie spojenia je podobný, na obrázku je znázornený spôsob štvorcestného podania si rukou (four-hand shake). Skrátene: [FIN] > [ACK],[FIN] > [ACK]. Existujú aj skrátené verzie ukončenia, trojcestne a dvojcestne podanie si rukou [FIN, ACK] < [FIN, ACK].



OBR.4 PRIEBEH TCP SPOJENIA A)NADVÄZOVANIE SPOJENIA B)STAVY PRI NADVEZOVANI SPOJENIA C) UKONČENIE SPOJENIA

4 ARP PROTOKOL

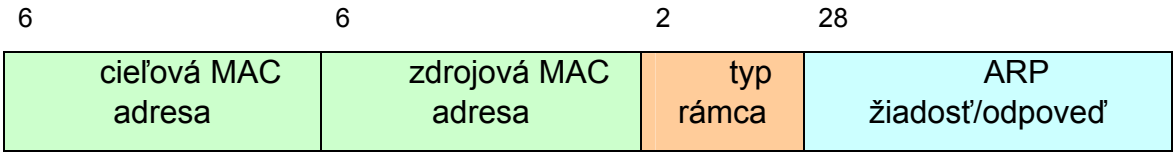
ARP (Address Resolution Protokol) sa používa pri znalosti cieľovej IP adresy stanice pre hľadanie príslušnej fyzickej adresy (MAC). Každá stanica , ktorá chce komunikovať so vzdialenou stanicou a pozná jej sieťovú adresu, potrebuje zistiť jej fyzickú adresu, aby sa mohol datagram zapúzdriť do rámca so správnou cieľovou adresou MAC. Zdrojová stanica preskúma svoju pamäť s informáciami o mapovaní fyzických a sieťových adries (ARP cache), pokiaľ nenájde informáciu, ktorá patrí hľadanej sieťovej adrese, musí použiť protokol ARP. Vyšle žiadosť protokolu ARP s informáciami o zdrojovej dvojici adries (IP a MAC) a s cieľovou IP adresou, ktorá je adresovaná ako broadcast. Očakáva sa odpoveď s vyplneným polom cieľovej MAC adresy.

Pokiaľ je cieľová stanica pripojená na jednom segmente, reaguje odpoveďou na ARP žiadosť. Ale ak sa cieľová adresa nachádza v inom segmente, na žiadosť odpovedá smerovač svojou MAC adresou.

Žiadosť o mapovanie adresy vzniká v okamžiku kedy stanica má pripravené data na odoslanie, má pripravený paket a do zapúzdrenia do rámca chýba iba cieľová fyzická adresa.

ARP cache uzlu obsahuje informácie o MAC adresách staníc, s ktorými komunikovali. Cache uchováva záznam asi 20 min.

4.1 Rámec ARP



OBR.5 SPRÁVA ARP ZAPUZDRENÁ DO RÁMCA ETHERNET

Rámce ARP nemajú záhlavie pevnej dĺžky, lebo môžu slúžiť pre rôzne sieťové technológie. Preto sa vždy na začiatku rámca špecifikujú dĺžky polí. Formát žiadosti a odpovede sa nemení.[6]

5 SKENOVANIE

5.1 Identifikácia funkčných systémov

5.1.1 Hromadný ping

Jeden zo základných krokov mapovania siete je automatický hromadný ping na interval IP adries, ktorý umožňuje identifikovať v rámci tohto intervalu fungujúce systémy. Ping pracuje tak, že zasiela cieľovému systému ICMP paket ECHO (typ 8), pokiaľ dostane odpoveď ICMP ECHO_REPLAY (typ 0), predpokladá sa že cieľový systém je funkčný. Použitie programu ping sa hodí na malé a stredne veľké siete, vo veľkých sieťach je veľmi neefektívny a môže trvať niekoľko hodín až dní.
Pre Windows alebo Unix existuje veľké množstvo utilít, ktoré umožňujú hromadný ping.

Najznámejšia utilita v Unix je fping. Väčšina bežných utilít čaká na odpoveď testovanej IP a až potom začne testovať ďalšiu IP adresu. Fping odošle na testované adresy niekoľko paktov súčasne, tým je schopný overiť funkčnosť systémov oveľa rýchlejšie.

Fping môže byť použitý dvoma spôsobmi. Buď sa budú jednotlivé IP adresy zapisovať na vstup, alebo sa budú čítať zo súboru.[5]

5.1.1.1 Ochrana proti hromadnému pingu

Tok ICMP sa dá filtrovať, ale pri tomto kroku musíme byť opatrný, lebo protokol ICMP slúži k diagnostike sieťovej prevádzky. Protokol ICMP používa viac správ ako len ECHO a ECHO_REPLY, preto si treba dôkladne zvážiť ktoré správy potrebujeme a ktoré nie.[5]

5.1.2 Nmap

Nmap je viacúčelový monitorovací nástroj so zabudovaným hromadným pingom. Stačí zadať zoznam IP adries alebo sietí a použiť prepínač –sP. S prepínačom –sP umožňuje nmap niečo viac ako obyčajný ICMP ping. Okrem bežného ICMP paketu posiela TCP paket ACK na port 80 (HTTP). I keď by bolo ICMP zablokované, TCP dotaz môže prejsť. Ak by bola odpoveď na ACK paket RST, bolo by jasné, že systém beží. [5]

5.1.3 ICMP dotazy

Poslaním ICMP správy typu 17 (ADDRESS_MASK_REQUEST) môžeme zistiť masku sieťového rozhrania. Táto informácia má veľkú hodnotu, pretože nám umožňuje zistiť ako sú definované podsiete. Potom stačí sústrediť útoky na konkrétnu podsieť.[5]

5.1.3.1 Ochrana proti ICMP dotazom

Jeden z najlepších postupov je blokovať jednotlivé pakety na hraničných smerovačoch.[5]

6 IDENTIFIKÁCIA BEŽIACICH SLUŽIEB

6.1 Skenovanie portov

Skenovanie portov je proces, kedy sa pripojujeme k TCP a UDP portom systému s cieľom identifikovať bežiace služby. Identifikácia otvorených portov nám umožňuje zistiť typ operačného systému a typ bežiacich aplikácii.[5]

Najdôležitejšie dosahované ciele pomocou skenovania portov:

- Identifikácia TCP a UDP služieb
- Identifikácia OS
- Identifikácia konkrétnej aplikácie

6.1.1 Typy skenov

Teraz popíšem techniky, ktoré sa pri skenovaní portov používajú.

- **TCP spojenie** Pri tomto type skenovania dochádza ku kompletnému trojcestnému (SYN, SYN/ACK, ACK) spojeniu na cieľový port
- **TCP SYN sken** Táto technika nadväzuje spojenie len polovičné (half-open scanning). Nedochádza k plnému naviazaní spojenia ako v predchádzajúcom prípade. Namiesto toho sa odošle SYN paket. Pokiaľ je spätne prijatý SYN/ACK paket, s veľkou pravdepodobnosťou je port otvorený. Pokiaľ je prijatý paket RST/ACK, port je zatvorený.
- **TCP FIN sken** Na cieľový port je zaslaný paket FIN. podľa RFC 793 by mal cieľový systém odpovedať RST paketom pre všetky zatvorené porty.
- **TCP XmasTree sken** Na cieľový port je odoslaný paket FIN, URG a PUSH. Podľa RFC 793 by mal cieľový systém odpovedať RST paketom pre všetky zatvorené porty.
- **TCP Null sken** Je odoslaný paket s vynulovaným návestím (flags). Na základe RFC 793 by mal cieľový systém odpovedať RST paketom pre všetky zatvorené porty.
- **TCP ACK sken** Tato technika sa používa k mapovaniu filtrov na firewallu. Umožňuje zistiť či sa jedná o paketový filter alebo o stavový firewall.

Nevýhodou týchto skenov je ich nespoľahlivosť. Spoľahnúť sa môžeme na TCP connect a TCP SYN skeny.[5]

6.2 Identifikácia služieb TCP a UDP

6.2.1 Netcat

Netcat umožňuje analýzu portov TCP a UDP. Prepínače –v a –w zapínajú podrobný a ešte podrobnejší výstup, prepínač –z sa používa pri skenovaní portov a –w2 umožňuje definovať časový interval medzi jednotlivými spojeniami. Implicitne netcat skenuje TCP porty. Na sken UDP portov sa používa prepínač –u. [5]

6.2.2 Nmap

Nmap patrí medzi najlepšie skenery súčasnosti. Podporuje asi každý spôsob sledovania ktorý sa objavuje. Viď tab. 1

Typ	prepínač	popis
TCP spojení	-sT	Kompletný prieskum cez TCP
SYN sken	-sS	Pošle iba pakety SYN
FIN	-sF	Pošle holý paket FIN
Xmas Tree	-sX	Pošle paket FIN,URG,PUSH
ACK	-sA	ACK prieskum

Tab. 1 Spôsoby sledovania pomocou nmap

V tab. 1 sa nachádzajú len najpoužívanejšie voľby, v skutočnosti ich existuje omnoho viac. [5]

6.3 Ochrana proti sledovaniu portov

Proti sledovaniu portov sa dá len veľmi ťažko brániť, firewally obvykle SYN prieskum blokujú automaticky.

7 ÚTOKY SMERUJÚCE K VYRADENIU PROVOZU

Útoky ktoré sieťovému zariadeniu alebo sieti zabraňujú obvyklé využitie sieťových zdrojov sú hromadne označované ako DoS (Denial of Servis). Tieto útoky obvykle slúžia k obťažovaniu užívateľov internetu, blokovaniu sieťovej prevádzky a k potlačeniu sieťovej existencie hostiteľov. [5]

7.1 Záplavy (floods)

Zaplavovanie je jednou z najstarších foriem DoS útoku. Spočíva v zasielaniu veľkého toku IP paketov konkrétnemu hostiteľovi, tým sa spotrebuje celá jeho prenosová kapacita a blokuje sa ostatná prevádzka. Záplavy sú najefektívnejšie keď útočník disponuje širším prenosovým pásmom ako cieľ. [5]

7.2 ICMP (ping) záplavy

Ping pošle cieľovému hostiteľovi paket ICMP ECHO_REQUEST a potom čaká na odpoveď, aby zistil či je cieľový hostiteľ dosiahnuteľný. Ak nie sú uvedené žiadne voľby, ping posiela malé pakety s jednosekundovým odstupom. Prepínač –f spôsobuje, že ping ping bude posielať pakety najrýchlejšie ako len bude môcť a voľba –s umožní zaslať väčšie pakety. [5]

7.2.1 Ochrana proti ICMP záplavám

ICMP záplavy sú u vysokorýchlostných sieťových pripojení málo efektívne ako na vytáčaných linkách ale i tak môžu priepustnosť obmedziť. Poskytovatelia internetového pripojenia na svojich smerovačoch a prepínačoch obmedzujú množstvo prepúšťaných

ICMP paketov a to znižuje účinnosť útokov. [5]

7.3 Smurf

Program posiela na vysielaciu adresu ICMP ECHO_REQUEST. Útočník obvykle použije sfalšovanú adresu odosielateľa, ktorá je totožná s adresou zariadenia ktoré chceme napadnúť. Všetky sieťové zariadenia odpovedia na ping a tým zaplavia hostiteľa. Zariadenia v sieti poslúžia ako zosilňovač pôvodného dotazu. Zvýšením efektivity útoku dosiahneme opakovaním príkazu. [5]

7.3.1 Ochrana proti Smurf

Pre ochranu je dôležité aby smerovače a firewally filtrovali prevádzku egress.[5]

8 TCP/IP ÚTOKY

8.1 Ping of Death (ping smrti)

Ide o vysielanie paketov v neštandardnej dĺžke, väčšie ako 65536 bytov. Paket pred prenosom musí byť fragmentovaný. Keď cieľové zariadenie príjme fragmenty a následne z nich zloží paket neštandardnej veľkosti, môže dôjsť k pretečeniu vyrovnávacej pamäti a nasleduje pád systému.

Dnes už máloktoré ovládače TCP/IP sú voči tomuto útoku zraniteľné a väčšina smerovačov tak veľké pakety filtruje. [7]

8.2 Teardrop (slza)

Teardrop sa pokúša zhodiť sieťové rozhranie cieľa zaslaním viacerých fragmentov, ktoré sa nedajú správne zložiť. Spôsobuje reštart zariadenia. [7]

8.3 Záplavy SYN

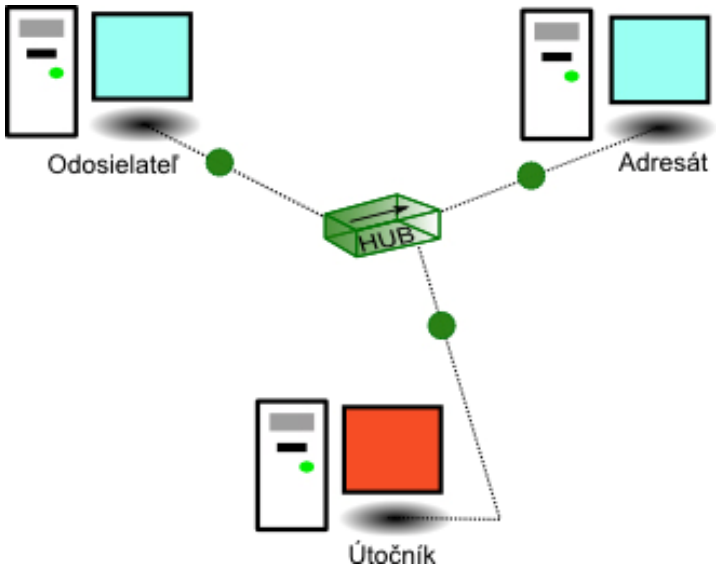
Otvorenie komunikačného kanálu protokolu TCP/IP medzi dvoma hostiteľmi prechádza inicializáciou (handshake). Klient najskôr zašle serveru TCP paket SYN. Server ho prijme a odpovie paketom SYN/ACK. Na to klient reaguje paketom ACK a inicializácia je ukončená. Spojením môžu ihneď prúdiť data. Keď server príjme paket SYN, vloží si ďalšiu položku do fronty polootvorených spojení. Chvíľu počká či nedostane od klienta i druhý inicializačný paket a potom spojenie z fronty odstráni. Problém nastane v okamžiku keď je nahlásených príliš veľa spojení u ktorých nie je inicializácia dokončená. Fronta má obmedzený počet miest a keď sa zaplní, server prestane prijímať ďalšie spojenia. Ak útočník stíha zapĺňať frontu serveru, záplava zablokuje všetky služby TCP.[5]

8.3.1 Ochrana proti záplavám SYN

Jednou z možností ochrany je zväčšenie fronty, ale to nie je optimálne riešenie. Druhou možnosťou je zmenšenie čakanie na RST/ACK. [5]

9 MAN IN-THE-MIDDLE-ATTACK

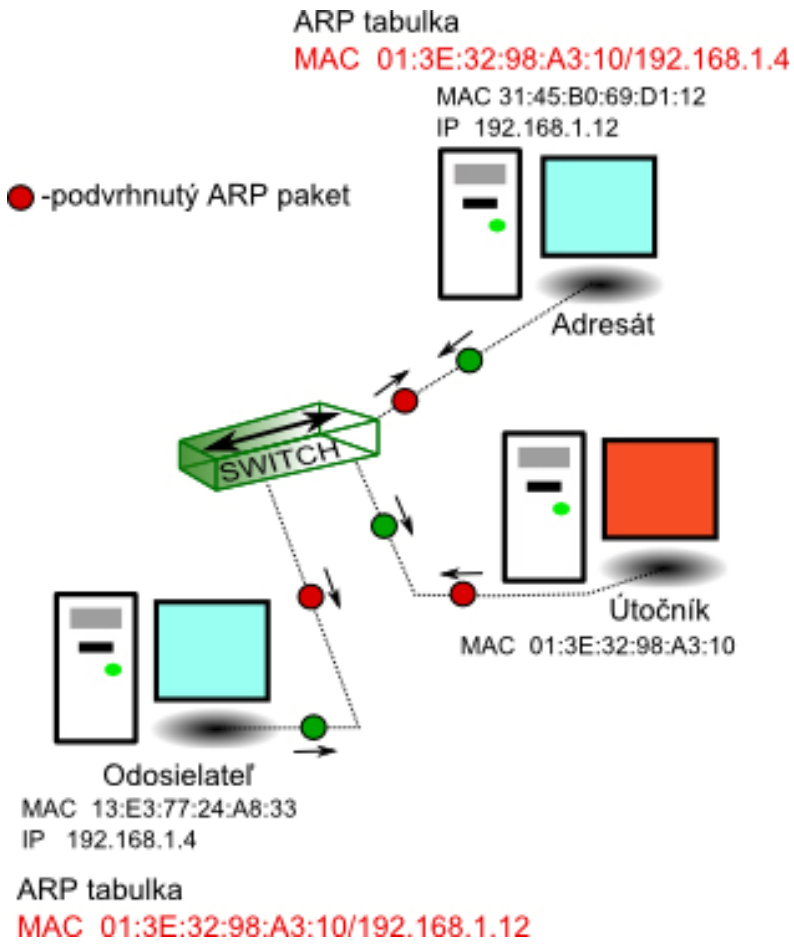
Jeden zo základných útokov je útok zo stredu, inak nazvaný zrkadlový, resp. spoofing. Spoofing je technika, kde sa jeden počítač predstavuje druhému počítači falošnou identitou. Útok je založený na odpočúvaní komunikácie medzi dvoma stranami. Spôsob útoku závisí na type siete. V prípade zdieľaného Ethernetu sú všetky počítače pripojené na jednej zbernici a paket určený konkrétnemu zariadeniu je odoslaný cez hub všetkým pripojeným staniciam. Každý počítač si vyhodnotí, či mu bol paket určený. Ak nie, tak paket zahodí. V takejto situácii stačí útočníkovi prepnúť svoju sieťovú kartu do promiskuitného režimu. V Linuxe sa použije príkaz *ifconfig eth0 promisc.* V tomto režime sieťová karta zachytáva celú komunikáciu na zbernici.[4][5][6]



OBR.6 ZDIEĽANÝ INTERNET, ÚTOČNÍK JE V PROMISKUITNOM MÓDE

9.1 ARP spoofing

ARP spoofing je technika využívajúca slabín ARP protokolu, ktorý nemá žiadne ochranné mechanizmy. Útok spočíva v tom že odosielateľ (obeť) a adresát pre vzájomnú komunikáciu budú dosadzovať MAC adresu útočníka. Útočník si prehliadne data a prepošle ich adresátovi.[2][4]

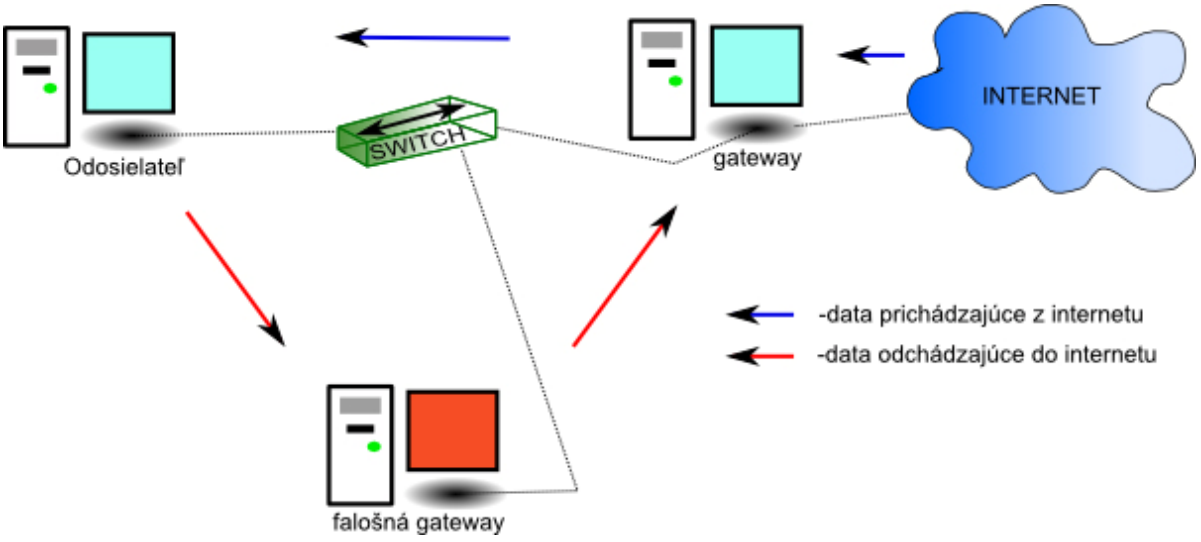


OBR.7 ARP SPOOFING

9.2 DHCP spoofing

DHCP (Dynamic Host Config guration Protocol) slúži k dynamickému prideľovaniu sieťových parametrov koncovým zariadeniam. DHCP spoofing využíva skutočnosti, že v jednej LAN môže fungovať viac DHCP serverov. Cieľom tohto útoku je nasadiť falošný DHCP server a podstrčiť obeti falošné údaje napr. gateway alebo DNS server. Funguje to tak, že keď sa pripojí počítač obeti do siete, pošle paket DHCP_Discover ako broadcast. Tento paket žiada o to, aby sa mu ozvali všetky DHCP servery v sieti. Servery odpovedajú paketom DHCP_Offer, kde mu ponúkajú parametre pripojenia. Platí tu pravidlo najrýchlejšieho. Najrýchlejšiemu serveru odpovedá počítač paketom DHCP_Request, ktorým žiada o dané parametre. Server odpovie DHCP_Ack a tým uzatvára dohodu. Tu treba zabezpečiť aby falošný server bol čo najrýchlejší. V prípade, že počítač bol v minulosti pripojený do siete, je presmerovanie dát na gateway zložitejší. V tomto prípade obeť posiela len paket DHCP_Request serveru, od ktorého naposledy získal sieťové parametre. Pri útoku je vhodné využiť parameter DHCP serveru *lease time*, ktorý udáva ako dlho majú byť

pridelené sieťové parametre. Pred skončením tejto doby musí každý klient požiadať o predĺženie inak server bude považovať dané parametre ako voľné a môže ich priradiť inej stanici. Aby bolo možné odstaviť skutočný DHCP server je potrebné ho zahltiť požiadavkami o pridelení sieťových parametrov. Keď sa zahltí, prestane odpovedať na DHCP_Discover. Teraz už len stačí počkať na uplynutie *lease time* a vyslanie nového paketu DHCP_Discover. Keď už bude komunikácia prebiehať cez falošnú gatewey, príslušným softwarom sa dajú odpočúvať data ale iba smerom do internetu. Ak by sme chceli zachytiť obojsmernú komunikáciu, treba použiť inú metódu, napr. DNS spoof. [2][4]



OBR.8 DHCP SPOOFING

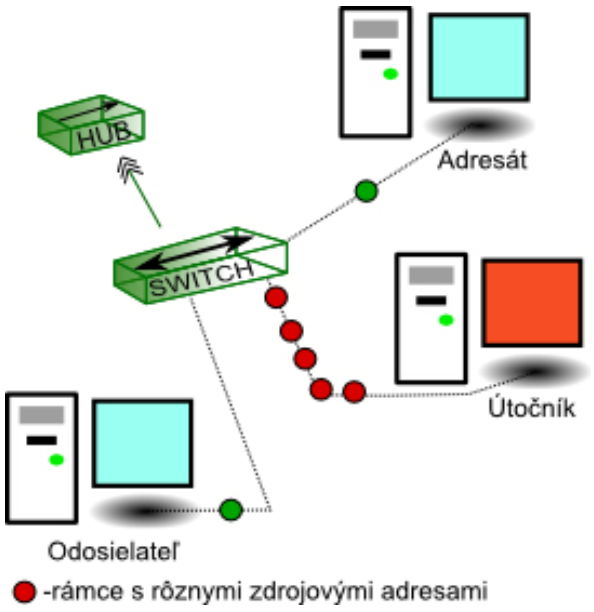
9.2.1 Obrana proti DHCP spoof

Obrana proti tomuto útoku prebieha pomocou služby DHCP Snooping. Porty na switchi sa rozdelia na trusted (dôveryhodné) a untrusted (nedôveryhodné). Pokiaľ sa na switch pripojí iný switch podporujúci túto službu, priradí sa mu stav trusted, všetky ostatné porty sú untrusted. V prípade že je DHCP server pripojený na port untrusted, switch to spozná a zahodí pakety.[2][4]

9.3 MAC flooding

Switch má v sebe zabudovanú tzv. CAM tabuľku (Content Addressable Memory), aby vedel prepínať data na príslušné porty. V tabuľke sú uložené páry jednotlivých portov switchu a MAC adresy. CAM má určitú kapacitu (rádovo tisíce párov adries, záleží od typu switcha), preto býva v určitom intervale premazávaná. MAC flooding je založený na

naplnení CAM tabuľky MAC adresami ktoré sú náhodne generované. Keď tabuľka naplní, switch sa prepne do stavu *fail open* a správa ako HUB.[2]



OBR.9 MAC FLOODING

9.4 Port stealing

Útok je založený na krádeži portu na sieťovom zariadení (switch). Po zistení MAC adresy adresáta, sa začnú posielať upravené pakety, ktoré budú mať cieľovú adresu totožnú s adresou útočníka a zdrojovú MAC adresu s adresou adresáta. Po odoslaní paketu, switch priradí adresátovi nový port, tj. port útočníka. Všetky pakety od odosielateľa switch smeruje na adresu útočníka. Pre zachovanie utajenia je potrebné preposlať paket adresátovi. V poslednom kroku je potrebné opäť upraviť CAM tabuľku a to napr. odoslaním ARP_Request paketu adresátovi, vyvolá sa reakcia ARP_Replay. Pokiaľ je útok vedený tak, že upravený paket ma cieľovú adresu totožnú s adresou útočníka, je ťažké takýto útok vysledovať, lebo switch už neposiela paket ďalej. [2][4]

9.4.1 Obrana proti port stealingu

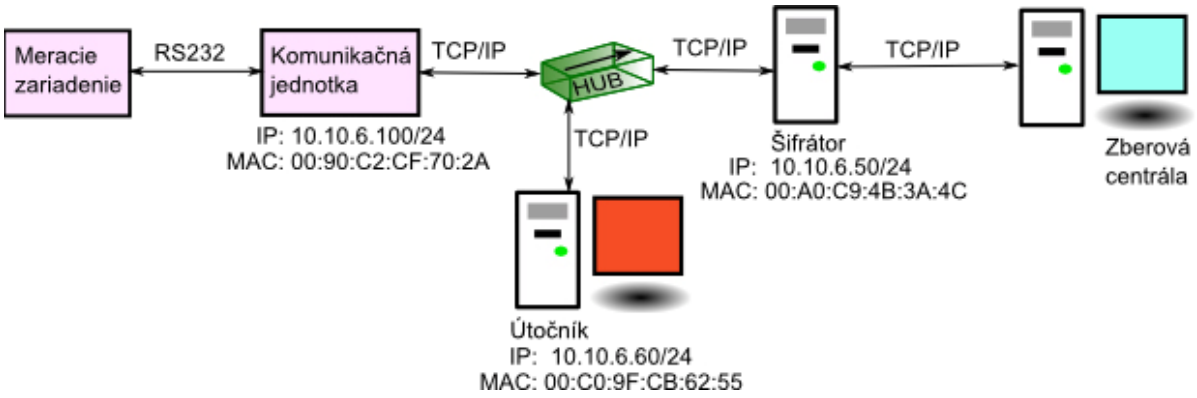
Obrana využíva služby DHCP snooping. Data prichádzajúce z untrusted portu sú zahadzované pokiaľ nie je nastavená zdrojová MAC a IP adresa stanice podľa záznamu v DHCP snooping tabuľke pre daný port.[2][4]

9.5 DNS spoofing

DNS spoofing falšuje IP adresy v pakete, ktoré sa vracajú ako odpoveď na žiadosť o preklad doménového mena na IP adresu. Pri tomto útoku môže byť prevádzka na sieti presmerovaná mimo lokálnu sieť. Užívateľ využíva k prekladu doménových mien iba DNS_Resolver. DNS_Resolver je sada požiadavkov, ktoré slúžia k práci s DNS protokolom. Pri preklade doménových mien vyšle DNS_Resolver požiadavku na DNS server, ktorý je nastavený na danej stanici. Keď dostane odpoveď, uloží si ju v lokálnej DNS cache na prípadné ďalšie využitie. Doba uloženia záznamu v DNS cache sa deklaruje ma DNS servery a je súčasťou odpovede serveru. Po vypršaní tejto doby je záznam vymazaný a pri opätovnej potrebe sa prevedie preklad.Aj tu platí výhra najrýchlejšieho.[2]

10 REALIZÁCIA ÚTOKOV

Pre realizáciu útokov som zvolil zapojenie s hubom. Útočník používa operačný systém Linux a je prepnutý do promiskuitného režimu príkazom *ifconfig eth0 promisc.*



OBR.10 SCHÉMA ZAPOJENIA ÚTOKU

Zistím aké zariadenia sa nachádzajú v podsieti. Použijem linuxové nástroje na detekciu aktívnych staníc.

```
bt ~ # fping -a -g 10.10.6.0/24
10.10.6.50
10.10.6.60
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.0
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.1
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.2
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.3
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.4
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.5
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.6
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.7
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.8
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.9
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.10
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.11
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.12
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.13
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.14
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.15
ICMP Host Unreachable from 10.10.6.60 for ICMP Echo sent to 10.10.6.16
10.10.6.100
```

OBR. 11VÝPIS PRÍKAZU FPING

Ako prvý som použil fping, prepínač –a by mal zobraziť iba aktívne zariadenia, s neznámych dôvodov sa nám zobrazili aj neaktívne adresy. Prepínač –g umožňuje zápis podsiete s dĺžkou prefixu.

S obrázkov 11. a 12. je vidieť že máme v podsieti 3 aktívne zariadenia s príslušnou IP adresou.

```
bt ~ # nmap -sP 10.10.6.0/24

Starting Nmap 4.20 ( http://insecure.org ) at 2008-11-27 09:11 GMT
Host 10.10.6.50 appears to be up.
MAC Address: 00:A0:C9:4B:3A:4C (Intel - Hf1-06)
Host 10.10.6.60 appears to be up.
Host 10.10.6.100 appears to be up.
MAC Address: 00:90:C2:CF:70:2A (JK microsystems)
Nmap finished: 256 IP addresses (3 hosts up) scanned in 44.525 seconds
```

OBR.12 VÝPIS PRÍKAZU NMAP

Požitím programu nmap sme zistili MAC adresy zariadení a ich výrobcov. Prepínač –sP znamená ping scan. JK microsystém bude hľadaná komunikačná jednotka. Keď sme si našli cieľ, začneme so skenovaním portov, aby sme zistili aké služby sú podporované komunikačnou jednotkou.

```
bt ~ # nmap -sS 10.10.6.100

Starting Nmap 4.20 ( http://insecure.org ) at 2008-11-27 10:03 GMT
Interesting ports on 10.10.6.100:
Not shown: 1694 closed ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
2000/tcp open  callbook
MAC Address: 00:90:C2:CF:70:2A (JK microsystems)

Nmap finished: 1 IP address (1 host up) scanned in 28.077 seconds
```

OBR.13 SKENOVANIE PORTOV

Opäť použijem viacúčelový nástroj nmap, ktorý patrí medzi najužívanejšie utility pri tvorbe útokov. Prepínač –sS zaručí SYN scan. Našli sme 3 otvorené porty. Port 80 je protokol http, je to nezabezpečený prenos informácii. Https je nadstavba protokolu http šifrovaná pomocou SSL alebo TLS. V základnom rozdelení portov je skupina takzvaných well know portov, sú to porty 0-1023 ne ktorých bežia najznámejšie služby. Porty sa nedajú využívať bez registrácie u IANA. Už poznáme cieľ aj služby na komunikačnej jednotke, tak pomocou príkazu hping sa pokúsime o odobratie služby. Parameter –flood zaručí, že budeme posielať pakety tak rýchlo, ako to len bude možné, –rand-source má za úlohu generovať náhodne IP adresu odosielateľa, -S ide o SYN pakety –p nám umožňuje vybrať port .

```
bt ~ # hping --flood --rand-source -S 10.10.6.100
HPING 10.10.6.100 (eth0 10.10.6.100): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

--- 10.10.6.100 hping statistic ---
1055644 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

OBR.14 HPING

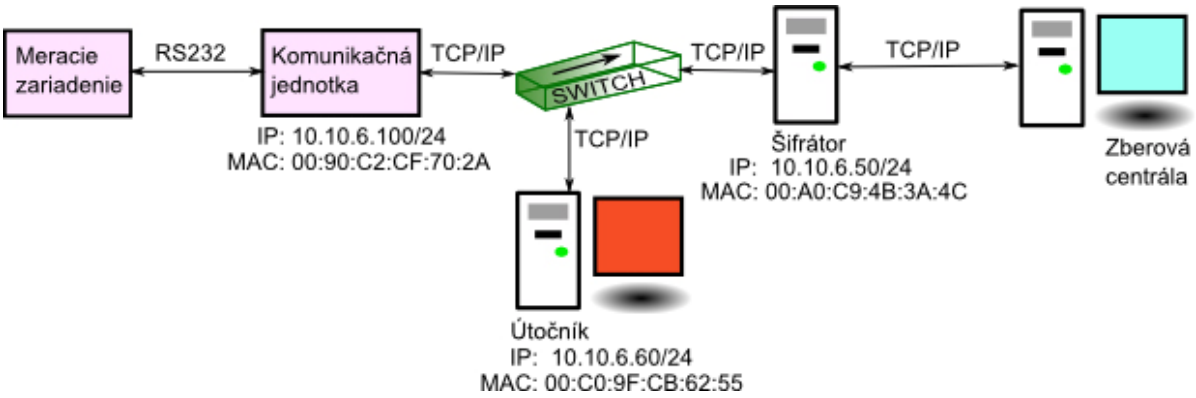
Pre názornejšie zobrazenie komunikácie máme nainštalovaný Wireshark na zachytávanie a analýzu komunikácie. Na obr.14 je vidieť priebeh útoku pri príkaze Hping.

3	0.000097	102.91.24.0	10.10.6.100	TCP	4652 > 0 [SYN] Seq=0 Len=0
4	0.000165	187.232.192.6	10.10.6.100	TCP	4653 > 0 [SYN] Seq=0 Len=0
5	0.000233	178.186.182.91	10.10.6.100	TCP	4654 > 0 [SYN] Seq=0 Len=0
6	0.000301	178.121.132.121	10.10.6.100	TCP	4655 > 0 [SYN] Seq=0 Len=0
7	0.000369	218.56.57.56	10.10.6.100	TCP	4656 > 0 [SYN] Seq=0 Len=0
8	0.000437	148.131.195.174	10.10.6.100	TCP	4657 > 0 [SYN] Seq=0 Len=0
9	0.000504	4.85.67.67	10.10.6.100	TCP	4658 > 0 [SYN] Seq=0 Len=0
10	0.000573	244.91.145.208	10.10.6.100	TCP	4659 > 0 [SYN] Seq=0 Len=0
11	0.000641	106.106.110.15	10.10.6.100	TCP	4660 > 0 [SYN] Seq=0 Len=0
12	0.000708	239.237.22.194	10.10.6.100	TCP	4661 > 0 [SYN] Seq=0 Len=0
13	0.000776	159.188.220.128	10.10.6.100	TCP	4662 > 0 [SYN] Seq=0 Len=0

OBR.15 VÝPIS S PROGRAMU WIRESHARK

Na komunikačnú jednotku prichádza veľké množstvo žiadostí na otvorenie spojenia a jednotka neni schopná otvárať ďalšie spojenia. Preto sa nemôže šifrátor spojiť s elektromerom. Pri tomto útoku komunikačná jednotka bola nedostupná pre každú aplikáciu. Útok svoj účel splnil.

Ďalší typ aplikovaného útoku bol arpspoof. Účelom je zachytiť data na prepínanom Ethernete.



OBR.16 TESTOVACIE ZAPOJENIE PRE ARPSPOOF

Príkazom *arpspoof –t 10.10.6.100 10.10.6.50* začneme falšovať pakety v jednom smere, preto arpspoof - t 10.10.6.50 10.10.6.100. Viď. obr. 17.

```
arp reply 10.10.60.100 is-at 0:c0:9f:cb:62:55
arp reply 10.10.60.100 is-at 0:c0:9f:cb:62:55
arp reply 10.10.60.100 is-at 0:c0:9f:cb:62:55
arp reply 10.10.60.100 is-at 0:c0:9f:cb:62:55
```

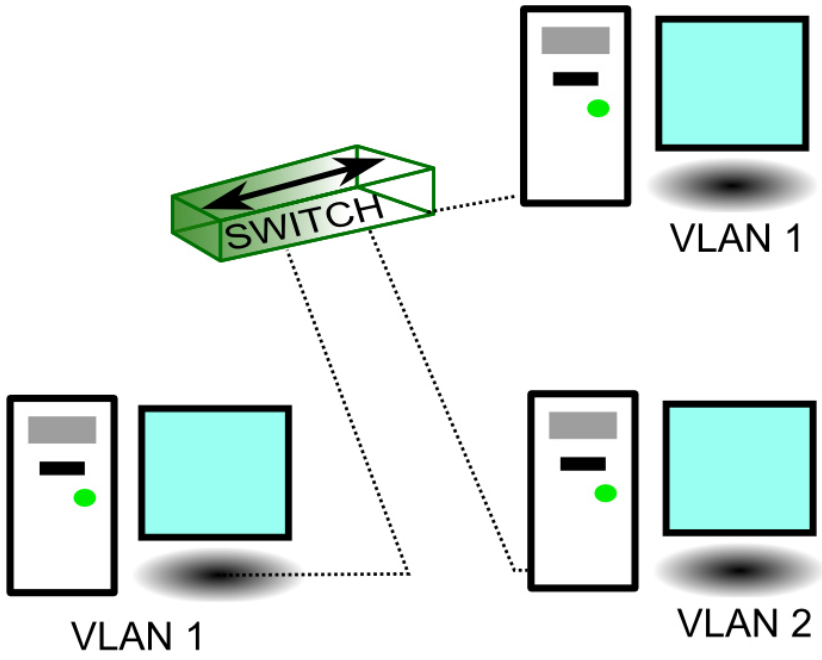
```
arp reply 10.10.60.50 is-at 0:c0:9f:cb:62:55
arp reply 10.10.60.50 is-at 0:c0:9f:cb:62:55
arp reply 10.10.60.50 is-at 0:c0:9f:cb:62:55
arp reply 10.10.60.50 is-at 0:c0:9f:cb:62:55
```

OBR.17 VÝSTUP ARPSPOOF PRE OBA SMERY

Na to aby sme sme sa neprezradili potrebujeme preposielať pakety adresátom. To umožníme príkazom *echo 1 > /proc/sys/net/ipv4/ip_forward.*

11 VLAN

VLAN (Virtual LAN) umožňujú umiestniť vybrané zariadenia do jednej broadcastovej domény. VLAN sa konfiguruje na sieťovom prvku switch (prepínač).



OBR. 18 VLAN

Dôvody tvorby VLAN sú nasledujúce:

- Segmentácia siete na menšie časti pre redukciu réžie
- Zníženie záťaže STP protokolu
- Tvorba bezpečnosti pre citlivé dáta

11.1 Trunking

Ak je naša sieť tvorená minimálne dvoma prepínačmi alebo jedným smerovačom, linku medzi nimi musíme nastaviť ako trunk, lebo táto linka prenáša pakety všetkých VLAN. Trunk označuje pakety, aby bolo možné pakety doručiť do správnej VLAN. Ako trunkovací protokol sa v dnešnej dobe používa 802.1Q.

12 REALIZÁCIA VLAN

Pre umiestnenie komunikačnej jednotky do VLAN, musíme nakonfigurovať sieťové zariadenie. V laboratórii budeme konfigurovať prepínač, ktorý je umiestnený pomocou WIC karty do smerovača cisco 2801.

12.1 Zapojenie a konfigurácia

Počítač prepojíme so smerovačom pomocou sériového kábla, na strane PC konektor com1 na druhej strane konektor console. Ako software pre konfiguráciu použijeme freeware TERATERM (obdoba hyperterminálu).

Nastavenie pre seriové spojenie:

Bit per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Po úspešnom pripojení sa dostaneme do užívateľského módu, príkazom *enable* sa prepneme do privilegovaného módu a následným príkazom *configure terminal* sa prepneme do globálneho konfiguračného módu viď obr. 19.

```
Router con0 is now available



Press RETURN to get started.




Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

OBR.19 UŽÍVATEĽSKÝ, PRIVILEGOVANY A GLOBALNY MOD

Z bezpečnostných dôvodov nastavím heslo pre pristup cez seriové rozhranie, heslo pre vstup do globálneho konfiguračného módu. Tento typ zariadenia nepodporuje pripojenie cez SSH ale iba protokolom telnet, ktorý napriek bezpečnosti nebudem konfigurovať.

```
Router(config)#enable secret rabbit
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

OBR. 20 UŽÍVATEĽSKÉ HESLO CISCO A PRIVILEGOVANÉ HESLO RABBIT

Vytvoríme VLAN číslo 10, pod názvom Rabbit a pridelíme jej porty, ktoré budú do nej patriť.

```
Router#vlan database
Router(vlan)#vlan 10 name Rabbit
```

OBR. 21 TVORBA VLAN S NÁZVOM RABBIT

Najskôr zistím akými portami naše zariadenie disponuje, a to pomocou príkazu z privilegovaného módu: show ip interface brief.

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES unset  administratively down down

FastEthernet0/1            unassigned      YES unset  administratively down down

FastEthernet0/1/0          unassigned      YES unset  up                    down

FastEthernet0/1/1          unassigned      YES unset  up                    down

FastEthernet0/1/2          unassigned      YES unset  up                    down

FastEthernet0/1/3          unassigned      YES unset  up                    down

Serial0/2/0                unassigned      YES unset  administratively down down

Vlan1                      unassigned      YES unset  up                    down
```

OBR. 22VÝPIS SHOW IP INTERFACE BRIEF

Teraz pridelím mnou vybrané porty do vytvorenej VLAN. Každý port na ktorý sa pripojuje koncové zariadenie musí byť nastavený ako access, port na ktorý sa pripojujú prepínač alebo smerovač musí byť nastavený ako trunk.

```
Router(config)#interface fastethernet 0/1/0
Router(config-if)#sw
Router(config-if)#switchport mode access
Router(config-if)#switchport acces vlan 10
Router(config-if)#exit
Router(config)#interface fastethernet 0/1/1
Router(config-if)#switchport mode access
Router(config-if)#switchport access vlan 10
Router(config-if)#exit
Router(config)#interface fastethernet 0/1/2
Router(config-if)#switchport mode access
Router(config-if)#switchport access vlan 10
Router(config-if)#exit
Router(config)#
```

OBR. 23 PRIDELENIE PORTOV DO VLAN

Pre overenie konfigurácie použijem príkaz show vlan-switch.

```
Router#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1/3
10   Rabbit                           active    Fa0/1/0, Fa0/1/1, Fa0/1/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

OBR. 24 VÝPIS KONFIGURÁCIE

Naše nastavenie sa nachádza v pamäti RAM, takže po vypnutí sa stratia všetky nastavenia, okrem nastavení VLAN, ktoré sú uložené na Flash v súbore vlan.dat. Pre zachovanie dát použijeme príkaz *copy runnuning-config startup-config* na kopírovane nastavenia do NVRAM

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

OBR. 25 KOPÍROVANIE KONFIGURÁCIE Z RAM DO NVRAM

12.2 Trunk

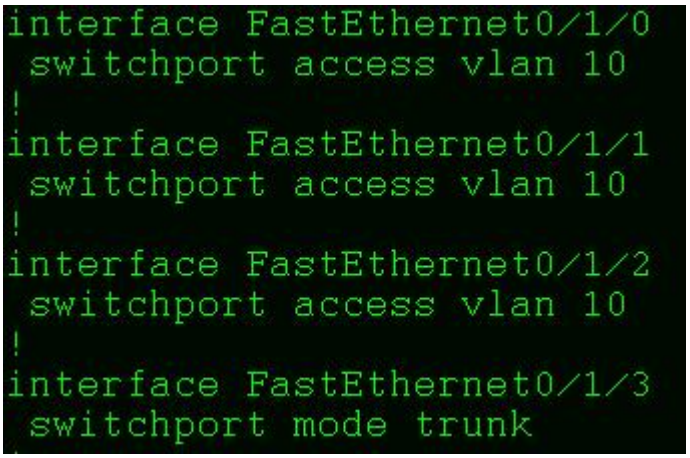
Pri zapojení viacerých prepínačov v jednej topológii je nutné nastaviť úsek medzi prepínačmi alebo medzi prepínačom a smerovačom ako Trunk, aby mohli prúdiť pakekty rôznych VLAN, s paketmi neoznačenými VLAN.

Ako trunk port nastavím FastEthernet 0/1/3.

```
Router(config)#interface fastEthernet 0/1/3
Router(config-if)#switchport mode trunk
```

OBR. 26 TRUNK PORT

Na overenie pridelenia jednotlivých portov do módu použijem príkaz show running-config. Pre prehľadnosť zverejním iba časť tohto výpisu.



OBR. 27 VÝPIS SHOW RUNNING-CONFIG

12.3 Bezpečnosť portov

Pre niektoré smerovače existuje možnosť zabezpečenia portov pomocou MAC adresy, proti neoprávnenému pripojeniu na prepínač. Ak neoprávnená MAC adresa sa pripojí na Prepínač, port sa zatvorí. Naše zariadenie túto funkciu nepodporuje.

13 BEZPEČNOSŤ

13.1 Základné pojmy

Kryptológia sa delí na kryptoanalýzu a kryptografiu. Kryptografia je náuka o metódach šifrovania a kryptoanalýza je metóda lúštenia šifier.

Plaintext - pôvodná správa

Šifrovanie – proces transformácie informácie do tvaru ktorý je nezrozumiteľný pre každého okrem príjemcu

Dešifrovanie – je proces transformácie šifrovanej správy do pôvodného tvaru

Kryptografický algoritmus – matematická funkcia používaná pri šifrovaní a dešifrovaní

13.2 Typy kryptografie

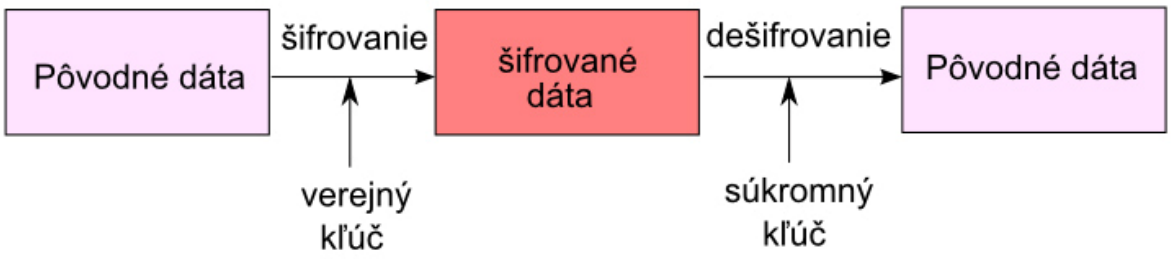
1.Symetrická kryptografia s tajným kľúčom obr. 28:

- s blokovým kryptografickým algoritmom
- s prúdovým kryptografickým algoritmom

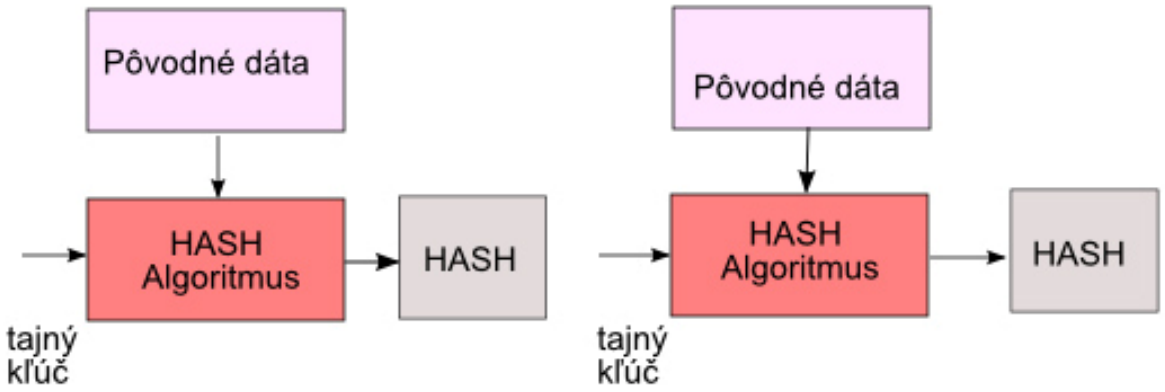
2.Asymetrická kryptografia s verejným a súkromným kľúčom obr. 29.

3.Jednocestné hash funkcie s kľúčom alebo bez kľúča obr. 30

OBR. 28 SYMETRICKÁ KRYPTOGRAFIA



OBR. 29 ASYMETRICKÁ KRYPTOGRAFIA



OBR. 30 HASH

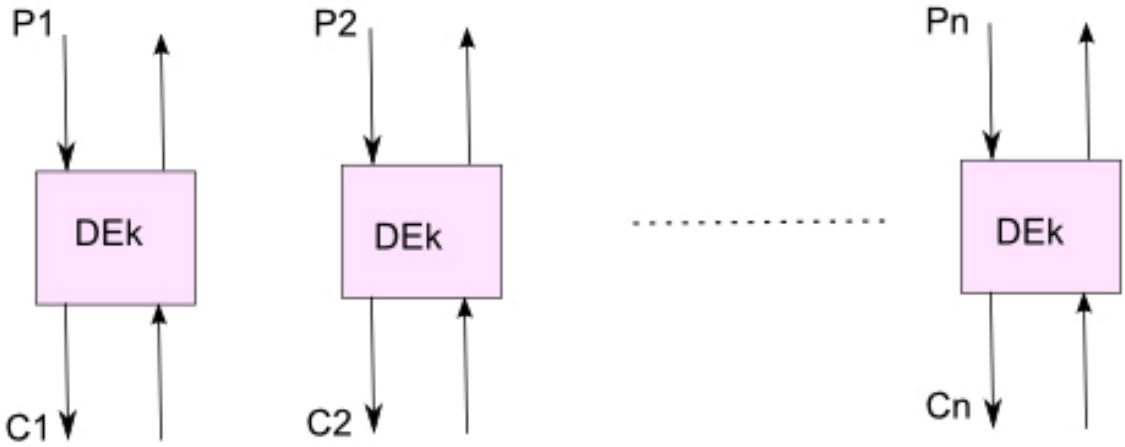
13.3 Kryptografické symetrické alogoritmy blokové

- data sú šifrované po blokoch konštantnej dĺžky
- šifrovací kľúč má rovnakú veľkosť so šifrovacími blokmi
- dĺžka šifry je rovnaká ako dĺžka dát

13.4 Štandardy pre režimy blokových šifier

13.4.1 Režim ECB

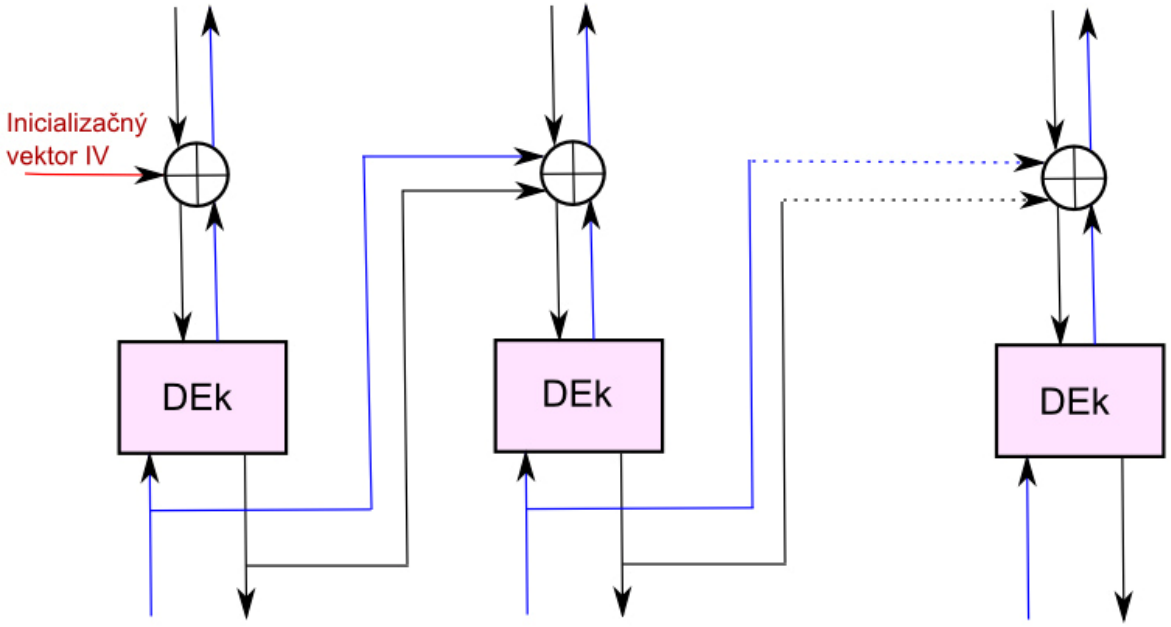
Plaintext je rozdelený na bloky, ktoré sú samostatne šifrované rovnakým kľúčom obr. 31.



OBR. 31 REŽIM ECB

13.4.2 Režim CBC

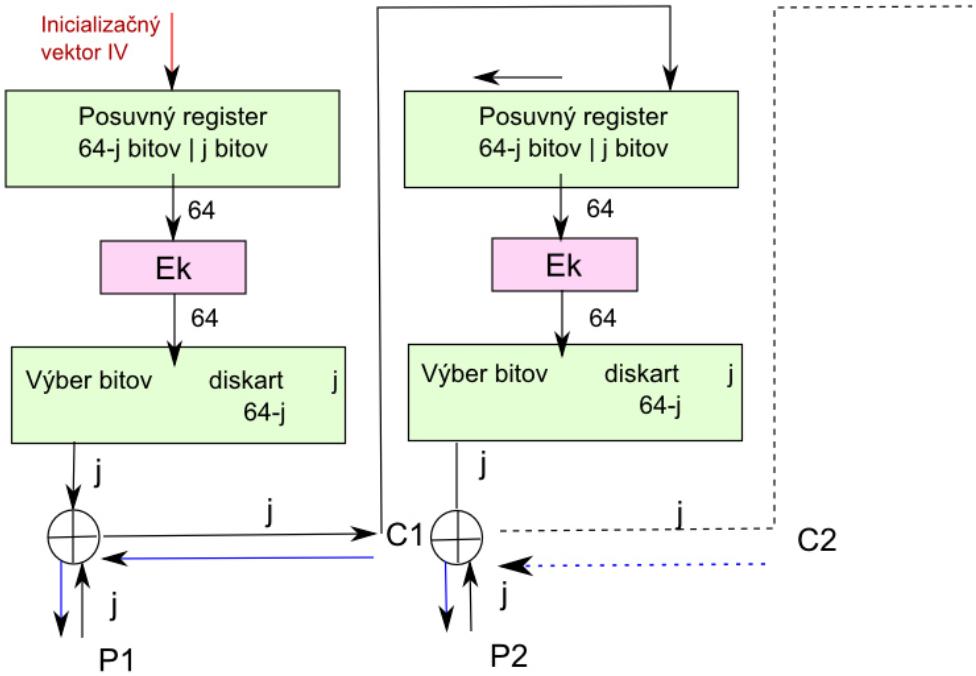
Plaintext je rozdelený na bloky, každý nasledujúci blok je pred šifrovaním zapracovaný so šifrou predchádzajúceho bloku operáciou XOR. Prvý blok je spracovávaný inicializačným vektorom obr. 32.



OBR. 32 REŽIM CBC

13.4.3 Režim CFB

Vstup je náhodný text, hardwarová implementácia obr. 33.



OBR. 33 REŽIM CFB

13.5 Kryptografické symetrické algoritmy prúdové

13.5.1 Režim CFB

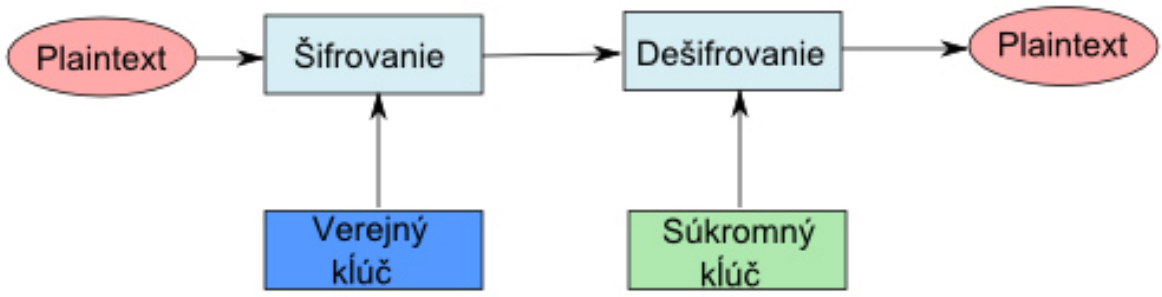
kľúč je pseudonáhodná postupnosť, ktorá sa generuje prostredníctvom blokovej šifry predchádzajúceho bloku. Blokový šifrovač negeneruje vlastnú šifru, ale dynamický kľúč, ktorým sa priebežne šifrujú bity správy

13.5.2 Režim OFB

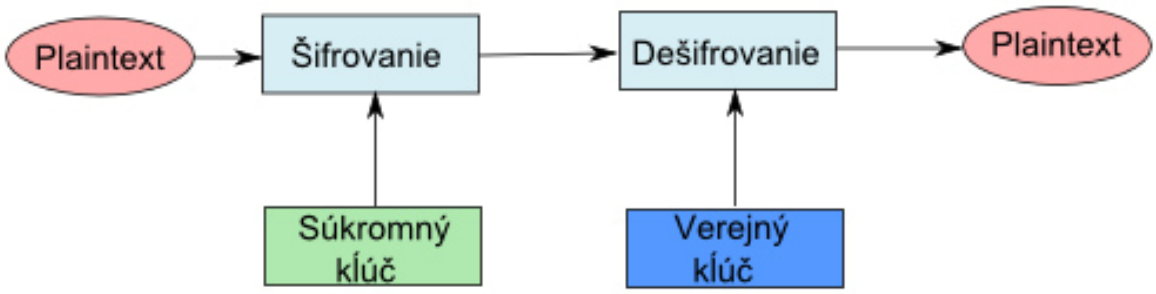
kľúč sa opakovane generuje inicializačným vektorom a výstupom generátoru. Kľúč nieje ovplyvnený šifrou.

13.6 Kryptografické algoritmy asymetrické

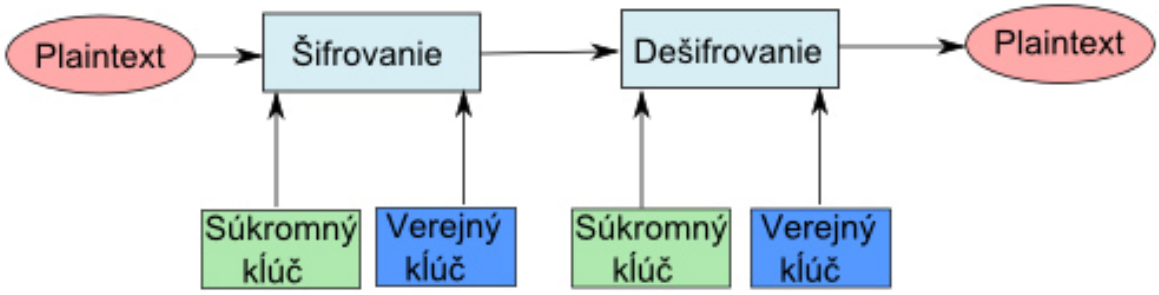
Systém generuje dva kľúče, jeden verejný a jeden súkromný. Súkromný kľúč sa používa na dešifrovanie a verejný na šifrovanie obr. 34, 35, 36. [17]



OBR. 34 KRYPTOGRAFICKÝ SYSTÉM PRE ZABEZPEČENIE DOVERNOSTI SPRÁVY



OBR. 35 KRYPTOGRAFICKÝ SYSTÉM PRE ZABEZPEČENIE AUTENTIČNOSTI SPRÁVY



OBR 36 KRYPTOGRAFICKÝ SYSTÉM PRE ZABEZPEČENIE DOVERNOTI A AUTENTIČNOSTI SPRÁVY

14 AES (ADVANCED ENCRYPTION STANDARD)

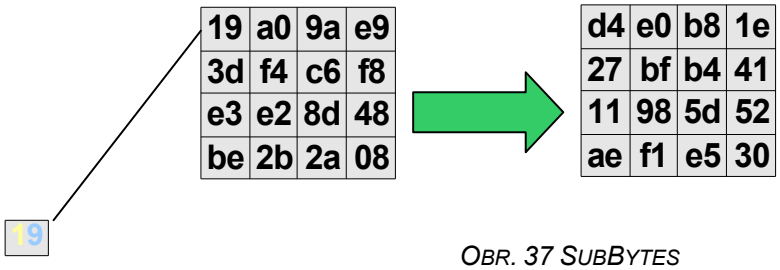
Rijndael je blokový šifrovací algoritmus. Je aplikovaný na dáta s pevne danou dĺžkou, v našom prípade 128 bitov. Pokiaľ sú dáta dlhšie, spracovávajú sa po jednotlivých blokoch. Ak sú kratšie, musia sa doplniť na požadovanú dĺžku. Existuje niekoľko algoritmov na doplnenie, od jednoduchých, doplnenie nulou až po zložitejšie schémy. Najčastejšie sa používa mechanizmus podľa PKCS #7 (RFC2315), a je obsiahnutý v .NET frameworku.

14.1 Popis šifrovania

Šifrovanie prebieha v štyroch krokoch, ktoré sa opakujú 10 krát.

14.1.1 SubBytes

Ide o jednoduchú substitúciu, kde každý byte je nahradený iným podľa daného kľúča, Rijandael-S-Box. Táto operácia zaisťuje nelineárnosť šifry a má zabrániť útokom založených na jednoduchých algebraických vlastnostiach. Hodnota 19 po substitúcii bude d4.



OBR. 37 SUBBYTES

Rijandael-S-Box

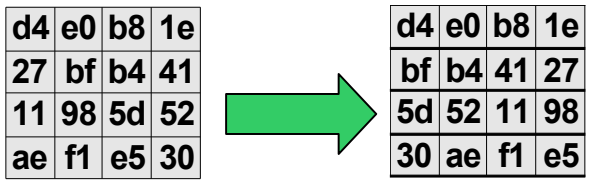
hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0																
1										d4						
2																
3																
4																
5																
6																
7																
8																
9																
a																
b																
c																
d																
e																
f																

OBR.38 S-BOX

14.1.2 ShiftRows

V tomto kroku sa jednotlivé byty posúvajú a to tak:

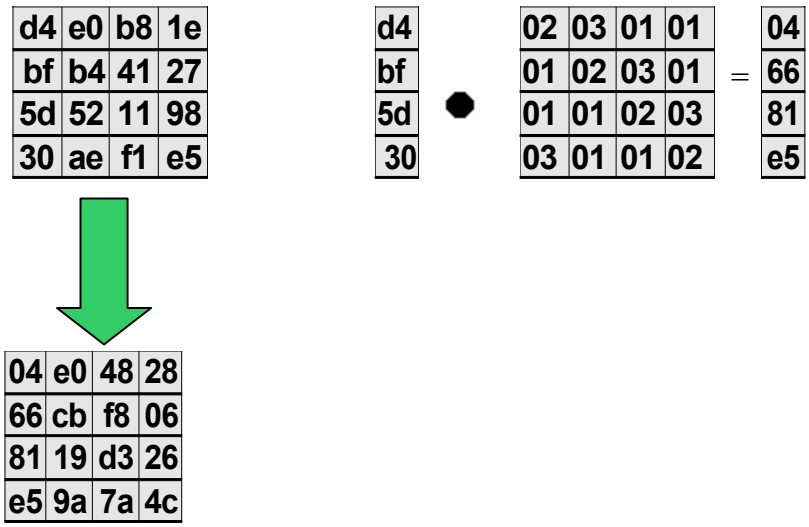
v prvom riadku o 0 bytov, v druhom o 1, v tretom o 2 a štvrtom o 3 byty.



OBR. 39 SHOFTROWS

14.1.3 MixColumns

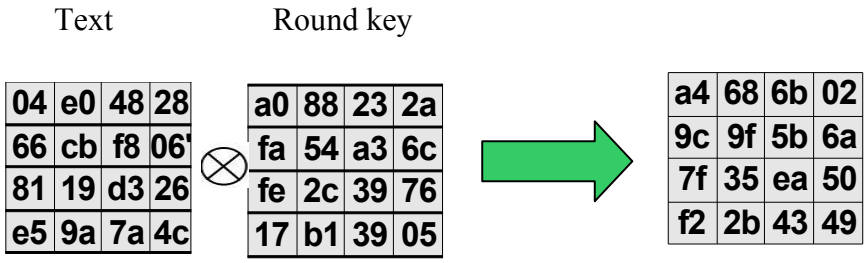
Tu dochádza k prehádzaniu stĺpcov a zároveň vynásobením rovnakým polynómom c(x).



OBR.40 MIX COLUMNS

14.1.4 AddRoundKey

Každý byt je skombinovaný so subkľúčom (sub kľúč sa získava pomocou hlavného kľúča) pomocou funkcie XOR..



$04 \otimes a0 = a4$

OBR. 41 ADD ROUND KEY

Tieto štyri kroky sú jedno kolo. Pre dĺžku 128 bit je kôl desať. Po desiatom kole by sme dostali zašifrovanú správu:

Ciphertext

39	02	dc	19
25	dc	11	6a
84	09	85	0b
1d	fb	97	32

OBR. 42 CIPHER TEXT

14.2 Výpočet kľúča pre každé kolo

Z hlavného kľúča sa vypočíta pomocou tabuľky Rcon kľúč pre každé kolo.

Hlavný kľúč

2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

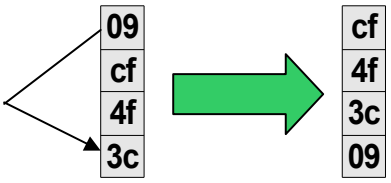
Tabuľka Rcon

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

OBR. 43 TABUĽKA RCON

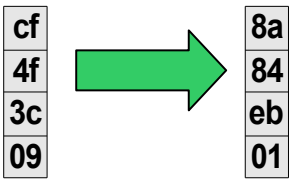
14.2.1 Postup:

1. Posledný stĺpec z hlavného kľúča: zámena prvého bytu za posledný



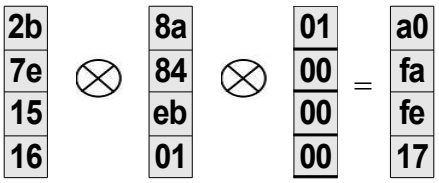
OBR. 44 KROK Č.1

2. Pomocou substitučnej tabuľky nahradíme celý stĺpec.



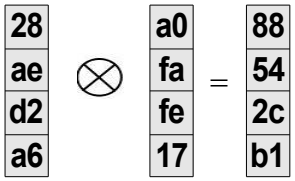
OBR. 45 KROK Č.2

3.Teraz spočítam prvý stĺpec hlavnej tabuľky, prvý stĺpec Rcon a substituovaný štvrtý stĺpec pomocou XOR. Výsledkom bude prvý stĺpec šifrovacieho kľúča pre prvé kolo.



OBR.46 KROK Č.4

4. Pre výpočet druhého stĺpca sa použije druhý stĺpec hlavného kľúča a nami vypočítaný prvý stĺpec kľúča pre prvé kolo a použije sa XOR.



OBR.47 KROK Č.5

5. Pre tretí stĺpec sa použije tretí stĺpec hlavného kľúča a druhý stĺpec kľúča pre prvé kolo. Pokračuje sa dovtedy, pokiaľ sa nevypočíta štvrtý stĺpec kľúča pre prvé kolo.

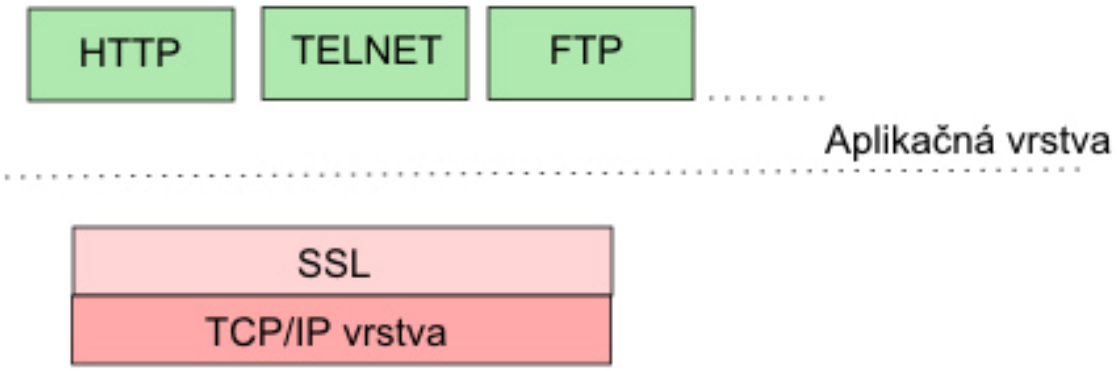
6.Pre výpočet kľúča pre druhé kolo sa pre začiatok namiesto hlavného kľúča použije kľúč pre prvé kolo.

Postup je rovnaký až po posledné kolo.[18]

15 SSL (SECURE SOCKET LAYER)

SSL je protokol, resp. vrstva vložená medzi vrstvu transportnú (TCP/IP) aplikačnú (HTTP), ktorá poskytuje zabezpečenie komunikácie šifrovaním a autentizáciou komunikujúcich strán.

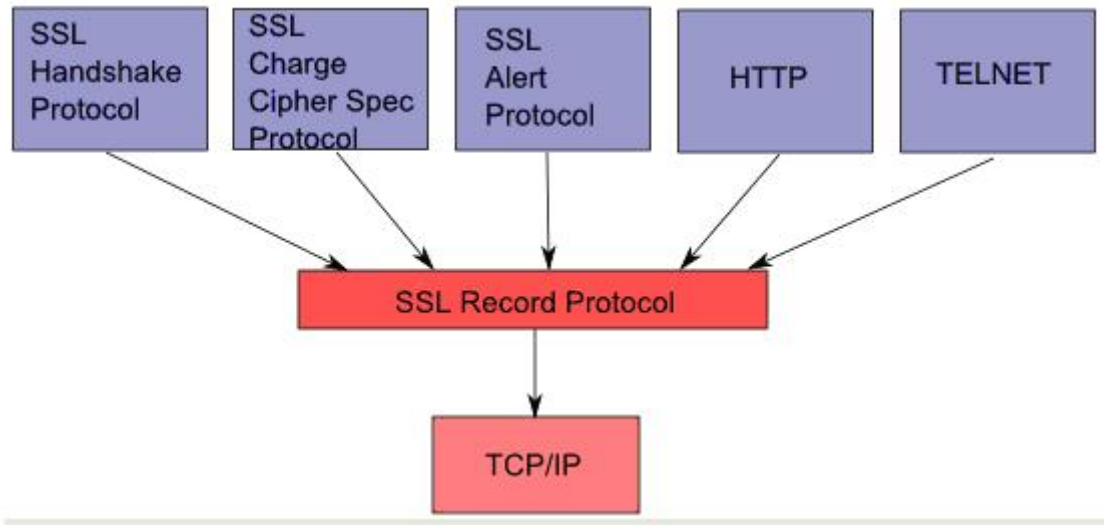
Protokol SSL sa využíva pre bezpečnú komunikáciu so serverom pomocou HTTPS, čo je zabezpečená verzia protokolu http. Po vytvorení SSL spojenia je komunikácia šifrovaná.



OBR. 48 UMIESTNENIE SSL VRSTVY

SSL má dve hlavné vrstvy: SSL Handshake a SSL Record Protokol. V dodatku má dva elementy SSL Change Cipher Spec Protocol a SSL Alert.

SSLRP je najnižšou vrstvou v SSL sade a je zodpovedný za zapuzdrenie informácii z vyššej vrstvy.



OBR. 49 HLAVNÉ VRSTVY SSL A JEJ ELEMENTY

SSL Handshake a dva elementy sú zodpovedné za manažment SSL komunikačných nastavení a bezpečnostných parametrov. SSLH zahrňuje používanie SSLRP.

15.1 Relačné a spojovacie stavy

SSL protokol má dva dôležité stavy: SSL relačný stav a SSL spojovací stav.

Relačný stav zahŕňa parametre:

- ID relácie, ľubovoľný byte pre identifikáciu relácie
- Certifikát X509.v3
- Definícia kompresného algoritmu
- Cipher spec: definícia šifrovania a MAC algoritmus, ktorý bol použitý, keď aplikačné dáta boli vyslané
- Master secret: tajná hodnota medzi klientom a serverom
- Znak pre identifikáciu keď bude relácia použitá pre iné spojenie

Spojovací stav zahŕňa:

- Náhodné číslo serveru a klienta
- Server-MAC-zapis-tajomná hodnota
- Klient-MAC-zápis-tajomná hodnota
- Server-zápis-kľúč
- Klient-zápis-kľúč
- Inicializačný vektor
- Poradové číslo (sequence number)

Každé spojenie je spojené s jednou reláciou, ale jedna relácia môže zahŕňať niekoľko rôznych spojení. Spojovací stav definuje MAC parametre, zatiaľ čo relačný stav definuje šifrovacie parametre, ktoré môžu byť použité v rôznom spojení. Každá relácia má štyri stavy: aktuálny operačný stav a nevyriešený operačný stav pre zápis a čítanie. V aktuálnom stave, CipherSuit ponúka šifrovanie a nie autentizáciu. Ak SSLH je vykonaný, nevyriešený stav sa stane aktuálnym stavom.

15.2 SSL Handshake Protokol

Protokol taktiež nazývaný key-exchange protokol, je dôležitý pre tvorbu a zabezpečenie relácie medzi dvoma stranami. SSLH môže byť rozdelený na niekoľko stupňov:

- Autentifikácia servera klientovi

- Vyjednanie bežného kryptografického algoritmu alebo šifry, ktoré server a klient podporujú
- Použitie verejného kľúča na šifrovanie pre výmenu šifrovacích parametrov (tajná hodnota)
- Vytvorenie zašifrovaného SSL spojenia

15.3 Štruktúra SSLH:

OBR. 50 ŠTRUKTÚRA SSLH

Typ: typ SSLH správy

Dĺžka: dĺžka správy

Obsah: prídavné parametre k správe

15.4 Typy SSL Handshake správy

Client_hello: táto správa je poslaná klientom na inicializáciu spojenia. Zahŕňa:

- verziu SSL
- náhodné data generované klientom
- ID relácie
- CipheSuit: zoznam key-exchange algoritmov a CipherSpecs podporovanú klientom
- Zoznam kompresných algoritmov podporované klientom

Server_hello: odpoveď na predchádzajúcu požiadavku. Obsahuje požiadavky na parametre pre klienta.

Server_certifikate: autentifikácia servera, vyslaná hneď po správe server_hello

Server_key_exchange: správa je vyslaná v prípade keď server nemá certifikát alebo má certifikát iba s podpisom jeho verejného kľúča. SSL ver. 3 podporuje algoritmy:

- RSA
- Stály Diffie-Hellman
- Jednodenný Diffie-Hellman

- Anonymný Diffie-Hellmanň
- Fortezza

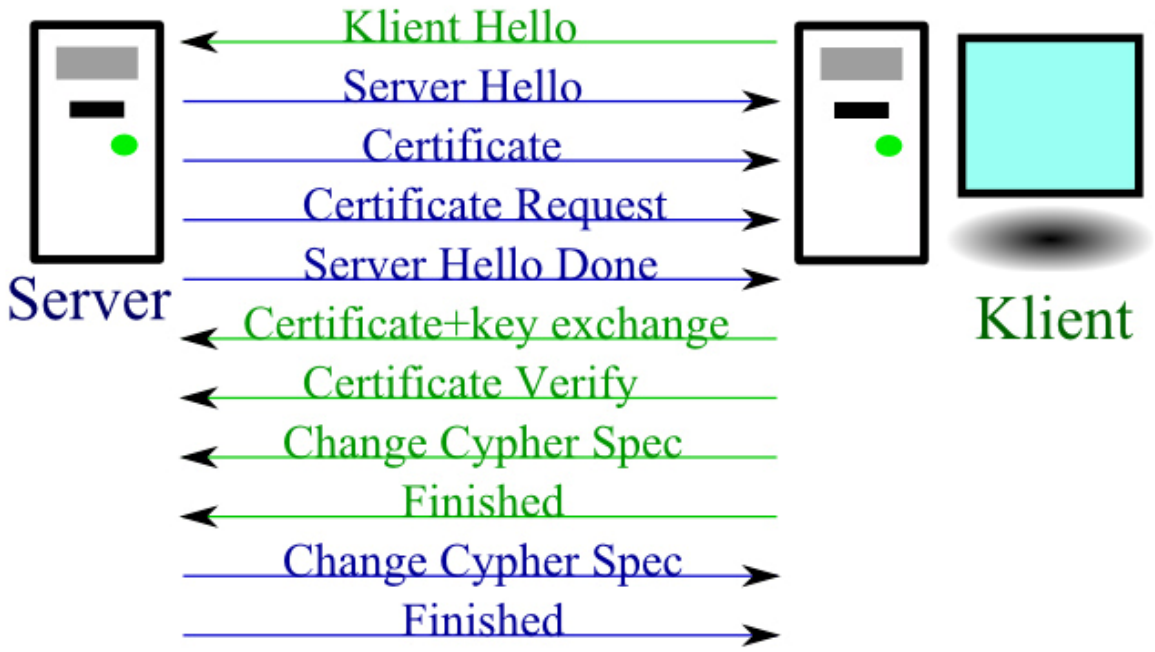
Certificate_request: táto správa je poslaná ak server požaduje klientov certifikát. Ak klient nemá certifikát tak je poslaná no_certifikate výstražná správa.
Client_key_exchange: táto správa je závislá na key-exchange algoritme definovaná serverom:

- ak RSA algoritmus je používaný pred master_secret, generovaný klientom, šifrovaný verejným kľúčom serveru
- v tomto prípade jednodenný alebo anonymný Diffie-Hellman je použitý, Diffie-Hellmana parametre verejného kľúča sú vyslané klientom
- Stály Diffie-Hellman algoritmus je použitý, táto správa nemá obsah pretože Diffie-Hellmana parametre boli práve odoslané v certifikačnej správe
- pri používaní Fortezza algoritmu, parametre Fortezza sú odoslané

Certificate_verify: táto správa je odoslaná v poradí poskytnúť konečnú verifikáciu na klientovom certifikáte. Je odoslaná nasledujúc všetkých klientskych certifikátov okrem tých, ktoré zahŕňajú stále Diffie-Helmana parametre. Teraz oba konečné body vypočítajú master_secret.
Change_cipher_spec: Oba klient a server použijú master secret na vygenerovanie kľúča relácie, ktorý je symetrický a použije sa na šifrovanie a dešifrovanie dát počas SSL relácie a na verifikáciu integrity
Finished: táto šifrovaná správa je odoslaná ihneď po SSL Change_cipher_spec správe od klienta, na indikáciu správnosti komunikačného nastavenia. Teraz klient čaká na server, pokiaľ neodošle SSL Change_cipher_spec a správu finished.

V tomto bode je handshake protokol kompletný a dáta putujú cez privátny kanál ktorý bol zrealizovaný.

Handshake protokol:



OBR.51 HANDSHAKE PROTOKOL

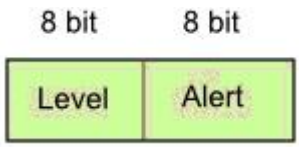
15.5 SSL Change Cipher Spec Protokol

Tento protokol je použitý ako posledný stupeň SSL Handshake protokolu v poradí, že nechá strany aby sa presunuli z nevyriadeného stavu na stav aktuálny. To znamená, že strany skončia užívať key_exchange algoritmus a budú používať šifrovanie a MAC algoritmus. Táto správa zaberá jeden byte obsahu správy a je šifrovaná a komprimovaná pod aktuálny CipherSpec.

OBR.52 SSL CHANGE SPEC PROTOKOL

15.6 SSL varovný protokol

Tento protokol je zodpovedný za informovanie vyskytnutých chýb, počas celého spojenia. Sú dva stupne výstrah: fatálna výstraha a varovná výstraha. Ak sa vyskytne fatálna výstraha, spojenie sa ukončí okamžite. Ostatné spojenia danej relácie môžu pokračovať, ale ID tejto relácie bude označené ako neplatné, takže sa nemôžu založiť nové spojenia v tejto relácii.



OBR.53 SSL ALERT PROTOKOL

Level: fatálny alebo výstražný

Výstraha: viď. tab. 2.

Fatálna výstraha	Varovná výstraha
Unexpected_message- nevhodná správa bola prijatá	**close_notify -** oznamuje prijemncu, že odosielateľ ukončil spojenie
Bad_record_mac- zlá MAC kalkulácia	**no_certifikate-** klient nemá vhodný certifikát
Decompressien_failure- dĺžka po dokompresii prekročila maximum	**bad_certifikate-** prijatý certifikát je zničený
Handshake_failure- indikuje chyby vo vyjednávaní v bezpečnostných parametroch	**Unsupported_certifikate-** certifikát je nepodporovaný
Illegal_parameter- nezrovnalosť s polom v Handshake protokole	**Certificate_revoked-** certifikát bol zrušený vlastníkom
	Certifikate_expired- platnosť certifikátu vypršala
	Certificate_unknown- vznikla neočakávaná záležitosť v procese certifikátu, tvorenie nevhodné

Tab.2 Typy výstrah

15.7 SSL record protokol (SSL záznamový protokol)

Každý záznam má záhlavie dĺžky 5 bytov. Pole záhlavia má:

Type (8 bit) – indikuje záznamové typy dát a ktoré má vyšší level protokol môže ovládať tieto záznamové dáta. Rôzne typy sú:

- change_cipher_spec
- výstraha
- handshake

- aplication_data

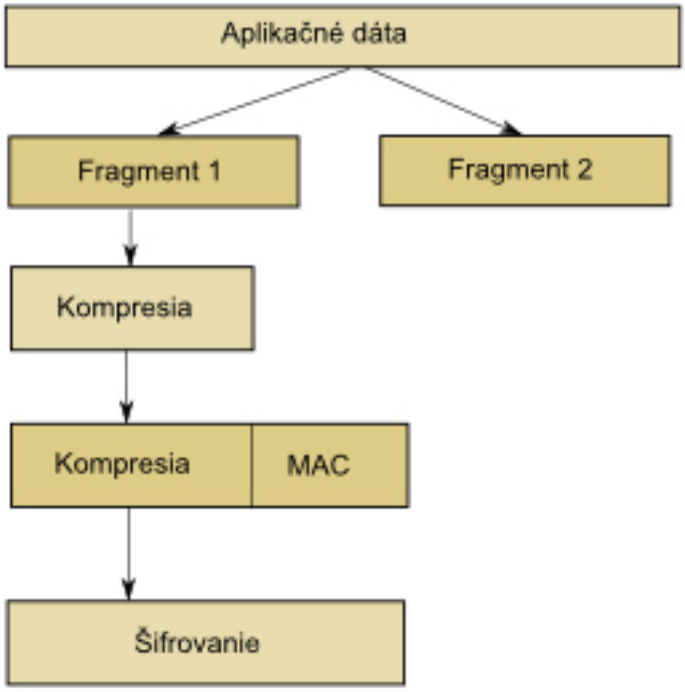
Verzia(16 bit) - obsahuje verziu SSL protokolu

Dĺžka (16 bit) – obsahuje záznam dĺžky dát

15.8 SSL Record data (SSL záznamové dáta)

Časť dát na záznamovej vrstve podrobujúca sa štvrtému stupňu:

- fragmentácia
- kompresia
- aplikácia MAC
- šifrovanie



OBR. 54 SSL RECORD DATA

Fragmentácia – dáta sú fragmentované do SSLPlaintext záznamu 2^{14} bytov, alebo menej

Kompresia – Kompresný algoritmus definovaný v Handshake. Pri kompresii sa nesmú stratiť žiadne dáta. Výsledkom je takzvaný SSLCompressed, ktorého dĺžka nesmie presiahnuť 2^{14} + 1024 bitov.

Použitie MAC (Message Authentication Code) – MAC je definovaný v Handshake, je pripojený do SSLCompressed. MAC kalkuluje nasledovne:

MAC-DATA = HASH (MAC-ZAPIS-TAJNA HODNOTA, PAD2, HASH(MAC-ZAPIS,TAJNA HODNOTA, PAD1 CISLO SEQUENCIE, SSLCompressed, typ, SSLCompressed, dĺžka, SSLCompressed, fragmentácia))

Hashovací algoritmus používaný na výpočet MAC je odvodený z CipherSuit. MAC-ZAPSI-TAJNA HODNOTA je tajné pre zdieľanie medzi klientom a serverom. PAD1 je 0x36 byte opakovaných 48 krát pre MD5 a 40 krát pre SHA. PAD2 je 0x5-c byte opakovaných ako PAD1. Sekvencia čísla sa používa ako čítač. Každá časť má dva čítače, jeden pre vyslanú správu a jeden pre prijatú. Vždy keď je správa odoslaná, čítač sa zvýši. Keď a change_cipher_spec správa je odoslaná alebo prijatá čítač je nastavený na nulu. SSL podporuje dva hashovacie algoritmy:

- MD5, 128 bitový hash
- SHA, Secure Hash Algoritm, 160 bitový hash

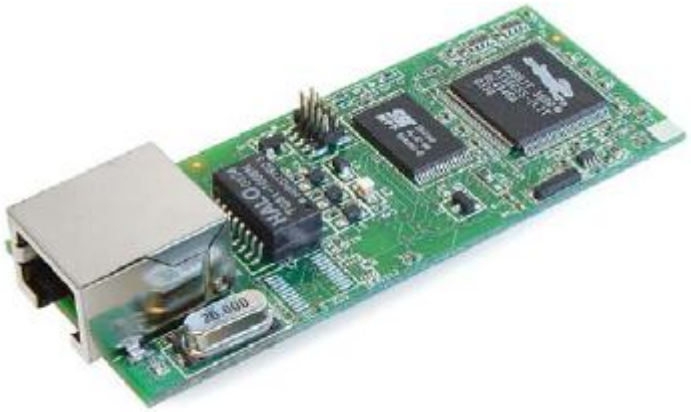
Šifrovanie: dva typy šifrovacích algoritmov sú použité v tejto sekcii: Keď algoritmus prúdovej šifry je použitý, nie sú potrebné žiadne doplnky. Ak je použitá bloková šifra, blok dát sa musí skladať menších blokov, ak nie, sú použité doplnky na doplnenie dĺžky dátových blokov, aby mohli byť rozdelené na menšie bloky šifry. Absolútna dĺžka po šifrovaní nesmie presahovať 2^{14} + 2048 bitov. [14]

15.9 Certifikačná autorita

Certifikačná autorita znamená v kryptografii objekt, ktorý vydáva digitálne certifikáty k použitiu ostatným používateľom.

16 RCM3700 RABBIT CORE

Moduly RCM boli navrhnuté pre implementáciu vložených systémov (embedded systems) s ethernetovým rozhraním. Modul určený na vývoj sa volá RCM3700 (viď obr.55)



OBR. 55 VÝVOJOVÝ MODUL RCM

Modul je spojený s vývojovou doskou pomocou 40 pinovej pätice. Jadrom modulu je osembitový mikroprocesor Rabbit 3000, ktorý pracuje na kmitočte 22,1 MHz. [8]

Software, ktorý sa dá v module implementovať:

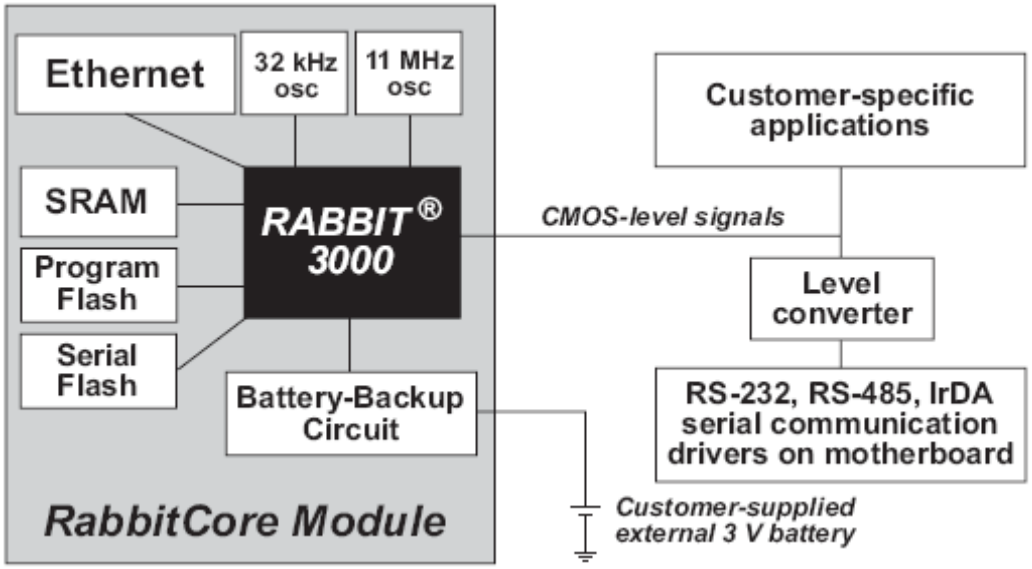
- AES- šifrovací algoritmus
- FAT- súborový systém
- PPP- point-to-point protokol
- SSL- šifrovací algoritmus
- Rabbit Web- http server

Mikroprocesor	Rabbit 3000® running at 22.1 MHz
FLASH	512K
SRAM	512K
Serial FLASH	1 Mbyte
Sériové porty	•4 vysokorýchlostné 3.3 V CMOS kompatibilné Konfigurovateľné asynchrónne porty (s IrDA) • 3 ako SPI a 1 ako HDLC • 1 asynchrónny sériový port pre programovanie

Tab.3 Špecifikácia modulu RCM3700

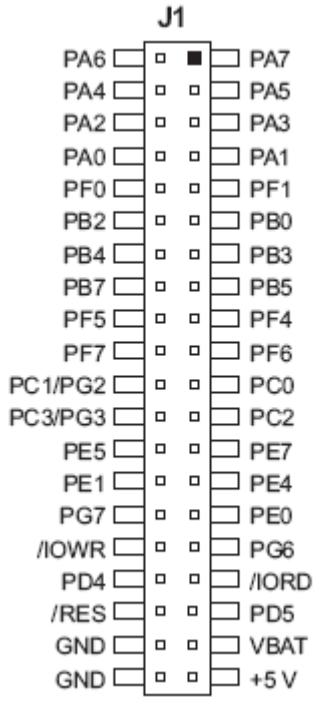
16.1 Vstupy a výstupy

Na obr.56 je znázornený hardwarový subsystém modulu Rabbit 3700.



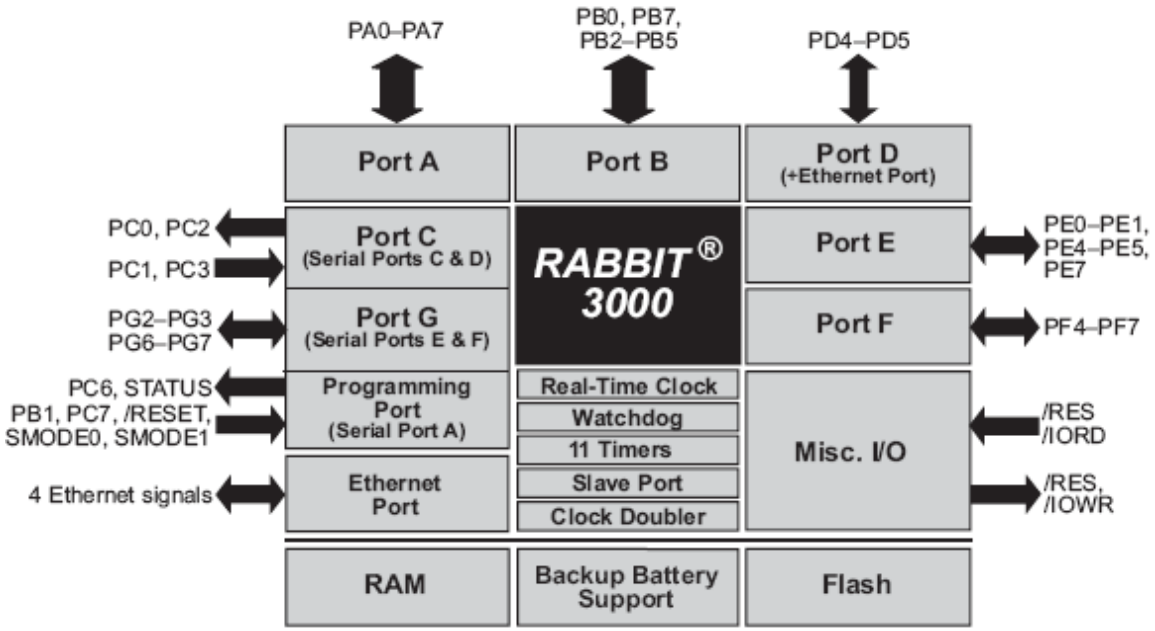
OBR. 56 VSTUPY A VÝSTUPY RCM 3700

Modul sa zasúva do pätice, ktorá je znázornená na obr.57 . Tieto piky je možné vidieť so spodnej časti modulu.



OBR. 57 PATICA PRE RCM 3700

Jadrom modulu je mikroprocesor Rabbit 3000, s použiteľnými portami viď. obr. 58.



OBR.58 PORTY RABBIT 3000

Porty na Rabbit 3000 mikroprocesor používané RCM 3700 sú konfigurovateľné a štandardné nastavenie sa môže prekonfigurovať. Tab. 4 Ukazuje na možnosti a využitie portov.[11]

PIN	Názov	Pôvodné použitie	Alternatívne použitie	Popis
1-8	Pa[7:0]	Paralelný I/O	Externá dátová zbernica(ID0-ID7)	Externá dátová zbernica
9	PF1	I/O	QD1A, CLKC	
10	PF0	I/O	QD1B, CLKD	
11	PB0	I/O	CLKB	
12	PB2	I/O	IA0, /SWR	Externá adresa 0
13	PB3	I/O	IA1, /SRD	Externá adresa 1
14	PB4	I/O	IA2, /SA0	Externá adresa 2
15	PB5	I/O	IA3, /SA1	Externá adresa 3
16	PB7	I/O	IA5, /SLAVEATTN	Externá adresa 5
17	PF4	I/O	AQD1B, PWM0	
18	PF5	I/O	AQD1A, PWM1	
19	PF6	I/O	AQD2B, PWM2	
20	PF7	I/O	AQD2A, PWM3	

21	PC0	Output	TXD	Sériový port D
22	PC1/PG2	I/O	RXD/TXF	Sériový port D a F
23	PC2	Output	TXC	Sériový port C
24	PC3/PG3	I/O	RXC/RXF	Sériový port C a F
25	PE7	I/O	I7, /SCS	I/O snímací impulz 7
26	PE5	I/O		
27	PE4	I/O		
28	PE1	I/O		
29	PE0	I/O		
30	PG7	I/O	RXE	Sériový port E
31	PG6	I/O	TXE	Sériový port E
32	/IOWR	Output		
33	/IORD	Input		
34	PD4	I/O	ATXB	Alternatívy sériový port B
35	PD5	I/O	ARXB	Alternatívy sériový port B
36	/RES	Reset Output	Reset input	Reset
37	VBAT			
38	GND			
39	+5V			
40	GND			

Tab.4 Špecifikácia modulu RABBIT 3000

16.2 Pamäťové I/O rozhrania

U Rabbit 3000 adresné spojenia (A0-A18) a všetky dátové spojenia (D0-D7) sú vnútorne smerovateľné do flash pamäte a SRMA čipu. I/O zápis (/IOWR) a I/O čítanie (/IORD) sú dostupné na rozhraniach pre externé zariadenia.

Paralelný port A môže byť použitý ako externý I/O dátová zbernica k izolovaniu externého I/O z hlavnej dátovej zbernice. Paralelný port B, piny PB2-PB5 a PB7 môžu byť použité ako pomocné adresné zbernice.[11]

16.3 Iné I/O

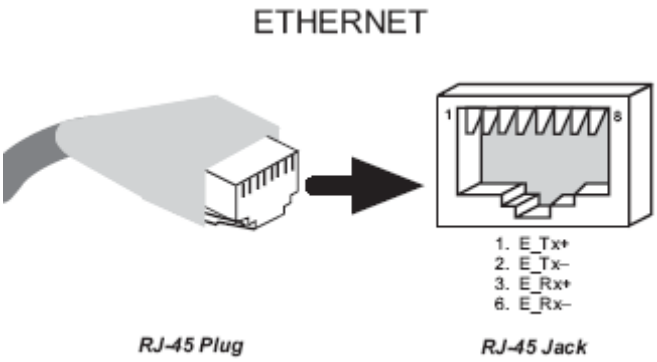
/RES tento pin môže byť použitý na resetovanie mikroprocesoru.[11]

16.4 Sériové porty

Modul RCM 3700 má 5 sériových portov pomenovaných ako sériové porty A, C, D, E a F. Všetky pracujú v asynchrónnom móde. Sériový port A je bežne používaný ako programovací port, ale môže byť použitý ako asynchrónny. Porty C a D sa môžu nakonfigurovať na prácu v synchrónnom móde. Porty E a F Môžu pracovať ako HDLC sériový port. IrDA protokol je tiež podporovaný ako SDLC formát pre tieto dva porty.[11]

16.5 Ethernet port

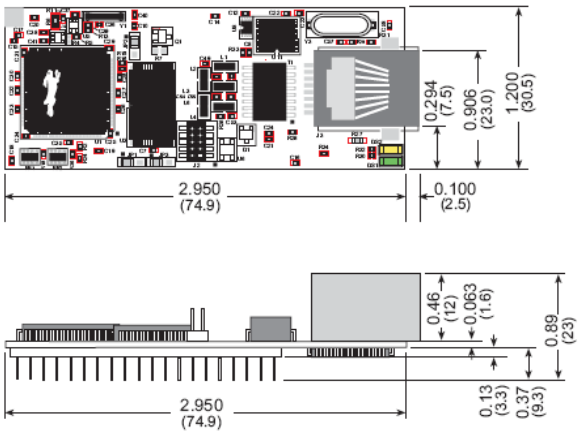
Na obr. 59 sú znázornené využívané piny pre Ethernet konektor. Dve LED diódy sú umiestnené vedľa RJ-45 konektoru na indikáciu linky a aktivity.[11]



OBR. 59 ETHERNET PORT

16.6 Elektrické a mechanické vlastnosti

Na obr. 60 vidíme mechanické vlastnosti, na ich základe budeme realizovať primerané rozmery základnej dosky. [11]



OBR. 60 RCM 3700

Parametre	RCM3700
Mikroprocesor	Rabbit 3000, 22.1 MHz
Ethernet port	10/100 10Base-T
Flash pamäť	512K
SRAM	512K
Sériová flash pamäť	1MB
Záložný zdroj	Ano
Prídavný I/O port	Reset
Sériová rýchlosť	CLK/8
Časovače	desať 8-bit časovačov
Watchdor	Ano
Napájanie	4.75 až 5.25 V DC
Pracovné teploty	40°C do 70°C

Tab.5 Parametre modulu RCM 3700

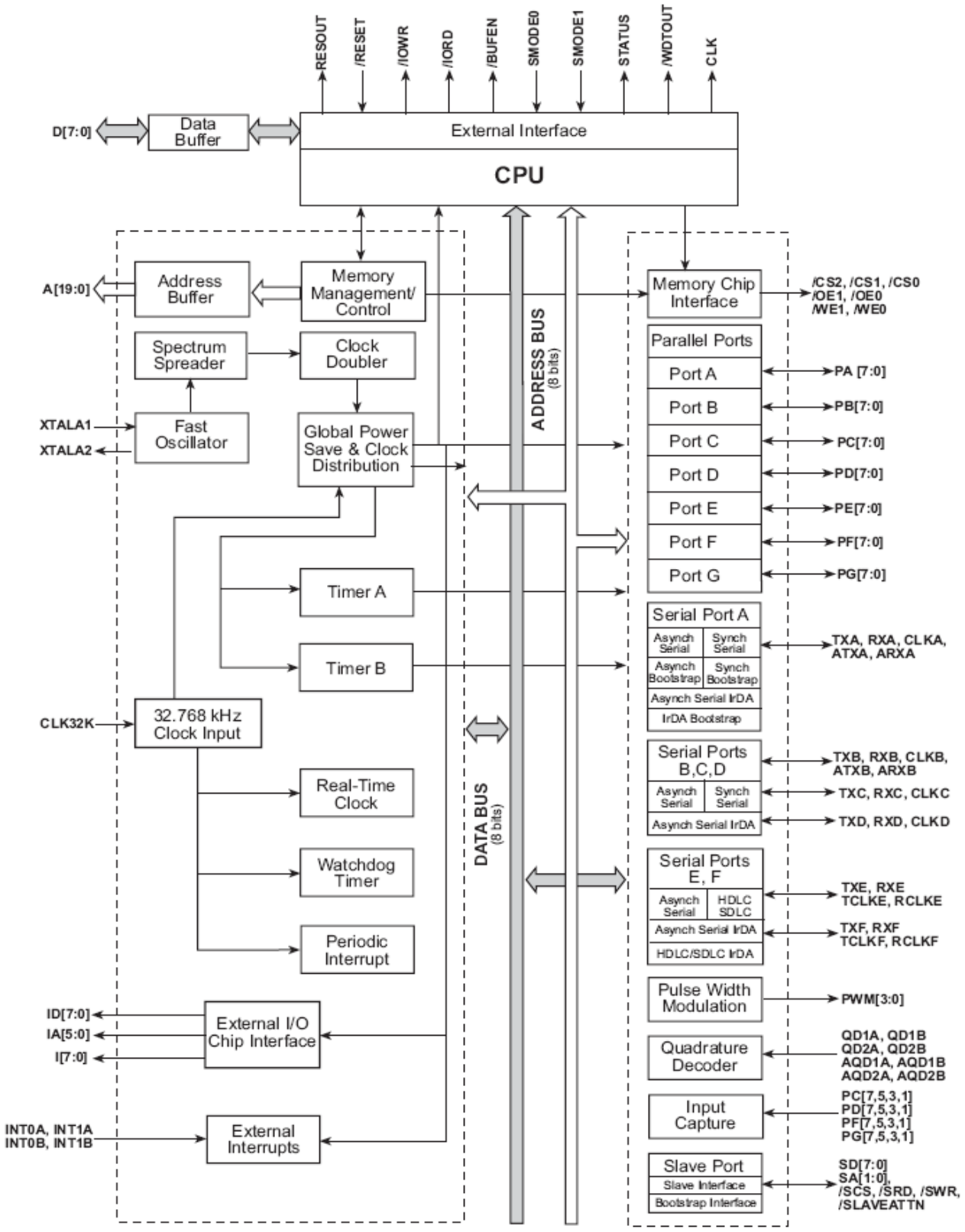
16.7 Rabbit 3000

Rabbit 3000 je vysokovýkonný mikroprocesor s nízkym elektromagnetickým rušením (EMI). 8-bitový mikroprocesor R3000 bol špeciálne navrhnutý na pripojenie ako radič, komunikátor a pre Ethernet spojenie. Sada inštrukcii je úzko založená na jednom zo Z80, iba I/O inštrukcie boli zmenené pre lepšie využitie programovacieho jazyka C. Adresná zbernica o šírke 20 bitov je schopná adresovať 1MB dát.[12]

16.8 Vlastnosti

R3000 má niekoľko silných vlastností na elimináciu problémov EMI, ktoré sú základné pre OEM, ktorý musí prejsť cez CE a regulárny rádio frekvenčný emisný test. Amplitúda každého elektromagnetického žiarenia je redukovaná vnútorným rozprestretím spektra, ktorý je synchronizovaný hodinami a odseparovaný od napäťových úrovní procesorového jadra a I/O pinov. Externá I/O zbernica môže byť použitá na umožnenie separácie zberníc pre I/O a pamäte alebo na ohraničenie zaťaženia pamäťovej zbernice na redukciu EMI. Táto externá I/O zbernica vykonáva duplikáciu dátovej zbernice na paralelnom porte A a používa paralelný port B na poskytovanie šesť alebo osem najmenej významných adresných spojov pre rozhranie s externými periférnymi zariadeniami. Vysoko účinná inštrukčná sada ponúka väčšiu výkonnosť a rýchlosť vykonávania kompilácie kódu. R3000 nevyžaduje externú pamäť alebo logické rozhranie, lebo 20 bitová adresná zbernica, 8 bitová dátová zvernica, tri výberové linky pre čip, dve výstupné linky a dve zapisovacie linky môžu byť medzi plošne, priamo spojené až do šiestich pamäťových zariadení. Až do 1MB pamäte môže byť

sprístupnený priamo cez Dynamic C vývojový software, do 6MB medzi plošne dodatkovým softwarovým vývojom.[12]



OBR. 61 BLOKOVÝ DIAGRAM

17 RS232

17.1 Základný technický popis

Štandard definuje asynchrónnu sériovou komunikáciu pre prenos dát. Poradie prenosu dátových bitov je od najmenej významného bitu (LSB) po bit najvýznamnejší (MSB). Počet dátových bitov je voliteľný, obvykle sa používa 8 bitov, dá sa také stretnúť so 7 nebo 9 bity. Logický stav „0“/„1“ prenášaných dát je reprezentovaný pomocou dvoch možných úrovní napätí, ktoré sú bipolárne a podľa zariadení môžu nadobúdať hodnôt ±5 V, ±10 V, ±12 V nebo ±15 V. Najčastejšie sa používa varianta pri ktorej logická hodnota 1 odpovedá napätie -12 V a logické hodnote 0 potom +12 V. Základné tri vodiče rozhrania (príjem RxD, vysielanie TxD a spoločná zem GND) sú doplnené ešte ďalšími slúžiacimi k riadeniu prenosu (vstupy DCD, DSR, CTS, RI, výstupy DTR, RTS). Tie môžu a nemusia byť používané. [13]

17.2 Popis signálov

Základný popis signálu pre RS232 viď. tab. 6: [13]

Signál	Popis
DCD - Data Carrier Detect	Detekcia nosné (niekedy len "CD). Modem oznamuje terminálu, že na telefónnej linke detekoval nosný kmitočet.
RXD - Receive Data	Tok dát z modemu (DCE) do terminálu (DTE)
TXD - Transmit Data	Tok dát z terminálu (DTE) do modemu (DCE).
DTR - Data Terminal Ready	Terminál týmto signálom oznamuje modemu, že je pripravený komunikovať).
SGND – Signal Ground	Signálová zem
DSR - Data Set Ready	Modem týmto signálom oznamuje terminálu, že je pripravený komunikovať).
RTS - Request to Send	Terminál týmto signálom oznamuje modemu, že komunikační cesta je voľná).
CTS - Clear to Send	Modem týmto signálom oznamuje terminálu, že komunikační cesta je voľná).
RI - Ring Indicator	indikátor zvonenia. Modem oznamuje terminálu, že na telefónnej linke detekoval signál zvonenia.

Tab. 6 Využitie portov

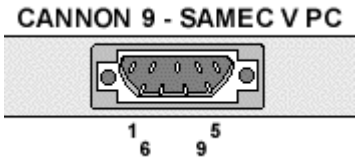
17.3 Zapojenie konektorov pre RS-232

Spojenie konektorov pre RS232 viď. (tab. 7) [13]

Cannon 9:

Pin	Názov	Smer
1	CD	<--
2	RXD	<--
3	TXD	-->
4	DTR	-->
5	GND	---
6	DSR	<--
7	RTS	-->
8	CTS	<--
9	RI	<--

Tab. 7 Spojenie konektorov pre RS232

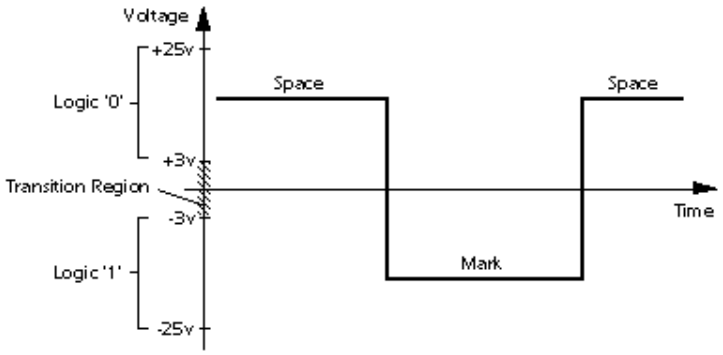


OBR.62 CANNON 9

17.4 Napäťové úrovne

RS 232 používa dve napäťové úrovne. Logickou 1 a 0. Log. 1 je niekedy označovaná ako marking state alebo tiež kľudový stav, Log. 0 sa prezíva space state.

Log. 1 je prenášaná zápornou úrovní, zatiaľ čo logická 0 je prenášaná kladnou úrovňou výstupných vodičov vid. Obr. 63. [13]



OBR. 63 NAPAŤOVÉ ÚROVNE

17.5 Synchronizácia RS232

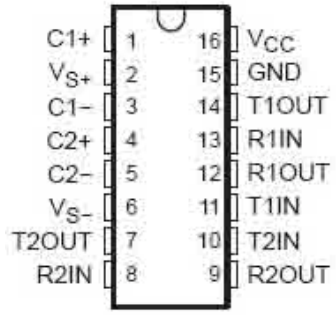
RS232 Používa asynchrónny prenos informácii. Každý prenesený byte konštantnou rýchlosťou je preto treba synchronizovať. K synchronizácii sa používa nábežná hrana tzv. Start bitu. Za ňou už nasledujú poslané data viď. obr. 64. [13]

OBR. 64 SYNCHRONIZÁCIA RS232

18 MAX 232

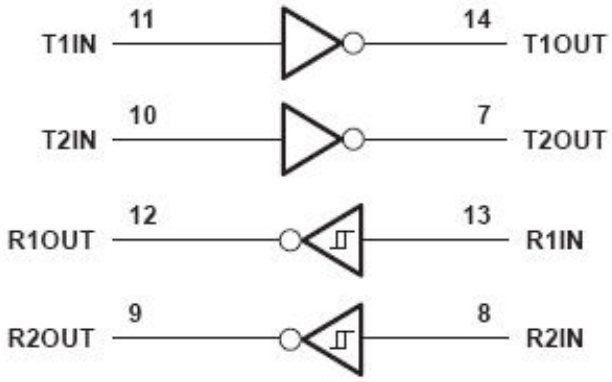
MAX232 je veľmi používaný prevodník úrovní RS-232 (sériová linka) na TTL úrovne. Napätie pre RS 232 sa získava pomocou nábojové pumpy a výstupné napätie, preto značne závisí na kvalite použitých kondenzátorov, ktoré u nich časom značne klesá. Nespornou výhodou je, že potrebuje iba jeden zdroj napätia a to +5V, a nie +15,-15 ako niektoré iné prevodníky. Obsahuje 2 prevodníky TTL=>RS232 a 2 prevodníky RS232=>TTL.

Popis pinov puzdra:



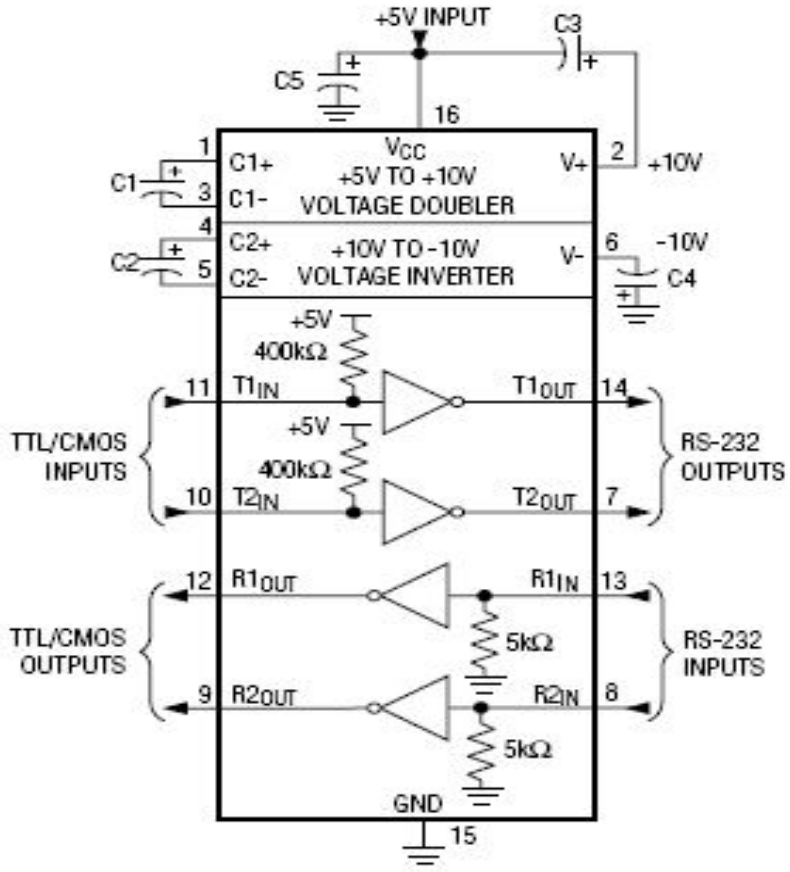
OBR. 65 POPIS PINOV PÚZDRA

Obvod zvláda operácie minimálne o rýchlosti 120kbitov/s, vstupnej úrovne na vstupoch RS232 môžu dosahovať úrovne až ±30V a odoberaný prúd je asi 8mA. Obvody neslúžia ako prosté budiče, ale sú to invertory viď obr.66.



OBR. 66 INVERTORY

Zapojenie tohto obvodu v praxi a pripojení kapacít pre jeho nábojovou pumpu je na obr.67.

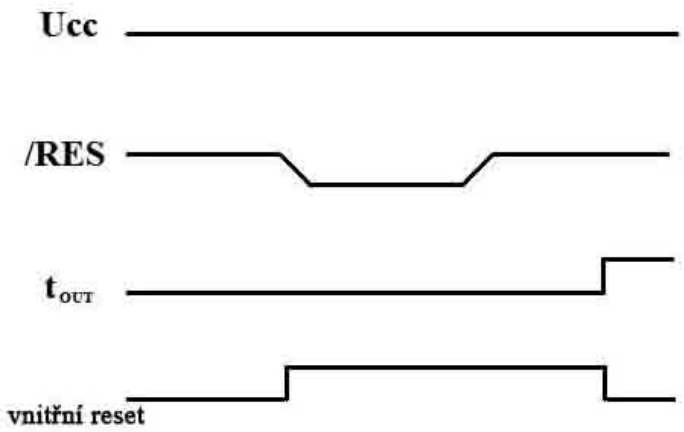


OBR.67 ZAPOJENIE KAPACÍT

U obvodu MAX232 sú všetky použité kapacity 1uF až na kondenzátor C3, ktorý podľa datasheetu je 10 uF. [13]

18.1 Reset

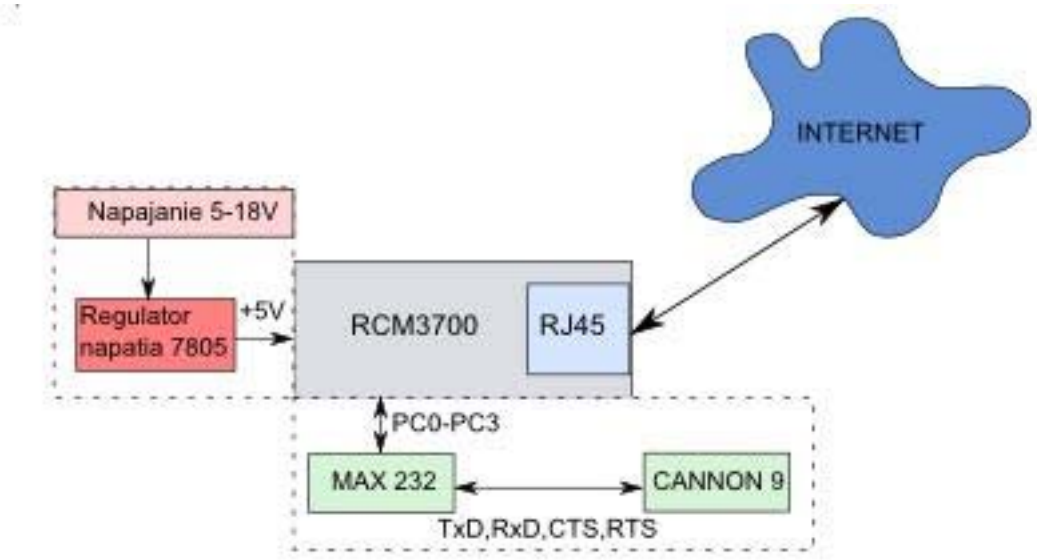
Vnútorný reset je generovaný log. 0 na vývodu /RESET. Pulzy dlhšie ako 50ns generujú reset i v prípade, že kryštálový oscilátor nebeží. Po pochodu úrovne u RST do log.1 je vnútorný reset generovaný až do uplynutí doby tOUT viď. obr. 68. [13]



OBR.68 RESET

19 NÁVRH DOSKY PLOŠNÉHO SPOJA

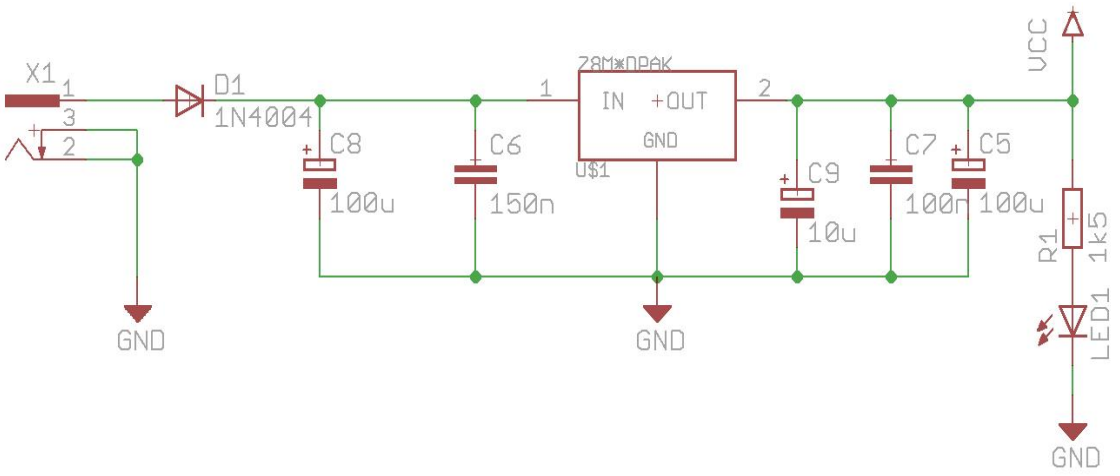
Táto kapitola sa zaoberá návrhom dosky plošného spoja pre modul RCM 3700. Modul musí byť napájaný vhodným napätím, musí mať resetovacie tlačítko, signalizačné diódy a komunikáciu cez rs232. Návrh dosky bol prevedený po dôkladnom preštudovaní technických a elektrických parametrov modulu RCM 3700. Pätica je základným komunikačným prostredníkom modulu RCM, obsahuje dvojradovú päticu po 20tich pinoch , ktorá je používaná v IDE kábloch stolných počítačov. [1]



OBR. 69 BLOKOVÉ SCHÉMA

19.1 Napájanie

Pred pripojením napätia k základnej doske je nutné napätie stabilizovať.
Stabilizovať napätie znamená udržať jeho veľkosť konštantnú, aj v prípade že sa bude meniť záťaž alebo kolísať napájacie napätie (sieťové).
Schéma zapojenia viď obr. 70.



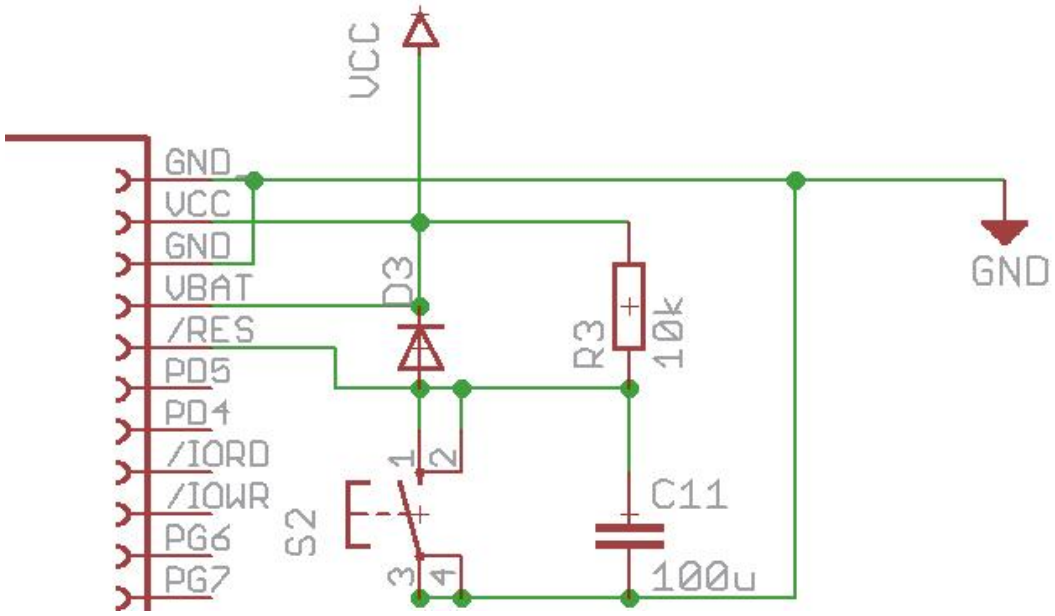
OBR. 70 NAPÁJANIE DOSKY PLOŠNÉHO SPOJA

Integrovaný obvod 7805 je integrovaným stabilizátorom pevného napätia o nominálnej hodnote 5V. K jeho funkcii postačia dva blokovacie kondenzátory, pripadne filtračný kondenzátor na vstupe. Doporučuje sa tiež spätná dióda z výstupu na vstup ako ochrana proti náhlemu zníženiu napájacieho napätia prípadne prítomnosti ďalšieho napájacieho napätia na výstupe stabilizátoru. [15]

19.2 Reset

Reset slúži na reštart modulu RCM do pôvodných nastavení.
Po pripojení napájania sa začne nabíjať pôvodne vybitý kondenzátor. Tým sa drží vstup /RESET na log. 0. Pomocou tlačítka RESET je možno obvod resetovať manuálne.

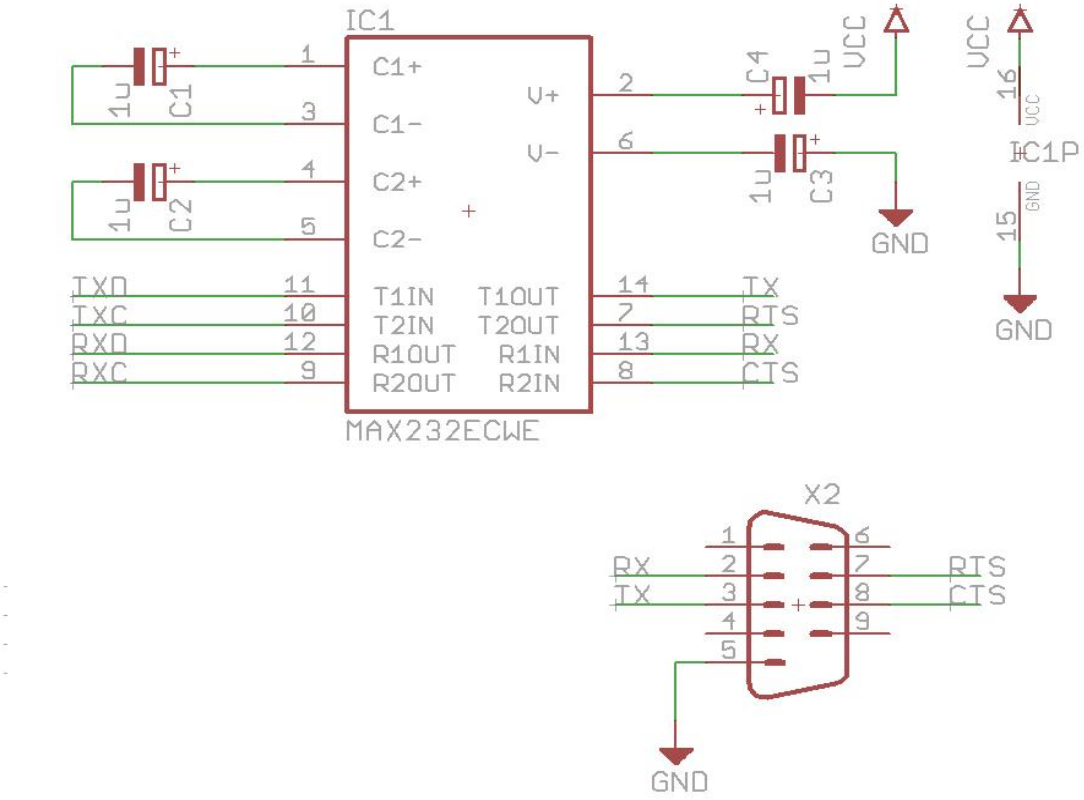
Zapojenie resetu viď obr. 71.



OBR. 71 RESET

19.3 RS232

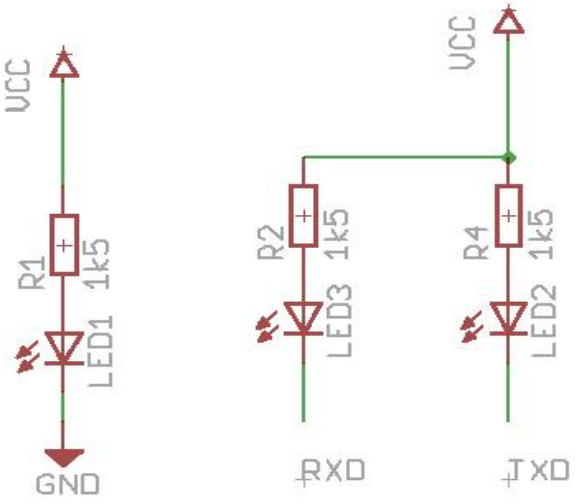
Ďalšou časťou základnej komunikačnej jednotky sú prvky obsahujúce sériové rozhranie modulu. Modul je vybavený sériovým rozhraním, ale neobsahuje prvky zaisťujúce požadovanú RS232 komunikáciu, ktorá potrebuje zvýšené napájacie napätie, ako je obvyklá hodnota TTL. Na základnú dosku bol pridaný ovládač sériového rozhrania RS232 MAX232, ktorý umožňuje obojstranne prevádzať napäťové úrovne RS232 a TTL. Jeho I/O brány sú pripojené na Port C a Port D mikroprocesoru. Zapojenie disponuje 5 drôtovú komunikáciu, i keď postačí iba 3 drôtová komunikácia. [1]



OBR. 72 ZAPOJENIE RS232

19.4 Signalizačné diódy

Signalizačné diódy sú použité na signalizáciu RS232 komunikácie a na signalizáciu napájania. Zapojenie diód viď obr. 73.



OBR. 73 SIGNALIZAČNÉ DIÓDY

20 ZÁVER

Spomenuté útoky sú charakteristické tým, že sa útočník musí pripojiť do lokálnej siete. Prvou ochranou je zakázať užívateľom inštalovať ľubovoľný software. Stále hrozí riziko že sa útočník pripojí do niektorých voľných zásuviek vlastným počítačom vybaveným príslušným softwarom. Sieťové zariadenia (huby, switche, routery) sú často umiestnené na jednom mieste do rackovej skrine. Ktorá by mala byť zamknutá a prípustná len oprávneným osobám. Rozvod LAN býva realizovaný štruktúrovanou kabelážou s vývodmi v rôznych miestach v budove. Pomocou niektorej metódy sociotechniky, sa môže útočník dostať k niektorej z týchto zásuviek a pripojiť sa na lokálnu sieť, preto najúčinnejšie je pravidelné kontrolovanie zásuviek. Medzi metódy patrí sledovanie LED diód na switchi alebo fyzické odpojenie nepoužívaných zásuviek na patch paneloch. Sofistikovanou metódou je overovanie užívateľov pomocou EAPOL (Extensible Authentication Protokol over LAN). Tento protokol filtruje porty na switchi. Pokiaľ sa chce užívateľ pripojiť do siete, musí sa prihlásiť. Je možné použiť rôzne prostriedky identifikácie napr. heslo, čipová karta, USB token. Totožnosť sa neoveruje na switchi ale pomocou autentizačného serveru. Na základe úspešných útokov z LAN som ako bezpečnostný faktor zrealizoval VLAN. Virtuálne LAN sa konfigurujú na prepínači a úspešne eliminujú útoky z LAN. V laboratórií som zrealizoval VLAN na CISCO prepínači 2801, zaoberá sa tým kapitola 12. V ďalšej časti práce bolo treba navrhnúť a zrealizovať dosku plošného spoja pre sieťový modul RCM 3700. Po zoznámení s modulom som sa začal zaoberať samotným návrhom DPS, ktorá bude obsahovať rozhranie RS232 pre komunikáciu s koncovým meracím zariadením, resetovacie tlačítko, signalizačné diódy a napájací zdroj (viď. Kapitola 19). Pred návrhom dosky som vyhľadal vhodnú krabičku pre umiestnenie zariadenia, na základe ktorej som zvolil správnu veľkosť dosky plošného spoja. Doska plošného spoja základnej dosky bola navrhnutá jednostranou cestou, čo umožnilo jednoduchšiu výrobu a napriek tomu bola testovaná na výskyt skratových ciest, lebo niektoré cesty boli vedené medzi piny pätice a pod MAX 232 o minimálnej hrúbke 0.4064 mm. Po osadení a pripojení dosky k zdroju napätia bola doska premeraná aby nedošlo v prípade chyby k poškodeniu modulu. Pri meraní som overil výskyt napätia 5V za stabilizátorom a odpovedajúce napätie 10V a 6.3V na nábojových pumpách MAX 232. Doska je umiestnená v hliníkovej krabičke, ktorej otvory sú vybrúsené (viď. Príloha III a IV). Týmto považujem cieľ práce za splnený.

21 POUŽITÁ LITERATÚRA

[1] KOUTNÝ, M.: *Komunikační jednotka koncového měřícího zařízení v energetice*. Diplomová práce VUT v Brně, FEKT, Ústav telekomunikací, 2007.

[2] CONNECT, IT časopis. Článek: *Nejznámější útoky v síti Ethernet*. Dostupný z WWW: http://connect.zive.cz

[3] RFC 793 : Transmission Control Protocol. *Internet RFC/STD/FYI/BCP Archives* [online]. 1982 [cit. 1981-09-01]. Dostupný z WWW: <http://www.faqs.org/rfcs/rfc793.html>.

[4] LUPA, Server o českém internetu. Článek: *Odposloucháváme data na přepínaném Ethernetu.* Dostupný z WWW: http://www.lupa.cz

[5] Stuart McClure, Joel Scambray, George Kurtz: *Hacking bez záhad*, Grada, Praha 2007, ISBN 978-80-247-1502-5

[6] PUŽMANOVÁ, Rita.
TCP/IP v kostce. České Budějovice: KNOPP, 2004. 608 s. ISBN 80-7232-236-2.

[7] HATCH Brian, LEE James, KURTZ George.
Linux-Hackarské útoky. Bezpečnost Linuxu-Tajemství a řešení. Praha: SoftPress, 2002. 567 s. ISBN 80-86-497-17-8.

[8] MLÝNEK, P.: *Systém pro testování odolnosti komunikační jednotky LAN dálkového sběru dat*. Diplomová práce VUT v Brně, FEKT, Ústav telekomunikací, 2008-12-03.

[9] MIŠUREC, J., MLÝNEK,P.: *Principy testování odolnosti komunikační jednotky LAN dálkového sběru dat*. Elektrorevue - Internetový časopis, Dostupný z WWW: http://www.elektrorevue.cz , 2008/16, ISSN 1213-1539.

[10] DOSTÁLEK, L. a kolektív.: *Velký průvodce protokoly TCP/IP a Bezpečnost*, 2. vydání. Computer Press 2002, 592 s, ISBN 80-7226-849-X.

[11] *Rabbit Semiconductor Inc.:* RabbitCore RCM3700 User's Manual ,2006

[12] *Rabbit 3000 Microprocessor : User's Manual*. 19th rev. edition : Rabbit Semiconductor Inc., 2006. 166p.

[13] *ENCYKLOPEDIE RS232* [online]. 2001 [cit. 2009-4-14]. Dostupný z WWW: http://hw.cz/rs-232

[14] Ssl-certifikaty *[online]*. 2008 [cit. 2009-04-14]. Dostupný z WWW: <http://www.ssl-certifikaty.cz/o-certifikatech/ssl-protokol/>

[15] *TL7805A : DataSheet*. 1st edition : Semiconductor Components Industries , 2005. 32p.

[16]*MAX232CWE : DataSheet*. 1st edition : Maxim Integrated Products , 2000. 36p.

[17] KUNDEROVÁ, Ludmila. Bezpečnost IS/IT. *Bezpečnost IS/IT* [online]. 2009 [cit. 2009 05-13]. Dostupný z WWW: <https://akela.mendelu.cz/~lidak/bis/8kryp.htm>.

[18] AES. *AES* [online]. 2009 [cit. 2009-05-13]. Dostupný z WWW: <http://www.kryptografie.wz.cz/data/aes.html>.

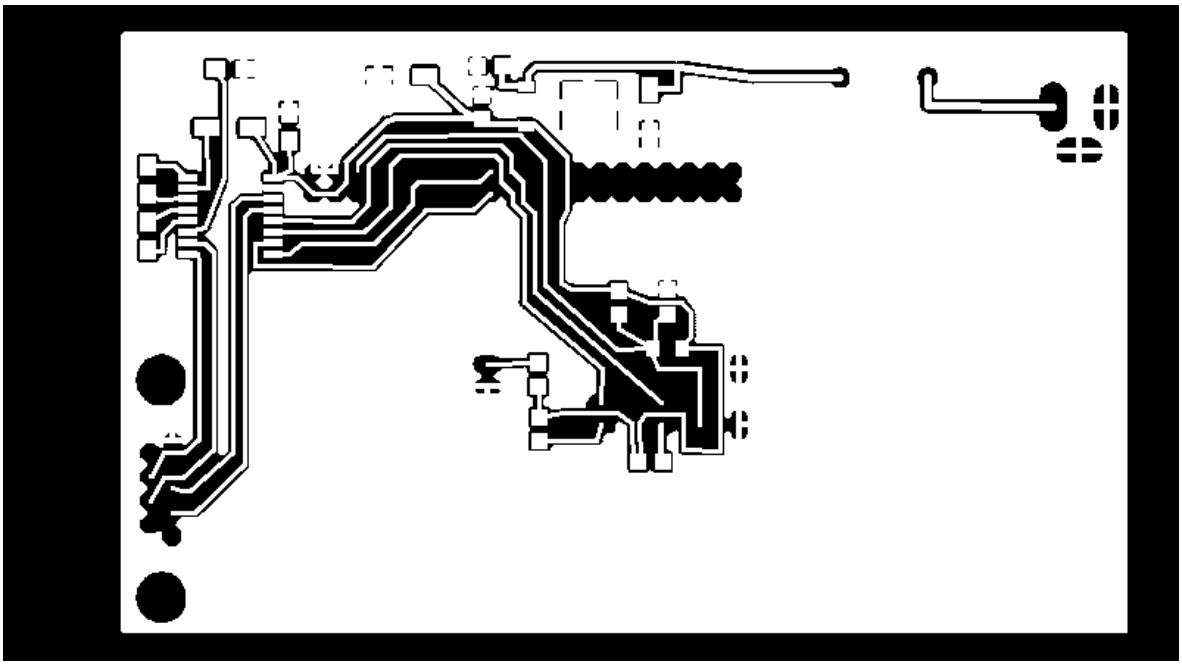
22 ZOZNAM POUŽITÝCH SKRATIEK

ACK	ACKnowledge
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CAM	Content-Addressable Memory
CBC	Cipher-block chaining
CFB	Cipher feedback
DCD	Data Carrier Detect
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSR	Data Set Ready
DTR	Data Terminal Ready
ECB	Electronic codebook
FAT	File Allocation Table
FIN	Finalize - No more data from sender
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local area network
LED	Light-emitting diode
LSB	least siginificant bit
MAC	Media Access Control
MSB	most significant bit
OFB	Output feedback
OS	Operating system
PPP	Point-to-Point Protocol
PSH	Posh function
RAM	Random-access memory
RSA	iniciály autorov Rivest, Shamir, Adleman
RST	Reset the conection
RTS	Request to Send
RxD	Receive Data
SEQ	Sequence number
SRAM	Static Random Access Memory
SSL	Secure Sockets Layer
STP	Spanning tree protocol
SYN	Synchronize sequence number
TCP	Transmission Control Protocol
TTL	Transistor-Transistor Logic
TxD	Transmit Data
UDP	User Datagram Protocol
URG	Urgent
VLAN	Virtual Local area network
WIC	WAN Interface Connection

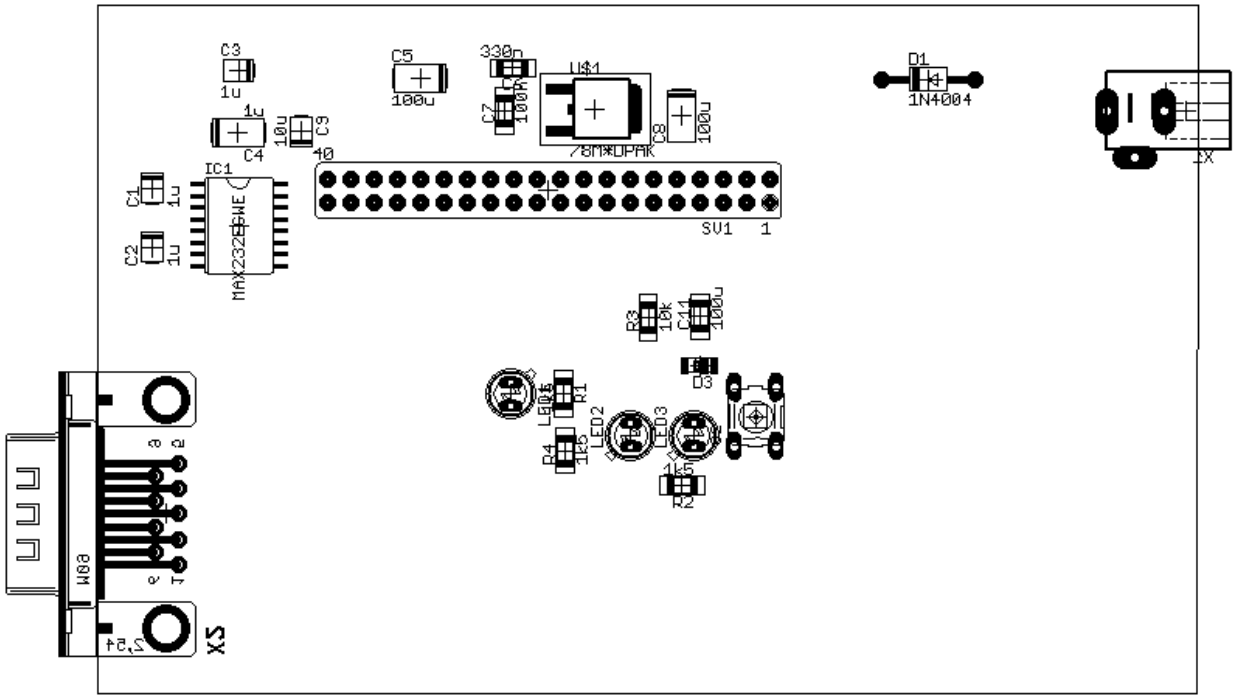
23 ZOZNAM PRÍLOH

A Prvá príloha	Základná doska-strana spojov
B Druhá príloha	Základná doska-strana súčiastok
C Tretia príloha	Základná doska-schéma
D Štvrtá príloha	Krabička - predná strana
E Piata príloha	Krabička - zadná strana

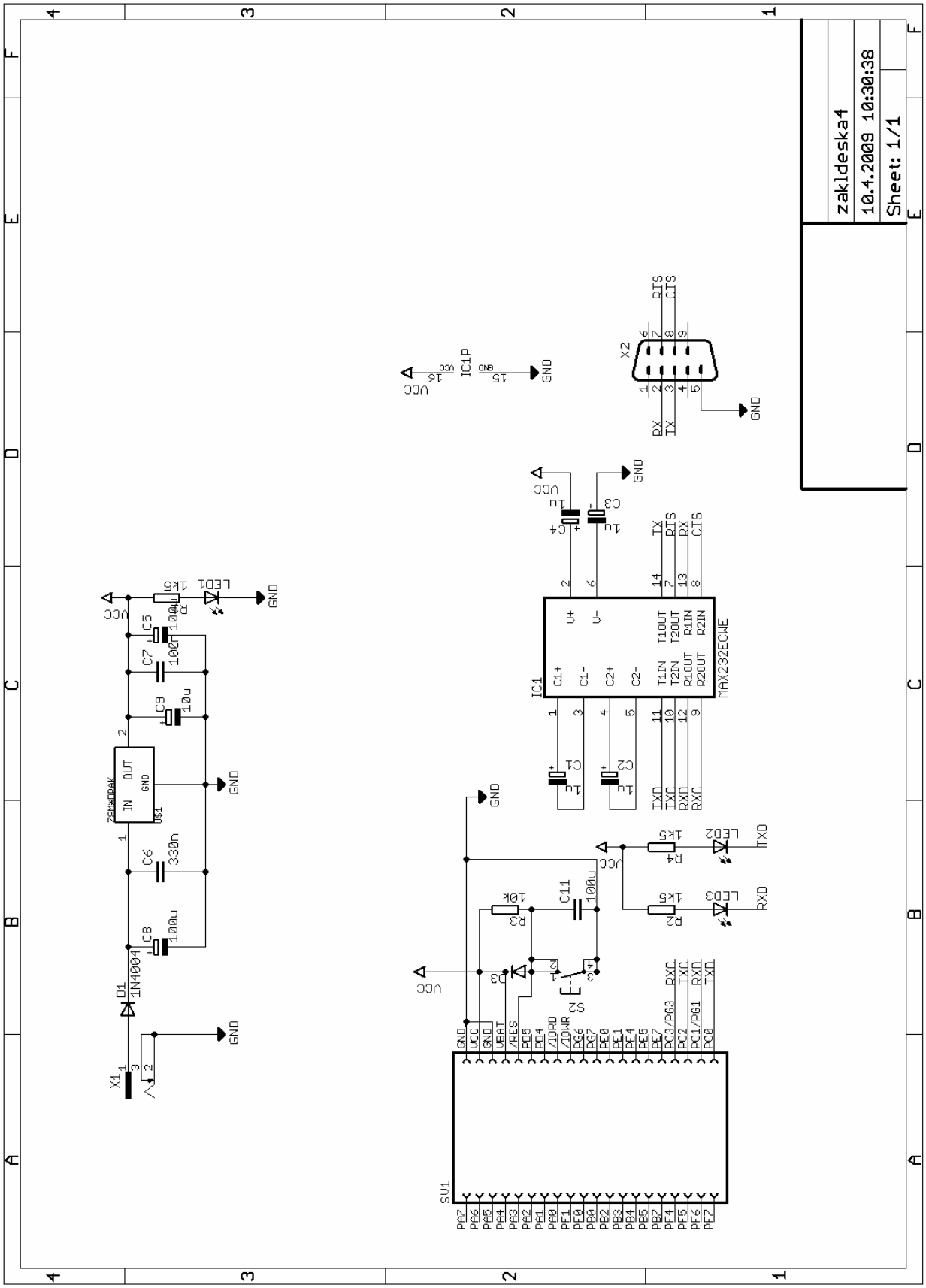
A Prvá príloha Základná doska-strana spojov



B Druhá príloha Základná doska-strana súčiastok



C Tretia príloha Základná doska-schéma



D Štvrtá príloha Krabička-predná strana

E Piata príloha Krabička-zadná strana