Úvod do sietí

1.Požiadavky pre internetové pripojenie.

Pripojenie na internet môžeme rozdeliť na fyzické, logické pripojenie a aplikácie.
Fyzické pripojenie: je tvorené špeciálnymi kartami ako modem alebo sieťová karta (NIC) z počítača do siete. Je použité na prenos signálov medzi PC vnútri siete a vzdialených zariadení na internete.
Logické pripojenie používa štandartné volacie protokoly. **Protokol** je formálny popis pravidiel a konvencií ktoré hovoria, ako komunikujú zariadenia na sieti. Primárnym protokolom je TCP/IP.
Aplikácie prekladajú dáta a zobrazujú informácie do pochopiteľnej formy ako poslednú časť spojenia. Pracujú s protokolmi na posielaní a prijímaní dát cez internet. Webové prehliadače zobrazujú HTML ako webové stránky. FTP je používané na posielanie a prijímanie súborov z internetu. Webové prehliadače používajú špeciálne **plug-in** moduly na zobrazenie špeciálnych dát.

1.1.3 Sieťová karta (NIC)

NIC je doska s plošnými spojmi, ktorá sprostredkováva sieťovú komunikáciu PC. Typ NIC musí súhlasiť s **médiom a protokolom** použitým v lokálnej sieti. NIC komunikuje so sieťou sériovo a s PC paralelne.
Pri výbere NIC zvažujeme nasledujúce faktory:

1. **Protokol** – Ethernet, Token Ring, or FDDI
2. **Typ média** – krútená dvojlinka, coax, bezdrôt alebo optiku
3. **Typ systémovej zbernice** – PCI alebo ISA

1.1.4 Inštalácia modemu a sieťovej karty

Modem /modulátor-demodulátor/ je zariadenie, ktoré poskytuje pripojenie PC na telefónnu linku. Delíme ich na externé a interné. Externé používajú na komunikáciu s PC sériový port alebo USB.
Sieťovú kartu (NIC) inštalujeme keď:

1. v PC nemáme žiadny NIC a chceme sa pripojiť do siete
2. pri výmene vadnej alebo poškodenej karty
3. pri upgrade z 10MB na 10/100MB

Na inštaláciu NIC alebo modemu potrebujeme:

1. znalosti ako adaptér konfigurovať
2. diagnostické nástroje
3. schopnosť odstrániť hardwarový konflikt

1.1.5 Prehľad high-speed a dial-up pripojenia

Od roku 1998 modemy pracujú na 56kbps, zaraďujeme ich do dial-up pripojenia.
Do high-speed pripojenia zaraďujeme DSL a káblové modemy. Hovoríme im tiež „**always on**" služby.

1.1.6 TCP/IP / Transmission Control Protocol/Internet Protocol/ popis a konfigurácia

1. je súbor pravidiel a protokolov vyvinutý na zdieľanie zdrojov v sieti. Na povolenie TCP/IP na pracovných staniciach musí byť nakonfigurovaný cez nástroje systému.

1.1.7 Testovanie pripojenia cez ping

Ping je nástroj na overenie sieťového pripojenia. Príkaz **ping** posiela viacnásobný IP paket na špecifikovaný cieľ. Každý vyslaný paket vyžaduje odpoveď.
Interný loopback – 127.0.0.1
Test cieľového pc – napr. ping 192.168.0.1

1.1.8 Webové prehliadače a pluginy

Funkcie:

1. pripojenie na web server
2. vyžiadanie informácie
3. prijatie informácie
4. zobrazenie výsledku na obrazovke

Webový browser je prgram, ktorý prekladá HTML, je to všeobecný znakový jazyk, ktorý môže zobraziť grafiku, prehrávať zvuk, filmy, a iné multimediálne súbory. Hiperlinky sú vložené vo webových stránkach ako rýchle odkazy na iné lokácie.
Najpopulárnejšie prehliadače:

1. IE Internet explorer
2. Netscape Communicator

Plug-in aplikácie: slúžia na zobrazenie špeciálnych alebo vlastných typov

1.1.9 Odstránenie porúch v internetovom pripojení

Podmienky:

1. definovanie problému
2. zhromaždenie faktov
3. posúdiť možnosti
4. vytvorenie plánu postupu
5. použitie plánu
6. posúdiť výsledky
7. dokumentovanie výsledku
8. zaviesť problém a riešenie

1.2 Sieťová matematika

Počítače pracujú s uloženými dátami použitím elektrických prepinačov 0/1

Units	Definition	Bytes*	Bits*	Examples
Bit (b)	Binary digit, a 1 or 0	1	1	On/Off; Open/Closed +5 Volts or 0 Volts
Byte (B)	8 bits	1	8	Represent the letter "X" as ASCII code
Kilobyte (KB)	1 kilobyte = 1024 bytes	1000	8,000	Typical Email = 2 KB 10-page report = 10 KB Early PCs = 64 KB of RAM
Megabyte (MB)	1 megabyte = 1024 kilobytes = 1,048,576 bytes	1 million	8 million	Floppy disks = 1.44 MB Typical RAM = 32 MB CDROM = 650 MB
Gigabyte (GB)	1 gigabyte = 1024 megabytes =1,073741,824 bytes	1 billion	8 billion	Typical Hard Drive = 40 GB or greater
Terabyte (TB)	1 terabyte = 1024 gigabytes = 1,099,511,627,778 bytes	1 trillion	8 trillion	Amount of data theoreti- cally transmittable in optical fiber in one second

Číselné sústavy:

1. desiatkový /0,1,2,3,4,5,6,7,8,9/ , počet symbolov 10

prevod: 2134 = $(2x10^3) + (1x10^2) + (3x10^1) + (4x10^0)$

1. dvojková /0,1/ , počet symbolov 2

prevod: 101102=(1 x 24)+(0 x 23)+(1 x 22)+(1 x 21)+(0 x 20)=22
pri prevode s 10 do 2 používame postup delenia 2, keď je bezozvyšku, zapisujeme 0, keď je zvyšok zapisujeme 1, delíme až do nuly.
Príklad: 168/2=84, 84/2=42, 42/2=21, 21/2=10.5, 10/2=5, 5/2=2.5, 2/2=1 1/2= 0.5
00010101 potom napíšeme číslo v opačnom poradí: 10101000

1. hexadecimálna /0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F/ , počet symbolov 16

prevod do binárnej „C9" 1100 1001
prevod do desiatkovej: najskôr do 2 a potom na 10

Logické operátory

1. NOT – neguje vstup /na vstupe 1 na výstupe 0/
2. AND – pozostáva z 2 vstupov a 1 výstupu. 1 na výstupe lem pri 1 na oboch vstupoch
3. OR – pozostáva z 2 vstupov a 1 výstupu. 1 na výstupe, ak aspoň jeden je rovný 1

Sieťové médiá

Delíme na:

1. medené káble, používané predovšetkým v LAN
2. optické vlákna, veľmi často používané pri dlhých trasách, vyznačujú sa širokou šírkou pásma, použitie v LAN a WANs
3. bezdrôtové médiá, priniesli prenosnosť počítačového sveta. V súčasnej dobe však neposkytujú vysoké rýchlosti a vysokú bezpečnosť. Jednoduché na inštaláciu.

3.1.1 Atómy a elektróny

Atóm sa skladá:

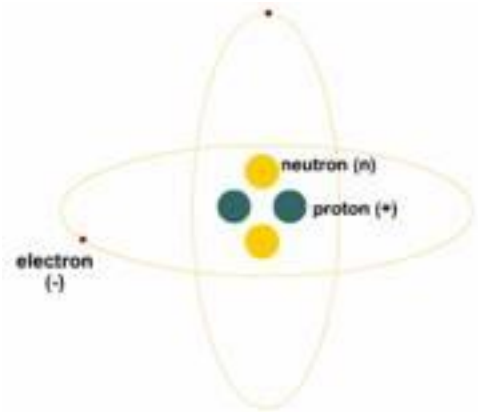
1. elektrónov, záporne nabitá častica
2. nukleónov, centrálna časť atómu zložená protónov a neutrónov
3. protónov, kladne nabité častice
4. neutrónov, častice, ktoré nenesú naboj

Periodická tabuľka prvkov

1 H																	2 He
3 Li	4 Be											5 B	6 C	7 N	8 O	9 F	10 Ne
11 Na	12 Mg											13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
19 K	20 Ca	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr
37 Rb	38 Sr	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe
55 Cs	56 Ba	57 La	72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn
87 Fr	88 Ra	89 Ac	104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Uuu	112 Uub						

58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Td	66 Dy	67 Ho	68 Er	69 Tm	70 Yb	71 Lu
90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No	103 Lr

Príklad: hélium má atómové číslo 2, čo znamená, že má 2 protóny a 2 elektróny. 2p+2e =4 4 je atómová hmotnosť. Po odčítaní 4 – 2(atómové číslo) dostaneme, že He má 2 neutróny. Dánsky fyzik, Niels Bohr, vyvinul jednoduchý model atómu:



Elektrina – je volný tok elektrónov
Statická elektrina – sú záporne nabité náboje, ktoré stoja na jednom mieste, môžu spôsobiť elektrický výboj (ESD). ESD môže spôsobiť vážne poškodenie elektricky citlivých zariadení.

3.1.2 Napätie

Elektrické napätie je rozdiel potenciálov, skratka je EMF, meria sa vo Voltoch. Sú 3 spôsoby vzniky napätia:

1. trením, statická elektrina
2. magnetizmom, elektrické generátory
3. svetlom, solárne články

3.1.3 Odpor

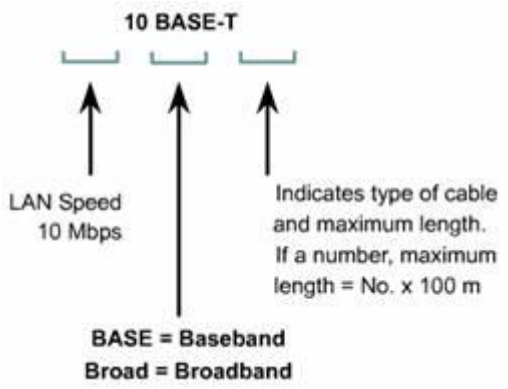
Vodiče – majú malý, alebo takmer žiadny, odpor
Izolátory – zamedzujú toku prúdu
Odpor – meriame ho v ohmoch
Elektrické izolátory – sú materiály, cez ktoré nemôže tiecť prúd
Elektrické vodiče – umožňujú tiecť prúdu, najlepšie sú zlato, striebro a meď
Polovodič- sú materiály, kde vodivosť je kontrolovaná, napr. Si

3.1.4 Prúd

1. je tok elektrónov, udáva sa v Ampéroch, označujeme ho I

Osciloskop - zariadenie, merá veličiny v čase
Multimeter - meranie napätia, prúdu, kapacity, ...

3.1.6. Špecifikácia káblov



10Base – rýchlosť prenosu 10Mbps, typ prenosu základný, T krútené 2-linka

10Base5 - rýchlosť prenosu 10Mbps, typ prenosu základný, 5 predstavuje kapacitu kábla, schopného preniesť signál na vzdialenosť 500m bezo strát

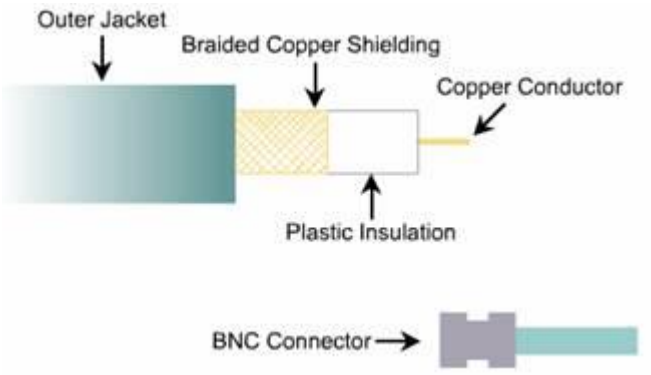
3.1.7. Koaxiálne káble

Kábel pozostáva z vonkajšieho plášťa, medeného opletenia alebo niekedy z hliníkovej fólie, plastového izolátora a samotného medeného vodiča.
Výhody:

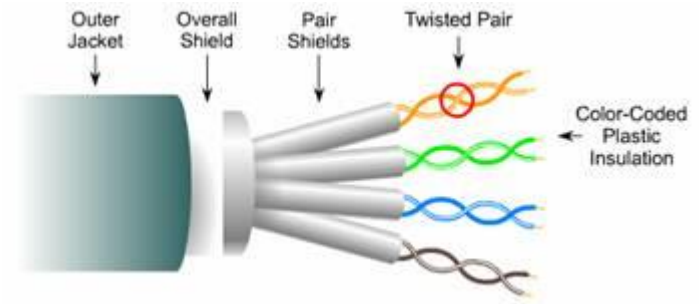
1. použiteľný na väčšie vzdialenosti ako STP/UTP na 500m bez opakovača
2. lacný, ľahká inštalácia

Nevýhody:

1. spoľahlivosť
2. nízka prenosová rýchlosť, do 10Mbps
3. zastaralá



3.1.8. STP kábel



Tienený krútený kábel, kombinuje technológiu tienenia a krútenia linky, každý pár je ovinutý kovovou fóliou a dohromady sú všetky 4 páry ovinuté fóliou.
Výhody:

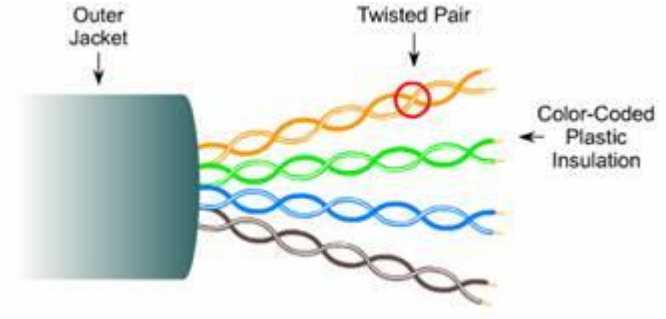
1. dobre odrušené
2. prenos od 10 – 100 Mbps na 100m

Nevýhody:

1. drahé
2. náročné na inštaláciu
3. maximálna vzdialenosť prenosu na 100m

Kompromisom medzi cenou a spoľahlivosťou je tienený UTP nazývaný FTP (ScTP), 4 páry sú zabalené do fólie
Metalická ochrana musí byť uzemnená na koncovom bode

3.1.9 UTP kábel



1. pozostáva s 8 káblov, každé 2 sú navzájom prepletené a všetky 4 páry sú tiež navzájom prepletené dookola.

Výhody:

1. jednoduché na inštaláciu
2. rýchlosť prenosu od 10,100,100Mbps na 100m
3. lacnejšie ako STP

Nevýhody:

1. náklonný k rušeniu od ostatných médií

Delenie káblov:

1. priamy, medi Hubom a PC / tip A alebo B/
2. crossover, prekrížený, medzi 2 PC alebo 2 Huby /na jednej strane tip A na druhej B/

- rollover, medzi PC a konzolovým portom na rutri /1s8,2s7,.../

3.2.1. Elektromagnetické spektrum

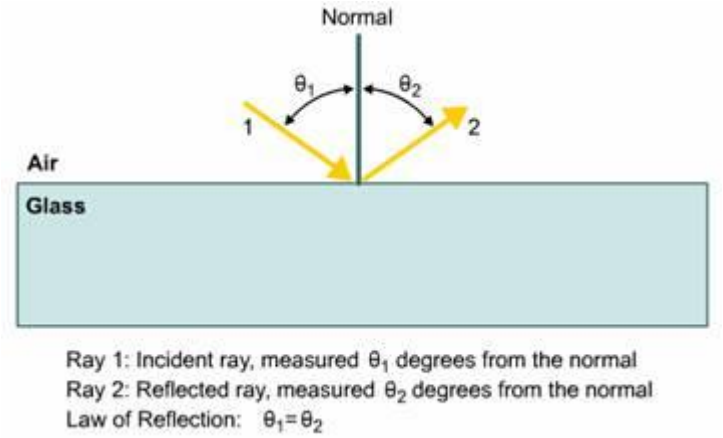
Svetlo použité v optických vláknach je jeden tip elektromagnetickej energie. Dôležitá vlastnosť každej energetickej vlny je vlnová dĺžka.
Typy elektromagnetickej energie: rádio, mikrovlny, radar, viditeľné svetlo, x-žiarenie, gama-žiarenie. Elektromagnetické vlny cestujú 300 000 km/s vo vákuu. V optických vláknach sa používa 850 nm, 1310 nm, alebo 1550 nm. Boli vybrané, pretože sa síria lepšie ako ostatné vlnové dĺžky.

3.2.2. Svetelný model svetla

Odrazený lúč : svetelný lúč prechádza z jedného okraja materiálu na druhý, niektoré svetelné energie budú odrazené späť
Zakrivenia svetelného lúča pri prechode cez 2 látky je dôvod, prečo môže svetelný lúč cestovať v optickom vlákne aj v zákrutách.
Optická hustota : popisuje, jak se množství světelných paprsků zmenší pri prechode cez materiál, najlepšia je vo vákuu

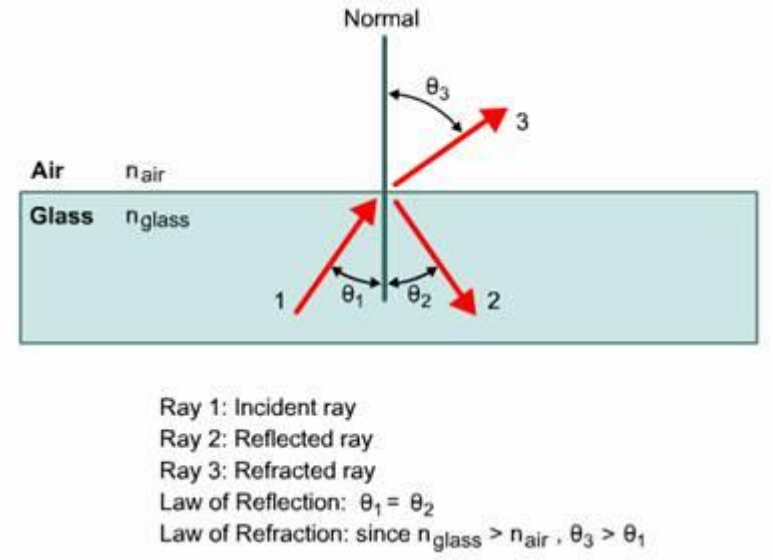
Index lomu: pomer rýchlosti svetla v materiály ku rýchlosti svetla vo vákuu, čím je menší, tým je materiál vhodnejší.

3.2.3. Odraz



Ohol, pod ktorým svetelný lúč dopadá na hladký, lesklý, povrch je rovnaký, ako lúč, pod ktorým sa odráža.

3.2.4. Lom



Pri náraze svetelného lúča na 2 transparentné materiály, dochádza k rozdelenie lúča na 2 časti. Časť sa odrazí v jednom materiály podľa uhla dopadu, a druhá prechádza do druhého prostredia. Ak je uhol 90 stupňov, lúč prechádza priamo cez sklo, ak nie je potom sa láme. Ak lúč prechádza s prostredia s menším uhlom lomu do prostredia s väčším, potom sa lúč láme k normal a opačne.

3.2.5. Úplný optický odraz

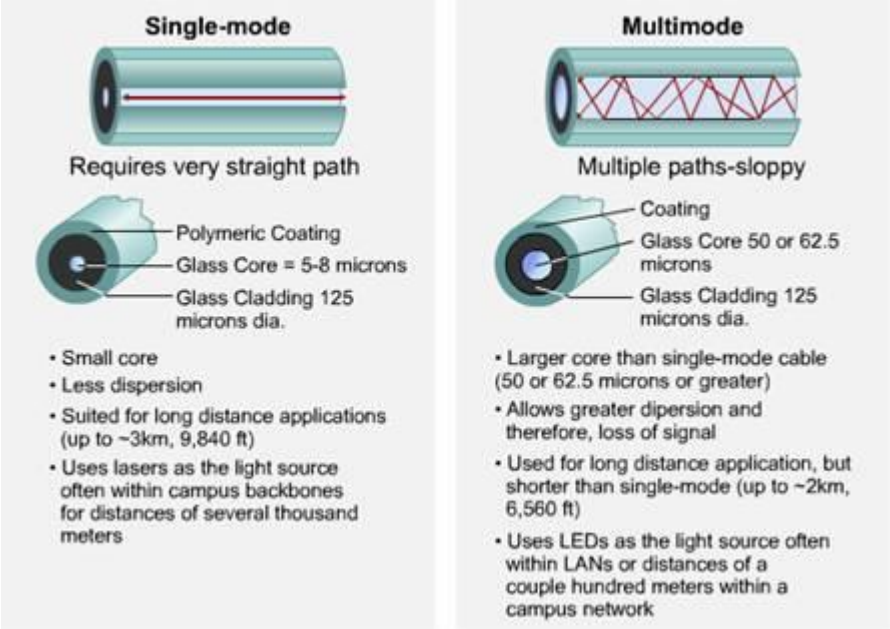
Podmienky pre optické vlákna:

1. jadro optického vlákna by malo mať väčší index lomu, ako plášť, ktorý ho obklopuje
2. uhol dopadu svetelného lúča je väčší, ako kritický uhol pre jadro a obal

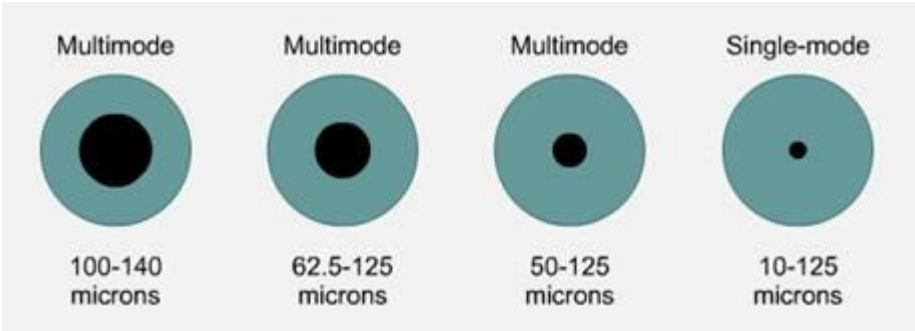
Úplný interný odraz: dosiahneme pri splnení oboch podmienok, vlastný svetelný lúč bude úplne odrazený späť vo vnútri vlákna

3.2.6 / 3.2.7 Multimódové a jednomódové vlákno

Módy: sú optické cesty
Multimódové vlákno: umožňuje jeho priemer viac ciest svetelným lúčom
Jednomódové vlákno: umoňuje len sírenie jedného lúča



Pri optických vláknach je vysoká bezpečnosť, pretože signál je len vo vnútri vlákna a nedá sa odpočúvať. Na prenos sa používajú vždy 2 vládna, jeden na príjem a druhý na vysielanie. Jeden kábel môže obsahovať 2 – 48 oddelených vlákien a viac.



Jednomódové kedenia sa používajú na vzdialenosť 3 km a mutli na 2 km.

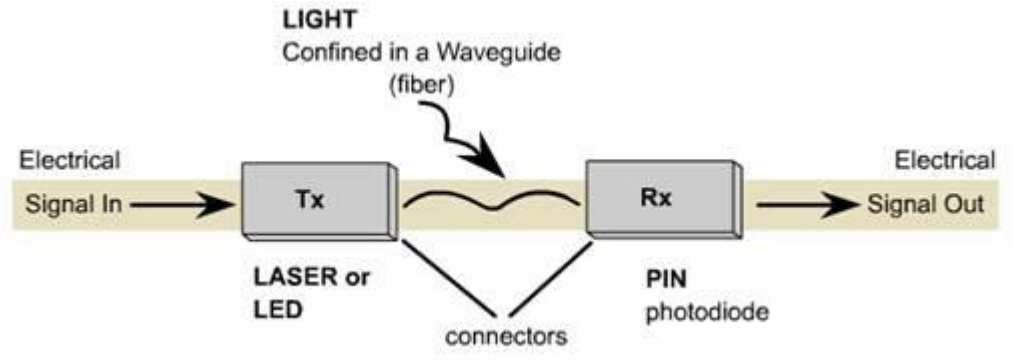
3.2.8. Ostatné optické komponenty

Na prenos dát v sieti sa používajú elektrické signály, preto je potrebné pri optických zariadeniach použiť prijímače a vysielače na prevod do a z optiky.
Transmiter:

1. používa 2 typy signálov LED, LASER

Prijímač (receiver)

1. jeho úlohou je prijať signál a spracovať ho na elektrické signály
2. používajú sa fotoleddiódy PIN



PIN sú vyrábané na citlivosť 850, 1310 alebo 1550nm.
Káble sú ukončené konektormi. Pre multi sú Subscriber Connector (SC) pre jednomódové Straight Tip (ST)

3.2.9. Signály a šum v optických médiách

Optické siete sú vhodné pre MANs a WANs. Veľmi podstatným faktorom sú straty. Sú zapríčinené mikroskopickými nečistotami vo vlákne, tie spôsobujú vytváranie malého množstva tepla. Ďalej sú to rôzna hrúbka vlákna a nerovnosti na konektoroch.

3.2.10. Inštalácia, ošetrenie, a testovanie optických káblov

Hlavné príčiny útlmu:

1. nesprávna inštalácia prílišné ťahanie a ohýbanie
2. absorpcia
3. nehomogenita
4. rozptyl

Meria sa dB, to hovorí koľko percent energie bolo stratenej.
Testovanie je veľmi dôležité a záznamy musia byť zachované. Najpoužívanejšie sú Optický stratový meter a optický časový doménový reflektomer.

3.3.1 Bezdrôtová LAN organizácia a štandarty

Štandardy pre bezdrôtové siete:

1. 802.11
2. 802.11a,b,g

802.11b je tiež nazývaný ako WiFi, 2.4GHz, alebo vysoko rýchlostný bezdrát. Pracuje na 11, 5.5, 2 a 1 Mbps. Je to dôležité kvôli spätnej kompatibilite.
802.11a pracuje na 5GHz, využitie v WLAN, prenosový rýchlosť 54Mbps, nekompatibilné s 802.11b
802.11g všetko rovnaké ako 802.11a ale kompatibilné s 802.11b

3.3.2. Bezdrôtové zariadenia a topológie

Skladajú sa s AP (access point) a wireless NIC. Topológia je podobná peer-to-peer. AP je pripojené do siete cez metalickú kabeláž. AP sú vybavené anténou a poskytujú konektivitu v špecifickej oblasti nazývanej bunka. V závislosti na použitej anténe a prostredí báva dosah od 91.44 do 152.4 m. Na pokrytie väčšieho územia sa môžu bunky prekrývať, vtedy hovoríme o roamingu.

Proces prepojenia: vyhľadávanie kompatibilných zariadení s rovnakým číslom SSID cez skenovanie aktívne alebo pasívne

3.3.3. Ako komunikujú bezdrôtové siete

Po pripojení WLAN na bod, uzol bude prenášať rámce rovnakým spôsobom ako na 802.X sieťach, ale WLAN nepoužíva štandard 802.3.
Štruktúra rámcov: kontrolné, riadiace a dáta.
WLAN rámce malú vždy veľkosť 1518 bitov.
Vysielanie: vyslanie rámca, vrátenie potvrdenia, Práve toto spôsobuje 50% zníženie šírky pásma. S postupnou vzdialenosťou od AP prenosová rýchlosť slabne.

3.3.4. Autentifikácia a asociácia

Vo WLAN zabezpečuje autentifikáciu 2 vrstva, ide o autentifikáciu zariadenia.
Metódy autentifikácie :

1. neautentifikovaný a neasociovaný: odpojený od siete a oddružený od AP
2. autentifikovaný a neasociovaný: autentifikovaný v sieti ale neasociovaný s AP
3. autentifikovaný a asociovaný: môžeme prijímať / vysielať data

Metódy autentifikácie:

1. otvorený systém, pre zabezpečený i nezabezpečený systém
2. spoločný kľúč, na pripojenie je potrebný 64/128 bitový kľúč, poskytuje vysoký úroveň zabezpečenie

3.3.5. Rádiové vlny a mikrovlné spektrum

PC posielajú signály elektronické, rádio vysielače ich konvertujú na rádio vlny. Tie sú vysielané a prijímané, počas cesty však slabnú vplyvom absobcie inými materiálmy ako mikrokvapôčky.
Druhy modulácie:

1. amplitúdová modulácia AM
2. frekvenčná modulácia
3. fázová modulácia

3.3.6. Signály a šum v WLAN

Bluetooth vysiela na 2.4 GHz, čo môže spôsobovať rušenie na 802.11b sieťach, ako aj 2.4GHz mobilné telefóny. Rušenie tiež môže zapríčiniť zlé počasie ako hmla, veľké vlhko, blesky.
Tip antény: dáva formu vysielania
- tyč - všesmerovo
- smerová - vytvára paprsok, prenos sa predĺži, tipicky ide o paraboly nebo YAGI antény

3.3.7. Bezdrôtová bezpečnosť

1. EAP rozšírený autentifikačný protokol, veľmi podobný heslám v bezdrôtových sieťach
2. LEAP ľahko rozšírený autentifikačný protokol, primárny typ v CISCO WLAN AP
3. užívateľská autentifikácia, len overeným úžívatelom je dovolený prenos
4. kriptovanie, kryptuje dáta
5. dátová autorizácia, zabezpečuje integritu dát

Testovanie káblov

4.1.1. Vlny

- je cestovanie energie s jedného miesta na iné

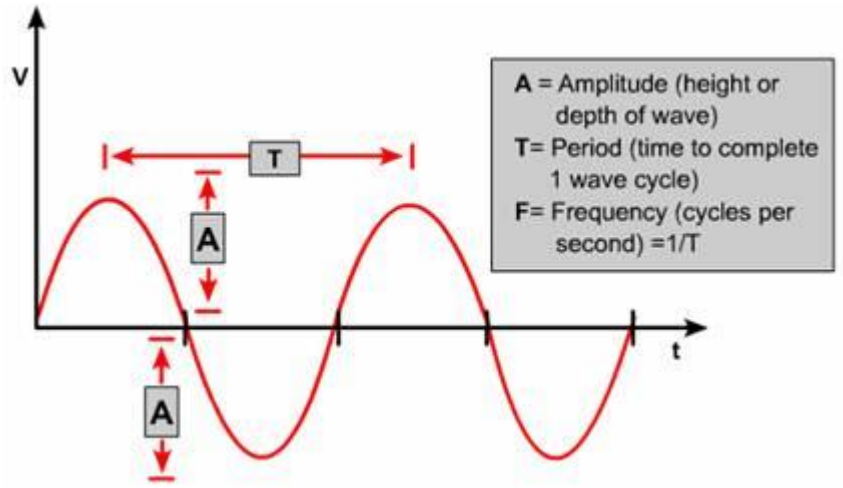
Perióda vĺn je hodnota času medzi vlnami, meraný v sekundách
Frekvencia je počet vĺn, ktoré narazia na breh za každú sekundu, meraná v Hz, 1Hz je rovný 1 vlne za 1s
Vlny:

- napäťové vlny v medených médiách
- svetelné vlny v optických vláknach
- elektromagnetické vlny

Perióda – hodnota času kompletného 1 cyklu v sekundách
Frekvencia – počet kompletných cyklov za sekundu v Hz
Impulz – zámerne spôsobené rušenie a impulzy sú pevné, predpovedatelné v dobe

4.1.2. Sínusové vlny a pravouhlé vlny

Sínusová vlna je grafom matematických funkcií, sú periodické.
Pravouhlé vlny sú tiež periodické, nie sú plynulo striedavé v čase. Vlna vydrží jednu hodnotu nejaký čas a potom sa naraz zmení na inú hodnotu, tá sa drží nejaký čas a potom sa rýchlo zmení na pôvodnú hodnotu.



4.1.3. Mocniny a logaritmy

Logaritmus – transformácia čísla podľa pravidiel, alebo matematických funkcií, napr: log 10^9=9

4.1.4. Decibely

Decibely charakterizujú intenzitu signálu. Pri výpočtoch používame 2 vzorce, 10 log pri meraní vo Watoch, 20 log pri meraní vo Voltoch.
Vzorce:
$dB = 10 \log_{10} (P_{final} / P_{ref})$, $dB = 20 \log_{10} (V_{final} / V_{ref})$

- dB popisujú straty alebo zisky energie vlny, obyčajne sú záporné , vtedy reprezentujú stratu, pri kladných zas zisk.
- log10 číslo v zátvorke bude transformované použitím pravidla pre 10 logaritmus
- Pfinal dodanú energiu vo Watoch
- Pref pôvodnú energiu vi Watoch
- Vfinal dodané napätie vo Voltoch
- Vreference pôvodné napätie vo Voltoch

Typickým príkladom merania vo W je meranie v optických vláknach alebo rádiových vlnách, Vo V medených kábloch.
Príklad: Ak dodaná energia 10-6 W a pôvodná energia je 10-3 W, potom bude strata -30dB.

4.1.5. Prezeranie signálov v čase a frekvencia

Osciloskop je dôležité elektronické zariadenie, používané na zobrazenie elektrických signálov ako napätie a impulzy v časovej oblasti. X-sová os reprezentuje čas a Y-lonová reprezentuje U alebo I. Inžinieri používajú frekvenčnú doménovú analýzu na štúdium signálov.
Spektrálny analyzér: zobrazuje frekvenčnú analýzu

4.1.7. Šum v čase a frekvencia

Šum je nežiadúci signál, môže vznikať v prírode alebo v technologických zdrojoch a je pridáva-ný do dátových signálov v komunikačných systémoch.
Možnosti vzniku šumu:

- blízko káblov, ktoré vedú dátové signály
- rádiové frekvenčné rušenie (RFI)
- elektromagnetické rušenie (EMI), blízkym zdrojom sú motory alebo svetlá
- laserový šum vo vysielačoch alebo prijímačoch optických signálov

Úzke rušenie – šum, ktorý ovplyvňuje malý rozsah frekvencií

4.1.8. Šírka pásma

- analógová, frekvenčný rozsah analógových el. systémov, pri rádio staniciach alebo zosilňovačoch, v Hz
- digitálna, popisuje ako veľa inf. môže pretiecť s jedného miesta na iné za určitý čas, bps

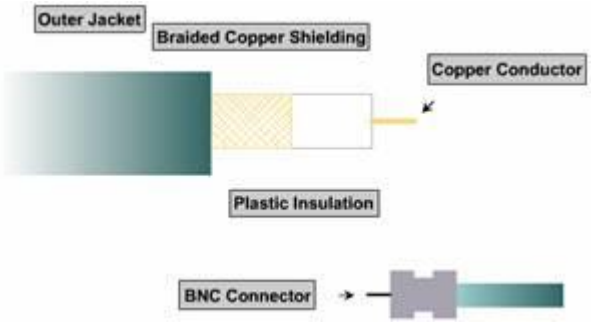
Počas testovania káblov je analógová šírka pásma použitá na určenie digitálnej šírky pásma, médiá, ktoré podporujú vyššiu analógovú šírku budú podporovať vyššiu digitálnu šírku

4.2.1. Signály cez optické a medené vedenia

Základné typy káblov:

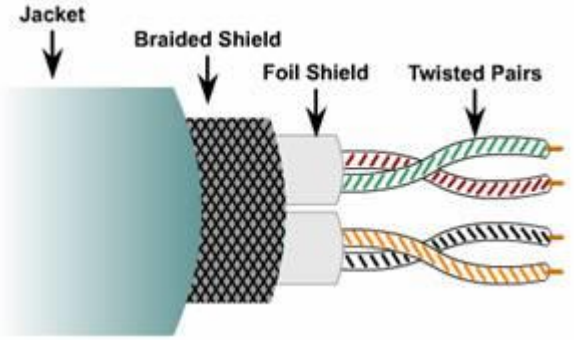
- netienený
- tienený, tieniaci materiál chráni dátové signály od externých zdrojov rušenia a šumom generovaným elektrickými signálmi medzi káblami.

Koaxiálny kábel – tienený kábel, pozostáva s pevného medeného vodiča, obklopeného izolujúcim materiálom a vodivým tienením. V LAN je opletenie uzemnené, pre ochranu vnútorného vodiča pred externým el. šumom.

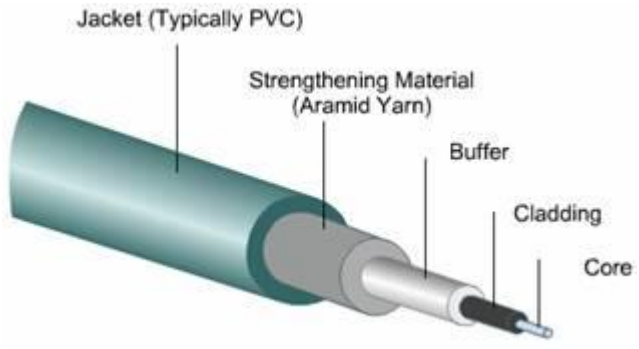


Krútená 2 linka:

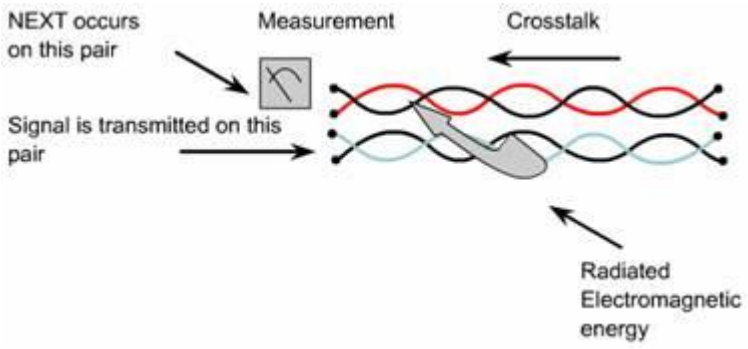
- netienená (UTP), neobsahuje tienenie
- tienená (STP), obsahujú vonkajšie vodivé tienenie, ktoré je uzemnené na odstránenie signálov s vonkajšieho ele. rušenia. STP tiež používajú vodivú fóliu na každom drôtovom páre na odstránenie šumu generovaného ostatnými pármi.



Optický kábel – na prenos používa zväčšovanie a zmenšovanie intenzity svetla Nepostihuje ich ele. šum, preto nepotrebujú uzemnenie. Využívajú sa medzi budovami alebo poschodiami.



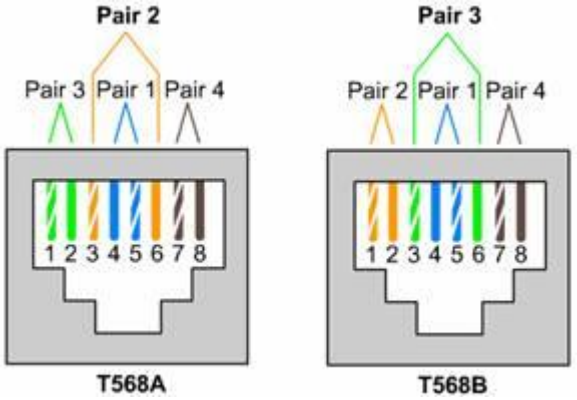
4.2.2. Útlm a straty v medených médiách



Útlum - väčšia vzdialenosť a vyššia frekvencia spôsobujú zvýšenie útlmu, preto sa používa vysoká frekvencia pre testovaní káblov. Udáva sa v dB v negatívnych číslach. **Odpor** v médiách sa prejavuje teplom, ďalšie straty spôsobujú vadné konektory a poškodená zvody na izolácii. Odpor je meraný striedavým prúdom (AC) v ohmoch, pri Cat5 je to 100Ohm. **Odpor nesúhlasný alebo nespojitý (mišmaš)** – pri rôznej impedancii vo vedeniach vplyvom zlých konektorov a poškodených vedení, tzv. časová nespojitost. **Echo** – časť prenášaného signálu je odrazená na vysielač vplyvom odporovej nespojitosti, potom pokračuje do prijímača

4.2.3. Zdroje rušenia v medených médiách

TIA/EIA-568-A/B – certifikát káblov vyžaduje testovanie na rôzne druhy šumov
Prieniky – zahrňujú prenikanie signálu s jedného drôtu do druhého vplyvom elektromagnetickej energie, je väčší, čim je vyššia frekvencia. Merajú sa káblovými testermi, ktoré merajú nežiadúce presluchy medzi 2 pármi
Krútený pár káblu pomáha redukovať prieniky dát alebo šumových signálov s vedľajšieho páru. Vyššia kategória UTP vyžaduje väčšiu zakrútenosť . Pri výrobe konektorov sa snažíme zabezpečiť čo najnižšiu nezakrútenosť káblov.



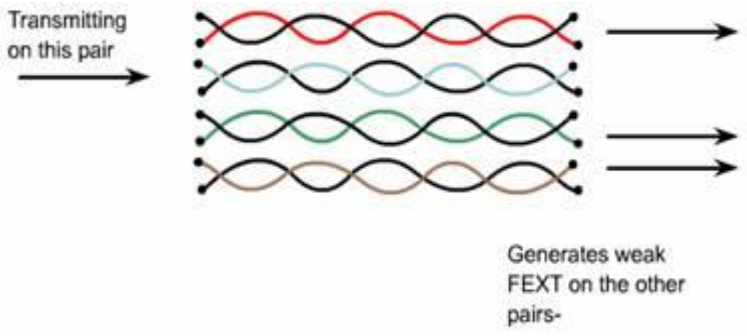
4.2.4. Typy presluchov

Typy presluchov:

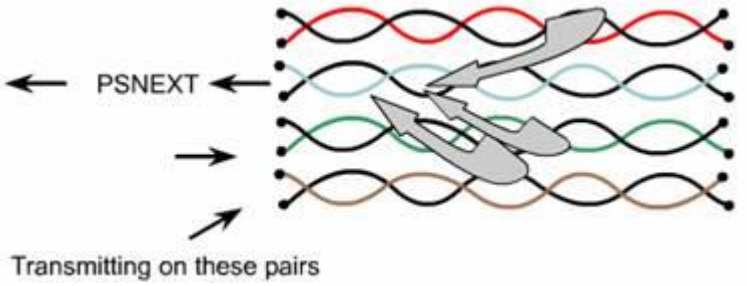
- NEXT near-end
- FEXT far-end
- PSNEXT power sun near-end

NEXT – je vypočítaný ako pomer napäťovej amplitúdy medzi testovaným signálom a presluchovým signálom na rovnakých koncoch linky, je v – dB, nízke – číslo indikuje vyšší šum. Pri dobrých kábloch to je 10dB, - sa neudáva. Meria sa medzi všetkými pármi a na oboch bodoch.

FEXT – menší šum na kábli, vzniknutý vplyvom presluchov na ceste od vysielača. Nie je taký významný, ako NEXT



PSNEXT – navrstvuje celkové efekty NEXT so všetkých drôtových párov káblu. Je vypočítaný pre každý drôtový pár založený na NEXT efekte s ostatných 3 párov. Kombinácia efektov presluchov s viacnásobne súčasne prenášaných zdrojov môže byť veľmi škodlivá pre signál Tento test je vyžadovaný pre TIA/EIA-568-B



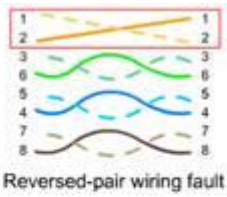
4.2.5. Štandardy testovania káblov

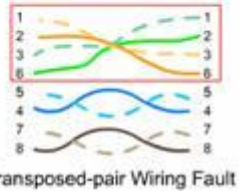
TIA-EIA-568-B definuje 10 testov pre medené káble, ktoré musia byť splnené pre použitie v moderných technológiách, pri vysoko rýchlostných LAN.
Potrebné testy pre štandard TIA/EIA:

- Mapa zapojenia – správna pozícia vodiča
- vložené straty
- NEXT
- PSNEXT
- ELFEXT
- PSELFEXT
- Vratné straty
- Šírenie oneskorení
- Káblová dĺžka
- Priečne oneskorenie

Každý pin má presnú funkciu. NIC prijíma signály na 1 a 2, vysiela na 3 a 6.

Chyby vo vedení:
Obrátený pár – keď 1 drôtový pár je správne nainštalovaný ne jednom konektore ale prehodený na 2 konektore.
Rozložený pár – keď sú 2 linky s 2 párov zapojené na nesprávne konektory
Krížový pár – keď je pár pripojený na úplne iný pin na konci





4.2.6. Ostatné testované parametre

Vkladané straty – kombinácia signálového útlmu a odporovej nespojitosti na komunikačnej linke
Presluchy - sa merajú v 4 oddelených testoch. Káblový test NEXT od použiteľného testu v jednom káblovom páre a meria amplitúdu presluchového signálu, prenášaných s ostatných párov v kábli.
NEXT je vypočítaná ako rozdiel amplitúdy medzi testovaným signálom a presluchovým signálom meraný na rovnakom koci kábla v -dB, čím väčšie, tým menší NEXT.
Pre ELFEXT test je potrebný FEXT. ELFEX medi pármi vypočítame ako rozdiel medzi nameraným FEXT a vkladanými stratami v drôtených pároch ktorých signály sú rušené podľa FEXT.
Súčet vyrovnaných úrovní na vzdialenom konci (PSELFEXT) je kombináciou efektu ELFEXT so všetkých párov.

4.2.7. Časovo založené parametre

Šírené oneskorenie – jednoduché meranie ako dlho trvá pre signál cesta signálu okolo káblu, meria sa v 100ns. TIA/EIA-568-B štandard určuje limity pre šírenie oneskorení pre rôzne kategórie UTP. Testery merajú dĺžku káblov na základe elektrických oneskorení v kábloch, nie podľa dĺžky plášťa, pretože sú káble vo vnútri skrútené. Pomocou tohto merania sa dá určiť aj vzdialenosť, kde je kábel poškodený.
Šikmé oneskorenie – odlišnosť oneskorenie medzi pármi, je dôležitá pre 1000BASE-T.

4.2.8. Testovanie optických káblov

Optické linky pozostávajú s 2 nezávislých optických vlákien fungujúcich ako nezávislé dátové cesty.
V optike nie sú presluchy. Vonkajšie elektromagnetické rušenie alebo šumy nepôsobia na optiku.
Najčastejšou príčinou odrazou sú nesprávne nainštalované konektory.

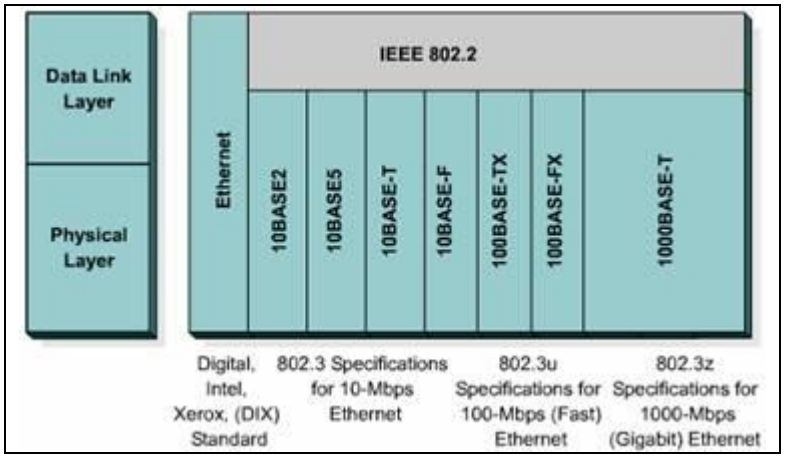
4.2.9. Nové štandardy

TIA 568 pridala v 20 júni 2002 kategóriu 6 (Cat 6). Oficiálny názov je ANSI/TIA/EIA-568-B.2-1. Oproti Cat5 musí prenášať frekvencie do 250MHz a mať nižšie presluchy a straty

Kabeláž v LAN

5.1.1. Lan fyzická vrstva

Každá počítačová sieť môže byť postavená s veľa typov médií.
Niektoré realizácie podporujú viacnásobné fyzické médiá.



5.1.2. Kabeláž v LAN

DIX – skupina, ktorá vytvorila prvú LAN špecifikáciu, bola tvorená Digitalon, Intelom a Xeroxom.

IEEE- institute of Elektrical and Elektronics Enginners
IEEE rozšírený 802.3:

1. 802.3u fast ethernet
2. 802.3z gigabitový ethernet cez optiku
3. 802.3ab gigabitový ethernet cez UTP

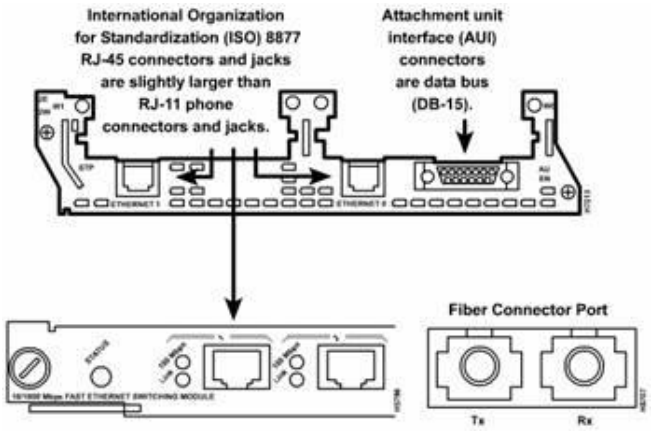
Použitie ethernetových sietí:

1. 10 Mbps pre používateľskú vrstvu
2. fast ethernet je používaný ako spojenie medzi užívateľmi a sieťovými zariadeniami , na prepojenie podnikových sietí
3. fast ethernet alevo gigabit ethernet medzi chrbticovými zariadeniami

	Ethernet 10BASE-T Implementation	Fast Ethernet Implementation	Gigabit Ethernet Implementation
End-user Level (End-user device to workgroup device)	Provides connectivity for low-to medium-volume applications.	Gives high-performance PC workstations 100-Mbps access to the server.	Not typically used at this level.
Workgroup Level (Workgroup device to backbone)	Not typically used at this level.	Provides connectivity between the end user and workgroups. Provides connectivity from the workgroup to backbone. Provides connectivity from the server block to the backbone layer.	Provides high-performance connectivity to the enterprise server block.
Backbone Level	Not typically used at this level.	Provides connectivity from the workgroup server block to the backbone.	Provides high-speed backbone and network device connectivity.

5.1.3. Ethernetové médiá a požiadavky na konektory

Porovnanie káblov a konektorov pre najpoužívanejšie ethernetové štandardy.
RJ45 – registered jack
AUI- attachment unit interface, používa sa na pripojenie adaptéra, ktorý umožňuje prechod s jedného tipu konektoru na iný, najčastejšie s AUI na RJ-45, koaxiálny alebo optický

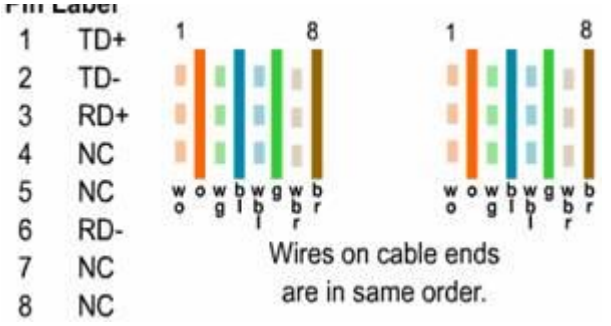


	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX
Media	50-ohm coaxial (Thinnet)	50-ohm coaxial (Thicknet)	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 5 UTP, two pair	62.5/125 multimode fiber
Maximum Segment Length	185 m (606.94 feet)	500 m (1640.4 feet)	100 m (328 feet)	100 m (328 feet)	400 m (1312.3 feet)
Topology	Bus	Bus	Star	Star	Star
Connector	BNC	Attachment unit interface (AUI)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface connector (MIC) ST or SC connector

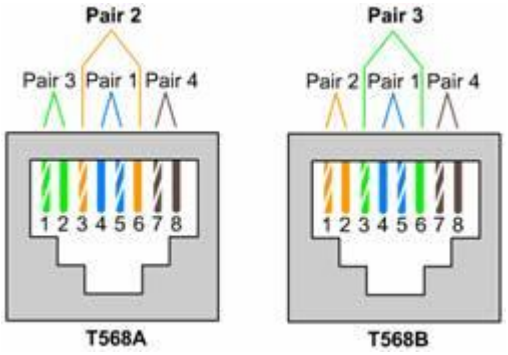
1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
STP	EIA/TIA Category 5 UTP, four pair	62.5/50 micro multimode fiber	62.5/50 micro multimode fiber; 9-micron single-mode fiber
25 m (82 feet)	100 m (328 feet)	275 m (853 feet) for 62.5 micro fiber; 550 m (1804.5 feet) for 50 micro fiber	440 m (1443.6 feet) for 62.5 micro fiber; 550 m (1804.5 feet) for 50 micro fiber; 3 to 10 km (1.86 to 6.2 miles) on single-mode fiber
Star	Star	Star	Star
ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	SC connector	SC connector

5.1.5. Implementácia UTP

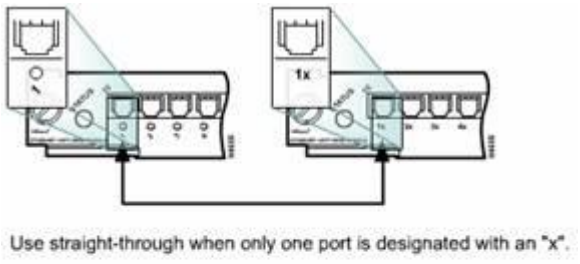
EIA/TIA špecifikuje konektor RJ45. Obsahuje 8 párov farebných vodičov, 4 sú označené ako „tip" (T1-T4) a vedú napätie, ostatné 4 ako „ring" (R1-R4) a sú uzemnené. 1 pár v konektore je označený ako T1 a R1. RJ45 je samčí konektor.



Zapojenie konektorov

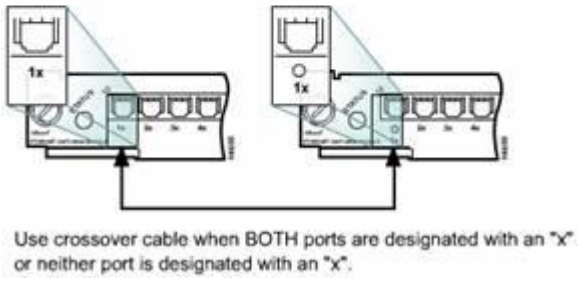


podľa EIA/TIA. T568A je používaný v USA a T568B v Európe. Pokiaľ sa na jednom kábli použije zapojenie A aj B, vytvoríme takzvaný crossover kábel.



Priamy kábel:

1. svič na rúter
2. svič alebo hub na PC alebo server



Prekrížený kábel:

1. svič na svič
2. svič na hub
3. hub na hub
4. rúter na rúter
5. PC na PC
6. Rúter na PC

5.1.6. Opakovač

Opakovače boli vytvorené na vytvorenie dlhších káblov, viac ako 100m, neanalyzuje dáta, je na fyzickém vrstve. Zosilňujú signál.

5.1.7. Hub

funguje ako multiportový opakovač, pokiaľ dáta prichádzajú na jeden port, je elektricky zosilnený na všetky ostatné porty, okrem toho, s ktorého prichádza. Tiež sa im hovorí koncentrátor.

Delenie hubov:

1. pasívne, použitie len na rozdelenie pre fyzické médiá, nepotrebuje napájanie
2. aktívne, potrebuje napájanie, pretože pred rozdelením najskôr signál zosilní, obsahujú konzolovú jednotku
3. inteligentné, v zásade funguje ako aktívny hub, ale tiež obsahujú mikroprocesory na diagnostiku

5.1.8. Bezdrôtová sieť

Na prenos sa používajú elektromagnetické vlny šírené vzduchom. Každé zariadenie má vysielač a prijímač. Pri prenose sú dáta konvertované na EW elektromagmetické vlny a pri príjme zas spätne konvertované na dáta. Vyrábajú sa v jednom prevedení a sú označované „transceiver" vysielač – prijímač alebo bezdrôtová sieťová karta. Bezdrôtová sieť sa správa ako HUB.

5.1.9. Most (Bridge)

Slúžia na prepojenie dvoch sieťových segmentov. Operujú na linkovej vrstve (2) OSI modelu, rozhodujú, či sa signál dostane do 2 siete, rozhodujú sa na základe MAC adresy.

5.1.10. Prepínače (switches)

Je niekedy popisovaný ako multiportový bridge. Na komunokácia používajú tabuľku, kde sú uložené MAC adresy. Pri komunikácii s jedného portu pošlú dáta na port, ku ktorú má presne pridelenú MAC adresu s tabuľky, tie si zistí pri prvotnej komunikácii. Výrazne ovplyvňujú kapacitu siete.

5.1.11. Hlavné pripojenia

Každá sieťová karta nesie jedinečný kód, zvaný MAC adresa.

5.1.12. Peet to peer

Klienti pôsobia ako rovnocenný partneri, užívateľ rozhoduje, čo bude zdieľať. Každý PC má vlastnú administráciu, archiváciu. Sú vhodné pre 10 a nemej PC.
Výhody:

1. lacné
2. nepotrebujú dodatočný špecializovaný sieťový administračný software
3. nepotrebujú administrátorov

Nevýhody:

1. každý užívateľ musí vedieť vyriešiť administrátorské požiadavky
2. nižšia bezpečnosť

5.1.13. Klient – server

Sieťové služby sú umiestnené na určenom PC zvonom server. Server je centrálny počítač, ktorý nepretržito odpovedá na požiadavky klientov pre súbory, tlač, aplikácie a iné služby. Aby mohol klient pristupovať ku zdrojom, musí byť najskôr identifikovaný a autorizovaný. Tento proces zabezpečujú prístupové mená a heslá. Umiestnením dát centrálne na serveri je zabezpečená jednodukšia spáva a zálohovanie.
Výhody:

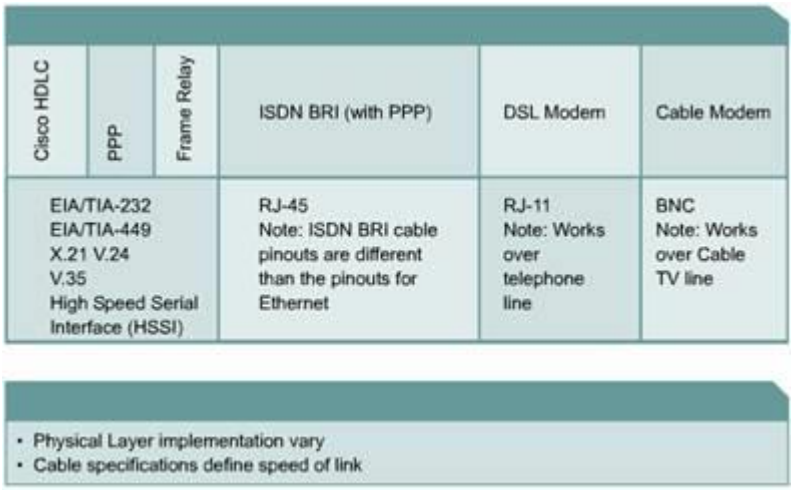
1. poskytnutie lepšej bezpečnosti
2. jednodukšie na administráciu pri veľkých sieťach, pretože administrácia je centrálna
3. všetky dáta sú zálohované lokálne, na jednom mieste

Nevýhody:

1. náklady na špecializovaných administrátorov a operačný systém
2. vyššie hardwarové nároky pre server
3. vyžadujú profesionálnych administrátorov
4. užívateľské dáta sú neprístupné, pokiaľ je server vypnutý

5.2.1. WAN fyzická vrstva

Sériové pripojenia sú použité pre WAN služby, ako prenajaté linky alebo frame relay. Rýchlosti do 2400bps
T1: 1.544mbps
E1: 2.048mbps
ISDN: BRI je založené na 2 nosných 64kb kanáloch a 1 16kb data kanále pre signalizáciu a servisné služby.
DSL, káblový modem: trvalé vysokorýchlostné pripojenie



5.2.2. WAN sériové pripojenie

Dáta sú posielané sériovo. Signály prenášané cez hlasové telefónne linky používajú 4kHz. Tento rozsah frekvenčného rozsahu je odkazovaný na šírku pásma v tabuľke.
Pre CISCO sa používajú 2 tipy komunikácie:

Data (bps)	Distance (Meters) EIA/TIA-232	Distance (Meters) EIA/TIA-449
2400	60	1250
4800	30	625
6900	15	312
19,200	15	156
38,400	15	78
115,200	3.7	—
T1 (1.544 Mbps)	—	15

1. 60 pinový konektor
2. smart serial konektor

Ak komunikácia je vytvorená priamo na servisného poskytovateľa, alebo zariadenie, ktoré poskytuje signálovú synchronizáciu, rúter bude dátový terminálovým zariadením (DTE) a použije sa DTE sériový kábel. Ale tu sú udalosti, kde lokálny rúter potrebuje synchronizovať rýchlosť a tak bude použitý dátový komunikačný kábel (DCE).

5.2.3. Rútre a sériová komunikácia

Vnútri LAN prostredia rúter obsluhuje „broadcasts", poskytuje lokálny adresový rozsah služieb, ako ARP a RARP, a veľa segmentov v sieti používajú podsieťovú štruktúru. Keď sa pripájame priamo na servisného poskytovateľa, alebo zariadenie ako CSU/DSU, potom bude prevádzaná časová synchronizácia, rúter bude DTE a budeme potrebovať DTE sériový kábel.

5.2.4. Rútre a ISDN BRI pripojenie

Pri BRI sú 2 typy pripojenia:

1. S/T – neobsahuje NT1
2. BRI/U – obsahuje network ternination 1 (NT1)

5.2.5. Rútre a DSL pripojenie

Na pripojenie ADSL linky do portu na rútri treba urobiť:

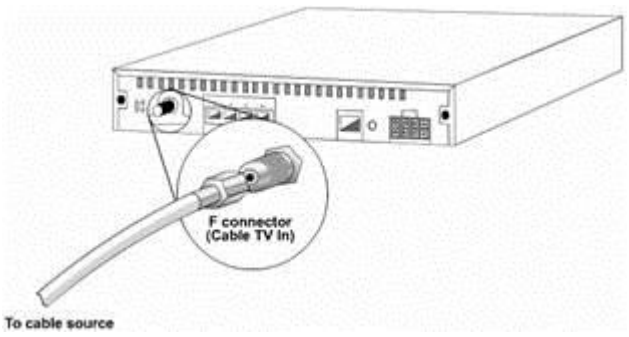
1. pripojiť telefónny kábel na ADSL port
2. pripojiť druhú koniec telefónneho kábla telefónny jack

Na pripojenie sa používa RJ-11

5.2.6. Rútre a káblové pripojenie

Cisco uBR905 káblový rúter poskytuje vysokorýchlostný prístup na káblový televízny systém, Pripája sa priamo na koaxiálny kábel označovaný ako F - konektor.
Postup pripojenia:

1. overiť, či rúter nie je pripojený na napájanie
2. nájsť RF koaxiálny kábel
3. nainštalovať konektor
4. pripojiť kábel k rútru



5.2.7. Nastavenie konzolového pripojenia

Conzolový port: na konfiguráciu, správu, monitoring hubov, svičov a rúterov.
Rollover cable: kábel na pripojenie ku terminálu s RJ-45, kábel je vyrábaný 1-8,2.-7,..8-1
Konfigurácia terminálu: 9600bps, 8 data bit, bez parity, 1 stop bit

Podstata ethernetu

6.1.1. Úvod do ethernetu

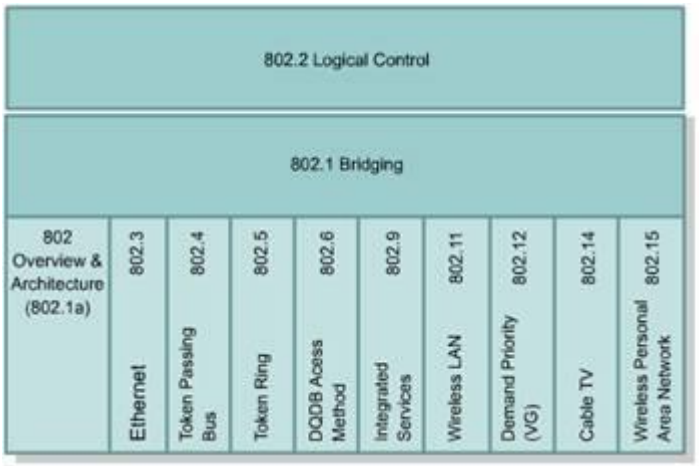
Úspech ethernetu:

1. jednoduchý a ľahký na údržbu
2. schopnosť začleniť nové technológie
3. spoľahlivosť
4. nízka cena inštalácia a zlepšenia

S narastajúcim počtom užívateľov nastali problémy so vzájomným rušením. Tento problém vyriešili na Havajskej univerzite a pomenovali ho Alohanet.
802.3 – štandard pre Ethernet
Rýchlosť sietí narastala z 10Mbps, na 100M, 1G a na 10Gbps
Ethernet je škálovatelný, časový pobyt paketu na sieti nemení jeho obsah, paket môže začať v 10Mb NIC, cestovať cez 10Gb ethernet a končiť v 100Mb NIC.

6.1.2. IEEE pravidlá pre pomenovanie Ethernetu

Základný frejmový formát a IEEE podvrstvy 1 a 2 zostávajú zhodný pre všetky formy Ethernetu. Na potreby rozšírenia Ethernetu sa pridávajú 1 alebo 2 písmená za 802.3.



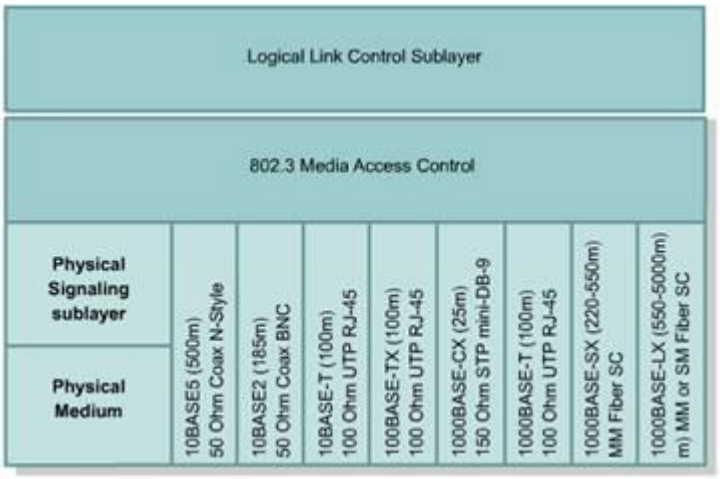
Skrátený popis pozostáva z:

1. číslo indikujúce počet prenášaných Mbps
2. svetový základ, indikujúci, ktoré základné pásmo signálov je použité
3. 1 alebo viac znakov indikujúcich tip použitého média(F-optika, T-medená netienená krútená 2-linka)

Speed	Signal Method	Medium
10	BASE	2
100	BROAD	5

Ethernet pôsobí na 2 vrstvách OSI modelu, v dolnej polovici dátovej linkovej vrstvy, známej ako MAC podvrstva a fyzickej vrstve. Často sa stáva, že medzi 2 stanicami je opakovač, ten zabezpečí zosilnenie signálu a prenos na ďalšie stanice.
Ethernetová vrstva 1 zohráva kľúčovú úlohu v komunikácii ktorá zaberá miesto medzi zaríiadeniami, ale každá funkcia je limitovaná. 2 vrstva adresuje tieto limity:

- Layer 1 cannot communicate with the upper-level layers.
- Layer 2 does this with Logical Link Control (LLC).
- Layer 1 cannot identify computers.
- Layer 2 uses an addressing process.
- Layer 1 can only describe streams of bits.
- Layer 2 uses framing to organize or group the bits.
- Layer 1 is unable to decipher which computer will transmit binary data from a group that are all trying to transmit at the same time.
- Layer 2 uses a system called Media Access Control (MAC).



Najpoužívanejšie možnosti ethernetu.

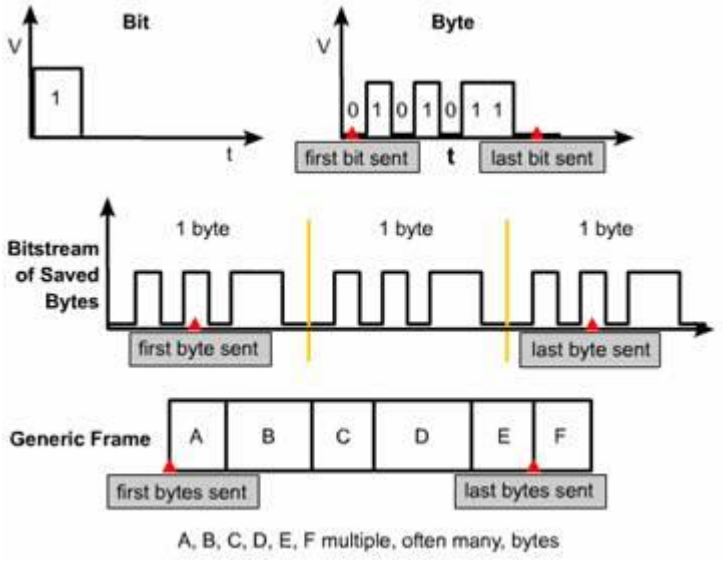
6.1.4. Pomenovanie

Ethernet používa MAC adresy, ktoré sú 48 bitov dlhé a sú vyjadrené ako 12 hexadecimálnych čísel. Organization Unique Identifer (OUI) - Prvých 6znakov s MAC identifikuje výrobcu alebo predajcu
SN- zvyšných 6 hexa znakov, alebo iná hodnota špecifikujúca zariadenie výrobcu
MAC adresy sú pevne napálené v ROM a sú kopírované do RAM, keď sa NIC inicializuje
V linkovej vrstve MAC hlavičky a ukončenia sú pridávané do hornej linkovej vrstvy. Obsahujú kontrolné informácie určené pre linkovú vrstvu v cieľovom systéme. Dáta s hornej vrstvy sú zapuzdrované v linkovej hlavičke a ukončení. Sieťová karta využíva MAC adresu na určenie, či správa môže byť prevzatá do hornej vrstvy OSI modelu, toto sa dele bez použitia CPU. Pri komunikácii NIC kontroluje hlavičku a číta MAC, ak nie je určené pre túto NIC, zahodí tieto dáta, pri zhode presúva tieto dáta do OSI vrstiev.
Všetky zariadenia pripojené do siete majú MAC.

6.1.5. Vrstva 2 rámcovanie

Rámcovanie pomáha získa podstatné informácie, ktoré by nemohli byť získané ináč, len s kódovaného bitového toku. Príklady takýchto informácií sú:

1. počítač komunikujúci s ostatným
2. keď komunikácia medzi jednotlivými PC začína a končí
3. poskytuje metódu pre detekciu chýb, ktoré sa vyskytujú počas komunikácie



Na zobrazenie bitov sa používa graf napätia a času.
Údaje v grafe sú čítané s ľava do prava.
Každý rámec má sekciu zvanú pole, každé pole pozostáva s bitov.
Mená polí:

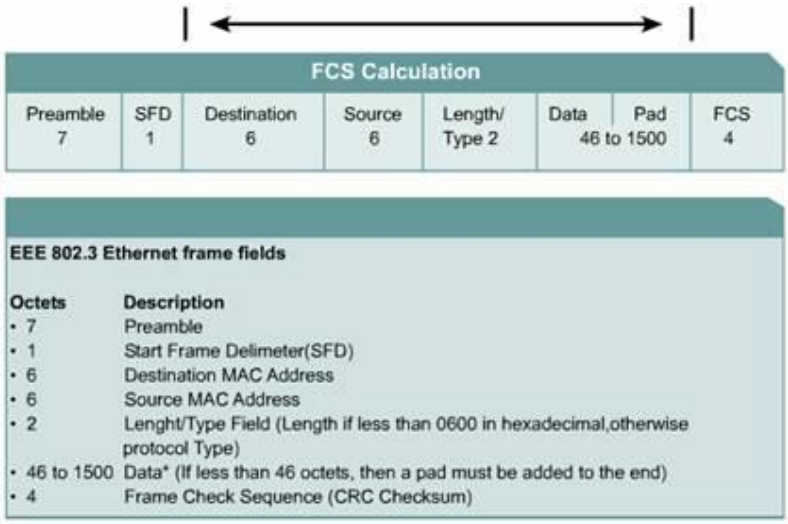
1. štartové rámcového poľa
2. adresové pole
3. dĺžka / typ poľa
4. dátové pole
5. kontrolný súčet

Všetky rámce vždy začínajú signalizačnou sekvenciou bitov.
Všetky rámce obsahujú menovité informácie, ako zdrojovú a cieľovú MAC.
Dôvodom posielania rámcov je dať hornej vrstve dáta, hlavne užívateľské aplikačné dáta, zo zdroja do cieľa.

Dátový paket má 2 časti:

1. užívateľské aplikačné dáta
2. zapuzdrené bity posielané na cieľový počítač.

V dátovom poli sú tiež obsiahnuté logické linkové kontrolné (LLC) byty. Vrstva 2 komunikuje s hornou vrstvou cez LLC.
Všetky rámce a bity, bajty, a polia obsiahnuté v nich, sú citlivé na chyby s množstva zdrojov. Rámcová kontrolná sekvencia (FCS) poľa obsahuje číslo, ktoré je vypočítané podľa zdrojového uzla založenom na dátach v rámci, je pridávaný na koniec rámca. Pri prenose rámcov je v cieľovej stanici FCS číslo prepočítané a porovnané s FCS číslom obsiahnutým v rámci, ak sú rozdielne, rámec je zahodený a vyžiada sa nový.
3 Základné cesty výpočtu FCS:
- cycli redundancy check (CRC), vykonáva sa z výpočtu dát
- 2 rozmerových parít, pridávaním ôsmeho bitu, ktorý vytvára párne alebo nepárne binárne číslo
- internetový kontrolný súčet, pridáva hodnoty od všetkých dátových bitov do súčtu.



FCS Calculation						
Preamble 7	SFD 1	Destination 6	Source 6	Length/ Type 2	Data / Pad 46 to 1500	FCS 4

EEE 802.3 Ethernet frame fields

Octets	Description
• 7	Preamble
• 1	Start Frame Delimeter(SFD)
• 6	Destination MAC Address
• 6	Source MAC Address
• 2	Lenght/Type Field (Length if less than 0600 in hexadecimal,otherwise protocol Type)
• 46 to 1500	Data* (If less than 46 octets, then a pad must be added to the end)
• 4	Frame Check Sequence (CRC Checksum)

6.1.6. Štruktúra rámcov v Ethernete

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimeter	Destination Address	Source Address	Length/ Type	802.2 Header and Data	Frame Check Sequence

Ethernet					
8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

6.1.7. Rámcové polia Ethernetu

Preambula je alternatívny vzor 1 alebo 0 používané pre časovú synchronizáciu v asynchrónnych 10Mbps alebo pomalších Ethernetoch. Rýchlejšie verzie sú synchrónne a preto táto informácia je prebytočná, ale ponechaná pre spätnú kompatibilitu.
Štartový rámcový oddeľovač pozostáva s 1 octetu poľa, ktorý značí koniec časovacej informácie a pozostáva zo sekvencie 10101011
Cieľové adresné pole MAC cieľovú adresu.

Zdrojové adresné pole obsahuje zdrojovú MAC adresu.
Dĺžka/typ poľa podporuje 2 rôzne využitia. Ak hodnota je menšia ako 1536, hodnota indikuje dĺžku. Dĺžka prekladu je použitá keď LLC vrstva poskytuje protokolovú identifikáciu. Pri väčšej hodnote ako 1536, tip a popis dátového poľa sú dekódované podľa protokolu.
Maximálny prenášaný unit (MTU) pre Ethernet je 1500 octetov, data by nemali presahovať túto veľkosť. Ethernet vyžaduje dĺžku dát od 46 do 1500 oktetov.
FCS obsahu 4 bity pre CRC

6.2.1. Media access control (MAC)

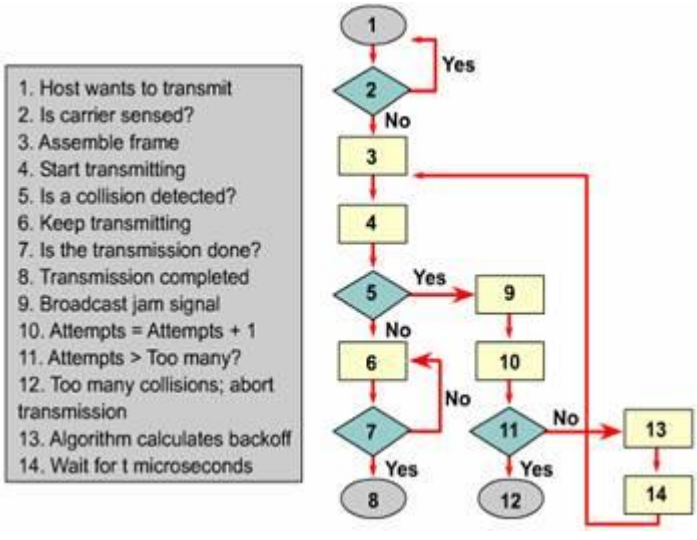
MAC sa odkazuje na protokoly ktoré určujú ktorý PC alebo zdieľané zariadenie môže vysielať. MAC a LLC sú súčasti 2 vrstvy.
Delia sa na deterministické (token ring a FDDI) a nedeterministické.
Token ring – hosti sú umiestnený v kruhu a špeciálne dáta tokenu cestujú dookola cez každého hosťa. Keď host chce vysielať, uchopí token, vyšle dáta pre limitný čas, a potom vyšle token k nasledujúcemu hostu. V token ring môže vysielať dáta len 1 host vo vyhradenom čase.
V nedeterministickom MAC protokole sa používa kto skôr príde, ten skôr melie. CSMA/CD je jednoduchý systém. NIC načúva, či niekto nevysiela, ak nie začne vysielanie. Ak naraz začnú vysielať 2 NIC, potom nastane kolízia a žiaden s nich nie je schopný prenášať.
Všeobecné technológie:

1. Ethernet, logická zbernicová topológia, fyzická hviezda alebo rozšírená hviezda, inf. prúdia po lineárnej zbernici
2. Token ring, logická kruhová topológia, inf. prúdia v kontrolovanom kruhu
3. FDDI, logická kruhová topológia, fyzická kruhová dvojitá topológia, inf. prúdia v kontrolovanom kruhu

6.2.2. MAC pravidlá a detekcia kolízií

Prístupová metóda CSMA/CD používa v Ethernete 3 funkcie:

1. prenášať a prijímať dátové pakety
2. dekódovať dátové pakety a kontrolovať ich na správnosť pred prechodom do vyššej vrstvy ISI modelu
3. detekovať chyby vo vnútri paketu alebo na sieti



V CSMA/CD prístupovej metóde sieťové zariadenie pred vysielaním pracuje v móde počúvaj- pred vysielaním, to znamená, že pred vyslaním dát čaká, kým sieť nebude používaná, čas testovania je náhodný. Pri nepoužívanej sieti začne vysielať a načúvať, či iné zariadenie nezačalo v tom istom čase vysielanie. Po ukončení dátového vysielania sa prepne do stavu počúvania.
Kolízie sa detekujú zväčšením amplitúdy signálu. Pri kolízii bude prenos na staniciach, ktoré vysielali, pokračovať po krátkom čase, keď sa ubezpečia, že všetky zariadenia počuli kolíziu. Vo všetkých zariadeniach sa spustí obnovovací algoritmus, v zariadenia sa vygeneruje náhodný čas, po ktorom opäť skúsia vysielať. Zariadenia, ktoré vyvolali kolíziu, majú najmenšiu prioritu.

6.2.3. Časovanie ethernetu.

V Ethernetovej sieti môžu nastať kolízie aj vplyvom oneskorení, tie sa vytvárajú jednak na opakovačoch a sieťových komponentoch.
Pokiaľ je stanica schopná naraz vysielať a prijímať, kolízie by nastať nemali. Plný duplex mení časovanie a eliminuje koncept pozičných časov.
Pri polovičnom dulpexe sa najskôr vysiela 64 bitov, známich ako preambula, na synchronizáciu a potom sa vysielajú nasledujúce informácie:

1. cieľová a zdrojová MAC
2. určené hlavičkové informácie
3. dáta
4. kontrolný súčet

Prijímacia stanica si najskôr overí CRC a potom posunie dáta vyššej vrstve.

Ethernet Speed	Bit time
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

10Mbps a pomalšie verzie Ethernetu sú asynchrónne, teda pred prijímacia stanica použije 8 oktetov na synchronizáciu.
100Mbps a rýchlejšie sú synchrónne, teda synchronizácia nie je potrebná, ale pre spätnú kompatibilitu je preambula a SFD zachovaná.
Slot time pre 10 a 100Mbps Ethernet je 512 bit-times alebo 64 oktetov
Slot time pre 1000Mbps Ethernet je 4096 bit-times alebo 512 oktetov
Slot time je počítaný s maximálnej predpokladanej dĺžky na najväčšej dovolenej sieťovej architektúre.
Výpočet slotového času pozostáva s času o niečo dlhšieho, ako je treba, aby signál prešiel s najvzdialenejšieho bodu, dostaním sa do kolízie s iným vysielaním a vrátil sa späť do vysielacej stanice, kde má byť zdetekovaný.

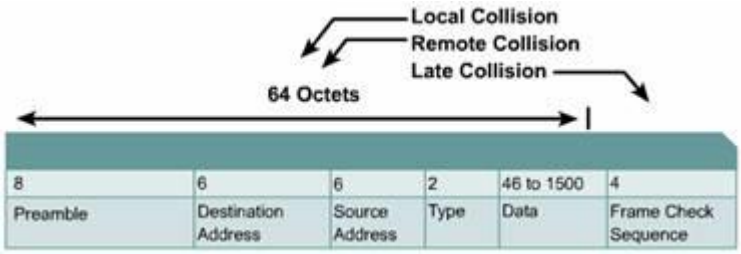
6.2.4. Medzirámcový odstup a backoff

Speed	Slot Time	Time Interval
10 Mbps	512 bit-times	51.2 µs
100 Mbps	512 bit-times	5.12 µs
1 Gbps	4096 bit-times	4.096 µs
10 Gbps	not applicable	not applicable

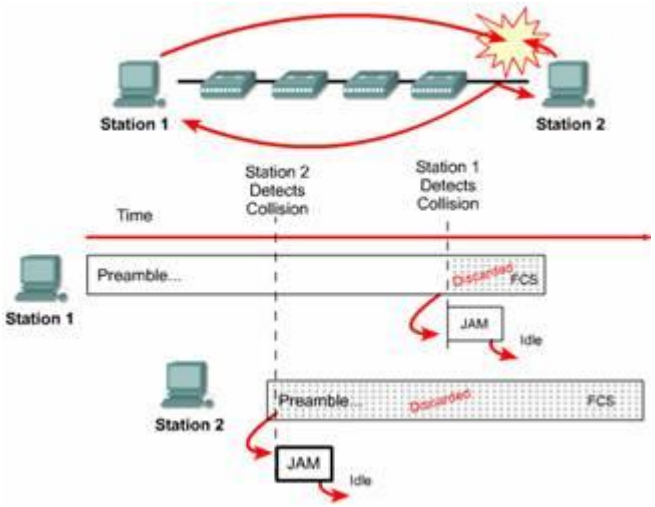
Medzirámcový odstup – minimálny odstup medzi 2 nekolíznymi rámcami

Po poslaní rámca, všetky stanice na 10 Mbps Ethernete musia minimálne čakať 96 bit-times (9,6ms), kým sa vyšle ďalší rámec. Na vyšších rýchlostiach ostáva odstup rovnaký. Tento interval je spacing gap. Tento úsek (gap) je plánovaný pre spracovanie predchádzajúceho rámca a pripravenie ďalšieho.
Pri kolízii sa všetky stanice stanú nečinnými, stanice, ktoré vyvolali kolíziu si vygenerujú náhodný čas, kým sa opäť pokúsia poslať kolízny rámec. Ak sa MAC vrstve nepodarí odoslať rámec po 60 pokusoch, vygeneruje sa chyba na sieťovej vrstve. Tento stav nastáva len zriedka a je príznakom nejakých fyzických problémov na sieti.

6.2.5. Spracovanie chýb.



Kolízie sú mechanizmom pre rozlíšenie sporov pre sieťový prístup. Kolízie majú za následok pokles šírky pásma spôsobenej oneskorením pôsobiacim na všetky body v sieti. Značná väčšina kolízií sa stáva na začiatku rámca, skôr než SFD. Hneď ako je detekovaná kolízia, stanica, ktorá vysielala, vyšle 32bit „jam" signál.
Popis obrázku:
2 stanice načúvajú, či je linka prázdna, začnú vysielať. Stanica 1 prenesie značnú časť signálu, keď dojde ku kolízii, hneď zastaví prenos dát a okamžite vyšle JAM signál. Stanica 2 odsekne aktuálne vysielanie a nahradí ho 32bitovým JAM signálom, nato zastaví prenos.



6.2.6. Typy kolízií.

Kolízie nastávajú pri súčasnom vysielaní 2 alebo viac staníc v kolíznej doméne.
Jednoduchá kolízia je vtedy, keď sa po 1. kolízii podarí uskutočniť prenos.
Viacnásobná kolízia je vtedy, ak 1 rámec počas prenosu má viacnásobnú kolíziu, kým je úspešne doručený.
Kolízia nastáva, keď dĺžka rámca je menšia ako 64 octetov alebo je nesprávne FCS
Typy kolízií:

1. miestna
2. vzdialená
3. oneskorená

Lokálna kolízia na koaxiálnom kábli, signál cestuje cez kábel až na razí na signál od inej stanice. Pri strete dojde k zvýšeniu napäťovej úrovne nad dovolenú úroveň.
Pri UTP kábli je kolízia detekovaná, keď stanica detekuje signál na RX páre v rovnakom čase ako vysiela na TX pár. Takéto kolízie nastávajú len pri polovičnom duplexe. Ak stanica nevysiela, nevie zdetekovať kolíziu.
Vzdialené kolízie sú charakteristické menšou dĺžkou rámca, nesprávny FCS, ale nezvyšujú napätie alebo nespôsobujú simultánnu RX/TX aktivitu.
Neskoré kolízie, ak nastane po prenose 64 oktetov, NIC kolíziu neprepošle automaticky.

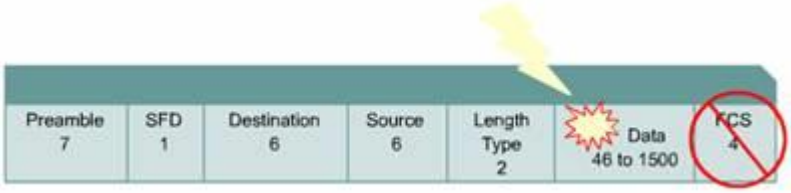
6.2.7. Chyby Ethernetu

Zdroje Ethernetových chýb:

1. kolízia alebo RUNT, simultánne vysielanie pred uplynutím slot time
2. lokálna kolízia, simultánne vysielanie po uplynutím slot time
3. Jabber, dlhé rámcové a rozsahové chyby, neprimerane dlhé vysielanie, od 20 000 - 5 0000 bit time

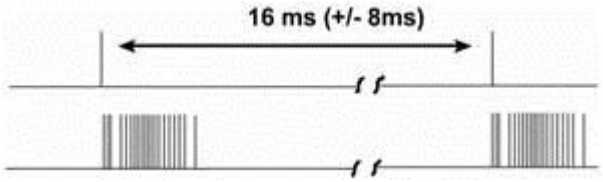
4. Krátky rámec, príliš krátke vysielanie
5. FCS chyby, poškodený prenos
6. Aligment chyby, nedostatočné alebo prebytočné číslo bitového prenosu
7. Chyba rozsahu, aktuálny a oznámený počet oktetov vo rámci nesúhlasí
8. Ghost alebo Jabber, nezvyčajne dlhá preambula alebo JAM udalosť

6.2.8. Kontrolný súčet (FCS)



Prijímané rámce, ktoré majú zlý FCS. V FCS je hlavička pravdepodobne správna, ale kontrolný súčet pre prijímaciu stanicu nesúhlasí so súčtom na konci rámcu, rámec bude zahodený.
Vysoký počet FCS s jednej stanice vždy indikuje vadný NIC alebo poškodený ovládač, alebo vadný kábel.
Vysoký počet FCS pri veľa staniciach indikuje vadnú kabeláž, alebo vadnú verziu NIC ovládača, vadný HUB port, alebo šumy v káblovom systéme.
Chyba Aligment – správy, ktoré nemajú oktetový koniec, rámec je odseknutý. Spôsobené to býva zlým softwarovým ovládačom alebo kolíziami, je sprevádzaný FCS.
Chyba rozsahu – správna hodnota dĺžky poľa ale nesúhlasí s aktuálnou hodnotou oktetov vypočítanej s dátového poľa
Chyba Ghosting – šumy detekované na vedení sa javia ako rámec, ale nemajú správnu SFD, musia byť dlhé min. 72 oktetov a obsahovať preambulu, inač sú klasifikované ako vzdialená kolízia.

6.2.9. Ethernet auto – negatiation



Auto negatiation of speed- automatické dohodnutie maximálnej rýchlosti, 2 zariadenia sa synchronizujú
Pri 10base-T sú vyžadované každých 16 ms pulzy, keď stanica nevysiela správu. Auto negatiation prijala tieto pulzy a premenovala ich na Normal Lipnk Pulse (NLP). Keď séria NLP je poslaná ako skupina pre účel auto n., skupina je nazvaná Fast Link Pulse (FLP). FLP sú posielané v rovnakom časovom intervale ako NLP.

6.2.10. Zavedenie linky a plný a polovičný duplex

Duplex sa dá nastaviť manuálne, ale všetky stanice ho musia mať nastavený rovnako.
Half duplex – všetky koaxiálne médiá, UTP a optika vie oboje
Full duplex – 10Gbps
V polovičnom môže vysielať len 1 stanica, v plnom viac.

Ethernetové technológie

7.1.1. 10Mbps Ethernet

Všeobecné črty Ethernetu:

1. časové parametre
2. rámcový formát

3. proces prenosu
4. základné dizajnové pravidlá

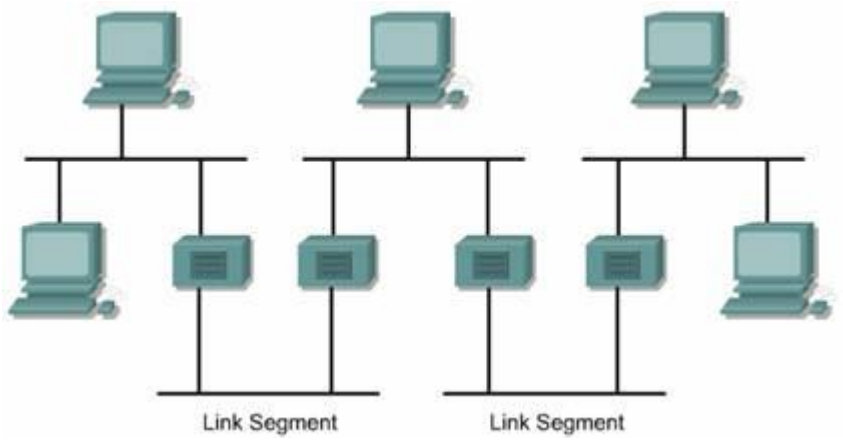
SQE (Signal Quality Error) – vždy použitý pri half duplexe, pri full nie je potrebný
SQE je aktívny:

1. v rozsahu 4-8 mikrosekúnd nasledovaný normálnym prenosom, indikuje, že odchádzajúci rámec bol správne prenesený
2. keď je kolízia na médiu
3. keď je nesprávny signál na médiu
4. keď prenos bol prerušený

Parametre časových limitov:

1. dĺžka kábla a jeho šírené oneskorenie
2. oneskorenie opakovačov
3. oneskorenie vysielačov
4. interfrejmový kúskový úbytok
5. oneskorenie vnútri stanice

Pravidlo 5-4-3: kvôli zachovaniu časových limitov 10mbps Ethernet pracuje maximálne v 5segmentoch, nie viac ako 4 opakovače, 3 segmenty s PC. Toto pravidlo platí len pre HUB.



7.1.2. 10BASE5

10BASE5 prenášal 10Mbps po koaxiálnej zbernici. Použité Menchester kódovanie. Výhoda bola dĺžka 500m, nevyžadoval konfiguráciu. Náchylný na zlyhanie 1 bodu(potom nejde nič). Dnes je zastaralý.
Pretože sa prenos realizoval po jednom kábli, mohla vysielať len 1 stanica, half duplex, maximálny prenos 10Mbps. Platí pravidlo 5,4,3.

7.1.3. 10BASE2

Prepojenie jez BNC konektory a T konektory, ukončenie cez 50 ohm terminátory. Použité Menchester kódovanie. Minimálna vzdialenosť medzi PC 0,5m. Maximálna vzdialenosť 185m. Tu môže byť maximálne 30 staníc na každom segmente. Môžu byť len 2 opakovače.

7.1.4. 10BASE-T

S počiatku bola sieť len half-duplex, neskôr sa prešlo na full-duplex. Všetka komunikácia je koncentrovaná v jednom zariadení, buď HUB alebo SWITCH. Zapojenie je hviezdicové. Maximálna vzdialenosť pre kábel je 90m. Je použitý RJ45 konektor. Pri prenose cez full-duplex je prenos 20Mbps.

Pin Number	Signal
1	TD+ (Transmit Data, positive-going differential signal)
2	TD- (Transmit Data, negative-going differential signal)
3	RD+ (Receive Data, positive-going differential signal)
4	Unused
5	Unused
6	RD- (Receive Data, negative-going differential signal)
7	Unused
8	Unused

7.1.5. 10BASE-T vedenia a architektúra

10BASE-T obvykle pozostávajú s pripojenie medzi stanicami a HUBOV alebo SWITCHOV. Použité Menchester kódovanie. HUB nedelí sieť na segmenty, je to multiportový opakovač, pri viacnásobnom prepojení dochádza k oneskoreniam
SWITCH a BRIDGE delia sieť na oddelenú doménu.
Vzdialenosť medzi SWITCHMI je 100m.

7.1.6. 100 Mbps Ethernet

Je tiež známi ako FAST Ethernet. Použité pre medené vodiče (TX) aj pre optiku (FX).
Na 100Mbps prejde 1 bit za 10ns. Fast Ethernet je citlivejší na šumy ako 10Mbps. Kódovanie 4B/5B.

7.1.7. 100BASE-TX

Používaný pre CAT5. Spočiatku half-duplex 100Mbps, neskôr nahradený full-duplex 200Mbps. HUB bol nahradený SWITCHOM. Použité kódovanie 4B/5B, ktoré sa konvertuje na multi-level transmit 3 MLT-3. Zapojenie pinov rovnaké, ako pri 10BASE-T.

7.1.8. 100BASE-FX

100Mbps optické vedenia sa využívajú pri prepojení poschodí, budov, chrbticové zapojenia a v miestach z vysokým šumom. V praxi sa moc neujal, bol hneď nahradený 1Gbps. Tiež je použitá 4B/B technológia kódovania.

Fiber	Signal
1	Tx (LED and laser transmitters)
2	Rx (high-speed photodiode detectors)

Je možný prenos 200Mbps prenos, pretože je oddelené vysielanie a príjem

7.1.9. Architektúra Fast Ethernet

Architecture	100BASE-TX	100BASE-FX	100BASE-TX and FX
Station to Station, Station to Switch, Switch to Switch (half or full duplex)	100 m	412 m	N/A
One Class I Repeater (half duplex)	200 m	272 m	100 m (TX) 160.8 m (FX)
One Class II Repeater (half duplex)	200 m	320 m	100 m (TX) 208 m (FX)
Two Class II Repeaters (half duplex)	205 m	228 m	105 m (TX) 211.2 m (FX)

Fast Ethernet obvykle pozostáva s prepojenia medzi stanicou a hubom alebo switchom.

7.2.1. 1000 Mbps Ethernet

Je používaný v optike aj v medených médiách.
1000BASE-X je 1Gbps cez plný duplex cez optické vlákna. Na 1000Mbps prejde 1 bit za 1ns.
Pri 1Gbps Ethernete je vysoká rýchlosť, preto je náchylnejší na rušenie.
1000BASE-X používa 8B/10B kódovanie, ktoré je simulovaná ako 4B/5B koncept.

7.2.2. 1000BASE-T

Fast Ethernet bol inštalovaný na zvýšenie šírky pásma, bol navrhnutý tak, aby mohol fungovať na existujúcich rozvodoch, po vykonaní testov na cet.5e. Na prenos sa používajú všetky 4 páry. Vďaka 4 párom sa môže prejsť na full duplex v tom istom vodiči. Cez 1 pár ide 250Mbps, rámec je rozdelený na 4 časti a prijímači opäť poskladaný . Je použitá 4D-PAM5 kódovanie.

7.2.3. 1000BASE-SX a LX

Výhody 1Gbps ethernetu cez optiku:

1. šumová imunita
2. nie je problém s potenciálom v uzemnení
3. výborná charakteristika na vzdialenosť

Kódovanie:

1. 8B/10B pre optické vlákna a tienené medené médiá
2. pulse amplitude modulation 5 (PAM5) pre UTP

10BASE-X: používa 8B/10B kódovanie konvertované na Non-Return to Zero (NRZ) priame kódovanie. NRZ signály sú potom impulzmi na vláknach, sú buď krátke alebo dlhé vlnové dĺžky vo svetelnom zdroji.
Vlnová dĺžka:

1. 850nm, laser alebo LED, pri multimóde LX

2. 1310nm, pri multi a single móde

V single móde môžeme pomocou laserového zdroja dosiahnuť až 5km.
Označenie vlákien:

1. Tx, vysielanie
2. Rx, čítanie, príjem dát

Pri prenose je povolený len 1 opakovač.

7.2.4. Architektúra gigabitového ethernetu

Limitácia vzdialenosti pri plnom duplexe je limitovaná len médiom a nie obehovým oneskorením.

Medium	Modal Bandwidth	Maximum Distance
62.5µm Multimode Fiber	160	220 m
62.5µm Multimode Fiber	200	275 m
50µm Multimode Fiber	400	500 m
50µm Multimode Fiber	500	500 m

Medium	Modal Bandwidth	Maximum Distance
62.5µm Multimode Fiber	500	550 m
50µm Multimode Fiber	400	550 m
50µm Multimode Fiber	500	550 m
10µm Multimode Fiber	N/A	5000 m

1000BASE-T UTP kábel je rovnaký ako 10BASE-T a 100BASE-TX, vzdialenosť 100m.

7.2.5. 10Gb Ethernet

10Gb prenos v plnom duplexe, vyvinutý pre MANs a WANs.
Kompatibilita:

1. rámcový formát je rovnaký
2. prenesenie 1 bitu trvá 0,1ns
3. len full duplex
4. možnosť prenosu na 40km
5. flexibilný, výkonný, spoľahlivý,
6. TCP/IP môže bežať cez LANs, MANs, WANs

7.2.6. Architektúra 10Gb Ethernetu

Veľmi dôležitá je synchronizácia, pretože je trvanie bitu krátke a je ho ťažké odlíšiť od šumu.
Kódovacie kroky:

1. užívateľské dáta reprezentujú kódy, prenos je výkonnejší
2. kódované dáta poskytujú synchronizáciu, zvyšujú šírku pásma

Väčšinou 10GbE produkty sú formou pre moduly, pre pridávanie pre hight-end switche a routre. Pre 10GbE existujú len optické médiá. Opakovače nie sú podporované, half-duplex nie je podporovaný.

7.2.7. Budúcnosť Ethernetu

IEEE a 10-Gigabit Ethernet Alliance teraz pracujú na 40, 100, dokonca na 160Gbps štandarde. Budúcnosť sieťových médií v 3 vrstvách:

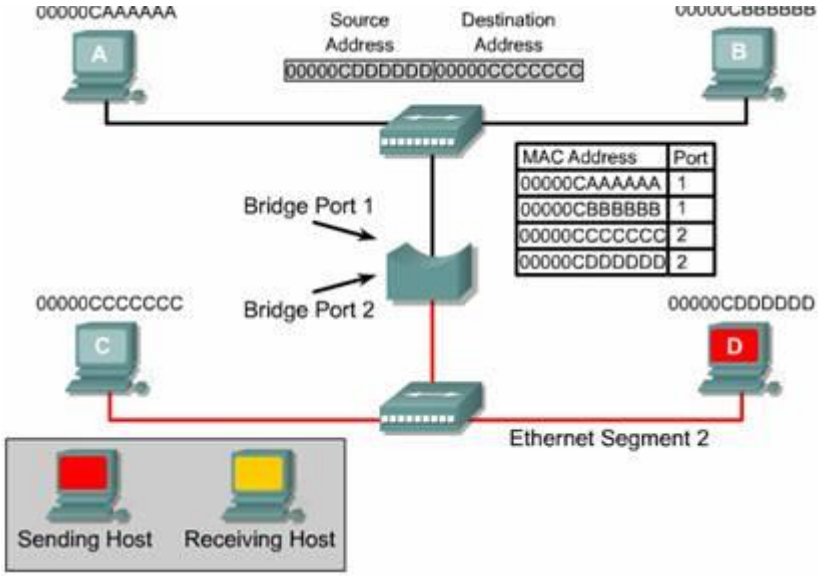
1. medené(do 1Gbps, možno viac)
2. bezdrôtové (približujú sa 100Mbps)
3. optické vlákna(na 10Gbps, čoskoro to bude viac)

Pri polovičnom duplexe sú možnosti kolízie, vhodný pre IP telefóniu a video vysielaie.

Prepínanie ethernetu

8.1.1. Premosťovanie vrstvy 2

Zvyšovaním počtom staníc v segmente narastá pravdepodobnosť kolízie a výsledkom je viac opakovaných prenosov. Riešením je rozdeliť kolíznu doménu na niekoľko menších, oddelených častí. Pri prepájaní využívajú bridže tabuľku MAC adries asociovanú s portami.



Operácie bridžov:

1. pri zapnutí je tabuľka prázdna, sleduje komunikáciu na sieti, ak nastane, bridž ju spracuje
2. A pingne B, dáta sú prenesené na celý kolízny systém
3. most si pridá záznam do bridge table.
4. cieľová adresa rámca je kontrolovaná v tabuľke, keď nie je nájdená, rámec je poslaný na druhý segment. Pri tomto prenose je zaznamenaná len zdrojová adresa.
5. B spracuje ping a pošle odpoveď A, bridge a A spracujú rámec
6. bridge si pridá zdrojovú adresu do tabuľky. Pretože zdrojová tabuľka nebola v tabuľke mostu a bola prijatá na port 1, zdrojová adresa musí byť asociovaná s portom 1 v tabuľke. Cieľová adresa rámca je opäť skontrolovaná v tabuľke, je nájdený záznam a rámec sa neposiela ďalej.
7. A pingne C, dáta obdrží celá kolízna doména, B ich zahodí, neboli preň určené.
8. Bridge pridá záznam do tabuľky, pretože záznam už existuje, tak ho len obnoví.
9. Bridge skontroluje cieľovú adresu, záznam nenájde, preto pošle rámec ďalej
10. C spracuje požiadavku a pošle odpoveď A. Dáta sú poslané celej kolíznej doméne. D dáta zahodí, lebo nie sú preň určené

11. Bridge si pridá zo zdrojovej adresy záznam do tabuľky a asociuje si ho s portom 2.
12. Bridge opäť skontroluje tabuľku, nájde záznam a pošle dáta na port 1
13. Podobne je to s D

8.1.2. Prepínanie na vrstve 2

Svitch je v podstate rýchly, multiportový bridge, ktorý môže obsahovať veľa portov. Radšej vytvoríme 2 kolízne domény, každý port vytvára vlastnú kolíznu doménu. Ak je 20 staníc zapojených do sviča, potom je vytvorených 20 samostatných kolíznych domén. Sviče si budújú content-addresable memory (CAM) /pamäť adresovaná podľa obsahu/, pre každý port má pridelenú MAC informáciu.

8.1.3. Spínacie operácie

Mikrosegment, na svič je pripojené jen 1 zariadenie. Použitím CAM je umožnené svičom priame nájdenie portu, ktorý je asociovaný s MAC, bez vyhľadávacieho algoritmu. To umožňuje znížiť záťaž na sieti.

8.1.4. Oneskorenie

Rôzne podmienky môžu zapríčiniť oneskorenia rámca cestujúceho so zdroja do cieľa:

1. oneskorenie v médách
2. kruhové oneskorenie, spôsobené elektronikou
3. programové oneskorenie, pri prechode s jednotlivý vrstiev a pri prepájaní

8.1.5. Módy sviču

Cut-trought - Svič môže zahájiť prenos rámca hneď po prijatí MAC adresy. Výsledkom je nižšie oneskorenie pri prepájaní. V tomto móde nie sú kontrolované chyby. Musí byť rovnaká rýchlosť cieľa aj zdroja, tiež nazývané synchronizované prepínanie.
Store-and-forward - v tohto móde svič príme celý rámec a pred posielaním skontroluje jeho kontrolný súčet. Pri chybe zahodí tento rámec. Rámec je pred vysielaním najskôr uložený. Pri tomto móde sa používa asynchrónne prepínanie.
Fragment–free mode - Je kompromis medzi predchádzajúcimi. Číta sa sekvence 64bitov, ktorá obsahuje hlavičku rámca, na základe toho začne prepájanie.

8.1.6. Spannig-Tree protokol

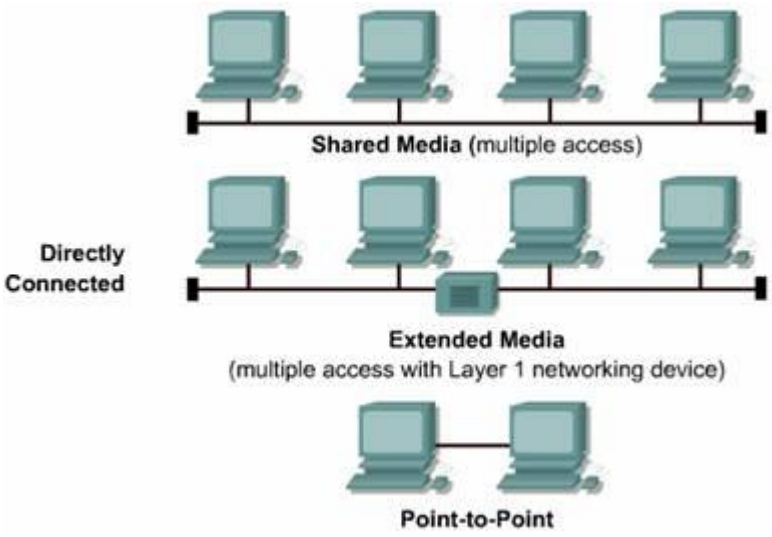
Prepínané siete sú často navrhované s nadbytočnými cestami na zabezpečenie spoľahlivosti. Na zabezpečenie proti zacyklenie bol vyvinutý Spannig-Tree protokol (STP). Každý svič vyšle špeciálnu správu Bridge Protocol Data Units (BPDUs), aby ostatné sviče o ňom vedeli. Sviče potom používajú Spanning-Tree Algorith (STA) na zamedzenie nadbytočnej prevádzky.
Sviče využívajú STP:

1. blokovaní
2. počúvaní
3. učení
4. odosielaní
5. zakázaný

Port presunie cez nasledujúcich 5 stavov:

1. s inicializácie do blokovania
2. s blokovania do počúvania alebo do zakázaný
3. s počúvania do učenia alebo do zakázaný
4. s učenia do dopravný alebo zakázaný
5. s dopravy do zakázaný

8.2.1. Zdieľané médiové okolie



Niektoré siete sú priamo spojené a všetky stanice zdieľajú vrstvu 1.
Zdieľané médiové okolie: keď viacnásobné stanice pristupujú na rovnaké médium, príkladom je, keď niekoľko PC pristupuje na rovnaké vedenie, optické vlákno alebo vzdušný priestor.
Rozšírené zdieľané médiové okolie: zdieľané mádiá môžu rozšíriť, prístup je na väčšie vzdialenosti
Okolie siete poit-to-point: používané v telefonickom pripojení, využívané predovšetkým domácimi používateľmi. Zariadenia sa priamo pripája na len 1 zariadenia, príkladom je, keď sa PC pripája na internet cez modem po telefónnom vedení.
Existujú pravidlá, kto môže pristupovať do siete, niekedy sa však nedajú použiť a nastávajú kolízie.

8.2.2. Kolízne domény

Kolízie zapríčiňujú nevýkonnosť sietí. Pri kolízii všetky stanice ukončia prenos na určitý čas.
Segmentácia: delenie kolíznej domény na menšie časti pomocou zariadení na 2 a 3 vrstve. Zariadenia na 1. vrstve nedelia kolíznu doménu, sú to napr. opakovače, huby.
Zväčšovaním počtov jednotlivých staníc a pridávaním hubov dochádza k väčšiemu počtu kolízií. Preto je definované pravidlo, že medzi 2 PC nesmie byť viac ako 4 opakovače alebo HUBy. Preto musí byť vypočítaná doba obehu, inak by všetky stanice nepočuli kolíziu v sieti.
Platí pravidlo: (oneskorenia na opakovači + oneskorenie na kábli + NIC oneskorenie)x2 misí biť menšie ako maximálna doba obehu. Pri porušení pravidla počet kolízií dramaticky narastá.
Pravidlo 5-4-3-2-1:

1. 5 segmentov v sieti
2. 4 opakovače alebo huby
3. 3 hostiteľské segmenty v sieti s PC
4. 2 linkové časti (bez PC)
5. 1 veľká kolízna doména

8.2.3. Segmentácia

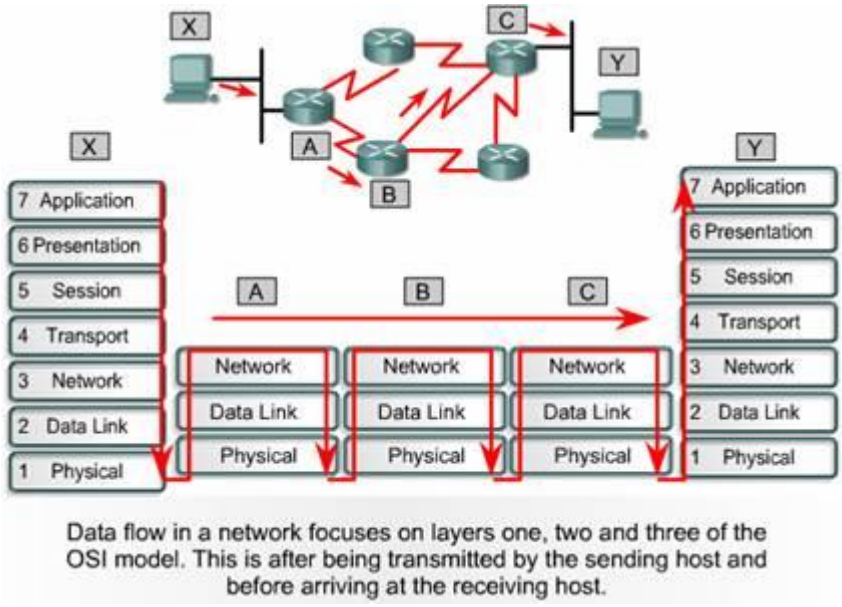
Zariadenia na 1. vrstve nedelia sieť do segmentov, len ju predlžujú.
Zariadenia na 2. vrstve delia sieť na segmenty, kolízna doména je efektnejšie rozdelená na menšie časti. Na vrstve 2, bridže a sviče, sledujú MAC adresy a v ktorom sú segmente.

8.2.4. Vrstva 2 Broadcasts

Na komunikáciu so všetkými kolíznymi doménami protokol používa broadcast a mutlicast rámec na vrstve 2 OSI modelu. Keď potrebuje stanica komunikovať so všetkými ostatnými v sieti pošle brodkástový rámec s cieľovou adresou MAC 0xFFFFFFFFFFFF. Na túto adresu odpovedajú všetky hosty. Môže sa sťať, že pri odpovedi všetkých staníc neostane volná šírka pásme pre aplikácie, existujúce sieťové pripojenie musí byť zrušené, situácia je známa ako brodkastová búrka. Niekoľko tisíc brodkastov alebo multicastov môže zhodiť mašinu. Broadcast pracovnej stanice Addres Resolution Protocol(ARP) sa vyžiada vždy, keď potrebujeme MAC adresu, ktorá nie je v ARP tabuľke. Broadcastovú búrku môže spôsobiť zariadenie vyžadujúce informáciu so siete, ktorá má príliš veľkú skupinu.

8.2.5. Broadcastové domény.

Broadcastová doména je zoskupenie kolíznych domén, ktoré sú spojené zariadeniami na 2 vrstve. Tým sa zvýši príležitosť každého hostu v sieti na získanie prístupu na médium. Broadcast musí byť kontrolovaný na 3 vrstve, rútre nepresúvajú brodkast. 3 vrstva je založená na cieľovej IP adrese a nie na MAC.



Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

8.2.6. Úvod do dátového prúdu

Dáta sú zapuzdrené v sieťovej vrstve s IP zdrojovou a cieľovou adresou a na linkovej vrstve s MAC adresou zdroja a cieľa.
Na zariadeniach na vrstve1 nie je filtrácia, všetko čo sa vyšle, prejde na druhú stranu.
Na zariadeniach na 2 vrstve je filtrácia založená na cieľovej MAC adrese.
Na 3 vrstve sú dáta filtrované na základe cieľovej IP adresy.

8.2.7. Čo je sieťový segment

1. Sekcia siete, ktorá je ohraničená bridžom, rútrom alebo svičom
2. S použitím zbernicovej topológie LAN, segment je pokračujúci elektrický obvod, ktorý je často pripojený na druhý taký segment cez opakovač
3. Termín použitý v TCP špecifikácii popisuje jednodielnu transportnú vrstvu jednotku informácií.

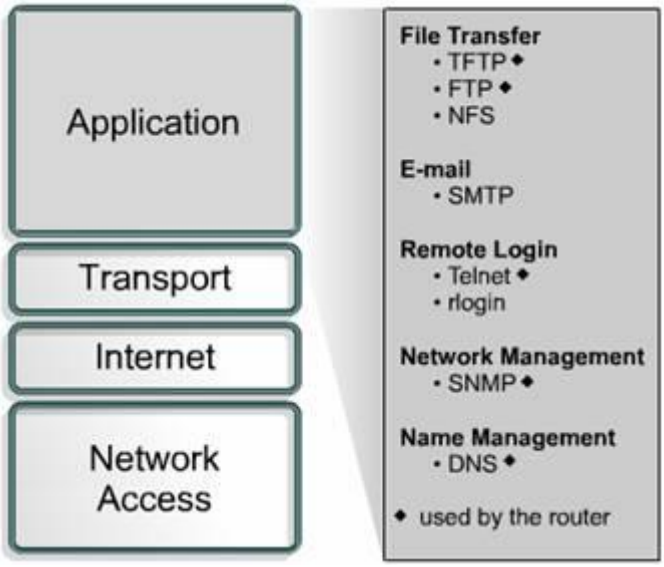
Pojem segment záleží na kontexte vety.

TCP/IP protokol a IP adresovanie

Zariadenuia, ktoré chcú v internete komunikovať musia mať jedinečnú IP adresu, IP preto, lebo rútre používajú trojvrstvový protokol na nájdenie najlepšej cesty. Na komunikáciu sa používal IP protokol verzie 4. Veľkým nárastom internetu hrozilo rýchle vyčerpanie IP adries, preto sa siete začali deliť do podsietí, Network Address Translation (NAT). Iná verzia protokolu IPv6 poskytla väčší adresný priestor s integrovaním metód bez chýb použitým s IPv4. Niektoré zariadenia majú statickú IP a iným sa pridelí IP vždy, keď sa pripájajú na sieť, tieto sú dynamické. MAC adresa – fyzická adresa IP adresa – logická adresa

9.1.1. História a budúcnosť TCP/IP

U.S. Department of Defence (DoD) /úrad pre obranu/ vytvoril TCP/IP model, aby bol schopný fungovať za každých podmienok.
Niektoré vrstvy V TCP/IP majú rovnaké mená ako v OSI, ale majú inú funkciu!
V prvej verzii internetu pri IPv4 boli adresy dlhé 32 bitov, zapísané v 10 sústave a každé 4 sú oddelené bodkou.
V IPv6 je adresa 128 bitová, zapísaná v hexa a každých 8 je odelená dvojbodkou. Počiatočné nuly môžu byť vynechané, napr. 0003 je3.

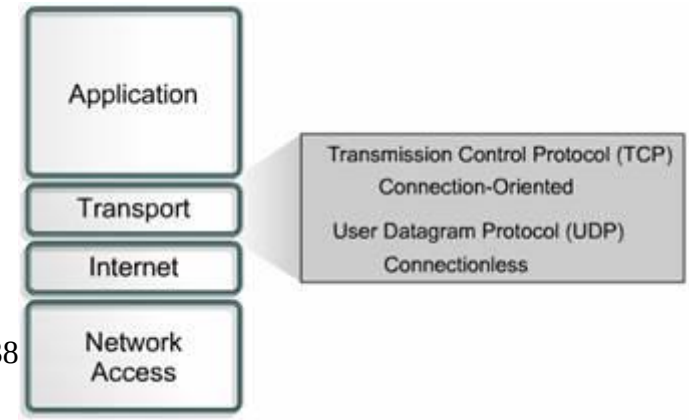


9.1.2. Aplikačná vrstva

Protokol vysokej úrovne, zabezpečuje reprezentovanie, kódovanie a dialogovú kontrolu. TCP/IP obsahuje protokol na podporu prenosu súborov, e-mail, vzdialené prihlasovanie.
File Transfer protokol (FTP): FTP je spoľahlivá, príkazovo orientovaná služba, ktorú používa TCP na prenos súborov medzi systémami, ktoré podporujú FTP.
Trivial File Transport Protokol (TFTP): používa sa na prenos konfiguračných súborov rútrov a CISCO IOS imidžov a tiež na prenos súborov medzi systémami, ktoré ho podporujú. Pracuje rýchlejšie ako FTP.
Network File System (NFS): vyvinutý Sun Microsystem na prístup k súborom v sieti, napríklad na prístup k sieťovým diskom
Simple Mail Transfer Protocol (SMTP): riadi prenos e-mailov cez počítačovú sieť.
Terminal Emutation (Telnet): umožňuje diaľkovo pristupovať na PC,
Simple Network Management Protocol (SNMP): umožňuje monitorovanie a kontrolovanie sieťových zariadení.
Domain Name System (DNS): slúži na preklad symbolickým mien sa IP adresy.

9.1.3. Transportná vrstva

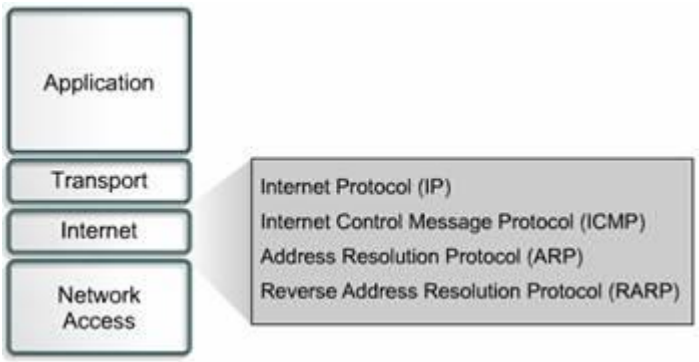
Transportná vrstva poskytuje transportné služby zdrojovým a cieľovým hosťom. Poskytuje logické prepojenie medzi vzdiale-



nými bodmi. Poskladá dáta do rovnakého dátového prúdu pre vyššiu vrstvu. Služby:
TCP a UDP: segmentuje dáta vyššej vrstvy, posiela segmenty s 1 zariadenia na druhé koncové zariadenie.
Len TCP: zabezpečuje spojenie end-to-end, poskytuje kontrolu pre kĺzavé okno, spoľahlivosť poskytovaná pre pre sekvenciu čísel a potvrdenie.

9.1.4. Internetová vrstva

Jeho funkcia je nájdenie najlepšep cesty paketu.
Protokoly operujúce na internetovej vrstve:



1. IP protokol, smerovanie paketov.
2. Internet Control Message Protokol (ICMP), poskytuje kontrolu a kapacitu správ
3. Address Resolution Protocol (ARP), určuje MAS zo známej IP
4. Reverse Address Resolution Protokol, určuje IP, keď MAC je známa

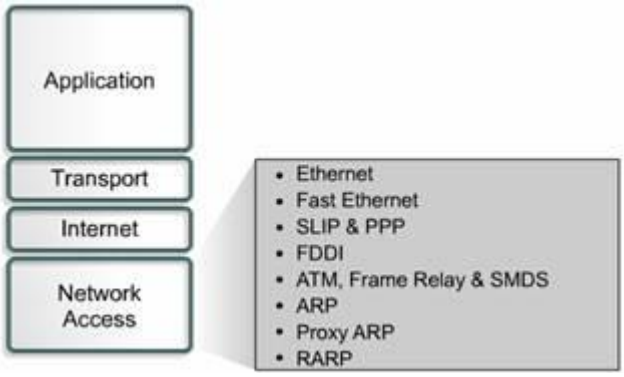
IP uskutočňuje nasledujúce operácie:

1. definuje pakety a adresové schémy
2. prenáša dáta medzi internetovou vrstvou a sieťovou vrstvou
3. smeruje pakety na vzdialený host

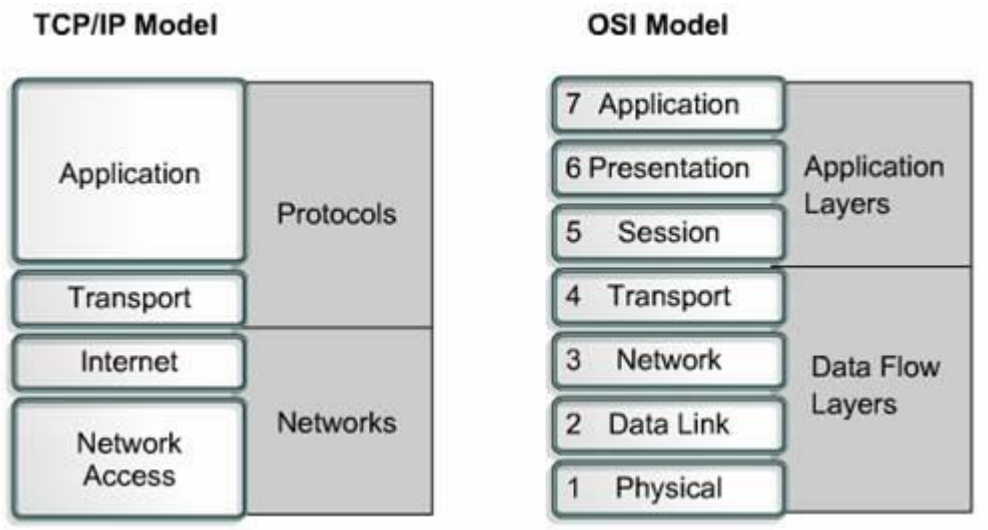
IP protokol je niekedy nazývaný aj ako nespoľahlivý, v tom zmysle, že nekontroluje chyby, na starosť to má vyššie vrstvy.

9.1.5. Sieťová vrstva

Tiež nazývaná ako host to network vrstva.
Zodpovedá všetky otázky, ktoré aktuálny paket potrebuje na vytvorenie fyzického pripojenia na sieťové médium. Ovládače pre modemy a ostatné zariadenie pracujú na sieťovej vrstve.
Funkciou sieťovej vrstvy je mapovanie IP adresy na fyzickom hardwerovej adrese a zapuzdrenie IP paketu do rámca.
Dobrým príkladom sieťovej vrstvy je inštalácia ovládačov pre sieťovú kartu, systém zistí, ak je pripojený nový hadrware a následne doinštaluje ovládače, ak sú jeho súčasťou, prípadne si vyžiada inštalačné médium.



9.1.6. Porovnanie OSI modelu a TCP/IP modelu



Spoločné črty OSI a TCP/IP modelu.

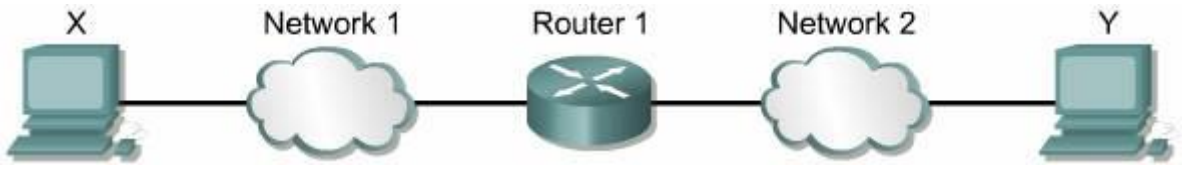
1. oba majú vrstvy
2. oba majú aplikačnú vrstvu, ale vykonávajú rozdielne služby
3. oba majú porovnateľnú sieťovú a transportnú vrstvu
4. prepínané pakety, nekruhové prepínanie, technológia je prevzatá
5. sieťový profesionáli potrebujú vedieť oba modely

Rozdiely medzi OSI a TCP/IP modelom:

1. TCP/IP kombinuje prezentačnú a relačnú vrstvu vaplikačnej vrstve
2. TCP/IP kombinuje OSI dátovú a fyzickú do 1 vrstvu
3. TCP/IP sa javí ako jednoduchší, pretože má menej vrstiev
4. TCP/IP trasnportná vrstva používa UDP, negarantuje doručenie paketu

9.1.7. Architektúra internetu

Sieť sietí je internet „i".



Prepojenie jednej fyzickej siete na inú cez špeciálny počítač zvaný rúter. Tieto siete sú priamo pripojené na rúter. Rúter potrebuje ukazovateľ nejakej cesty na určenie, kadiaľ budú PC komunikovať.

9.2.1. IP adresovanie

Kombinácia znakov (sieťová adresa) alebo číslic (host adresa) vytvára jedinečnú adresu pre každé zariadenie v sieti. Každý počítač v TCP/IP sieti musí mať jedinečný identifikátor alebo IP adresu. Táto adresa pracuje na 3 vrstve, umožňuje jednému počítaču nájsť iný. Všetky počítače majú jedinečnú fyzickú adresu, známu ako MAC, pracuje na 2 vrstve.
IP adresa je 32 bitová sekvencia 1 a 0. Je zapísaná ako 4 decimálne, bodkou oddelené, čísla, hovorí sa mu bodkový desiatkový formát. Každá časť je zvaná oktet.

9.2.2. Desiatkové a dvojkové konverzie

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Na prevod použijem tabuľku. Jednoduchá metóda, sú aj iné.
S binárneho na desiatkovú: 01100101 = 64+32+0+0+4+0+1 = 101
S desiatkovej do dvojkovej: 101 =č oho súčet sa bude = 101? 64,32,16,8,4,2,1=1100101

9.2.3. Adresovanie v IPv4

Rútre posúvajú pakety s originálnej siete do cieľovej cez IP protokol. Paket obsahuje identifikátor zdroja a cieľa. Použitím cieľovej adresy pre použitú sieť, rúter môže doručiť paket do správnej siete. Keď paket príde na rúter, pripojený na cieľovú sieť, rúter použije IP adresu na nájdenie príslušného počítača pripojeného do siete. Podobne ako na pošte.
IP adresa má 2 časti, 1 identifikuje sieť a 2 počítač alebo zariadenie. Každá oktetový rozsah siete je v rozsahu 0-256.
Adresy sú rezdelené na triedy podľa veľkosti. A,B,C,D

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

9.2.4. Triedy A,B,C,D a IP adresy

IP adresy sú rozdelené do tried podľa veľkosti. Každá 32 bitová IP adresa je rozdelená na adresu siete a zvyšok je pre počítače. Bitová sekvencia na začiatku určuje tip siete A,B,C,D,E.

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

Trieda A bola navrhnutá pre extrémne veľké siete, viac než 16 miliónov hostiteľských adries, v tejto sieti sa používa na identifikáciu siete len 1. oktet, zvyšné 3 sú pre hostiteľské adresy. Prvý bit je vždy 0.Pre sieť môžeme použiť rozsah od 1-126, 0 a 127 sú rezervované.
Adresa 127.0.0.0 je vyhradená pre slučkové testovanie. Počítač posiela pakety sám sebe.
Trieda B bola navrhnutá pre veľmi rozľahlé siete. Na identifikovanie sieťovej adresy sa využívajú prvé dva oktety. Prvé dva bity 1. oktetu sú vždy 10. Môže sa použiť rozsah 128-191
Trieda C bola určená pre malé siete, maximálny počet užívateľov je 254. 1. tri bity 1. oktetu vždy začínajú 110, rozsah adries je 192-223
Trieda D bola na povolenie multicasting v IP adresách. Prvé bity začínajú 1110, rozsah je 224-

239
Trieda E je určená pre výskum, v internete sa nepoužíva, začína 1111, rozsah 240-255

9.2.5. Rezervované IP adresy

Niektoré adresy sú rezervované a nemôžu byť použité v sieti.
Adresy obsahujú:

1. adresy siete, na identifikáciu siete, končí 0, napr. 192.168.1.0
2. adresa brodkastu, vyšle sa všetkým PC s sieti, končí 255, napr. 192.168.1.255

9.2.6. Verejné a privátne adresy

V internete je potrebné, aby každý mal jedinečnú IP adresu. Zabezpečuje to Network Information Center (InterNIC).
Verejné adresy: sú jedinečné, dva mašiny, ktoré sú pripojené na verejnú sieť, nemôžu mať rovnakú IP adresu, pretože verejné adresy sú globálne a štandardizované. Sú prideľované Internet service provider (ISP). Rozsah IP adries sa stával nedostatočný, preto bol vyvinuté nové adresové schémy ako classless intermain routing (CIDR) a IPv6.
Privátne IP adresy: privátne siete, ktoré nie sú pripojené do internetu, môžu používať akékoľvek IP adresy, ale vo vnútornej sieti musia byť jedinečné.

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

RFC vyčlenil 3 bloky adries pre privátne použitie, sú vybraté z A,B,C triedy.
Network Address Translation (NAT) – preklad privátnych adries na verejné

9.2.7. Úvod do podsietí

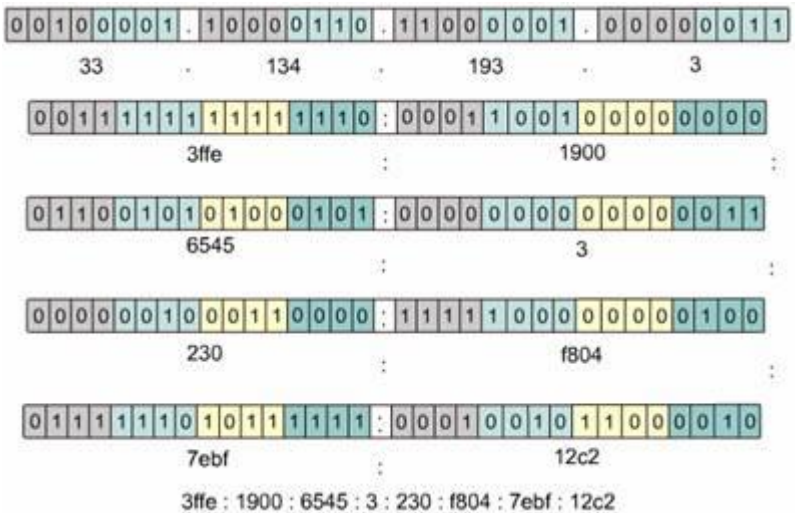
Podsiete sú inou metódou manažovania IP adries. Podsiete je možné rozdeliť pomocou sieťových masiek. Pri návrhu si je dôležité uvedomiť koľko podsietí budeme potrebovať, či sieť nie je limitovaná triedou A, B alebo C. Maska podsiete obsahuje časť siete s pôvodnej siete plus hostiteľské pole. Na vytvorenie sieťovej masky si požičiame niekoľko bitov s hostiteľského poľa a stanový ich ako sieťové pole. Napr. maska je 255.255.255.0 a po aplikácii bude 255.255.255.248. Minimálny počet požičaných bitov je 2.

9.2.8. IPv4 verzus IPv6

Špecifické problémy s IPv4:

1. vyčerpanie ostávajúcich, nepridelených IP adries
2. rapídny nárast veľkosti Internetu, 32 bitové adresovanie bolo nedostatočné.

IPv6 je viac škálovatelná, používa 128 bitov, sú vyjadrené v hexa, predtým boli v desiatkovej podobe, 1 pole je dlhé 16 bitov, predtým bolo 8, polia sú oddelené „:"



9.3.1. Získavania internetových adries

Sieťový hosti potrebovali získať globálnu jedinečnú adresu na prácu v internete. MAC adresu je možné využiť len v lokálnych sieťach, rútre ich neprenášajú. Adresu je možné prideliť staticky a dynamicky.

9.3.2. Statické pridelenie IP adresy

Pracujú na malých sieťach, kde nedochádza ku častým zmenám. Administrátori ručne pridelia IP adresu každému PC, tlačiarni alebo serveru v intranete.

9.3.3. RARP IP pridelenie adresy

Reverse Address Resolution Protocol (RARP) združuje známu MAC adresu s IP adresou. RARP požiadavky sú vyslané na sieť cez brodkast a sú zodpovedané RARP serverom, zvyčajne rútrom.
Príklad: pc potrebuje IP, vyšle RARP požiadavky cez brodkast, všetky počítače spracujú požiadavku, ale nenájdu zdrojovú IP, tak paket zahodia, okrem brodkastového servera, ten pridelí IP adresu počítaču s danou MAC a vyšle paket, všetky PC ho spracujú, ak neobsahuje ich MAC tak zahodia, ak MAC adresa sedí, náš PC získa IP adresu.

9.3.4. BOOT IP pridelenie adresy

Bootstrap protokol (BOOTP) pracuje v klient server prostredí a vyšle jednoduchý paket na získanie IP informácie. Na rozdiel od RARP môže obsahovať IP adresu rútra, servera alebo výrobcom predefinovanú informáciu.
BOOTP získava IP pri štarte cez UDP zapuzdrenom s IP, vysiela sa cez broadcast 255.255.255.255. BOOTP server prijme broadcast a pošle späť broadcast. Klient príjme rámec a skontroluje MAC adresu. Ak klient nájde MAC adresu v cieľovom poli a je zhodná s jeho, uloží si IP adresu a ostatné informácie dodané v správe.

9.3.5 Pridelenie IP adries cez DHCP

Dynamic host configuration protocol (DHCP) je nástupca BOOTP. Umožňuje získať IP adresu dynamicky, bez vytvárania profilu pre zariadenie. Jediné, čo je vyžadované, je zadefinovaný rozsah IP adries na DHCP serveri. Ako sa hosti jednotlivo prihlasujú, DHCP server im prenajíma IP adresy. Celá sieťová konfigurácia môže byť obsiahnutá v jednej správe.
Výhoda oproti BOOTP je mobilita užívateľov.

9.3.6 Problémy s rozlíšením adries

Address resolution protocol (ARP) automaticky získava MAC a IP adresy pri lokálnom prenose. Pri vysielaní paketov sa do hlavičky zadáva cieľová a zdrojová MAC a IP adresa.
TCP/IP má premennú ARP zvanú proxi ARP, ktorá bude poskytovať MAC adresy pre dočasné zariadenia pri vonkajšom prenose na iný sieťový segment.

9.3.7 Address Resolution Protocol (ARP)

V TCP/IP sieťach musia dátové pakety obsahovať cieľovú IP a MAC adresu.
ARP tabuľky obsahujú IP a MAC adresu zariadenia, býva uložená v RAM pamäti odkiaľ sa čítajú informácie pri posielaní.
Keď zdroj určí IP adresu cieľa, nahliadne do jeho ARP tabuľky, či obsahuje MAC adresu, ak je prázdna, vyšle ARP požiadavku a určenie MAC a následne vyšle dáta, ak v ARP tabuľke nájde záznam dôjde k poslaniu dát. Tabuľka sa môže nahrať pri sledovaní sieťového prevozu, druhou možnosťou je, že počítač vyšle ARP požiadavku s IP adresou, keď súhlasí, PC pošle späť odpoveď s IP-MAC párom. Ak nedostane odpoveď, je generovaná chyba.
Ak je IP pre inú sieť, použije sa iný proces. Rúter neposúva broadcastový rámec, pri doručení požiadavky pre inú sieť nahliadne do proxy ARP, odpovie žiadateľovi a pošle mu MAC adresu s proxy ARP. Náš počítač spracuje požiadavku, vyšle dáta, rúter zistí, že MAC je s inej siete a prepošle dáta do druhej siete.
Inou možnosťou, ako poslať dáta do inej siete, je nastavenie default gateway. Host pošle dáta na rúter, ten určí cieľovú IP, ak nieje z rovnakého segmentu, presunie dáta do druhej siete, MAC adresu číta s jeho ARP.

Podstata smerovania a podsiete

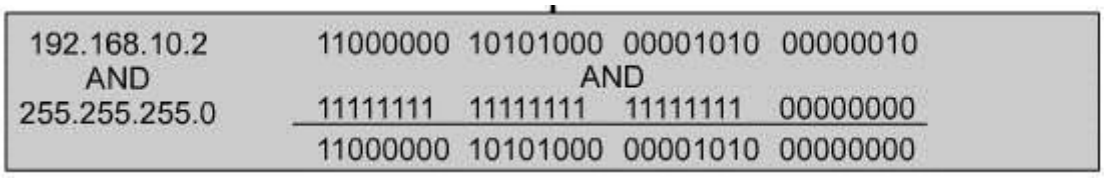
Internet protokol je smerovaný protokol internetu. IP adresovanie povolí paketom smerovanie so zdroja do cieľa použitím najlepšej cesty. Cesta sa určuje so smerovacích tabuliek. Siete možno deliť do podsietí.

10.1.1. Smerovanie a smerovaný protokol

Protokol je pravidlo, ktorý určuje, ako komunikuje PC s ostatnými PC cez sieť.
Protokol popisuje nasledujúce:

1. formát, aký správy musia dodržať
2. cestu, po ktorej si počítače vymieňajú správy

Smerovací protokol umožňuje rútrom odoslať dáta medzi rôznymi sieťami.
IPX protokol potrebuje pre smerovanie len adresu siete, zvyšok si určuje s hostiteľskej MAC
IP protokol vyžaduje kompletnú adresu pozostávajúcu so sieťovej adresy a adresy stanice.
Tieto protokoly vyžadujú tiež sieťovú masku.



Sieťová adresa sa získa použitím sieťovej masky a AND. Vždy končí 0. V tomto prípade 192.168.10.0

10.1.2. IP ako smerovaný protokol

IP protokol je nespojitý, to znamená, že neexistuje priame prepojenie, ale určí sa najlepšia cesta pre dáta, založené na smerovacom protokole. Ďalej je nespoľahlivý a najvýkonnejší, čo znamená, že IP neoveruje, ktoré dáta dorazia do cieľa, túto funkciu zabezpečuje vyššia vrstva protokolu.

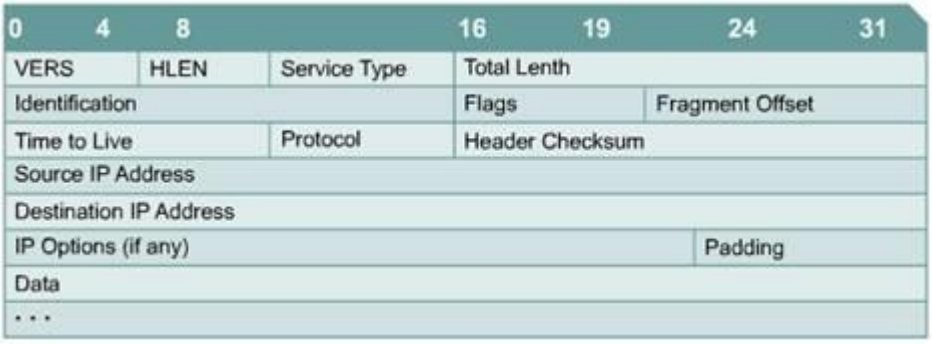
10.1.3. Šírenie paketov a prepínanie medzi rútrami.

Ak paket cestuje cez podsieť do cieľa, na vrstve 2 je odstránená hlavička a ukončenie rámca a je nahradený na každej vrstve 3 zariadenia. Vrstva 2 je pre lokálnu komunikáciu, vrstva 3 je pre end-to-end adresovanie.
Pri prenose rámcu cez rúter je extrahovaná MAC adresa, ten ju kontroluje a určí, či je určená pre neho, ak nie bude odhodený, ak áno, extrahuje jeho CRC (cyclic redundancy check) a vypočíta na overenie, čí rámcové dáta sú bez chýb. Ak nie, rámec je zahodený, ak je bez chýb, rámcová hlavička a ukončenie sú odstránené s paketu a prechádza na vrstvu 3. Paket je kontrolovaný, či je pre rúter alebo iné zariadenie v sieti. Ak cieľová IP adresa súhlasí s portom rútra, hlavička 3. vrstvy je odstránená a dáta prechádzajú do 4 vrstvy. Ak paket bude smerovaný, cieľová IP adresa bude porovnaná zo smerovacou tabuľkou. Ak súhlasí, alebo je tu implicitná cesta, paket bude poslaný na špecifické rozhranie podľa smerovacej tabuľky. Keď paket je prepnutý na odchádzajúce zariadenie, bude vypočítané nové CRC, a pridá sa správna rámcová hlavička paketu. Rámec je poslaný do nasledujúcej brodkastovej domény ku cieľu.

10.1.4. Internet protokol (IP)

Delí sa na spojovo a nespojovo orientovaný. Tieto dve služby poskytujú end to end prenos dát v internete.
Nespojito orientované systémy: dva pakety sa dostanú ku cieľu inou cestou, ale v cieli budú opäť poskladané, počas posielania paketu nie je cieľ pripojený. Dobrým príkladom je poštový systém, adresát tiež nevie, kadiaľ jeho list cestoval. Často sa odkazujú na packet switched proces. Pri prechode paketov zo zdroja do cieľa môže odbočiť na inú cestu, dokonca môže dôjsť poškodený. Cesta sa určuje podľa rôznych kritérií.
Spojivo orientované systémy: počas celého prenosu je vytvorené spojenie medzi odosielateľom a prijímateľom. Príkladom je telefónny hovor. Odkazujú sa na circuit switched processes. Pri prenose je nadviazané spojenie a až potom sú posielané dáta, pakety cestujú postupne cez sieť rovnakou cestou.
Internet je jednou veľkou nespojito orientovanou sieťou v ktorej všetky pakety sú riadené cez IP.
TCP pridaný na vrstvu 4 tvorí spojito orientovanú službu k IP.

10.1.5 Anatómia IP paketu



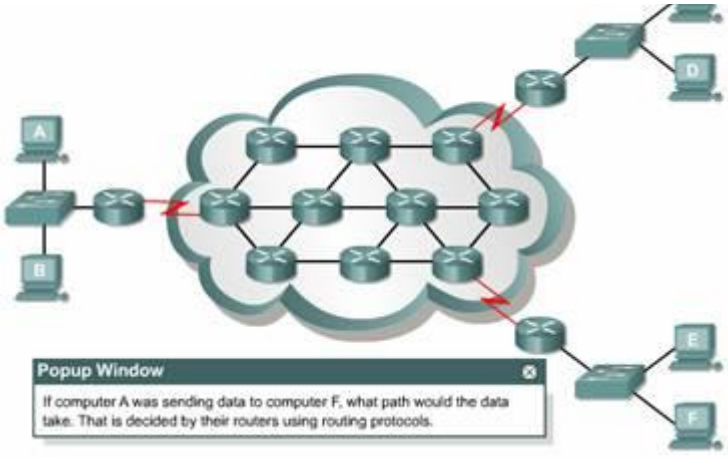
0 4	8		16 19	24 31
VERS	HLEN	Service Type	Total Lenth	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
IP Options (if any)				Padding
Data				
. . .				

Všetky IP pakety pozostávajú s dát z horných vrstiev plus IP hlavička.
IP hlavička pozostáva:

1. verzia, určuje verziu použitého protokolu
2. dĺžka IP hlavičky (HLEN), identifikuje datagramovú dĺžku v 32bitovom slove
3. typ služby (TOS), špecifikuje úroveň dôležitosti, 8 bitov
4. úplná dĺžka, určuje úplný dĺžku paketu v bitoch, vrátene dát a hlavičky
5. identifikácia, obsahuje číslo, ktoré identifikuje aktuálny datahram, 16 bitov
6. flags, 3-bitové pole, dolné 2 kontrolujú fragmentácia. Jeden bit určuje, či paket môže byť fragmentovaný, a ostatné špecifikujú, či paket je posledným fragmentom v sérii fragmentovaných kaketov.
7. fragmentový ofset, použité na pomoc pospájania kúskov datagramových fragmentov
8. time to live (TTL), určuje počet preskokov pri cestovaní paketu, pri prechode rútrom sa zmenšuje, keď dosiahne 0, paket bude zohodené
9. protokol, identifikuje tip protokola, TCP alebo UDP
10. kontrolný súčet hlavičky, pomáha zabezpečiť integritu hlavičky
11. zdrojová adresa, určuje odosielateľovu IP adresu
12. cieľová adresa, určuje cieľovú adresu
13. options, umožňuje IP protokolu premenné nastavenia, ako bezpečnosť alebo premenlivá dĺžka
14. padding (výplň), pridané 0, aby bĺžka paketu bola 32 bitov
15. dáta, obsahuje informácie vyššej vrstvy, premenná dĺžka do 64Kb

Informácie z hlavičky poskytujú hornej vrstve protokolu definovanie dát v pakete.

10.2.1. Prehľad smerovania



Smerovanie má na starosti 3. vrstva OSI modelu. Smerovanie je hierarchická organizačná schéma, ktorá dovolí individuálnym adresám byť zoskupením do hromady. Tieto individuálne adresy sú spracované ako samostatná jednotka, až kým cieľová adresa potrebuje pre konečné doručenie dát. Smerovanie má za úlohu nájsť najefektívnejšiu cestu z jedného zariadenia na druhé. Smerovanie vytvá-

rajú rútre.

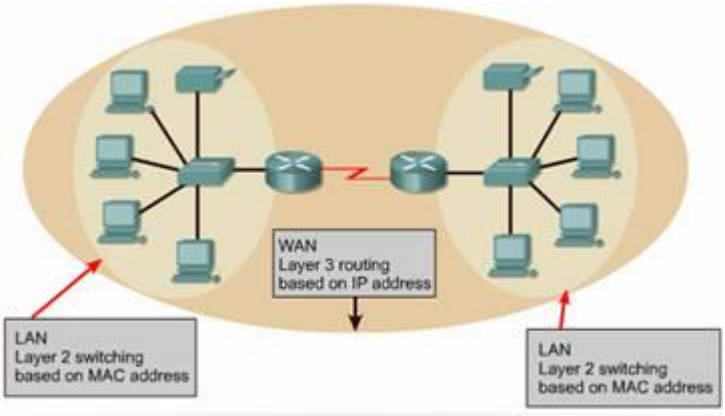
Primárne funkcie rútrov:

1. rútre musia udržiavať smerovaciu tabuľku a preveriť ostatné rútre na zmeny v sieti, rútre si vymieňajú informácie pomocou smerovacieho protokolu
2. pri príchode paketu musí rúter určiť zo smerovacej tabuľky, kam ho poslať. Pri prepínaní pridáva potrebné informácie pre rozhranie a potom prenáša rámec.

Smerovacie protokoly využívajú premenné kombinácie metriky na určenie najlepšej cesty dát.
Smerovanie zabezpečuje IP protokol, sú aj iné ako IPX/SPX, AppleTalk.
NetBEUI je nesmerovatelný protokol

10.2.2. Smerovanie proti prepínaniu

Smerovanie je často protikladom prepínania. Smerovanie ja na 3. vrstve OSI a prepínanie je na 2. vrstve OSI, čo vytvára rozličné informačné procesy pri presune dát zo zdroja do cieľa.



Layer 2 switching takes place within the LAN. Layer 3 routing moves traffic between broadcast domains. This requires the hierarchical addressing format that a Layer 3 addressing scheme like IP provides.

Každý počítač a rúter obsahuje ARP tabuľku pre vrstvu 2, obsahuje informácie o brodkastovej doméne. Rútre udržiavajú smerovaciu tabuľku, ktorá umožní prenos dáv von zo siete.
Na vrstve 2 vie svič rozpoznať len MAC adresu, nevie zachytiť IP vrstvy 3. Keď hosť má dáta nie pre lokálnu IP, pošle dáta na default gateway. Hosť využije MAC adresu rútra ako cieľovú MAC adresu.
Svič uchováva tabuľku známych MAC adries, rúter udržuje tabuľku IP adries, známu ako smerovacia tabuľka.
Rútre neprepúšťajú broadcast, preto poskytujú vyšší stupeň zabezpečenia.

10.2.3. Smerový verzus smerovanie

Protokoly používané v sieťovej vrstve na prenos dát s jedného hosta na iný cez rúter sú smerované protokoly. Smerovacie protokoly umožňujú rútrom výber najlepšej cesty dát zo zdroja do cieľa.
Smerované protokoly obsahujú:

1. dosť informácií v sieťovej vrstve na prenos dát na nasledujúce zariadenie a napokon do cieľa
2. definície formátu a využitie polí vnútri paketu

Príkladom smerovacieho protokolu sú Internet Protocol (IP) a Novell's Internetwork Packet Exchange (IPX)
Smerované protokoly umožňujú rútrom smerovať smerovacie protokoly.
Funkcie smerovacích protokolov:

1. poskytnúť proces pre zdieľane smerovacích informácií
2. umožniť rútrom komunikovať s ostatnými rútrami na udržiavanie a aktualizáciu smerovacích tabuliek

10.2.4. Určenie cesty

Výber cesty nastáva na sieťovej vrstve. Rúter nahliadne do rútovacej tabuľky a vyberie najlepšiu cestu.

1. statické, konfigurované administrátorom
2. dinamické, učia sa od iných rútrov použitím smerovacích protokolov

Rúter si prečíta informácie s hlavičky paketu a pošle ho do cieľa, hovorí sa o smerovacom pakete. Každý rúter, ktorý paket stretne, je nazývaný hop. Počet hop určuje vzdialenosť.
Proces určovania smerovanej cesty:

1. cieľová adresa je získaná z paketu
2. porovnanie adries v smerovacej tabuľke
3. ak súhlasí, paket je poslaný na port daného výstupu
4. ak nesúhlasí, porovnáva sa záznam z nasledujúceho portu
5. ak nie je nájdený žiadny záznam, rúter kontroluje, či je nastavený default cesta
6. ak je nastavený predvolený port, poket je naň poslaný, default route nastavuje admin
7. ak nie je default route, paket je zahodený, obyčajne sa pošle správa zdrojovému zariadeniu, že cieľ je nedosiahnutelný.

10.2.5. Smerovacia tabuľka

Rútre využívajú smerovacie protokoly na postavenie a udržiavanie smerovacej tabuľky, ktorá obsahuje smerovacie informácie. Broadkástové doména sa prepájajú ma 3 vrstve.
Rútovacia tabuľka obsahuje:

1. typ protokolu, vytvára smerovaciu tabuľku
2. cieľová/next-hop asociácia, pri prechode paketu cez rúter sa porovná cieľová adresa zo smerovacou tabuľkou, ak má v tabuľke cieľ, prepojí paket, ak nie presunie ho na nasledujúci next-hop
3. rútrovacia metrika, rozličné rútrovacie protokoly používajú rôznu metriku
4. odchádzajúce rozhranie, sem sa posielajú dáta, aby dosiahli cieľ

Rútre medzi sebou komunikujú pomocou rútrovacích aktualizačných správ.
Prenos zmien:

1. periodicky
2. len pri zmenách v sieti

Prenos tabuľky:

1. prenos celej tabuľky
2. prenos len zmien

10.2.6. Smerovacie algoritmy a metrika

Ciele smerovacích protokolov:

1. optimalizácia, určí najlepšiu cestu pomocou výpočtov
2. jednoduchosť a nízky overhead, jednoduchý algoritmus nenáročný na CPU a pamäť v rútri, dôležité vo veľkých sieťach ako internet
3. robustné a stabilné, algoritmu, ktorý si vie poradiť s neočakávaným stavom, ako zlyhanie hardweru
4. flexibilita, algoritmus sa musí rýchlo prispôsobiť sieťovým zmenám
5. rýchla konvergencia, konvergencia je proces dohôd medzi rútrami, pri zmene na sieti sú vyžadované zmeny na zabezpečenie spojenia

Rútrovacie algoritmy používajú rôzne výpočty na určenie najlepšej cesty. Všetky smerovacie algoritmy generujú metrickú hodnotu, pre každú časť siete. Sofistikované algoritmy ich kombinujú do kompozitnej metrickej hodnoty, menšie číslo indikuje lepšiu cestu.
Metrika použitá v smerovacích protokoloch:

1. šírka pásma, dátová kapacita linky, 10Mbps je preferovaná pred 64kbps
2. oneskorenie, čas potrebný na prechod paketu cez sieť, závislé na šírke pásma
3. load /záťaž/, hodnota aktivity na sieti
4. spoľahlivosť, odkazuje sa na chyby každej sieťovej linky
5. počet hop, počet rútrov na ceste k cieľu
6. ticks, oneskorenie na dátovej linke, používané IBM
7. cost, ľubovolná hodnota, pridelená administrátorom

IGP a EGP

Smerovacie protokoly:

1. Interior Gateway Protocols (IGPs)
2. Exterior Gateway Protocols (EGPs)

IGPs smeruje dáta vnútri autonómnych systémov.
EGPs smeruje dáta medzi autonómnymi systémami.

Linkové stavy a vzdialenosti vektorov

Smerovaný protokol môže byť IGP aj EGP, určuje, či skupina je pod jednoduchou správou. Rúter využíva distance-vector algoritmus na overenie stavu priľahlých rútrov, vykonáva sa pravidelne, aj keď nenastanú zmeny na sieti.
Príklady distance-vector protokolu:

1. Routing Information Protocol (RIP), najbežnejší v IGP v internete, používa ako metriku počet preskokov
2. Interior Gateway Routing Protocol (IGRP), tento IGP bol vyvinutý Ciscom na smerovanie vo veľkých heterogénnych sieťach
3. Enhanced IGRP (EIGRP), tento IGP obsahuje veľa čŕt link-state smerovacieho protokolu.

Link-state smerovací protokol bol vyvinutý na prekonanie limitácií distance-vector smerovacieho protokolu. Odpovedá rýchlo na zmeny v sieti, je vysielaný len pri zmene stavu siete. Posiela link-state refreš po 30 minútach.
Pri zmene stavu na linke vyšle zariadenie, ktoré zdetekovalo zmenu, link-state advertisement (LSA) /oznámenie/ všetkým susedným zariadeniam. Každé susedné zariadenie zoberie kópiu LSA, aktualizuje jeho link-state databázu a pošle LSA na všetky susedné zariadenia.
Link-state algoritmus použije svoju databázu na určenie najkratšej cesty.
Príklad Link-state algoritmu:

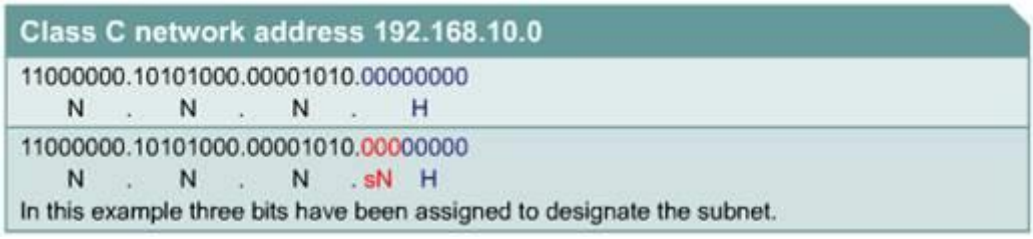
1. Open Shortest Path First (OSPF)
2. Intermediate System to Intermediate System (IS-IS)

Smerovacie protokoly

RIP je distance-vector smerovací protokol, ktorý na určenie nejlepšej cesty používa počet preskokov, čo však neznamená, že určí najrýchlejšiu cestu. **RIPv1** je limitovaný maximálne do 15 preskokov a rovnakou maskou siete.
RIPv2 umožňuje smerovanie aj pre rozdielnu sieťovú masku v smerovacej tabuľke.
IGRP je distance-vector smerovací protokol vyvinutý Ciscom. Je vyvinutý vyslovene na adresovanie problémov spojených so smerovaním vo veľkých sieťach, ktoré boli nad rozsah RIP. Určí rýchlejšiu cestu ako RIP.
Určenie rýchlejšej cesty v IGRP: oneskorenie, šírka pásma, zaťaženie a spoľahlivosť.
OSPF – link-state smerovací protokol určený na smerovanie vo veľkých sietí, kde sa nedal použiť RIP.
Intermediate System to Intermediate System (IS-IS) je link-state protokol určený na smerovanie iných protokolov ako IP.
IGRP a EIGRP sú Cisco protokoly, poskytuje lepšiu operačnú efektívnosť ako rýchla konvergencia a nízka stropná šírka pásma. Je hybridný smerovací protokol.
Border Gateway Protocol (BGP) je príkladom EGP, prenáša informácie medzi autonómnymi systémami. Robí rozhodnutia založené na sieťovej politike

10.3.2. Úvod a dôvod pre podsiete

Na vytvorenie podsietí si požičiavame bity s ľavej časti oktetu danej podsiete. Podsieťové adresy obsahujú sieťovú časť A,B,C, plus podsieťové pole a hostiteľské pole. Podsieťové pole a hostiteľské pole sú vytvorené z originálneho hostiteľského poľa hlavnej IP adresy.



Delenie siete do podsietí umožňuje administrátorom poskytovať broadcastovú kontrolu a nízkoúrovňovú bezpečnosť cez access lists.

10.3.3. Vytvorenie masky podsiete

Pri výpočte bude potrebné určiť maximálny počet staníc a na základe toho si požičiame potrebný počet bitov. Posledné 2 bity v poslednom oktete nemôžu byť rezervované pre podsiete. Masku určíme tak, že do pozície požičaných bitov zadáme 1 a zvyšok sú 0.
Na určenie počtu rezervovaných bitov potrebujeme poznať počet hostov a počet podsietí. Pri výpočte treba zvážiť, že samé 1 a 0 nie sú povolené (adresa siete a broadcast), teda pri výpočte treba -2. Teda ak potrebujem 30 hostov, tak 25 je 32 a – 2 je 30.

10.3.4. Aplikovanie sieťovej masky

Subnetwork #	Subnetwork ID	Host Range	Broadcast ID
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Pri rezervovaní 3 bitov je možné sieť rozdeliť do 8 podsietí. 1110 0000. 0 a 7 sa nedá použiť, lebo obsahuje samé 0 a 1 v oblasti pre podsieť. Ďalej každá podsieť obsahuje adresu siete a broadcast, tie sa tiež nepoužívajú pre hostov.

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		

10.3.5. Podsiete triedy A a B

Pre podsieť A je rezervovaných 22 bitov a pre B je 14 bitov.

Network Address	132.217.0.0
Number of Usable Subnets	205
Number of Hosts Per Subnet	10
Subnet Mask	255.255.255.0

Check Answer

Correct

Try Again

- ○ ClassA
- ◉ ClassB
- ○ ClassC
- ○ All Classes

Pri výpočte je podstatných počet podsietí, ak je 205 podsietí pri triede B, použijeme všetkých 8 bitov 2 oktetu a výjde nám maska 255.255.255.0 .

10.3.6. Výpočet príslušnej siete použitím AND

0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

Rútre používajú podsieťové masky na určenie domácej podsiete cez ANDing. ANDing je binárny proces, v ktorom rútre vypočítajú podsieťové ID pre prichádzajúci paket.
Kombináciu IP adresy a sieťovej masky cez AND dostaneme adresu siete, rúter potom použije informácie na presun paketu do siete.

Packet address	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Mask	255.255.255.224	11111111.11111111.11111111.11100000
Subnetwork ID	201.10.11.64	11001001.00001010.00001011.01000000