**STREDNÁ ODBORNÁ ŠKOLA INFORMAČNÝCH TECHNOLÓGIÍ HLINÍCKA 1, 831 52 BRATISLAVA**

**ROČNÍKOVÁ PRÁCA**

**Šk. rok: 2024/2025                                               LADISLAV MARŠOVSKÝ**

**STREDNÁ ODBORNÁ ŠKOLA INFORMAČNÝCH TECHNOLÓGIÍ HLINÍCKA 1, 831 52 BRATISLAVA**

**OPRAVA A ÚDRŽBA POČÍTAČOVEJ SIETE**

2682 K - mechanik počítačových sietí

**Bratislava, 2025                                                      LADISLAV MARŠOVSKÝ**

**ČESTNÉ VYHLÁSENIE**

Čestne vyhlasujem, že ročníkovú prácu som vypracoval samostatne, neporušil som autorský zákon a použitú literatúru som uviedol na príslušnom mieste.

Bratislava 30.3.2025                                                                             ..................................

                                                                                                                            Podpis

**OBSAH**

[1. ÚVOD 4](#_Toc194227300)

[2. Počítačová sieť 4](#_Toc194227301)

[2.1 História počítačovej siete 5](#_Toc194227302)

[3. Rozdelenie počítačovej siete 6](#_Toc194227303)

[3.1 Rozdelenie podľa rozlohy 6](#_Toc194227304)

[3.2 Rozdelenie podľa architektúry 7](#_Toc194227305)

[3.3 Podľa fyzickej typológie (usporiadanie zariadení v sieti) 8](#_Toc194227306)

[3.4 Podľa logickej topológie (spôsobu, akým sa posielajú údaje v rámci siete) 10](#_Toc194227307)

[4. Základné časti počítačovej siete 12](#_Toc194227308)

[4.1 Sieťový hardvér 12](#_Toc194227309)

[4.2 Sieťové Káble 16](#_Toc194227310)

[4.3 Sieťové zabezpečenie 18](#_Toc194227311)

[5. Praktická časť - Oprava a údržba počítačovej siete 21](#_Toc194227312)

[5.0.1 Napájanie zariadenia 22](#_Toc194227313)

[5.1 Softvérová diagnostika 23](#_Toc194227314)

[5.1.1 Kvalita pingu 23](#_Toc194227315)

[5.1.2 Príkazy do príkazového bloku CMD 25](#_Toc194227316)

[5.1.3 Wireshark 27](#_Toc194227317)

[5.2 Údržba sieťových zariadení 29](#_Toc194227318)

[5.2.1 Kontrola internetových káblov 29](#_Toc194227319)

[5.3 Optimalizácia siete 30](#_Toc194227320)

[5.4 Bezpečnosť siete: 31](#_Toc194227321)

[6. Záver 32](#_Toc194227322)

# 1. ÚVOD

Túto tému som si vybral, pretože počítačové siete sú dnes neoddeliteľnou súčasťou nášho každodenného života. Bez nich by sme si len ťažko vedeli predstaviť fungovanie internetu, komunikáciu medzi zariadeniami či prenos dát v rôznych oblastiach – od malých domácností až po veľké firmy. Počítačové siete umožňujú rýchlu a efektívnu výmenu informácií, vďaka čomu môžeme pracovať, študovať a komunikovať bez ohľadu na vzdialenosť. Okrem toho, že sieťová infraštruktúra zjednodušuje bežné úlohy, je zároveň kľúčová pre bezpečnosť a ochranu dát. V súčasnosti sa čoraz viac rieši otázka kybernetickej bezpečnosti a správnej správy sietí, čo robí túto tému ešte dôležitejšou. Chcem sa preto venovať nielen základnej charakteristike počítačových sietí, ale aj ich praktickému využitiu, správe a obsluhe. Pri praktickej časti si ukážeme správne zaobchádzanie pri údržbe počítačovej siete a jej oprave na danom príklade

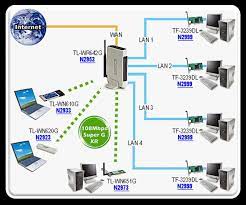
# 2. Počítačová sieť

**Počítačová sieť** je systém vzájomne prepojených najmenej dvoch počítačov, za účelom ich komunikácie. Prepájajú sa prostredníctvom káblov alebo bezdrôtového spojenia. Pre správne fungovanie počítačovej siete nestačí počítače iba fyzicky prepojiť, musí existovať aj sieťový softvér, prostredníctvom ktorého prebieha komunikácia, pri používaní (dodržiavaní) sieťového protokolu.

## 2.1 História počítačovej siete

Snaha používateľov spoločne využívať svoje počítače má korene v historických udalostiach, ktoré ovplyvnili technologický vývoj. Jednou z nich bolo vypustenie Sputnika, prvej umelej družice Zeme, v roku 1956 Sovietskym zväzom. Tento míľnik spôsobil zdesenie v armáde Spojených štátov amerických, pretože naznačoval, že Sovieti sú vo vedecko-technickom výskume a vývoji napred.

V 50. rokoch boli prvé počítače dostupné len odborníkom a ich programovanie bolo mimoriadne zložité, keďže prebiehalo v strojovom kóde. Postupne sa však začali objavovať prvé programovacie jazyky, ako Fortran a Algol, ktoré zjednodušili tvorbu programov. V 60. rokoch sa rozšírilo používanie diernych štítkov, ktoré umožňovali zadávanie údajov do počítača, no vyžadovali si vysokú presnosť a ich spracovanie trvalo dlho. Neskôr sa začali využívať terminály, ktoré umožňovali zadávať údaje do počítača a okamžite zobrazovať výsledky, čím sa práca s počítačmi výrazne zjednodušila.



Obrázok 1 Počítačová sieť

# 3. Rozdelenie počítačovej siete

Siete rozdeľujeme podľa rozlohy, architektúry, logickej a fyzickej typológie

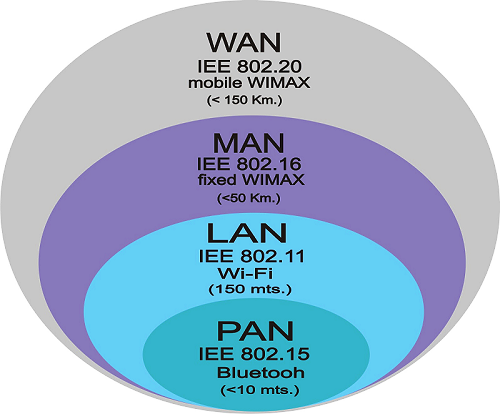
## 3.1 Rozdelenie podľa rozlohy

**PAN** (Personal Area Network - osobná počítačová sieť) - spolupracujúce zariadenia slúžia len jednej osobe (typické prepojenie myši, tlačiarne alebo mobilu a počítača, notebooku, PDA,...) spája zariadenia rádovo v dosahu metrov. Na prepojenie sa obvykle používajú bezdrôtové technológie Bluetooth, IrDA, Wi-Fi.

**LAN** (Local Area Network) - lokálna počítačová sieť, ktorej počítače sú navzájom vzdialené rádovo desiatky až stovky metrov, teda sú umiestnené v jednej prípadne v niekoľkých susedných budovách. Ide o siete firemné, školské, podnikové a pod. Slúžia hlavne pre zdieľanie dát a zariadení v rámci jednej firmy, budovy, lokality... LAN sú obvykle v súkromnej správe, sú tvorené jedným káblovým systémom (alebo iným prenosovým prostriedkom - rádiové vlny a pod.). Prenosové rýchlosti dosahujú rádovo 10 Mbps až 10 Gbps.

**MAN** (Metropolitan Area Network) - mestská počítačová sieť s rozlohou rádovo desiatky km štvorcových . Metropolitné siete umožňujú rozšírenie pôsobnosti LAN ich predĺžením, zvýšením počtu uzlov, zvýšením prenosovej rýchlosti. Rýchlosť v MAN býva vysoká, ale charakterom sa radí k sieťam LAN.

**WAN** (Wide Area Network) - globálna, veľkoplošná počítačová sieť v rámci celých kontinentov až sveta. Spája rôzne LAN a MAN siete v pôsobnosti krajín, kontinentov ale i sveta. Prenosové rýchlosti môžu dosahovať rádovo až Gbps.



Obrázok 2 Rozdelenie siete podľa rozlohy

## 3.2 Rozdelenie podľa architektúry

**peer-to-peer** (rovný s rovným, označuje sa tiež ako p2p sieť): Všetky počítače v sieti sú rovnocenné. Každá stanica v sieti môže vyčleniť nejaký svoj prostriedok (diskový priestor, tlačiareň, mechaniku...) na zdieľanie. Iná stanica môže tieto prostriedky využívať. Tento typ siete obvykle nemá centrálnu správu, každý uzol sa spravuje sám. Zdieľanie prostriedkov je možné aj cez internet.

**klient/server**: V praxi sa častejšie vyskytuje zapojenie, pri ktorom je jeden z počítačov nadradený, riadiaci. Takýto počítač nazývame **server.** Ostatné počítače sa správajú ako **klienti** (workstation, pracovná stanica), ktorí požadujú určité služby od servera. Serverov môže byť viacero typov - podľa typu poskytovaných služieb - súborový server, tlačový server, poštový server, www server, ftp server,... Nemusí platiť vzťah, že jeden server je jeden počítač, resp. na jednom fyzickom počítači môže existovať viacej serverov. Server máva špeciálny sieťový operačný systém (UNIX, Linux, Novell NetWare, Microsoft Windows NT, Microsoft Server 2008,...), často na ňom „bežia“ mnoho užívateľské programy . Typickým príkladom servera je počítač, na ktorom sú umiestnené elektronické poštové schránky, do ktorých môže 24 hodín denne prichádzať elektronická pošta (e-mail). Klient si svoju poštu pozrie, keď napr. príde domov a pripojí sa svojim počítačom na server (požiada o službu – prezretie došlej pošty).



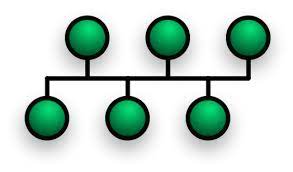
Obrázok 3 peer-to-peer



Obrázok 4 Komunikácia klienta/router

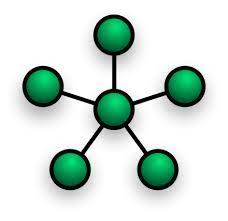
## 3.3 Podľa fyzickej typológie (usporiadanie zariadení v sieti)

**Zbernicová** topológia je základnou štruktúrou siete, kde stanice sú pripojené k zbernici prostredníctvom odbočovacích prvkov. Prenosovým médium môže byť koaxiálny kábel alebo krútená dvojlinka. Táto topológia neobsahuje centrálnu stanica a umožňuje prístup všetkým staniciam. Je jednoduchá na inštaláciu, avšak pri prerušení kábla sa sieť stáva nefunkčnou. Jej využitie v súčasnosti klesá.



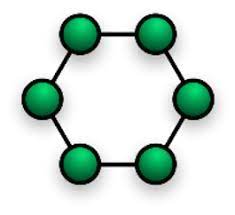
Obrázok 5 Typológia zbernicovej schémy

V sieti **hviezdicovej** topológie pôsobí v centre siete centrálny uzol, ktorým môže byť prepínač (switch), v starších sieťach rozbočovač (hub) alebo, najmä pri bezdrôtových sieťach, opakovač (repeater). K centrálnemu uzlu sú pripojené stanice siete samostatnými linkami, najčastejšie pomocou symetrického kábla (krútená dvojlinka). Pri poruche centrálneho uzla je celá sieť vyradená z prevádzky.



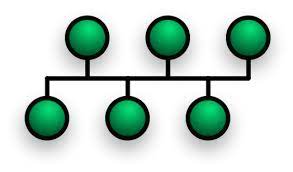
Obrázok 6 Typológia hviezdicovej schémy

**Kruhové** stanice siete sú prepojené vedením do tvaru súvislého kruhu. Dáta sa pohybujú v kruhu od odosielateľa (prechádzajú postupne k najbližšiemu susedovi) postupne cez všetky následné uzly až k príjemcovi (adresovanej stanici ) – smer pohybu je daný spôsobom prepojenia siete. Na riadenie smeru prenosu dát sa používa riadiaca značka - Token. Pomocou nej sa dátové správy odovzdávajú postupne jedným smerom medzi stanicami. Stanica siete, ktorá má riadiacu značku, môže vysielať, ostatné stanice môžu iba prijímať. Týmto je odstránená možnosť vzniku kolízii pri súčasnom vysielaní niekoľkými stanicami. Výpadok ľubovoľnej stanice spôsobí nefunkčnosť celej siete.



Obrázok 7 Typológia kruhovej schémy

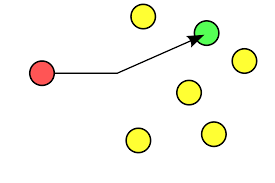
**Stromová** topológia kombinuje vlastnosti hviezdicovej a zbernicovej topológie. Využíva sa najmä v širokopásmových sieťach a optických vláknach. Je spoľahlivá, ale náročná na káble a má obmedzenú rozšíriteľnosť. V prípade výpadku spojenia však dáta môžu putovať k cieľu alternatívnymi linkami.



Obrázok 8 Typológia stromovej schémy

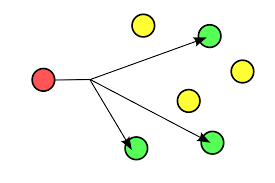
## 3.4 Podľa logickej topológie (spôsobu, akým sa posielajú údaje v rámci siete)

**Unicast** je sieťový komunikačný model, kde jeden zdrojový bod komunikuje priamo s jedným určeným cieľom alebo príjemcom v sieti. V tomto modeli je správa alebo paket dát odoslaný z jedného zdroja a určený presne jednému príjemcovi. To znamená, že správa je adresovaná konkrétnemu sieťovému uzlu alebo koncovému bodu v sieti a nie je distribuovaná všetkým uzlom v sieti. Unicastový model je často využívaný pre individuálne komunikácie medzi jedným zdrojom a jedným cieľom v sieti, čo umožňuje presnú a cielenú komunikáciu.



Obrázok 9 Topológia typ Unicast

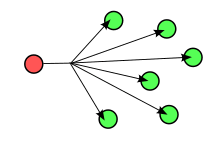
**Multicast** je zariadenie, ktoré obsahuje údaje, ktoré sa odošlú celej skupine len raz z počítača a tie sa podľa potreby v uzle kopírujú; existujú multicastové skupiny, do ktorých sa možno pripojiť a prijímať posielané údaje; výhoda je v tom, že sa údaje pošlú len raz a pre jednotlivé počítače sa vetvia v uzle, až vznikne potreba; nevýhoda je, že server nevie, kto prijíma a či boli údaje doručené.



Obrázok 10 Topológia typ Multicast

**Broadcast**

Údaje sa posielajú na všetky počítače v dosahu (obvykle sa jedná o lokálnu sieť); neexistuje tu žiadne poradie, ktoré musia jednotlivé stanice dodržiavať, aby mohli pristupovať k sieti („kto prv príde, ten skôr vysiela“). Používajú ho napr. niektoré chatovacie programy, alebo hry pri hľadaní servera (na LAN). token pasing (odovzdávanie tokenu – „štafetového kolíka, pešiaka“) posielať údaje môže iba tá stanica, ktorá vlastní Token. Ak už stanica nechce posielať žiadne údaje, odovzdáva Token ďalšej stanici.



Obrázok 11 Topológia typ Broadcast

# 4. Základné časti počítačovej siete

Sieťovú infraštruktúru môžeme rozdeliť do viacerých kategórií. Prvou z nich je sieťový hardvér, ktorý zahŕňa všetky technické prostriedky potrebné na fungovanie siete, ako sú smerovače, prepínače, sieťové karty či prístupové body. Ďalšiu dôležitú súčasť tvoria sieťové káble, ktoré zabezpečujú fyzické prepojenie zariadení a umožňujú prenos dát. Okrem toho je nevyhnutné venovať pozornosť aj zabezpečeniu siete, ktoré chráni prenášané dáta pred neoprávneným prístupom a kybernetickými hrozbami, pričom zahŕňa rôzne metódy, ako sú firewally, šifrovanie či autentifikácia používateľov.

## Sieťový hardvér

**Sieťová karta** alebo LAN karta alebo sieťový adaptér alebo NIC (Network Interface Card) je rozširujúci modul počítača, ktorý zabezpečuje jeho komunikáciu s ďalšími zariadeniami siete.



Obrázok 12 Sieťová karta

**HUB** je jednoduché zariadenie, ktoré spojuje skupinu používateľov. Prepravuje rôzne dátové typy medzi pracovnými stanicami pripojenými k jednému portu. Všetci používatelia na jednom HUBe tvoria jeden segment s rovnakou kapacitou.



Obrázok 13 Internetový HUB

**SWITCH** je vylepšené zariadenie s vnútornou pamäťou, ktorá uchováva adresy všetkých pripojených zariadení v sieti (tzv. MAC adresy). Keď switch prijme dáta, vie presne, na ktorý port je pripojené cieľové zariadenie, a posiela dáta len tam. Tento spôsob rýchlo a efektívne zrýchľuje komunikáciu v sieti a umožňuje využitie celého komunikačného pásma pre každé pripojené zariadenie.



Obrázok 14 Switch

**Smerovač alebo router** je zariadenie, ktoré spojuje rôzne lokálne siete alebo pripája lokálnu sieť k širšej sieti, známej ako WAN (Wide Area Network – rozsiahla sieť). Jeho úlohou je riadiť tok dátových správ medzi rôznymi sieťami na základe ich sieťových adries a smerovacích protokolov. Smerovač správy presmerúva len do tých sietí, kam sú určené, a jeho hlavným cieľom je usmerniť dátové balíky do konkrétnej počítačovej siete.



Obrázok 15 Router

**MODEM** prevádza digitálne signály z počítača na analógové pre prenos cez telefónnu sieť a opačne. Umožňuje počítaču komunikovať cez rôzne médiá, ako sú telefónne linky, káblová televízia, alebo rádiový prenos.



Obrázok 16 Modem

**Bezdrôtový prístupový bod (WAP)**, známy aj ako wireless access point, je zariadenie, ktoré spája rôzne bezdrôtové komunikačné zariadenia medzi sebou, vytvárajúc tak bezdrôtovú sieť. Tento prístupový bod má schopnosť poskytovať pripojenie bezdrôtovým zariadeniam k sieti. Môže fungovať ako fyzický zosilňovač alebo opakovač signálu, rovnako aj ako smerovač.



Obrázok 17 Bezdrôtový prístupový bod

**Repeater** je zariadenie, ktoré slúži na zosilnenie signálu v domácnostiach alebo vo verejných budovách na dosahovanie kvalitnejšieho signálu.



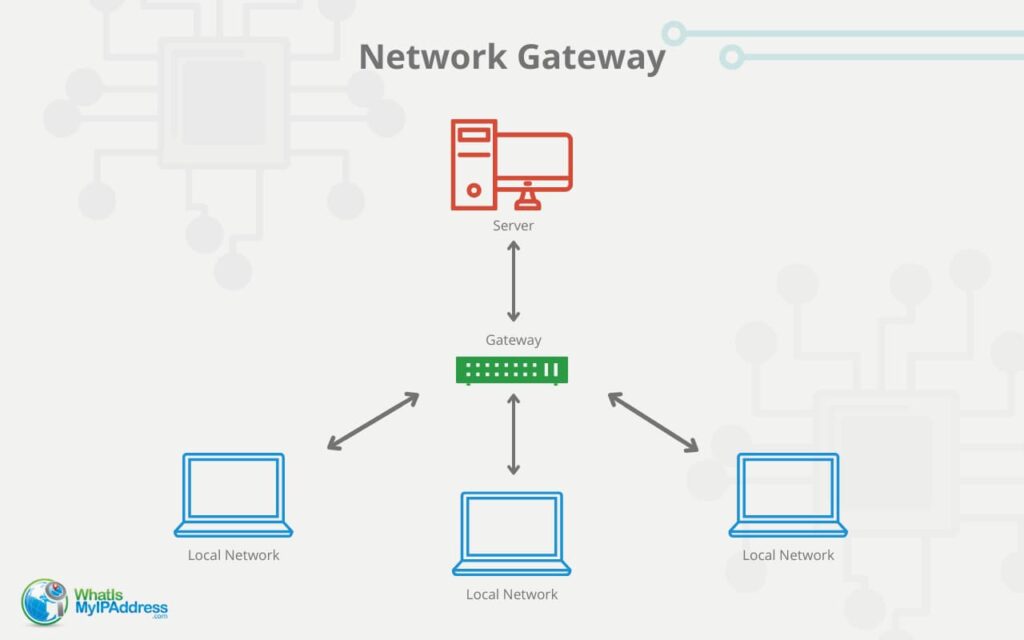
Obrázok 18 Repeater / Zosilňovač

**Most** (bridge) je zariadenie, ktoré umožňuje prepojenie medzi dvoma alebo viacerými sieťami, ktoré majú podobné vlastnosti a používajú rovnaké prenosové metódy. Jeho hlavným účelom je spájanie týchto sietí na úrovni dátovej linky, umožňujúc tok dát medzi nimi.



Obrázok 19 Most

**Gateway** je špeciálny typ smerovača, ktorý má schopnosť slúžiť ako rozhranie alebo prepojovací bod medzi rôznymi lokálnymi sieťami, ktoré môžu byť založené na rôznych technológiách, alebo medzi lokálnou sieťou a širšou, rozsiahlejšou sieťou, ako napríklad internetom. Jeho úlohou je umožniť komunikáciu a prenos dát medzi týmito rôznymi typmi sietí, čím umožňuje zariadeniam v jednej sieti komunikovať s tými v druhej, bez ohľadu na ich štruktúru alebo technológiu, ktorú používajú.



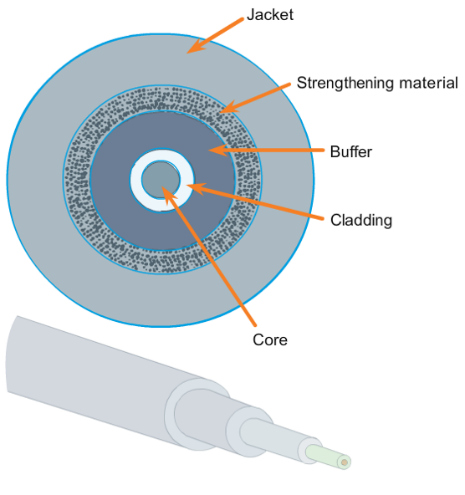
Obrázok 20 Príklad siete so zariadením Gateway

## 4.2 Sieťové Káble

Medzi základné typy sieťových káblov patrí koaxiálny kábel, optický kábel a krútená dvojlinka. Koaxiálny kábel sa vyznačuje dobrým tienením proti rušeniu a v minulosti bol široko používaný v počítačových sieťach, no dnes ho postupne nahrádzajú modernejšie technológie. Optický kábel zabezpečuje vysokorýchlostný prenos dát na veľké vzdialenosti a využíva svetelné signály namiesto elektrických impulzov, čo znižuje riziko rušenia. Krútená dvojlinka je najbežnejším typom sieťového kábla, ktorý pozostáva z dvojíc vodičov vzájomne skrútených pre minimalizáciu elektromagnetického rušenia a je široko využívaný v eternetových sieťach.

**Koaxiálny kábel** je typ kábla používaný pre prenos dát v sietiach. Skladá sa z centrálneho vodiča obklopeného izoláciou, ktorý je ďalej obklopený kovovou mriežkou a vonkajším plastovým obalom. Tento typ kábla sa používa pre prenos televízneho signálu, káblové internetové pripojenia alebo iné formy prenosu signálu v rôznych komunikačných prostrediach. Jeho konštrukcia umožňuje stabilný prenos signálu s minimálnymi rušeniami a stratami.

**Optický** kábel je typ kábla, ktorý sa využíva na prenos dát pomocou svetelných signálov. Skladá sa z tenkého vlákna zo skla alebo plastu, nazývaného vlákno, ktoré je schopné prenášať svetlo. Vlákno je obklopené ochrannými vrstvami na zabezpečenie ochrany a odolnosti. Optický kábel sa využíva pre vysokorýchlostné prenosy dát v internetových pripojeniach a v rôznych sieťových aplikáciách, ponúkajúc vysokú rýchlosť prenosu a menšie rušenia.



Obrázok 21 Jednotlivé vrstvy optického kábla

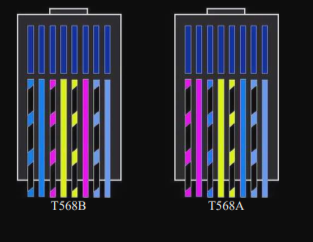
**Krútená dvojlinka** je jedným z najbežnejších typov kabeláže používaných v sieťových a telekomunikačných technológiách. Existujú dva hlavné typy: **Unshielded Twisted Pair (UTP)** a **Shielded Twisted Pair (STP)**.

**UTP** je najrozšírenejšia forma krútenej dvojlinky, využívaná predovšetkým v domácich a kancelárskych sieťach. Hoci je cenovo dostupná a ľahko sa inštaluje, jej nevýhodou je absencia tienenia, čo ju robí náchylnejšou na elektromagnetické rušenie. Tento typ sa často používa pre Ethernetové siete, konkrétne v kategóriách 5e, 6 a 6a.

Naopak, **STP** je vybavená dodatočným tienením vo forme kovového plášťa alebo fólie, ktorá znižuje elektromagnetické interferencie. To ju robí ideálnou pre prostredia s vysokým rizikom rušenia, napríklad v priemyselných alebo telekomunikačných zariadeniach.

Medzi hlavné **výhody krútenej dvojlinky** patrí predovšetkým **nákladová efektívnosť**, keďže je lacnejšia a jednoduchšia na inštaláciu v porovnaní s optickými káblami. Je tiež **veľmi flexibilná**, čo umožňuje jej využitie v rôznych aplikáciách, ako sú telefónne linky či Ethernetové siete. Navyše, vďaka svojmu krútenému dizajnu je **odolná voči elektromagnetickému rušeniu**, keďže vzájomné krútenie vodičov pomáha minimalizovať interferencie.

Na druhej strane, jej **nevýhody** spočívajú v **obmedzenej vzdialenosti prenosu**, keďže signál cez krútenú dvojlinku je stabilný len do vzdialenosti približne 100 metrov, kým optické vlákna umožňujú podstatne dlhší prenos. Okrem toho, krútená dvojlinka ponúka **nižšiu šírku pásma**, čo môže byť v niektorých prípadoch limitujúce oproti modernejším optickým riešeniam.



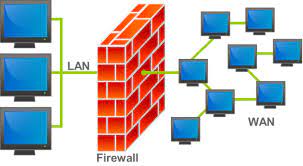
Obrázok 22 Zapojenie internetového káblu podľa typu A alebo B

## 4.3 Sieťové zabezpečenie

**Firewall je** sieťové zariadenie alebo softvér, ktorý slúži na kontrolu prichádzajúcej a odchádzajúcej sieťovej prevádzky na základe definovaných pravidiel. Jeho hlavnou úlohou je chrániť sieť pred neautorizovanými prístupmi, útokmi a inými hrozbami. Firewally môžeme rozdeliť na dva základné typy – hardvérové a softvérové. Hardvérové firewally sú fyzické zariadenia, ktoré spravujú prístup do siete, zatiaľ čo softvérové firewally sú programy bežiace priamo na operačnom systéme, kde filtrujú sieťovú prevádzku.

Z hľadiska spôsobu filtrovania prevádzky existujú rôzne prístupy. Pri filtrácii na základe paketov firewall kontroluje každý paket podľa informácií, ako sú IP adresy, porty a protokoly. Ďalšou metódou je stavové sledovanie (Stateful Inspection), pri ktorom firewall sleduje stav relácie a povolí iba tie pakety, ktoré patria k existujúcej relácii. Špecifickým typom firewallu je proxy firewall, ktorý funguje ako sprostredkovateľ medzi klientom a serverom, pričom filtruje všetky požiadavky.

**Firewall** funguje na základe vopred definovaných pravidiel, ktoré určujú, či pripojenie povolí alebo zablokuje. Tieto pravidlá môžu byť založené na IP adresách, čím umožňujú alebo blokujú prístup z konkrétnych zariadení. Ďalej môže firewall riadiť sieťovú prevádzku na základe portov, napríklad povolením alebo blokovaním komunikácie na portoch, ako je port 80 pre HTTP. Okrem toho pravidlá určujú aj použitie protokolov, pričom definujú, ktoré z nich, ako napríklad TCP alebo UDP, sú povolené.



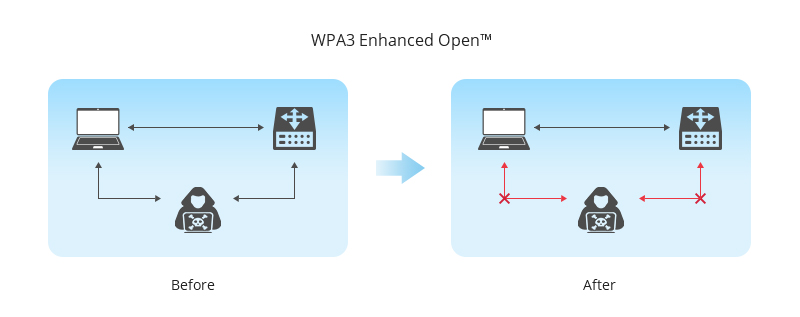
Obrázok 23 Počítačová sieť so zabezpečením Firewall



Obrázok 24 Fyzický Firewall

**4.3.1 Šifrovanie (WEP, WPA, WPA2 a WPA3)**

**WPA3** je najnovší štandard na zabezpečenie bezdrôtových sietí, ktorý oproti predchádzajúcim verziám výrazne zlepšuje úroveň zabezpečenia a ochrany údajov. Tento protokol poskytuje vysoký stupeň šifrovania údajov a ochrany proti pokusom o prelomenie hesla, čím zabezpečuje bezpečnosť vášho bezdrôtového pripojenia. Protokol WPA3 tiež zlepšuje ochranu vašich údajov vo verejných sieťach a individuálne šifruje každé pripojenie, čím zabraňuje tomu, aby útočník mohol dešifrovať údaje jedného používateľa a získať prístup k všetkým údajom. Vďaka protokolu WPA3 si môžete byť istí, že vaše bezdrôtové siete sú lepšie zabezpečené a vaše súkromie a údaje sú chránené pred potenciálnymi hrozbami.



Obrázok 25 Ukážka šifrovania WPA3 proti hackerom

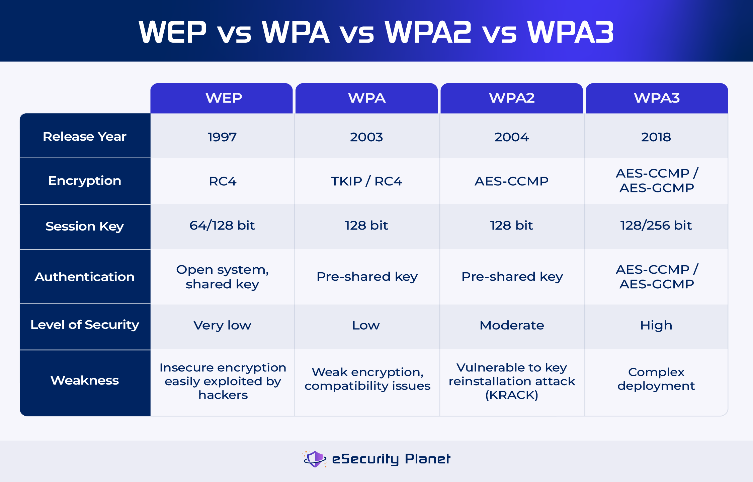
Na používanie WPA3 potrebujete router a zariadenia, ktoré ho podporujú. Väčšina moderných routerov a smartfónov (vydaných po roku 2018) už WPA3 podporuje, ale stále je potrebné skontrolovať, či je funkcia povolená v nastaveniach.

**Hlavné vlastnosti WPA3**

WPA3 prináša výrazné vylepšenia v oblasti bezpečnosti bezdrôtových sietí. Na rozdiel od svojho predchodcu WPA2 využíva protokol SAE (Simultaneous Authentication of Equals) namiesto tradičného PSK (Pre-Shared Key), čím poskytuje lepšiu ochranu proti útokom hrubou silou. Veľkou výhodou je aj ochrana pred offline útokmi – útočník nemôže jednoducho zachytiť komunikáciu a následne sa pokúšať dešifrovať heslo mimo siete, pretože každý autentifikačný pokus musí prebehnúť priamo medzi zariadením a routerom.

WPA3 zvyšuje bezpečnosť aj v prípade slabších hesiel, čím znižuje riziko úspešného napadnutia siete. Ďalším dôležitým prvkom je individuálne šifrovanie pre každé pripojené zariadenie, čo znamená, že jedno zariadenie nemôže odpočúvať komunikáciu iného, aj keď sú pripojené k rovnakej Wi-Fi sieti.

Významným vylepšením je aj podpora funkcie Easy Connect, ktorá uľahčuje pripájanie IoT zariadení, ako sú smart žiarovky či termostaty, prostredníctvom QR kódov alebo iných jednoduchých metód. Pre profesionálne a podnikové siete WPA3 ponúka ešte vyšší štandard bezpečnosti v podobe 192-bitového šifrovania, čím zaisťuje ochranu aj pre najcitlivejšie dáta.

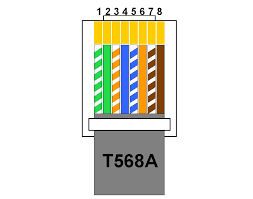
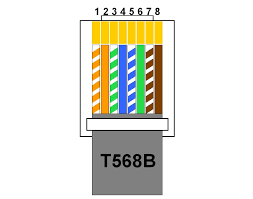


Obrázok 26 Rozdiel medzi jednotlivými WPA šifrovaniami

# 5. Praktická časť - Oprava a údržba počítačovej siete

V tejto časti sa pozrieme na základné postupy **pri oprave a údržbe počítačovej siete**, pričom kľúčovým krokom je diagnostika siete. Prvým a najdôležitejším krokom diagnostiky je základná fyzická kontrola, ktorá pomáha identifikovať bežné problémy s pripojením. Je nevyhnutné skontrolovať správne zapojenie sieťových káblov, či už ide o UTP alebo optické káble, a overiť ich funkčnosť a nepoškodenosť. V mnohých prípadoch môže jednoduchá výmena poškodeného kábla vyriešiť problém s pripojením.

Okrem toho je dôležité dbať na správne zapojenie internetového kábla podľa štandardov série A alebo B, aby sa predišlo komplikáciám spojeným s nekompatibilitou či nesprávnym prenosom signálu. Táto prvotná kontrola je základným krokom pri riešení problémov v sieti a často dokáže predísť zložitejším diagnostickým zásahom.



Obrázok 27 Zapojenie káblov podľa štandardu A alebo B

**Stav LED indikátorov na zariadeniach**

Obrázok, na ktorom je text, smerovač, elektronika, merač

Automaticky generovaný popis**LED indikátory** na zariadeniach slúžia na zobrazenie aktuálneho stavu zariadenia alebo jeho jednotlivých funkcií. Tieto svetelné indikátory sú často používané na elektronických zariadeniach, ako sú počítače, smerovače, modemy, servery, tlačiarne a iné sieťové zariadenia, a poskytujú vizuálne informácie o rôznych procesoch alebo problémoch.

## 5.0.1 Napájanie zariadenia

Správne napájanie zariadení v počítačových sieťach je nevyhnutné pre ich bezproblémovú prevádzku. Je dôležité uistiť sa, že všetky zariadenia, ako switche, routery, modemy či prístupové body, sú správne zapojené do elektrickej siete a nevykazujú žiadne problémy s napájaním. Stabilné napájanie zabezpečuje ich nepretržitú prevádzku a minimalizuje riziko výpadkov siete.

Pre zvýšenie spoľahlivosti sa často využívajú záložné zdroje napájania (UPS), ktoré umožňujú zariadeniam fungovať aj počas výpadkov elektriny. Tieto záložné zdroje sú kľúčové najmä pre ochranu citlivých zariadení, ako sú servery, switche, routery či pracovné stanice, a pomáhajú predchádzať strate dát alebo poškodeniu hardvéru spôsobenému náhlymi výpadkami prúdu.



Obrázok 28 Záložný zdroj UPS

**Stabilizátory napätia**

Stabilizátory napätia sú zariadenia určené na udržiavanie stabilnej hodnoty elektrického napätia dodávaného do pripojených zariadení. Ich hlavnou úlohou je chrániť elektroniku pred poškodením spôsobeným výkyvmi napätia, ako sú prepätia, podpätia alebo náhle zmeny napätia.



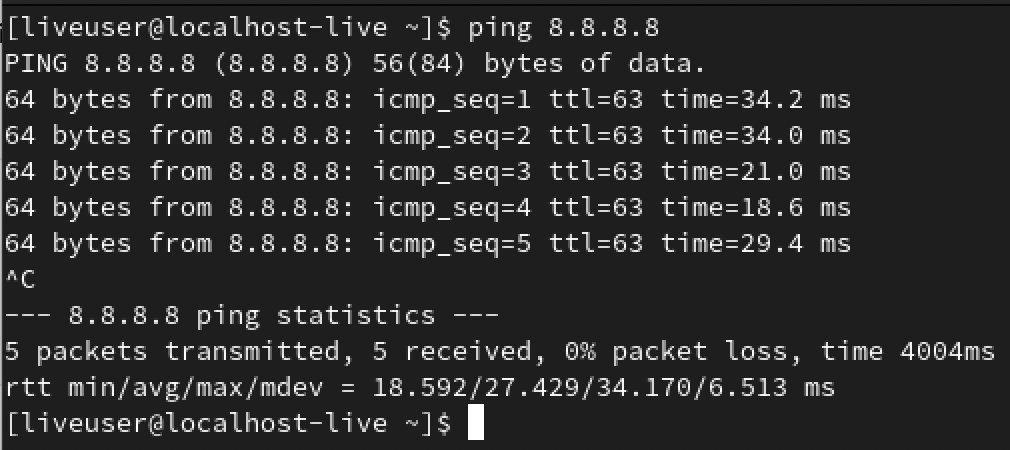
Obrázok 29 Stabilizátor napätia

## 5.1 Softvérová diagnostika

**Ping** je nástroj používaný na testovanie dosiahnuteľnosti zariadení v počítačovej sieti. Funguje tak, že odosiela ICMP (Internet Control Message Protocol) Echo Request pakety na cieľovú IP adresu a čaká na odpoveď vo forme ICMP Echo Reply. Pomocou neho je možné diagnostikovať rôzne sieťové problémy. Umožňuje zistiť odozvu medzi dvoma zariadeniami, teda či je cieľová IP adresa dostupná a aká je doba odozvy. Okrem toho dokáže odhaliť stratu paketov – ak počas testu nedôjde k odpovedi na požiadavky, môže to naznačovať problémy v sieti. Ping tiež meria latenciu, teda čas, ktorý zaberie paketom prejsť z jedného bodu na druhý, pričom tento čas sa zvyčajne uvádza v milisekundách.

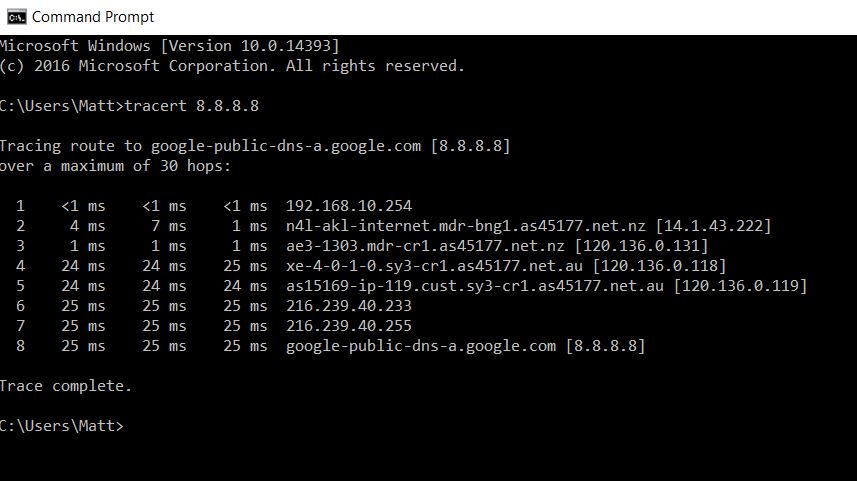
### 5.1.1 Kvalita pingu

Kvalita pingu sa dá rozdeliť do viacerých kategórií. Ping v rozmedzí 0 – 50 ms je výborný a odporúčaný pre hranie multiplayerových hier, pretože zabezpečuje plynulé pripojenie bez oneskorenia. Ak je ping medzi 50 – 100 ms, stále sa dá označiť za chválitebný, avšak môže spôsobiť mierne zhoršenie kvality pri hraní hier. Pri hodnotách 100 – 200 ms je ping už len dostatočný, čo znamená, že multiplayerové hry budú mať značné oneskorenie, no na bežné prehliadanie internetu to postačuje. Ak sa ping pohybuje v rozmedzí 200 – 1000 ms, kvalita je zlá, multiplayerové hry sú takmer nehrateľné, no prehliadanie internetu je ešte možné. Ak ping presiahne hodnotu 1000 ms, ide už o nedostatočnú kvalitu spojenia, ktorá spôsobuje výrazné problémy s internetovým pripojením a pripojenie na servery môže byť nestabilné.



Obrázok 30 Kontrola pingu pomocou CMD

**Traceroute** je nástroj, ktorý poskytuje informácie o trase, ktorou pakety prechádzajú zo zdrojového zariadenia na cieľové zariadenie v sieti. Pomáha diagnostikovať problémy v sieti tým, že zobrazuje každú sieťovú vrstvu (hop), cez ktorú prechádzajú dáta, a ukazuje časy odozvy medzi jednotlivými uzlami. Keď spustíme príkaz traceroute (alebo tracert na Windows), nástroj pošle ICMP Echo Request alebo UDP pakety na cieľovú IP adresu a postupne identifikuje smerovače a siete, cez ktoré pakety prechádzajú. Výstup traceroute obsahuje zoznam všetkých hopov, čas odozvy medzi jednotlivými uzlami a môže indikovať miesta, kde sa vyskytujú problémy, ako napríklad preťažené smerovače alebo chyby v určitých sieťových segmentoch.



Obrázok 31 Trace Route v príkazovom riadku CMD

**IPConfig/Ifconfig**

ipconfig a ifconfig sú príkazy v príkazovom riadku, ktoré slúžia na zobrazenie a správu sieťových nastavení na rôznych operačných systémoch.

**Ipconfig:**

Operačný systém: Používa sa predovšetkým v systéme Windows.

Účel: Zobrazuje aktuálne hodnoty konfigurácie TCP/IP siete a umožňuje spravovať sieťové rozhrania.

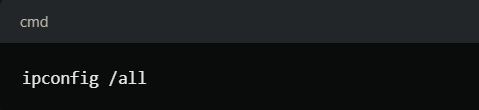
### 5.1.2 Príkazy do príkazového bloku CMD

**ipconfig z**obrazuje základné informácie o sieti, ako sú IP adresa, maska podsiete a predvolená brána.



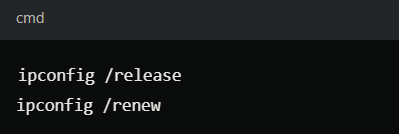
Obrázok 32 Ipconfig v CMD

**ipconfig/all** ukazuje podrobné informácie o všetkých sieťových rozhraniach, vrátane DNS serverov a MAC adries.



Obrázok 33 Príkaz ipconfig /all v CMD

**ipconfig /release a ipconfig /renew** používajú sa na uvoľnenie a obnovenie DHCP prenájmov.



Obrázok 34 Príkaz /release a /renew v CMD

**Ipconfig /flushdns** tento príkaz vymaže cache, čím sa odstránia potenciálne problémy a zariadenie získa aktuálne DNS informácie.



Obrázok 35 Príkaz /flushdns v CMD

**Ifconfig**

Operačný systém sa využíva predovšetkým v Unixových operačných systémoch, ako sú Linux a macOS.

Účel: Konfiguruje a zobrazuje parametre sieťových rozhraní.

**Bežné použitie:**

Obrázok, na ktorom je text, snímka obrazovky, písmo, dizajn

Automaticky generovaný popis**ifconfig:** Zobrazuje aktuálnu konfiguráciu sieťových rozhraní. (interface configuration) slúži na zobrazenie alebo zmenu sieťových nastavení na zariadení.

Obrázok, na ktorom je text, písmo, snímka obrazovky, grafika

Automaticky generovaný popis**ifconfig <rozhranie> up:** Aktivuje špecifikované sieťové rozhranie.

**ifconfig <rozhranie> down:** Deaktivuje špecifikované sieťové rozhranie.

Obrázok, na ktorom je text, písmo, snímka obrazovky, grafika

Automaticky generovaný popis

Obrázok, na ktorom je text, písmo, snímka obrazovky, grafika

Automaticky generovaný popis**ifconfig <rozhranie> <IP\_adresa>:** Priradí novú IP adresu špecifikovanému sieťovému rozhraniu.

### 5.1.3 Wireshark

Wireshark je bezplatný open-source nástroj na analýzu sieťovej komunikácie v reálnom čase, dostupný pre systémy Windows, Mac, Unix a Linux. Umožňuje zachytávať dátové pakety prechádzajúce sieťovým rozhraním, ako je Ethernet, LAN alebo SDR, a prevádza ich na cenné informácie využiteľné pre IT profesionálov a tímy kybernetickej bezpečnosti.

Jednou z hlavných vlastností Wiresharku je schopnosť detailne analyzovať sieťový prenos v reálnom čase, vďaka čomu je možné sledovať každý paket prechádzajúci sieťou. Používatelia môžu vidieť aj nízkoúrovňové detaily, ako sú hlavičky a obsah paketov. Wireshark podporuje viac než 2000 sieťových protokolov, vrátane bežných ako TCP, UDP, HTTP či DNS, a umožňuje analyzovať všetky vrstvy komunikačných protokolov.

Nástroj tiež ponúka pokročilé možnosti filtrácie a vyhľadávania v zachytených dátach, vďaka čomu môžu používatelia rýchlo identifikovať relevantné informácie. Filtre je možné aplikovať podľa adresy, portu, protokolu alebo iných parametrov, pričom môžu byť jednoduché alebo veľmi komplexné.

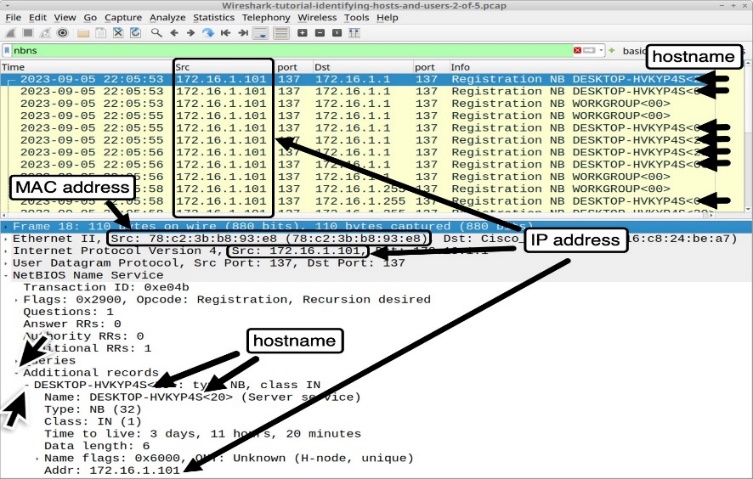
Obrázok, na ktorom je text, elektronika, snímka obrazovky, displej

Obsah vygenerovaný umelou inteligenciou môže byť nesprávny.Okrem toho Wireshark poskytuje aj analýzu výkonu siete a latencie, pričom dokáže identifikovať časové oneskorenia medzi paketmi a zobrazovať štatistiky o výkonnosti siete. Tieto funkcie robia z Wiresharku neoceniteľný nástroj na diagnostiku a riešenie problémov v počítačových sieťach.

Obrázok 36 Aplikácia Wireshark

Wireshark je nástroj, ktorý môže byť veľmi užitočný pri detekcii rôznych bezpečnostných problémov v sieťovej komunikácii. Pomáha pri sledovaní nezabezpečených protokolov, ako je nešifrované HTTP, alebo pri detekcii neobvyklých vzorcov v sieťovej komunikácii, napríklad pokusov o pripojenie na neexistujúce porty. Tento nástroj dokáže zachytávať pakety na rôznych sieťových médiách, ako sú Ethernet, Wi-Fi, Bluetooth a ďalšie.

Typické použitie Wiresharku zahŕňa diagnostiku problémov so sieťou, kde pomáha identifikovať problémy ako pomalé pripojenia, straty paketov alebo nesprávnu konfiguráciu sieťových zariadení. Ďalej sa často používa pri bezpečnostných auditoch a penetračných testovaniach na identifikovanie zraniteľností v sieťových protokoloch, ako sú nezabezpečené pripojenia alebo sledovanie komunikácie, ktorá môže obsahovať citlivé údaje. Wireshark sa tiež využíva na výkonové analýzy, kde pomáha analyzovať latenciu, stratu paketov a ďalšie parametre ovplyvňujúce výkon siete. Okrem toho je Wireshark veľmi užitočný aj na vzdelávacie účely, pretože umožňuje detailné štúdium sieťovej komunikácie a protokolov.

Wireshark funguje tak, že využíva špeciálne zariadenia, ako napríklad sieťové adaptéry v režime "promiscuous mode", aby zachytil všetky pakety prechádzajúce sieťou. Po zachytení týchto paketov ich Wireshark dekóduje a zobrazuje v čitateľnej forme. Používateľ si môže nastaviť filtre na zameranie sa na konkrétne pakety a analyzovať ich obsah. Napríklad je možné sledovať všetky pakety týkajúce sa HTTP komunikácie alebo sledovať pakety s konkrétnou IP adresou. Okrem toho Wireshark generuje štatistiky o komunikácii, ako sú histogramy, grafy a prenosové rýchlosti, čo umožňuje lepšie pochopiť stav a výkon siete.

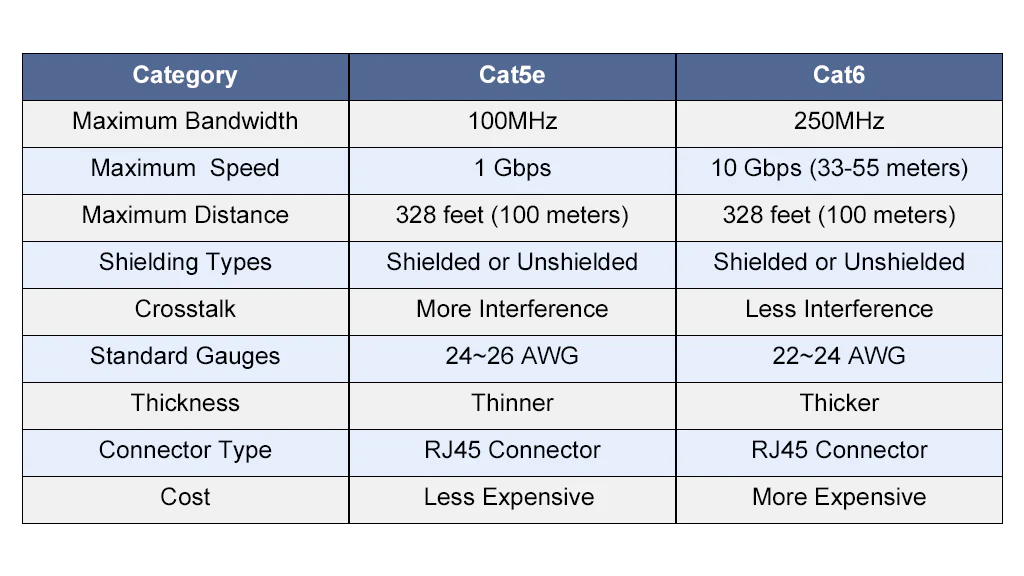
Obrázok 37 Skúška siete cez aplikáciu Wireshark

## 5.2 Údržba sieťových zariadení

Správna údržba sieťových zariadení, ako sú switche a routery, je kľúčová pre stabilnú a bezpečnú sieť. Jedným z najdôležitejších krokov je pravidelná aktualizácia firmvéru, ktorá nielenže chráni zariadenia pred bezpečnostnými hrozbami, ale tiež často zlepšuje ich výkon a pridáva nové funkcie. Ak sa zariadenie začne správať neštandardne, môže pomôcť reset do továrenského nastavenia, ktorý odstráni možné chyby spôsobené nesprávnou konfiguráciou. Dôležitou súčasťou údržby je aj kontrola portov – pomocou sieťového analyzátora možno overiť ich funkčnosť a v prípade potreby vymeniť poškodené porty alebo celé zariadenie.

### 5.2.1 Kontrola internetových káblov

Okrem samotných sieťových zariadení je potrebné venovať pozornosť aj káblom, ktoré zohrávajú kľúčovú úlohu pri prenose dát. Poškodené káble môžu spôsobovať výpadky siete alebo znižovať prenosovú rýchlosť, preto je vhodné ich pravidelne kontrolovať a v prípade potreby nahradiť kvalitnejšími variantmi, napríklad Cat 5e alebo vyššími, ako je Cat 6. Na overenie správneho zapojenia a ukončenia RJ-45 konektorov je užitočné použiť tester káblov, ktorý dokáže odhaliť chyby v zapojení, skraty či prerušené vodiče.



Obrázok 39 Rozdiel medzi Cat5 a Cat6

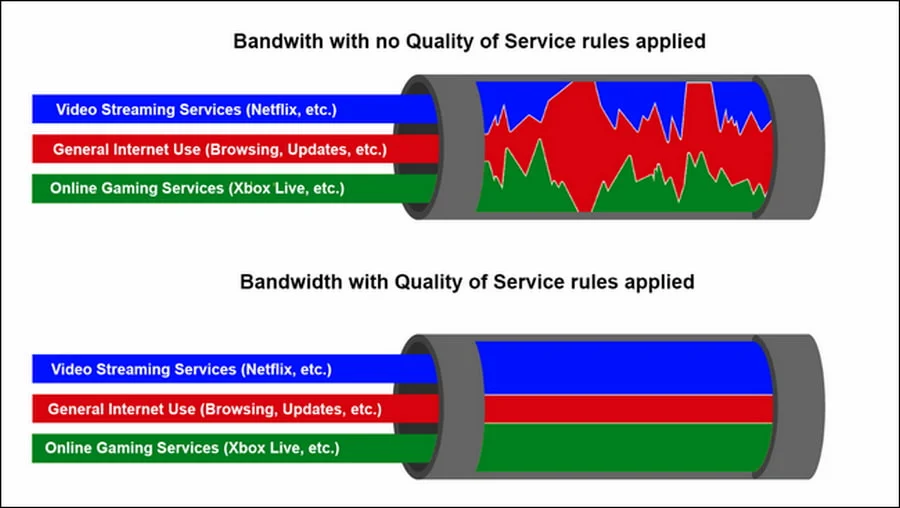


Obrázok 38 Tester RJ45 káblov

## 5.3 Optimalizácia siete

**Quality of Service (QoS)** je technológia, ktorá zabezpečuje efektívne využitie sieťových zdrojov tým, že uprednostňuje dôležité typy komunikácie. V praxi to znamená, že na routeri možno nastaviť pravidlá QoS, ktoré určujú prioritu pre rôzne aplikácie. Napríklad VoIP hovory a videokonferencie môžu dostať vyššiu prioritu, čím sa minimalizuje oneskorenie a zabezpečí plynulá komunikácia. Ďalším dôležitým aspektom je rozdelenie prenosovej šírky – router môže vyhradiť určitú kapacitu pre kritické služby, ako sú online hry alebo streamovanie videa, čím sa predchádza výpadkom alebo zníženiu kvality prenosu.

Pre zabezpečenie stabilného a kvalitného Wi-Fi pripojenia je kľúčové optimalizovať pokrytie signálom. V prípade rozsiahlejších priestorov môžu pomôcť Wi-Fi extendery alebo moderné mesh systémy, ktoré efektívne rozširujú signál a eliminujú miesta so slabým pripojením. Dôležité je aj správne nastavenie bezdrôtového kanálu – Wi-Fi routery fungujú na rôznych frekvenciách, pričom výber najmenej rušeného kanálu môže výrazne zlepšiť stabilitu a rýchlosť pripojenia. Nemenej podstatné je aj samotné umiestnenie routera – ideálne je ho umiestniť do centrálnej časti domácnosti alebo kancelárie, aby sa signál šíril rovnomerne a nedochádzalo k jeho výraznému útlmu v okrajových častiach priestoru.



Obrázok 40 Rozdiel medzi použitím QoS a bez

## 5.4 Bezpečnosť siete:

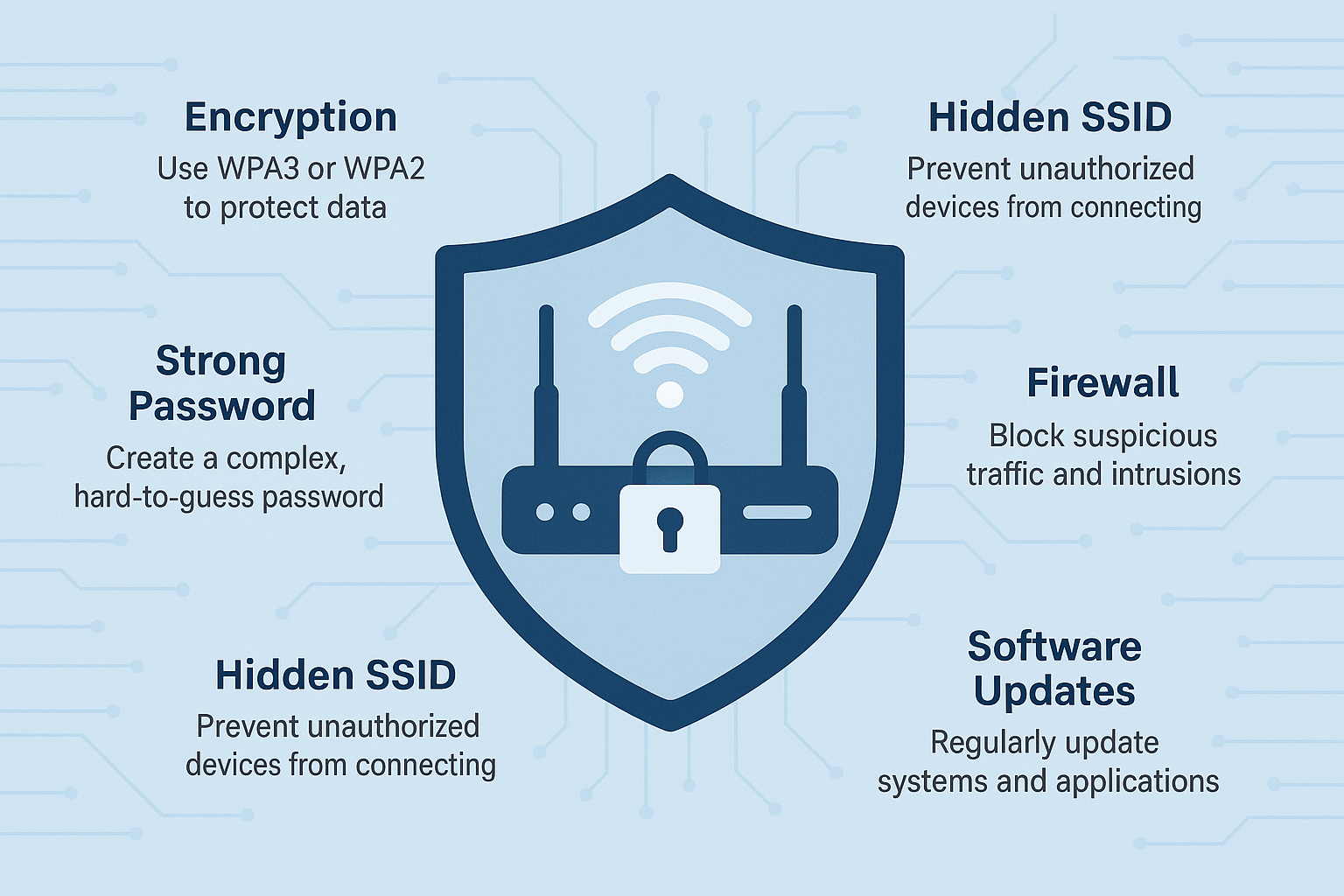
Na zabezpečenie Wi-Fi siete je dôležité použiť moderné metódy ochrany. Prvým krokom je **šifrovanie** – ideálne WPA3, prípadne WPA2, ak zariadenia nepodporujú novší štandard. Tieto technológie zabezpečujú, že prenos dát medzi zariadeniami je chránený pred odposluchom a neoprávneným prístupom.

Rovnako dôležité je **nastavenie silného hesla**. Odporúča sa používať kombináciu veľkých a malých písmen, číslic a špeciálnych znakov, aby bolo heslo ťažké uhádnuť. Vyhnite sa jednoduchým heslám, ako sú „123456“ alebo „admin“, pretože sú ľahko prelomené.

Ďalším bezpečnostným opatrením môže **byť skrytie SSID, teda názvu Wi-Fi siete**. Keď SSID nie je viditeľné, náhodní používatelia ho nevidia v zozname dostupných sietí, čím sa znižuje riziko, že sa k nej pokúsia pripojiť neoprávnené zariadenia.

**Firewall** predstavuje ďalšiu vrstvu ochrany vašej siete. Môže byť nakonfigurovaný tak, aby blokoval komunikáciu s podozrivými IP adresami a zabránil prístupu neznámym alebo škodlivým zariadeniam. Okrem toho je vhodné používať systémy detekcie a prevencie narušenia (IDS/IPS), ktoré dokážu v reálnom čase identifikovať a zastaviť pokusy o prienik do siete.

Napokon, nezabúdajte na pravidelné aktualizácie softvéru. Operačné systémy, aplikácie aj firmvér sieťových zariadení môžu obsahovať bezpečnostné zraniteľnosti, ktoré hackeri využívajú na neoprávnený prístup. Aktualizácie tieto chyby opravujú a znižujú riziko kybernetických útokov.



Obrázok 41 Odporúčané pravidlá pre zabezpečenie siete

# 6. Záver

Na zabezpečenie stabilnej a spoľahlivej siete je dôležité dôkladne kontrolovať všetky sieťové zariadenia – nielen po fyzickej stránke, ale aj ich interné nastavenia. Pravidelná údržba, ako je aktualizácia firmvéru, kontrola portov a testovanie káblov, pomáha predchádzať problémom a predlžuje životnosť zariadení. Rovnako je nevyhnutné dbať na kybernetickú bezpečnosť – používať silné a jedinečné heslá, povoliť pokročilé zabezpečenia ako firewall či šifrovanie, a chrániť sieť pred neoprávneným prístupom. Správnou kombináciou fyzickej kontroly, softvérovej údržby a bezpečnostných opatrení možno zabezpečiť stabilnú, rýchlu a bezpečnú sieť pre každodenné použitie ako pre mále domácnosti, tak aj pre obrovské firmy a verejnosť a predísť tým kybernetickým a nežiadúcim útokom, ktoré by mohli skomplikovať chod týchto sietí.

**Použitá literatúra**

**Zoznam použitých kníh**

1. Opravujeme si počítač, Autor: Jiří Král, Rok vydania: 2003
2. Řešení problémů s PC, Autor: Zdeněk Valečko, Rok vydania: 2010
3. Počítačové sítě pro začínající správce , Autori: Jaroslav Horák a Milan Keršláger, Rok vydania: 2014

**Zoznam použitých zdrojov**

1. <https://cloud-0.edupage.org/cloud/Pocitacove_siete_prezentacia.pdf?z%3ApmCKZgtzm0rxC1p2zUFza5nX7aYqAYegvLyoPIiPi2EPlXSm6rLZYaPwt5YyzOT2>
2. <https://www.gymparnr.edu.sk/obsah/predmety/subory/informatika/siete.pdf>
3. <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~types-of-firewalls>
4. <https://cs.wikipedia.org/wiki/Traceroute>
5. <https://sk.wikipedia.org/wiki/Sie%C5%A5ov%C3%BD_priechod>
6. <https://en.wikipedia.org/wiki/Network_bridge>
7. <https://www.ibm.com/docs/sk/aix/7.1?topic=network-tcpip-security>
8. <https://www.lifewire.com/how-to-improve-wifi-signal-5189250>
9. <https://www.tp-link.com/cz/wpa3/>
10. <https://sk.wikipedia.org/wiki/Ping>
11. <https://www.quora.com/What-are-ipconfig-and-ifconfig>
12. <https://www.upguard.com/blog/what-is-wireshark>