

Kryštof Novosad

Ročníková práce

Stavba a provoz malé počítačové sítě

Obsah

[Úvod 4](#_Toc105157851)

[I. Topologie sítě 5](#_Toc105157852)

[A. Logické rozdělení 5](#_Toc105157853)

[1. Posílání signálu (broadcast) 5](#_Toc105157854)

[2. Předávání známky (token passing) 5](#_Toc105157855)

[B. Fyzické rozdělení 5](#_Toc105157856)

[1. Sběrnicová topologie 5](#_Toc105157857)

[2. Kruhová topologie 6](#_Toc105157858)

[3. Hvězdicová topologie 6](#_Toc105157859)

[4. Stromová topologie 7](#_Toc105157860)

[5. Mesh topologie 7](#_Toc105157861)

[II. TCP/IP 8](#_Toc105157862)

[A. Charakteristika 8](#_Toc105157863)

[B. Důležité protokoly 8](#_Toc105157864)

[1. IP (Internet Protocol) 8](#_Toc105157865)

[2. ICMP (Internet Control Message Protocol) 9](#_Toc105157866)

[3. ARP (Address Resolution Protocol) 9](#_Toc105157867)

[4. IGMP (Internet Group Management Protocol) 10](#_Toc105157868)

[5. TCP (Transmission Control Protocol) 10](#_Toc105157869)

[6. UDP (User Datagram Protocol) 11](#_Toc105157870)

[III. Ethernet 12](#_Toc105157871)

[A. Charakteristika 12](#_Toc105157872)

[B. Prvky sítě Ethernet 12](#_Toc105157873)

[1. Opakovač 12](#_Toc105157874)

[2. Most 12](#_Toc105157875)

[3. Přepínač 12](#_Toc105157876)

[IV. IP adresa 13](#_Toc105157877)

[A. Charakteristika 13](#_Toc105157878)

[1. Speciální adresy 13](#_Toc105157879)

[2. Síťová maska 14](#_Toc105157880)

[3. Adresy v intranetu 14](#_Toc105157881)

[V. Směrování 15](#_Toc105157882)

[A. Předávání a filtrace 15](#_Toc105157883)

[B. Směrovací tabulky 16](#_Toc105157884)

[C. Směrovací protokoly 16](#_Toc105157885)

[1. LSP, RVP 16](#_Toc105157886)

[2. IGP, EGP 17](#_Toc105157887)

[VI. DHCP 17](#_Toc105157888)

[A. Charakteristika 17](#_Toc105157889)

[B. Klient / Server 17](#_Toc105157890)

[C. Proces zápůjčky 18](#_Toc105157891)

[VII. Aktivní a pasivní prvky sítě 19](#_Toc105157892)

[A. Základní rozdělení 19](#_Toc105157893)

[B. Aktivní prvky 19](#_Toc105157894)

[C. Pasivní prvky 20](#_Toc105157895)

[VIII. Konfigurace prvků sítě 20](#_Toc105157896)

[A. Opakovač 20](#_Toc105157897)

[B. Rozbočovač 20](#_Toc105157898)

[C. Most 20](#_Toc105157899)

[D. Směrovač 21](#_Toc105157900)

[E. Přepínač 21](#_Toc105157901)

[F. Brána 21](#_Toc105157902)

[IX. Připojení k internetu 21](#_Toc105157903)

[A. Síť Internet 21](#_Toc105157904)

[B. Typy připojení 22](#_Toc105157905)

[1. Drátové připojení 22](#_Toc105157906)

[2. Bezdrátové připojení 22](#_Toc105157907)

[3. Mobilní připojení 22](#_Toc105157908)

[C. DNS 22](#_Toc105157909)

[X. Wi-Fi 23](#_Toc105157910)

[A. Charakteristika 23](#_Toc105157911)

[B. Bezpečnost 23](#_Toc105157912)

[1. WEP (Wired Equivalent Privacy) 24](#_Toc105157913)

[2. WPA (Wi-Fi Protected Access) 24](#_Toc105157914)

[3. WPA2 24](#_Toc105157915)

[4. WPA3 24](#_Toc105157916)

[XI. Sdílení v síti 24](#_Toc105157917)

[A. Souborový systém 24](#_Toc105157918)

[1. Sdílení složek 25](#_Toc105157919)

[2. Datové úložiště 26](#_Toc105157920)

[B. Tiskárny, fax 27](#_Toc105157921)

[C. Vzdálená správa 27](#_Toc105157922)

[XII. Bezpečnost 28](#_Toc105157923)

[A. Firewall 29](#_Toc105157924)

[B. Možné hrozby 29](#_Toc105157925)

[XIII. Diagnostika 29](#_Toc105157926)

[A. Softwarové nástroje 29](#_Toc105157927)

[1. Ping 30](#_Toc105157928)

[2. Netcat 30](#_Toc105157929)

[3. Wireshark 30](#_Toc105157930)

[B. Hardwarové nástroje 31](#_Toc105157931)

[XIV. Závěr 32](#_Toc105157932)

[XV. Rejstřík 32](#_Toc105157933)

# Úvod

Tato práce shrnuje všechny mnou dosavadně získané znalosti z předmětu Počítačové sítě za dobu studia na Obchodní akademii Kroměříž v oboru Informační technologie. V této práci popisuji základní teorii stavby malé počítačové sítě a k ní dodatečnou terminologii, jež je základním podkladem pro pochopení dané problematiky.

# Topologie sítě

Topologií sítě se rozumí uspořádání síťových prvků uvnitř počítačové sítě. Popisuje a udává strukturu fyzické a logické podoby sítě.

## Logické rozdělení

Zabývá se způsobem vzájemné komunikace a výměnou dat mezi jednotlivými uzly sítě. Nahlíží se na to, který uzel má přednost v zasílání informací. Nejčastějšími logickými topologiemi jsou posílání signálu (broadcast) a předávání známky (token passing).

### Posílání signálu (broadcast)

V této topologii neexistují žádná pravidla, podle kterých by zařízení dostávala oprávnění k odesílání dat. Hlavním principem této topologie je, že každé zařízení může odesílat data okolním zařízením kdykoliv, v jakémkoliv pořadí. Tohoto principu se drží například síť Ethernet.

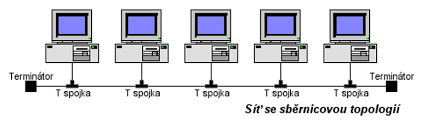
### Předávání známky (token passing)

Principem této topologie je oběh speciální známky od zařízení k zařízení. V případě, že chce zařízení odeslat data musí v daný okamžik známku držet, nebo na ní počkat. Po odeslání dat předává známku dalšímu zařízení v pořadí. Tohoto principu se hojně používá například v kruhové topologii.

## Fyzické rozdělení

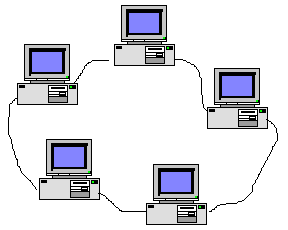
Udává, jakým způsobem jsou jednotlivé uzly propojeny. Toto propojení je realizováno pomocí kabelů (kroucené dvojlinky, koaxiálním kabelem, optickým kabelem), nebo bezdrátově (rádiové vlny, infračervený přenos). Fyzické topologie rozdělujeme do několika základních typů, a to podle vzhledu jejich zapojení, které však nemusí nutně odpovídat opravdovému provedení.

### Sběrnicová topologie

Je realizována pomocí jednoho souvislého úseku kabelu, na který jsou zapojeny všechna zařízení pomocí spojek či odboček. Na obou koncích se nachází terminátor signálu, aby nedocházelo k jeho zpětnému odrážení. Data z jednoho zařízení jsou vyslána všem zařízením současně, ale pouze adresát tyto data zpracuje. Výhodou je jednoduché sestavení a napojení dalších zařízení v případě potřeby. Je však vhodná pouze pro malé sítě, jelikož s větším počtem dochází k ústupu rychlosti a při problému s hlavním kabelem může dojít k úplnému výpadku sítě.

Obrázek ‑

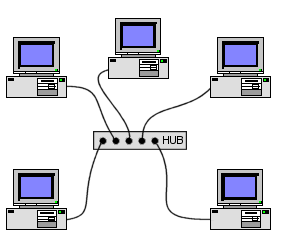
### Kruhová topologie

Je realizována propojením jednotlivých zařízeních tak, aby tvořily uzavřený kruh. Data v této síti obíhají od vysílajícího zařízení přes všechna ostatní zařízení v síti a mohou si je přečíst jen ty, kterým jsou určena. Hlavní výhodou této topologie je, že každé zařízení slouží jako opakovač, který signál při přeposílání posiluje. Nevýhodou je však riziko výpadku celé sítě v případě poruchy kteréhokoliv zařízení.

Obrázek ‑

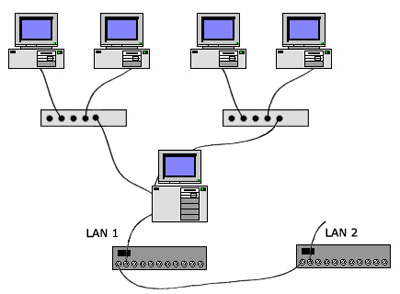
### Hvězdicová topologie

Je realizována připojením všech zařízení do jednoho rozbočovače nebo přepínače. Rozbočovač nakonec data nasměruje k správnému zařízení. Tato topologie řeší nevýhody jak sběrnicové, tak kruhové topologie. Data již neprochází každým uzlem sítě a při poruše kteréhokoliv zařízení nedochází k odstávce celé sítě. Hlavní výhodou je také jednoduché napojení nových zařízení a jednoduchá instalace. Nevýhodou je závislost na parametrech centrálního rozbočovače.



Obrázek ‑

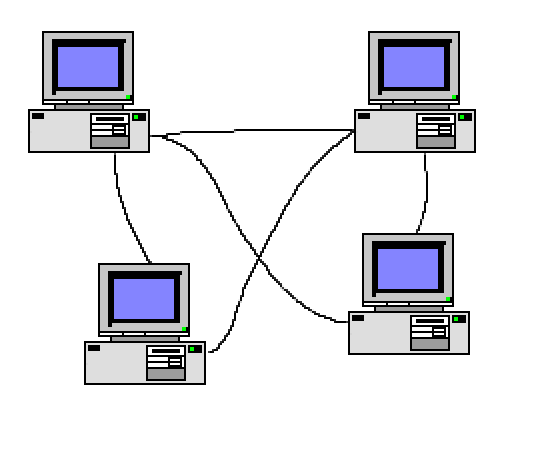
### Stromová topologie

Je realizována složením několika hvězdicových topologií, které jsou navzájem propojeny rozbočovači. Tato topologie má stejné výhody a nevýhody jako má topologie hvězdicová. Tato topologie se uplatňuje především ve větších sítích.

Obrázek ‑

### Mesh topologie

Jedná se o topologii, v které je každé zařízení propojené s každým (full mesh) nebo může být použita alternativa, při které se některé spoje vynechají (částečný mesh). Výhodou této topologie je velká spolehlivost. Když některý spoj vypadne, data si k cíli najdou jinou cestu. Nevýhodou je obtížná instalace a velká spotřeba kabeláže.



Obrázek ‑

# TCP/IP

## Charakteristika

Protokol TCP/IP je v současnosti chápán jako standard pro komunikaci v počítačové sítí. Používá se například v celosvětové síti Internet.

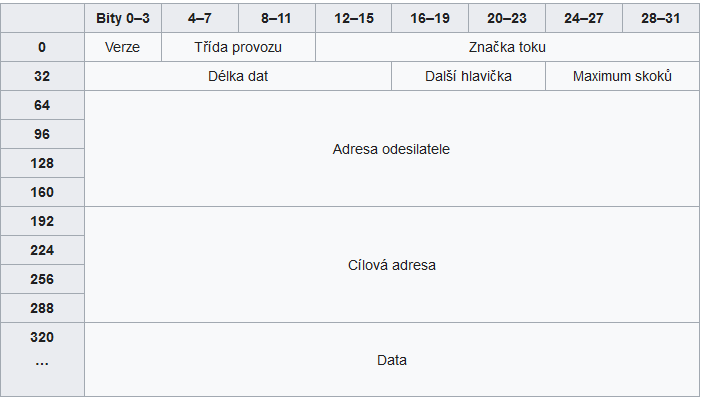
Architektura TCP/IP zahrnuje jednak vlastní přenos datových paketů sítí (zajišťuje protokol IP), dále rozhraní pro nespojované, nepotvrzované zasílání datagramů UDP a protokol logického kanálu TCP. Protokol TCP prostřednictvím potvrzování zajišťuje spolehlivost v prostředí sítí, kde přenos dat na nižších úrovních se děje principiálně nespolehlivě, s nezaručeným pořadím doručování paketů, s možností fragmentace a zahození dat na cestě. Protokol TCP je vybaven řízením toku dat a ochranou proti chybám, které mohou vzniknout opakovaným navazováním spojení

Strukturálním uspořádáním protokolu TCP/IP jsou čtyři vrstvy. Jedná se o:

* Aplikační vrstvu – jednotlivé aplikační protokoly (např. FTP, HTTP)
* Transportní vrstvu – o chod dat se starají protokoly TCP a UDP
* Síťovou vrstvu – směrování, předávání datagramů a adresace
* Fyzickou a linkovou vrstvu – přenos dat přes fyzické uzly

## Důležité protokoly

### IP (Internet Protocol)

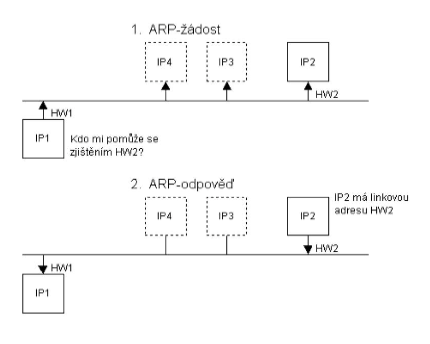
Univerzální přenosový protokol síťové vrstvy, jediný přenosový protokol rodiny TCP/IP. Protokol slouží k nespolehlivému, nespojovanému přenosu dat mezi zdrojovým počítačem a příjemcem. Protokol je implementován v koncových uzlech a přenášená data se nazývají IP datagramy neboli IP pakety. Každý paket obsahuje hlavičku, ve které nese metadata (řídící informace) a vlastní přenášená data (payload). V současnosti jsou paralelně používány dvě verze protokolu, IPv4 a IPv6, avšak dominuje starší verze IPv4.

Obrázek ‑ (IP datagram)

### ICMP (Internet Control Message Protocol)

Slouží pro generování a odesílání chybových zpráv, diagnostické a testovací účely. Protokol ICMP pracuje nad protokolem IP, takže jsou pakety tohoto protokolu obaleny do IP paketů. Protokol ICMP upozorní odesílatele například na zacyklení nebo na nedostupnost koncového uzlu. Tvoří tedy nedílnou funkční součást protokolu TCP/IP a musí být v síti povinně implementován.

### ARP (Address Resolution Protocol)

Slouží k překladu IP adres na MAC adresy, a to metodou dotaz – odpověď. Společně s RARP, který slouží pro překlad MAC adresy na IP adresu, tvoří linkovou vrstvu protokolu TCP/IP. Protokol ARP odešle do sítě dotaz a zařízení, kterého se dotaz týká, na něj odpoví.

Obrázek ‑

### IGMP (Internet Group Management Protocol)

Protokol IGMP je podobně jako protokol ICMP služebním protokolem TCP/IP,   
je tedy opět obalen do IP datagramu. Slouží k šíření adresných oběžníků (multicast) v rámci sítě. Pomocí protokolu si mohou zařízení vyměnit informace o členství ve specifických skupinách a s jeho pomocí se do skupin přihlašovat a ze skupin odhlašovat. Následně mohou jednotlivá zařízení odesílat a přijímat data v rámci skupiny.

### TCP (Transmission Control Protocol)

Základní protokol transportní vrstvy. Umožňuje aplikacím vytvářet spojení   
a přenášet data spolehlivě s kontrolou jejich doručení. Protokol garantuje doručení dat ve správném pořadí, navíc prostřednictvím portů rozlišuje různé aplikace spuštěné na stejném zařízení.

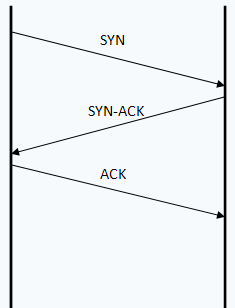
TCP využívá pro odesílání paketů nespolehlivý protokol IP, spolehlivost pak zajišťuje kontrolou doručení paketu pomocí potvrzování, pakety dále na straně příjemce protokol TCP uspořádá pro zajištění správného pořadí doručení.

K uzavření a potvrzení spojení slouží tzv. třísměrný handshake. V průběhu se obě strany dohodnou na číslu potvrzování a číslu sekvence. Pro navázaní spojení se vysílají datagramy s příznaky SYN a ACK.

**Průběh handshake**:

1. Klient vyšle na server požadavek s příznakem SYN a náhodným číslem sekvence a číslem potvrzování 0.
2. Server odpovídá s číslem potvrzování nastaveným na číslo sekvence klienta a přičte k němu číslo 1. Následně náhodně vygeneruje své číslo sekvence, příznaky nastaví na SYN, ACK.
3. Klient odešle odpověď s příznakem ACK, číslem potvrzování nastaveným na číslo sekvence serveru a přičte k němu číslo 1. Nakonec přičte ke svému číslu sekvence číslo 1 a nastaví příznaky na ACK.

Protokol TCP při přenosu vytváří iluzi proudu jednotlivých dat. Na straně odesílatele protokol TCP shromažďuje jednotlivá data do vyrovnávací paměti a po jejím naplnění odesílá celý takto vytvořený blok, nazývaný segment, protější straně. Na straně příjemce je poté přijatý segment uložen do vyrovnávací paměti a aplikaci jsou data poté poskytována ve formě celé zprávy.



Obrázek ‑ (handshake)

Obsah obrázku text

Popis byl vytvořen automaticky

Obrázek ‑ (TCP datagram)

### UDP (User Datagram Protocol)

Obsah obrázku stůl

Popis byl vytvořen automatickyProtokol UDP je jednoduchou alternativou pro protokol TCP. Protokol UDP je na rozdíl od protokolu TCP nespojovou službou, tj. nenavazuje spojení. Odesílatel odešle UDP datagram příjemci a už se nestará o to, zdali se datagram náhodou neztratil. Jedinou zárukou je kontrola integrity dat, jelikož obsahuje kontrolní součet.

Obrázek ‑ (UDP datagram)

# Ethernet

## Charakteristika

Ethernet je internetový protokol, který definuje způsob, jak posílat data v rámci sítě LAN. Podle protokolu Ethernet se data posílají v Ethernetových rámcích (frames). Rámec tedy slouží k uložení a přenosu veškerých informací po sítí.

## Prvky sítě Ethernet

Původně se Ethernet zaváděl na tlustém koaxiálním kabelu, přičemž taková síť měla označení 10BASE5. Později se však přešlo na tenký koaxiálním kabel s označením 10BASE2. Takové sítě se dnes v praxi téměř nevyskytují. Dnes se místo koaxiálního kabelu používá kroucená dvojlinka s označením sítě 10BASE-T nebo 100BASE-TX.

### Opakovač

Maximální teoretická délka jednoho segmentu LAN je 500 metrů. Rozsah LAN je možné zvětšit tím, že použijeme více segmentů, které mezi sebou propojíme tzv. opakovači. Opakovač je tvořen dvěma nebo více síťovými kartami, které jsou vzájemně propojeny. Objeví-li se nějaký datový rámec na jednom rozhraní, pak je automaticky zopakován na všechny ostatní.

### Most

Oproti opakovači mezi sebou most spojuje jednotlivé uzly LAN, ale neopakuje všechny rámce, které se na jeho portech objeví.

Most je realizován specializovaným počítačem, který má předávací tabulku. V této tabulce je seznam všech linkových adres všech síťových rozhraní LAN. U každé adresy má poznamenáno, za kterým síťovým rozhraním mostu se nachází. Objeví-li se datový rámec na nějakém síťovém rozhraní mostu, pak se most podívá do datového rámce na adresu příjemce a z předávací tabulky zjistí, za jakým rozhraním se adresát nachází. Rámec pak zopakuje pouze do rozhraní, za kterým je adresát. V případě, že se adresát nachází za stejným rozhraním, jej neopakuje vůbec.

### Přepínač

Přepínačem se označují výkonnější mosty, které umí opakovat rámce nejen mezi jednotlivými segmenty Ethernetu, ale i např. mezi Ethernetem a Fast Ethernetem, mezi Ethernetem a FDDI apod. Přepínač musí umět nejenom změnit tvar rámce např. z Ethernetu na FDDI, ale pokusit se i překlenout rozdíl mezi přenosovými rychlostmi.

# IP adresa

## Charakteristika

Slouží jako unikátní identifikátor k označení jednotlivých zařízení v rámci sítě Internet. Existují dvě verze IP adresace, a to IPv4 a IPv6, přičemž IPv4 disponuje 32bitovou adresou, zatímco IPv6 adresou 128bitovou. V současnosti stále převládá využití verze IPv4.

Samotná IP adresa se skládá ze dvou částí: adresy počítače a adresy sítě. Kolik bytů z IP adresy tvoří adresu sítě určují počáteční bity IP adresy. Ty se dělí do pěti tříd:

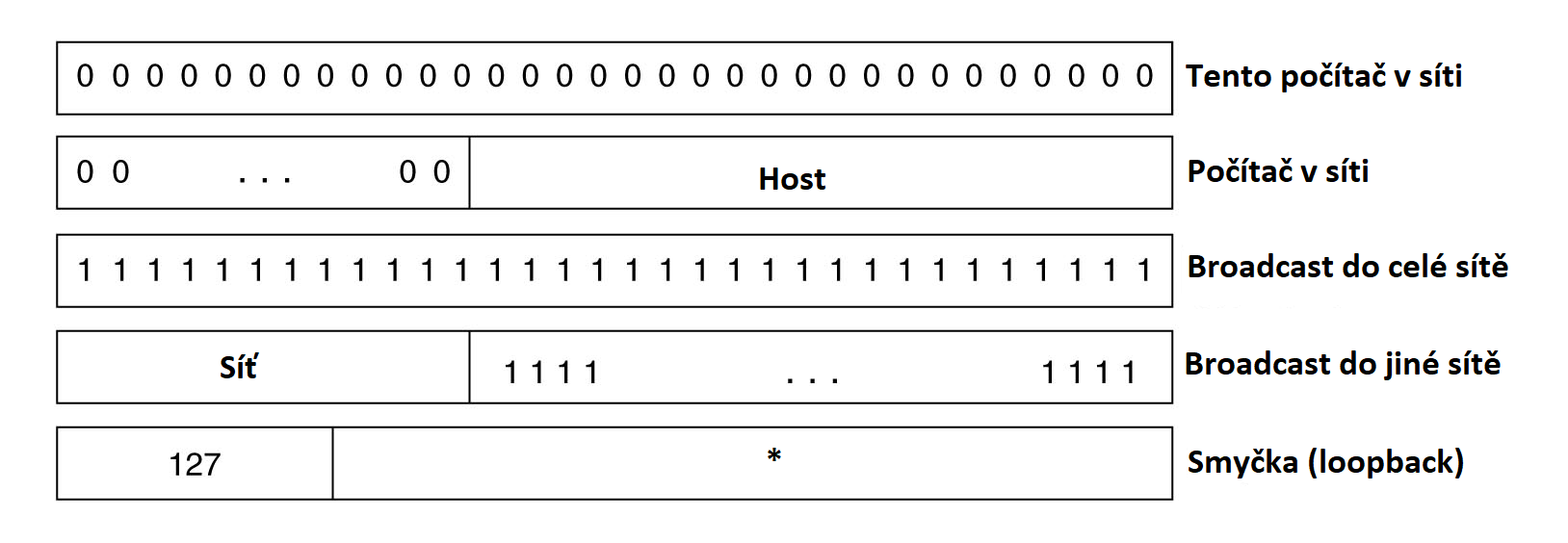
* Třída A – Obsahuje 27 sítí, v každé síti je 224 adres pro jednotlivá zařízení.
* Třída B – Obsahuje 214 sítí a v každé sítí je 216 adres pro jednotlivá zařízení
* Třída C – Obsahuje 222 sítí a v každé síti je 28 adres pro jednotlivá zařízení
* Třída D – Slouží pro adresné oběžníky (multicast)
* Obsah obrázku stůl

  Popis byl vytvořen automatickyTřída E – Rezervní adresy

Obrázek ‑

### Speciální adresy

Mimo adresy definované v prostoru tříd se zde nachází speciální IP adresy sloužící k testovacím účelům nebo k účelům adresných oběžníků. Jedná se o tyto adresy:



Obrázek ‑

### Síťová maska

Síťová maska se používá pro určení adresy sítě. Adresa sítě je totiž součástí IP adresy a za pomocí síťové masky můžeme určit, které bity adresa sítě tvoří. Síťová maska je opět čtyřbajtové číslo a je vyjádřeno ve dvojkové soustavě, která má v bitech určujících adresu sítě samé jedničky a v ostatních bitech samé nuly.

Jednotlivé třídy sítí používají jako adresu sítě různě dlouhou část IP adresy. Například Třída A používá pro adresu sítě první byte. Čili standardní síťová maska pro adresy třídy A má v prvním bytu samé jedničky a ve zbylých třech bytech samé nuly.

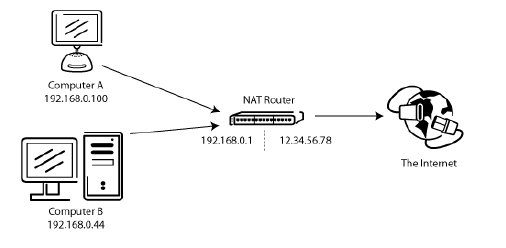
### Adresy v intranetu

Použití sítě Internetu uvnitř lokální sítě se nazývá intranet. Jelikož IP adresy musí být v síti Internet jednoznačné a unikátní, nesmí adresy intranetu kolidovat s adresami v síti Internet. Jediným způsobem, jak propojit síť Internet se sítí intranet je tedy přečíslování adres.

Obsah obrázku stůl

Popis byl vytvořen automatickyJako řešení vznikl standard určující, které sítě jednoznačně patří do intranetu a nelze je použít v rámci sítě Internet. K následnému přečíslování poté slouží automatický systém zvaný NAT (Network Address Translator). Nevýhodou systému NAT je ovšem překrytí několika zařízení za jedinou IP adresou, proto firmy často nakupují IP adresy pro jednotlivá zařízení zvlášť.

Obrázek ‑ (Adresy dostupné intranetu)



Obrázek ‑ (NAT)

# Směrování

Ke směrování dochází pouze pokud zasíláme data do jiné sítě, než se nacházíme. Jedná se o proces předávání paketů z bodu A do bodu B za pomocí přeskoků mezi jednotlivými uzly sítě a zahrnuje i výpočet optimální cesty. Směrování a předávání IP datagramů jsou dva procesy, které jsou nedílnou součástí sítě Internet.

## Předávání a filtrace

Při odesílání dat přes síť mohou data putovat přes několik uzlů, než dorazí ke svému cíli. Díky předávání mohou jednotlivá zařízení pracovat jako směrovač, přes která mohou data volně proudit. Pokud daný uzel dostane IP datagram, který není adresován pro něj, pak se jej pokouší předat dále.

Ne vždy ale chceme, aby náš systém svévolně předával datagramy po sítí. Předávání je tedy volitelné a lze jej zakázat, a to například v nastavení daného zařízení nebo v nastavení operačním systému. Lepším řešením je ovšem nastavit takzvaný filtr.

Předávaný IP datagram se předá filtračnímu procesu, který ho na základě nastaveného filtr schválí, nebo zamítne. Filtr lze nastavit na základě těchto informací:

* IP záhlaví – například podle adresy IP
* TCP záhlaví – podle čísla portu nebo příznaků SYN, ACK
* Aplikačního protokolu probíhajícím na daném portu

## Směrovací tabulky

Při směrování musí zařízení vědět, který adresát se pod danou IP adresou skrývá a jakému rozhraní má IP datagram předat. Takovému zařízení, které směruje datagramy z rozhraní do rozhraní, se říká směrovač.

Obsah obrázku stůl

Popis byl vytvořen automatickySměrovači k rozhodování slouží směrovací tabulka. Ta většinou obsahuje cílovou síť a její masku, IP adresu rozhraní dalšího skoku a metriku daného pravidla. Směrovači poté stačí projít tabulku od shora dolů a uplatnit první platné pravidlo, kde se IP adresa po uplatnění masky sítě rovná adrese sítě. Pokud ovšem datagram splňuje více pravidel současně, uplatní se vždy pravidlo s nejnižší hodnotou metriky.

Obrázek ‑ (příklad směrovací tabulky)

## Směrovací protokoly

Směrovací protokoly jsou aplikační protokoly, které neslouží uživatelům (osobám), ale směrovačům, aby si vzájemnou komunikací mezi sebou automaticky naplnily směrovací tabulky. Existuje dvojí rozdělení směrovacích protokolů:

### LSP, RVP

Protokol RVP (Routing Vector Protocol) pracuje na principu výměny obsahu směrovacích tabulek se sousedními směrovači. Směrovač odesílá ostatním směrovačům vektory (jeden řádek směrovací tabulky) a ty doplňují své vlastní směrovací tabulky   
o chybějící záznamy.

Protokol LSP (Link State Protocol) pracuje na principu adresných oběžníků. Směrovač nejdříve zjistí, jaké směrovače má za své sousedy a v pravidelných intervalech testuje jejich dostupnost. Následně zasílá oběžníky, ve kterých informuje ostatní směrovače o svých sousedech.

Nevýhodou obou algoritmů je zaplavováním sítě velkým počtem datagramů, a proto se tedy protokoly používají pouze rámcově nebo v sítích méně rozsáhlých. Na větší sítě se naopak používají protokoly IGP a EGP.

### IGP, EGP

Protokol IGP (Interior Gateway Protocol) je určen pro činnost v rámci autonomního systému. Slouží například firmám, které vlastní rozsáhlejší sítě.

Protokol EGP (Exterior Gateway Protocol) slouží například poskytovatelům internetového připojení pro výměnu směrovacích informací, jelikož na rozdíl od IGP dokáže protokol EGP zohlednit směrovací politiku (např. kdo komu platí)

# DHCP

## Charakteristika

Protokol DHCP zjednodušuje správu konfigurace adresy IP pomocí automatického konfigurování adres pro síťové zařízení. Službu DHCP zajišťuje pro celou síť jedno společné zařízení, na kterém běží server DHCP a automaticky přiřazuje adresy IP.

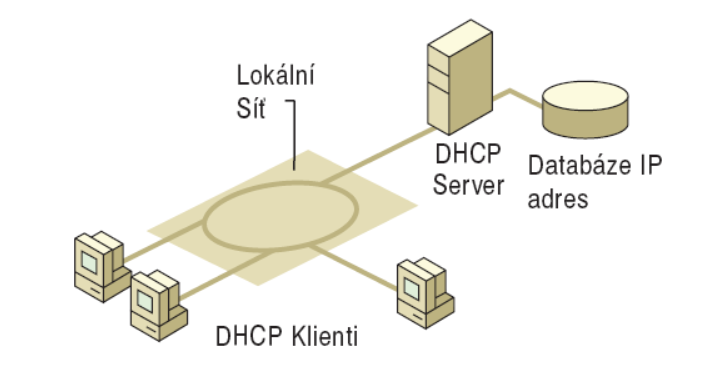
Každé zařízení na síti, založené na protokolu TCP/IP, musí mít jedinečnou IP adresu, aby bylo schopno přistupovat k síti a jejím prostředkům. Bez protokolu DHCP je nutno provést nakonfigurování protokolu IP u nových počítačů ručně, nebo u počítačů přesunovaných z jedné podsítě na jinou a u počítačů ze sítě odebíraných.

## Klient / Server

Protokol DHCP je založen na modelu klient/server, kdy správce sítě zakládá po většinou jeden server DHCP, který udržuje informace o konfiguraci sítě a použitých adresách. Tento server poté poskytuje klientům na vyžádání volné IP adresy ve formě nabídky a zápůjčky.

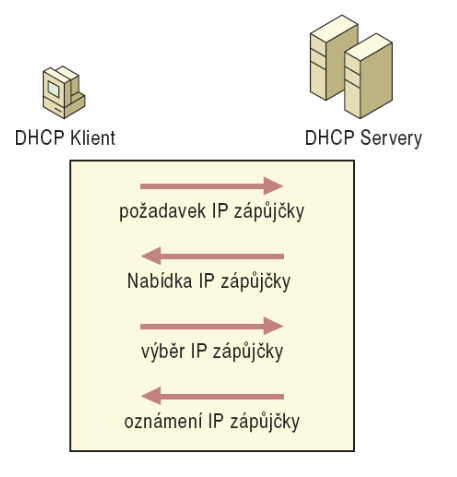
Server uchovává ve své konfiguraci několik parametrů:

* Platnou konfiguraci TCP/IP v rámci sítě
* Platný rozsah IP adres sloužící k zapůjčení klientům
* Dobu trvání zápůjčky nebo dobu po kterou může být adresa využívána
* Rezervované IP adresy pro určité klienty podle adresy MAC (statické adresy)



Obrázek ‑a (model klient/server)

## Proces zápůjčky

Při procesu zápůjčky klient podporující službu DHCP obdrží od serveru DHCP odpověď ve tvaru IP adresy a doby trvání zápůjčky. Ještě před vypršením časového omezení zápůjčky musí server DHCP tuto zápůjčku klientovi obnovit, jinak musí klient obdržet zápůjčku novou.

Obrázek ‑b (proces zápůjčky)

# Aktivní a pasivní prvky sítě

## Základní rozdělení

Všechny prvky a uzly sítě dělíme na dvě základní kategorie:

* **Aktivní** – starají se o logický chod sítě
* **Pasivní** – kabeláž, montáž

## Aktivní prvky

Dělí se na:

* **Hardwarové** – Specializované, jednoúčelová zařízení ve fyzické podobě
* **Softwarové** – Algoritmus, který simuluje činnost hardwarového zařízení

A mezi takové prvky patří:

* **Síťové karty (Network Interface Card)**

– slouží k připojení zařízení do sítě

* **Rozbočovač (Hub)**

– propojuje vícero zařízení mezi sebou

* **Most (Bridge)**

– odděluje provoz mezi dvěma lokálními sítěmi

* **Přepínač (Switch)**

– rozděluje lokální síť do několika podsítí (chytrý most)

* **Směrovač (Router)**

– umožňuje předávání datagramů v rozsáhlých sítích

* **Opakovač (Repeater)**

– posiluje a opakuje signál

* **Převodník (Transceiver)**

– převádí mezi různými typy signálů

* **Brána (Gateway)**

– propojuje dvě nezávislé sítě

## Pasivní prvky

Patří sem:

* **Kabeláž**

– kroucená dvojlinka, koaxiální či optický kabel

* **Zásuvky RJ45**

– slouží k připojení několika zařízení do sítě, uschovává kabel bezpečně za krytkou a umožňuje vést kabeláž např. ve zdi

* **Patch panely**

– Propojovací panel s několika zásuvkami RJ45

* **Racky**

– Rozvodná skříň; ukládá jak pasivní, tak aktivní prvky sítě

# Konfigurace prvků sítě

## Opakovač

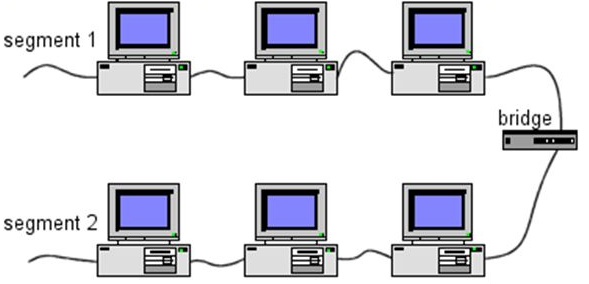
Instalace a konfigurace opakovače je vesměs jednoduchá. Opakovač totiž není ve své podstatě nic jiného než obousměrný zesilovač. Používáme jej pouze jako prostředek pro zvětšení vzdálenosti, kterou jsme schopni v lokální síti obsáhnout. Nedisponuje žádnou vnitřní konfigurací.

## Rozbočovač

Rozbočovač plní jedinou funkci a to, že větví přenášený signál a tím umožňuje rozšiřování sítě o další pracovní stanice. Vše, co mu přijde na jeho vstupy, ihned odesílá na všechny výstupy. Bohužel, většinu rozbočovačů nelze konfigurovat a signál na vstupu tedy odesílá na všechny výstupy i přes to, že se cílové zařízení nemusí na straně výstupu nacházet. U rozbočovačů je rozhodujícím parametrem počet portů.

## Most

Mosty pracují na rozdíl od opakovačů na zcela jiném principu a jsou používány pro spojení dvou různých lokálních sítí. U mostu je důležité správně nastavit masky obou podsítí a dodržet unikátnost MAC adres.



Obrázek ‑ (dvě sítě propojené mostem)

## Směrovač

Směrovač pracuje na obdobném principu jako most, s tím rozdílem, že využívá informací ze síťové vrstvy. Směrovač tedy dokáže přesně a efektivně předat data druhé sítí tak, aby ji nezahltil, a proto se uplatňuje při propojení komplexnějších topologií sítě. Narozdíl od mostu má navíc adresu sítě ve své konfiguraci.

## Přepínač

Jedná se o chytřejší rozbočovač. K předávání dat používá MAC adres k určení příjemce a nezahlcuje tak všechny své výstupy. Switch nemusíme nijak konfigurovat, jelikož znalost sítě získá monitorováním odchozích a příchozích datagramů.

## Brána

Používá se k propojení dvou různých sítí pracujících pod různými protokoly. Obvykle kombinuje software a hardware k dosažení daného převodu. Jedná se prakticky o chytřejší most, který operuje na síťové úrovni namísto linkové.

# Připojení k internetu

## Síť Internet

Celosvětový systém navzájem propojených počítačových sítí, které mezi sebou komunikují přes protokol TPC/IP. Každý počítač má svojí unikátní IP adresu, avšak k lepšímu zapamatování se používají domény přes protokol DNS.

## Typy připojení

Existuje několik způsobů, jak se k sítí internet připojit. Každý typ se liší řadou parametrů, jako například maximální rychlostí, odezvou, cenou a průtokem dat. Nejzákladnějšími typy bývají drátová připojení, bezdrátová připojení a mobilní připojení.

### Drátové připojení

Je realizováno kabeláží. Mezi hlavní výhody patří jeho stabilita a vysoký průtok dat. Způsoby, jakými lze navázat spojení jsou (seřazeno podle dostupnosti sestupně):

* ADSL/VDSL (telefonní kabely)
* CATV/IPTV (přes kabelovou televizi)
* Ethernet (kroucená dvojlinka)
* Optická síť

Nejrychlejším připojením je přes optickou síť, která dosahuje rychlostí až 10Gbps. Takové připojení však není ve všech oblastech dostupné. Hned druhým nejrychlejším bývá připojení přes Ethernet, s rychlostí až 1Gbps. Dnes už ve městech a některých vesnicích není problém se k takové síti připojit. Pokud se ovšem k Ethernetu připojit nemůžete, nebo vám bohatě stačí levnější varianta, máte pravděpodobně ADSL/VDSL o rychlosti maximálně 100Mbps.

### Bezdrátové připojení

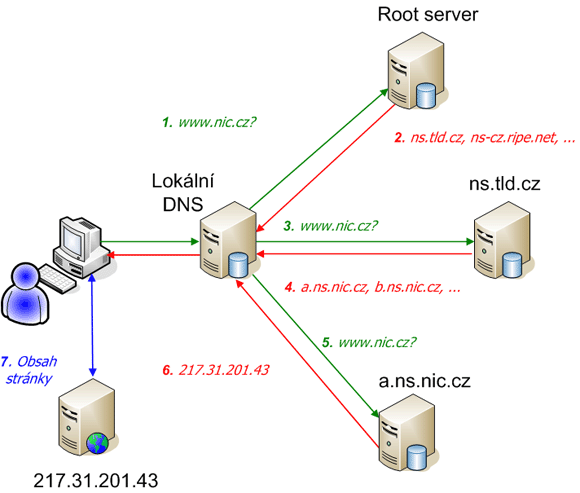
Značeno jako Wi-Fi nebo anténové připojení. Výhodou je dostačující rychlost   
a dobrá dostupnost v horších lokalitách. Nevýhodou je vyšší latence, možné výpadky při horších povětrnostních podmínkách a vyšší pořizovací náklady např. za techniku. Rychlost se pohybuje v řádu desítek megabitů za sekundu.

### Mobilní připojení

V České republice málo rozšířené. Dnes se tento typ připojený rozlišuje na připojení přes mobil (tethering) a připojení přes modem. Ze všech možných způsobů připojení je tento nejhorší. Dosahuje pomalých rychlostí (při horším pokrytí) a vysoké latence. Je bráno spíše jako poslední záchranou.

## DNS

Slouží k překladu doménových adres na adresy IP. Všechny uzly sítě používají ke komunikaci právě IP adresy, které jsou ovšem těžce zapamatovatelné. Proto vznikly tzv. domény, které reprezentují právě jednu unikátní IP adresu ve formátu názvů či slov.



Obrázek ‑ (příklad překladu domény)

Tento proces tak usnadňuje celkovou práci v síti Internet, jelikož bez DNS bychom si museli k navštívení libovolného serveru pamatovat číselnou formu celé IP adresy.

# Wi-Fi

## Charakteristika

Jedná se o bezdrátovou technologii operující v pásmu 2.4 a 5 GHz založenou na protokolu IEEE 802.11. Používá se pro bezdrátové připojení jednotlivých zařízení a pro přenos signálu v rámci sítě LAN. Wi-Fi je ideální pro stavbu sítě bez nutnosti kabeláže, a protože se jedná o technologii, která využívá bezlicenční frekvenční pásmo, může Wi-Fi síť využívat kdokoliv.

## Bezpečnost

Většina moderních směrovačů je dnes vybavena technologií Wi-Fi, ale ne vždy chceme umožnit úplně komukoliv se připojit k naší síti. Proto jsou směrovače vybaveny různými protokoly, které zamezují v přístupu neoprávněných zařízení do naší sítě a šifrují datovou komunikaci.

### WEP (Wired Equivalent Privacy)

Je nejstarším protokolem pro zabezpečení bezdrátových sítí. Umožňoval heslovanou i neheslovanou autentizaci. Dnes se však v praxi nepoužívá, jelikož bylo v protokolu odhaleno několik kritických bezpečnostních chyb. Díky jeho prolomení však vzniklo několik lepších variant.

### WPA (Wi-Fi Protected Access)

Byl vytvořen jako náhrada za prolomený protokol WEP. Disponoval větším, 128bitovým šifrovacím klíčem a kontrolou integrity dat. Navzdory prodloužení klíčů se však i tento protokol podařilo prolomit, ze stejných důvodů jako protokol WEP.

Má dva módy autentizace:

* WPA-Personal (WPA-PSK) – Jedno sdílené heslo
* WPA-Enterprise – Uživatelé s hesly

### WPA2

Druhá verze výše zmíněného protokolu obohacená o nový algoritmus založený na šifrovacím standardu AES, která je dodnes považována za zcela bezpečnou. Je základním vybavením všech certifikovaných směrovačů.

### WPA3

Třetí verze protokolu WPA, která byla poprvé představena v roce 2018. Disponuje větším, 192bitovým šifrovacím klíčem a řeší problémy předešlé verze WPA2.

# Sdílení v síti

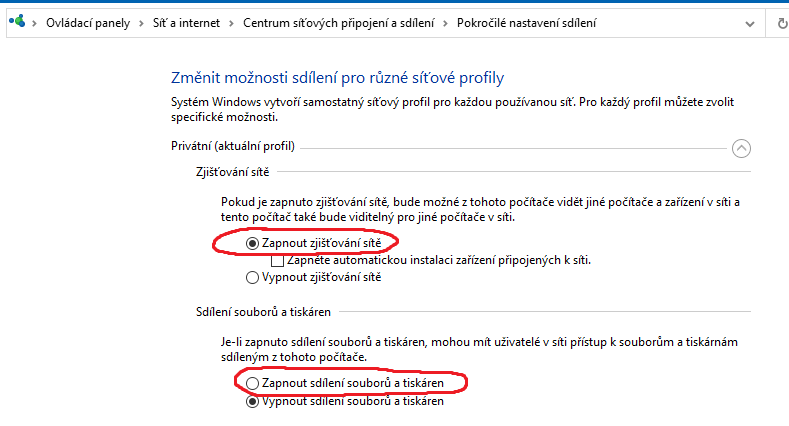
V dnešní moderní síti je možné sdílet jak jednotlivá zařízení (tiskárny, fax, NAS), tak například i systémové soubory prostřednictvím nastavení operačního systému. Celý nápad sdílení dat v síti přišel s nástupem rozšířeného internetu (IoT). Toho se hojně využívá například ve firemních sítích, ale výjimkou nejsou ani sítě domácí.

## Souborový systém

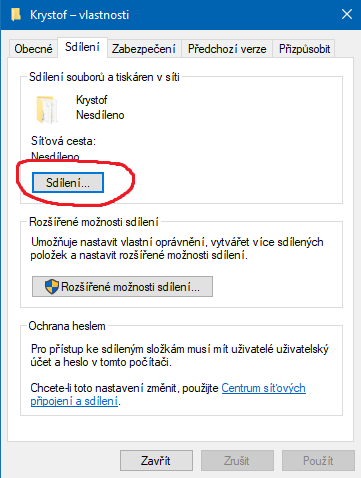
Sdílení souborové systému může být provedeno dvěma způsoby: sdílení přes operační systém (např. sdílení složek v systému Windows), nebo sdílení přes fyzické datové úložiště (NAS).

### Sdílení složek

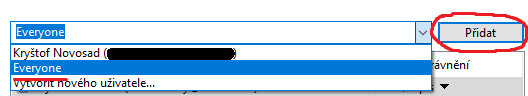
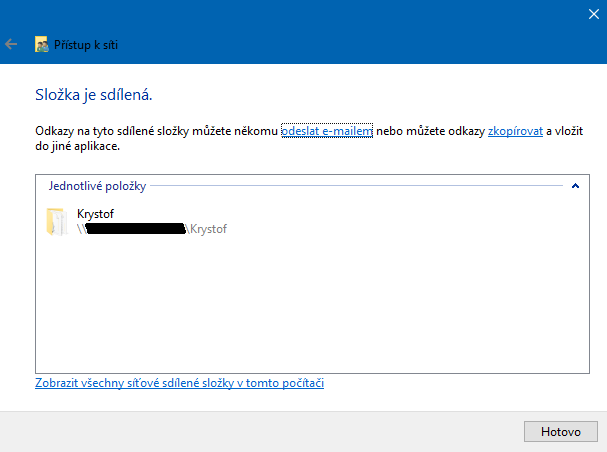
K sdílení složek v operačním systému Windows slouží buď lokální síť, nebo cloudové úložiště OneDrive. Pro zlehčení si ukážeme postup pro sdílení v lokální síti.

Prvním krokem je povolit sdílení složek v ovládacích panelech. Druhým krokem je vybrat možnost sdílení ve vlastnostech souboru. Třetím krokem přidáme požadovanou skupinu a následně potvrdíme.

Obrázek ‑ (krok 1)



Obrázek ‑ (krok 2)



Obrázek ‑ (krok 4)

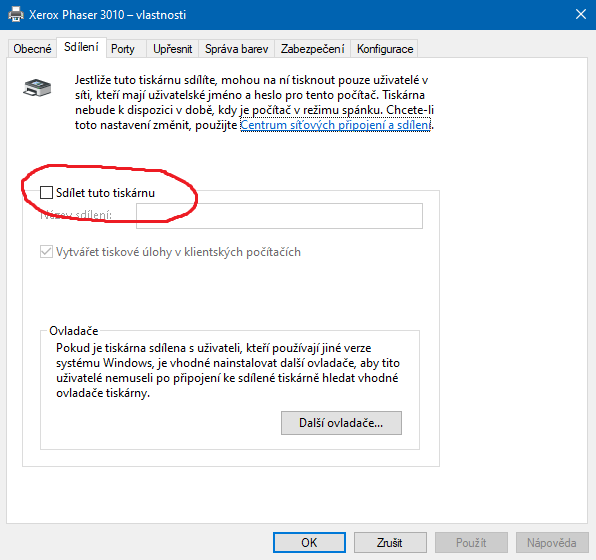
Obrázek ‑ (krok 3)

### Datové úložiště

Slouží jako souborový systém připojený k lokální síti. Můžeme k němu přistoupit jak ze sítě, tak i vzdáleným přístupem. Většina výrobců nabízí několik funkcí navíc jako webový klient, či podporu RAID.

Obrázek ‑

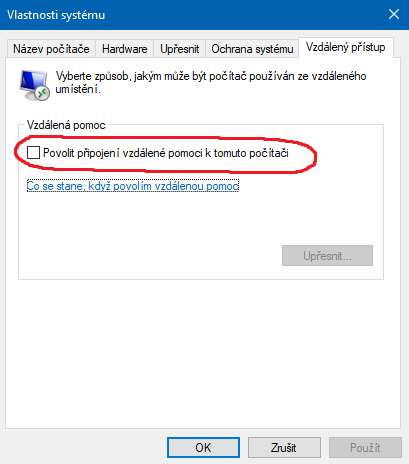
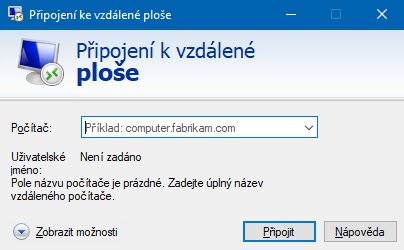
## Tiskárny, fax

Postup pro sdílení tiskáren v operačním systému Windows je obdobný jako postup pro sdílení složek v síti. Ve vlastnostech tiskárny stačí zvolit možnost sdílení.

Obrázek ‑

## Vzdálená správa

Operační systém má vestavěnou podporu vzdálené správy skrze možnost technologie vzdálené plochy. V nastavení systému stačí povolit vzdálený přístup a skrze program Připojení ke vzdálené ploše se můžete k systému připojit.



Obrázek ‑

Obrázek ‑

# Bezpečnost

Před nevyžádaným přístupem či dokonce kybernetickým útokem je dobré chránit naši síť bezpečnostními pravidly a aktivním antivirovým programem. Zabezpečení zahrnuje oprávnění přístupu k datům a zařízením v síti, popřípadě autentizaci uživatelů.

## Firewall

Zabezpečení sítě začíná ověřením, obyčejně s uživatelským jménem a heslem. Následně uživateli nastavíme, ke kterým službám bude mít přístup a musíme zabránit veškerému škodlivému softwaru v průniku do naší sítě. O tohle vše se stará software zvaný Firewall. Ten může být nainstalovaný jak na všech zařízeních v síti, tak na hlavním přístupovém bodu sítě.

## Možné hrozby

Pokud nebudeme dbát na zabezpečení sítě, může se stát, že útočník provede řadu útoků, díky kterým může vzdáleně odposlouchávat či dokonce spouštět škodlivý kód na všech zařízeních sítě. Tyto útoky se dělí na pasivní a aktivní, podle toho, dochází-li ke spouštění škodlivého kódu.

Pasivní útoky:

* Sken portů
* Odposlouchávání

Aktivní útoky:

* Spouštění kódu (RCE)
* Odepření služby (DDOS)
* Útok prostředníka (MITM)
* Trojské koně a červi

# Diagnostika

Diagnostiku sítě provádíme v případě, že naše síť nepracuje podle našich představ nebo některá zařízení nepracují vůbec a chceme tedy tyto problémy vyřešit. K vyřešení problémů v síti máme v dostupnosti několik nástrojů.

## Softwarové nástroje

Softwarové nástroje pro diagnostiku použijeme v případě, kdy nefunguje připojení na síťové úrovni, tj. nedaří-li se nám například připojit k síti Internet nebo nefunguje-li sdílená tiskárna kvůli špatné konfiguraci. Pro takové problémy jsou dostupné nástroje pracující se servisním protokolem ICMP, či nástroje pro odposlech rámcové komunikace.

### Ping

Obsah obrázku text

Popis byl vytvořen automatickyZákladní nástroj pro testovaní dostupnosti služby či zařízení. Pro zjištění funkčnosti spojení zasílá IP datagramy a čeká na odpověď příjemce ve formě ICMP zprávy. Nakonec změří časovou odezvu mezi odesláním požadavku a příjmem odpovědi.

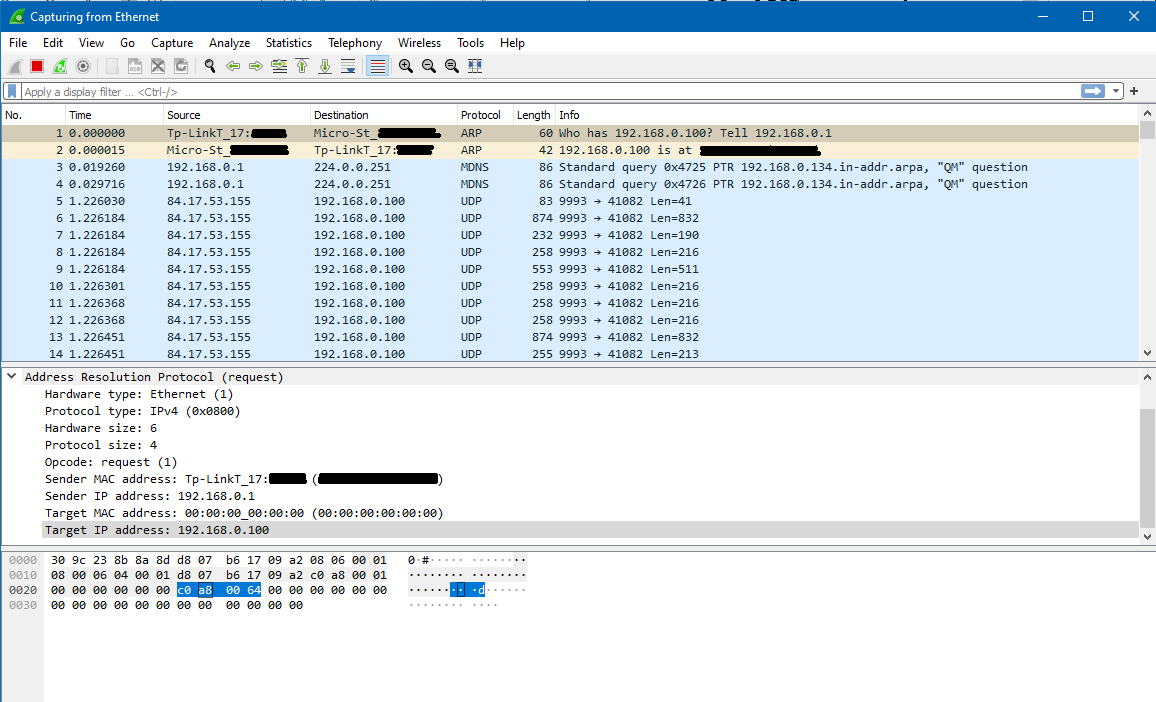
Obrázek ‑

### Netcat

Notoricky známý nástroj pro zápis a čtení skrze protokol TCP či UDP. Jeho využití spočívá v testování funkčnosti dané služby na určitém portu. Známý je ale především kvůli jeho zneužití k vytváření zadních vrátek do počítačové sítě.

### Wireshark

Velice užitečný nástroj sloužící k odposlechu a analýze provozu v počítačové síti. Využívá se nejen jako diagnostický nástroj, ale také i pro studijní či vývojářské účely. Výhodou oproti předchozím programům je přívětivé grafické rozhraní.



Obrázek ‑ (výstup programu Wireshark)

## Hardwarové nástroje

Hardwarovými nástroji se rozumí nástroje pro testování především kabeláže sítě. Máme-li problém, který nelze vyřešit softwarovými nástroji, nebo se zařízení nejeví jako připojené, měli bychom prověřit funkčnost a správnost fyzického zapojení.

Obrázek ‑ (zařízení určené k testování kroucené dvojlinky)

# Závěr

Cílem této práce bylo uvést a objasnit problematiku počátečních a malých počítačových sítí. Závěrem bych rád poděkoval panu učiteli Petru Novotnému, který nás předmětem Počítačové sítě po celou dobu doprovázel a vše potřebné nás patřičně naučil.

# Rejstřík

Adresát, 5, 12, 16

Adresný oběžník, 10, 13, 16

Algoritmus, 17

Antivirus, 28

ARP, 9

Bezdrátové, 22

Brána, 19, 21

Broadcast, 5

Datagram, 11, 15, 16

DDOS, 29

DHCP, 17, 18

Diagnostika, 29

DNS, 21, 22, 23

Doména, 21, 22

EGP, 17

Ethernet, 5, 12, 13, 22

FDDI, 13

Filtrace, 15

Firewall, 29

FTP, 8

Handshake, 10

Hardware, 19, 21, 31

Hrozba, 29

HTTP, 8

ICMP, 9, 10, 29, 30

IGMP, 10

IGP, 17

Integrita, 11, 24

Internet, 8, 9, 10, 13, 14, 15, 21, 23, 24, 29

Intranet, 14

IP, 8, 9, 10, 13, 14, 15, 16, 17, 18, 21, 22, 23, 30

IP adresa, 9, 13, 14, 16, 17, 18, 21, 22, 23

IPv4, 9, 13

IPv6, 9, 13

Kabeláž, 7, 19, 20, 22, 23, 31

Klient, 10, 17

Koaxiální kabel, 12

Konfigurace, 17, 20, 21, 29

Kontrolní součet, 11

Kroucená dvojlinka, 12, 20, 22

LAN, 12, 23

Linková, 12, 21

LSP, 16

Metrika, 16

MITM, 29

Most, 12, 19, 20, 21

Multicast, 10, 13

NAT, 14

Netcat, 30

OneDrive, 25

Opakovač, 6, 12, 19, 20

Paket, 8, 9, 10, 15

Payload, 9

Ping, 30

Port, 10, 12, 15, 20, 29, 30

Protokol, 8, 9, 10, 11, 12, 16, 17, 21, 23, 24, 30

Proud, 10

Předávání, 5, 8, 15, 19, 21

Přenos, 8, 10, 12

Přepínač, 12, 19, 21

Příjemce, 10, 11, 12, 21, 30

RAID, 26

Rámec, 12, 13, 29

RCE, 29

Rozbočovač, 6, 19, 20

Rozhraní, 8, 12, 16, 30

RVP, 16

Sdílení, 24, 25, 27

Sekvence, 10

Server, 10, 17, 18, 23

Signál, 6, 19, 20

Síť, 5, 6, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31

Síťová karta, 12

Síťová maska, 14

Služba, 29, 30

Směrovač, 15, 16, 19, 21, 23, 24

Směrování, 8, 15, 16

Software, 19, 21, 29, 31

Spojení, 8, 10, 11, 20, 22, 30

Standard, 8, 14

Systém, 14, 15, 17, 21, 24, 25, 26, 27

Šifrování, 23

TCP, 8, 9, 10, 11, 15, 17, 30

TCP/IP, 8, 9, 10, 17

Token, 5

Topologie, 5, 6, 7

UDP, 8, 11, 30

Útok, 28, 29

Uzel, 5, 8, 12, 15, 19, 22

Uživatel, 29

Vzdálený přístup, 26, 27

webový klient, 26

WEP, 24

Wi-Fi, 22, 23, 24

Windows, 24, 25, 27

Wireshark, 30

WPA, 24

WPA2, 24

WPA3, 24

Zápůjčka, 17, 18

Zařízení, 5, 6, 7, 9, 10, 13, 14, 15, 16, 17, 19, 20, 23, 24, 29, 30, 31