ZÁKLADY SÍTÍ

Co-funded by the
Erasmus+ Programme
of the European Union

Spis treści

1. Úvod

Co je to kybernetická bezpečnost? Co to je a proč je to tak důležité? V době, kdy jsou technologie všude, nesmíme v tomto digitálně pohodlném světě zapomínat na naši kybernetickou bezpečnost. Na internetu nejsme neviditelní a naše aktivity za sebou zanechávají různé stopy nebo informace. Prakticky každý den využíváme možnosti internetu, ať už na sociálních sítích, fórech nebo nejrůznějších prodejních platformách. Kde sdílíme své osobní a finanční údaje, posíláme čísla účtů, platíme kartami, telefony a různými digitálními měnami.

Jaká jsou rizika na internetu? Krádež identity, klonování platebních karet, ztráta soukromých souborů/dat, phishing bankovních účtů, podvody. V životě dbáme na svou bezpečnost, hlídáme se, kupujeme léky, předvídáme. Proč to neděláme online? Kolik z vás má v počítači nainstalovaný antivirový program? Všechny? A v telefonu? Je tu někdo? Zde bychom si měli položit otázku, zda opravdu trávíme většinu času na webu před obrazovkou počítače nebo třeba na telefonu?

Podle různých statistik již více než 70 % veškerého webového provozu pochází z mobilních zařízení, zejména chytrých telefonů. Koupili jste si někdy něco na telefonu nebo jste ho použili k zadání fakturačních údajů při různých transakcích? Správně připravená zařízení pro web jsou jen polovinou úspěchu; druhým faktorem, který zaručuje relativní bezpečnost, je informovanost uživatele internetu. Můžete být nejlépe připraveni a mít nejlepší vybavení, ale bez správného know-how si můžete zadělat na spoustu zbytečných a nepříjemných problémů.

1.1. Komunikace v síti

Dnes si už jen málokdo dokáže představit svět kolem nás bez počítačů, telefonů a dalších zařízení, a mnoho dalších zařízení spotřební elektroniky. Tato zařízení nám nabízejí mnoho funkcí a schopnosti, které nám usnadňují každodenní činnosti a pomáhají nám při práci a studiu. Mnoho z těchto funkcí by bylo zbytečných bez důležitého aspektu, kterým je schopnost rychlé komunikace a výměny dat.

Díky této možnosti jsme schopni během několika vteřin kontaktovat přátele, kteří se právě nacházejí na druhém konci světa, během několika vteřin zaplatit účet za elektřinu nebo si koupit nové tenisky, aniž bychom opustili domov. Samozřejmě zde nebudu rozebírat všechny výhody přístupu k internetu, protože to není hlavní téma kurzu, ale doufám, že si uvědomíte, že vše, co můžete dělat s počítačem nebo chytrým telefonem, má jedno společné. Tímto společným jmenovatelem je, nebo spíše je, počítačová síť, která vznikla před několika desítkami let a je základem dnešního internetu.

Co je dnes internet? Není to nic jiného než počítačová síť, a to velmi složitá, s mnoha připojenými zařízeními, ale stále se jedná o síť.

2. Základní pojmy

Definujme základní pojmy týkající se počítačových sítí:

Počítačová síť - soubor zařízení, jako jsou počítače, tiskárny, telefony a televizory, která jsou vzájemně propojena za účelem výměny dat. K propojení zařízení se používá přenosové médium a k přenosu dat komunikační protokol.

Adresa IPv4 - Jedná se o 32bitové číslo, které se pro snadnější použití zadává v desítkové soustavě (např. 192.168.31.190) a slouží k identifikaci zařízení a adresních údajů v síti.

HOST - Zařízení s adresou IP, které je zdrojem nebo příjemcem dat odesílaných po síti, tj. přijímá data od jiných zařízení nebo tato data odesílá. Termín hostitel se někdy používá zaměnitelně s termínem koncové zařízení, protože obvykle označuje počítač, tablet nebo chytrý telefon, tj. zařízení, se kterým je uživatel sítě v přímém kontaktu.

Klient - Zařízení, přesněji jeho software, využívá služby poskytované serverem. Nejběžnějším klientem je dnes webový prohlížeč, který uživateli umožňuje prohlížet obsah webových stránek hostovaných webovým serverem. Příkladem klienta může být také FileZilla, která umožňuje výměnu souborů přes Internet, a nejrůznější e-mailový software usnadňující používání pošty. Herní konzole nebo chytré telefony budou také klienty, pokud jsou samozřejmě připojeny k internetu.

Server - Jedná se o počítač s nainstalovaným specializovaným softwarem, který podporuje ostatní počítače. Služba, kterou může server poskytovat, je například webová stránka, e-mail nebo zdroj souborů. Serverem může být jakýkoli počítač, na kterém je takový software nainstalován a nakonfigurován, například APACHE, který se používá ke správě a sdílení webových stránek, nebo MySQL, což je systém pro správu databází. Server je obvykle vyhrazený počítač s vysokým výpočetním výkonem, který je schopen zpracovávat více připojení a dotazů současně.

Přenosové médium - Jinými slovy médium, které je síťovým prvkem, jehož prostřednictvím spolu zařízení komunikují a vyměňují si data. Tímto médiem může být měděný kabel, optický kabel a rádiové vlny (WiFi).

Komunikační protokol - Jedná se o způsob nebo jazyk komunikace a výměny dat mezi zařízeními, který definuje pravidla a zásady této komunikace.

Internet - Jedná se o soubor vzájemně propojených rozsáhlých sítí, které tvoří globální počítačovou síť. Počátky internetu sahají až k vytvoření sítě ARPANET na konci 60. let 20. století a první internetové připojení v Polsku bylo spuštěno v září 1990. Mnozí považují internet za soubor stránek k prohlížení, ale není tomu tak, protože internet je soubor mnoha rozsáhlých sítí rozprostřených po celém světě a webové stránky jsou specifické síťové služby.

Intranet - jedná se o soukromou interní síť, která používá stejné komunikační standardy (protokoly) jako internet, ale přístup k ní mají pouze oprávnění uživatelé, například zaměstnanci dané společnosti. Ve většině případů je přístup k intranetu, tedy k interní podnikové síti, zajištěn prostřednictvím webových stránek, takže se říká, že komunikace probíhá podle stejných standardů jako na internetu.

Extranet - je rozsáhlá odrůda intranetu, která umožňuje přístup ke svým zdrojům nejen zaměstnancům dané společnosti, ale i dalším uživatelům.

DNS (Domain Name System) - síťová služba, která mění lidsky čitelný název, tzv. mnemotechnické jméno, na IP adresu zařízení v síti. Jedná se o základní službu internetu, která mění adresy webových stránek na odpovídající IP adresy serverů, kde jsou tyto stránky uloženy, např. změna internetové adresy onet.pl na IP adresu 214.180.141.140.

DHCP (Dynamic Host Configuration Protocol) - je automatický konfigurační protokol, který hostiteli přiřazuje IP adresu, masku podsítě nebo adresu výchozí brány. Jedná se o nejběžnější metodu přidělování IP adres počítačům v síti, protože nevyžaduje ruční konfiguraci IP adres v každém počítači.

3. Datové jednotky v sítích

Základní jednotkou používanou ve výpočetní technice k ukládání dat je 1 bit [b].

V počítačových sítích se naopak jednotka bitů za sekundu používá k určení šířky pásma (rychlosti) sítě, která se vyjadřuje v b/s nebo bps (bits per second).

Je zřejmé, že 1 bit/s je malá hodnota, takže násobky této jednotky pro označení velikosti souboru, kapacity disku nebo operační paměti, bez ohledu na to, zda se jedná o bity nebo bajty, jsou tyto násobky:

1. kilobit [Kb],

2. Megabit [Mb],

3. gigabit [Gb],

4. Terabit [Tb].

Protože v počítačové síti se na rozdíl od velikosti souboru nebo kapacity disku, kde se místo bitů[b] používají bajty[B], používá jednotka v bitech, vzniká zde problém s konverzí, tj. převodem jednotek.

1 bajt[B] se rovná 8 bitům[b] Pokud tedy chceme zjistit velikost souboru v bajtech, musíme počet bajtů vynásobit 8. Chceme-li například vypočítat, kolik megabajtů obsahuje soubor o velikosti 3 megabajty, vynásobíme jeho velikost 8. Výsledek je 24 MB.

3 MB - 8 = 24 MB

Pro inverzní převod, tj. z bitů na bajty, musíme provést inverzní násobení, tj. dělení. Například: soubor o velikosti 40 Mb bude převeden na 5 MB.

40 MB ÷ 8 = 5 Mb

Schopnost převádět jednotky se nejlépe hodí k provádění výpočtů na konkrétních příkladech. Níže jsou popsána dvě řešení.

Příklad 1

Za předpokladu, že šířka pásma našeho připojení je pevně stanovena na 300 Mb/s, vypočítáme, kolik dat stáhneme z internetu za dvě hodiny.

údaje:

Čas: 2 hodiny

Šířka pásma: 300 Mb/s

Vypočítat:

1. Sekundy minut se násobí minutami:

120 minut - 60 sekund = 7200 sekund

2. převedeme jednotku přenosu dat z megabitů na megabajty za sekundu:

300MB/s ÷ 8 = 37,5MB/s

3. vynásobíme propustnost časem:

37,5 MB/s - 7200 sekund = 270000 MB ~ 270 GB

Odpověď na příklad 1: Za dvě hodiny stáhneme 270 GB.

Příklad 2

Vypočítejme dobu potřebnou ke stažení souboru o velikosti 5 GB za předpokladu, že šířka pásma našeho připojení je konstantní a dosahuje 300 Mb/s.

Údaje:

Velikost souboru: 5 GB

Šířka pásma připojení: 300 Mb/s

Vypočítat:

1. Převeďte jednotku přenosu dat z megabitů na megabajty za sekundu:

300 Mb/s ÷ 8 = 37,5 MB/s

2. převést jednotky pro ukládání souborů z gigabajtů na megabajty:

5 GB => 5120 MB

3 Vydělte velikost souboru propustností:

5120 MB ÷ 37,5 MB/s = 136,5 sekundy ~ 2 minuty 16 sekund

Odpověď na příklad 2: Soubor o velikosti 5 GB stáhneme přes připojení 300 Mb/s přibližně za 2 minuty a 16 sekund.

ÚKOLY TYPU "UDĚLEJ SI SÁM

Vypočítejte, kdy lze obsah disku DVD (4,7 GB) přenést prostřednictvím linky o rychlosti 50 Mb/s.

Vypočítejte, kolik dat lze přenést přes připojení 500 Mb/s za 15 minut.

4. Přenosová média

Přenosová média jsou v souvislosti s počítačovými sítěmi nesmírně důležitou otázkou. Důvodů je mnoho, nejdůležitějším z nich je, že volba správného média je základem a zárukou normálního a efektivního fungování počítačových sítí.

4.1. Medium

Jinými slovy médium, které je síťovým prvkem, jehož prostřednictvím spolu zařízení komunikují a vyměňují si data. Tímto médiem může být měděný kabel, optický kabel a rádiové vlny (Wi-Fi).

ROZDĚLENÍ PŘENOSOVÝCH MÉDIÍ

TYP	**MĚDĚNÝ KABEL**		**MĚDĚNÝ KABEL**		**OPTICKÝ KABEL**		**OPTICKÝ KABEL**	
TYP	KOAXIÁLNÍ	KABEL	KROUCENÁ	DVOJLINKA	JEDNOVIDOVÉ OPTICKÉ	VLÁKNO	MNOHOVIDOVÉ OPTICKÉ	VLÁKNO

4.2. Koaxiální kabel

1. Konstrukce:

- měděné jádro,

- plastová izolace,

- měděný štít,

- Vnější obal.

Končí konektorem BNC. Někdy se na konci koaxiálního kabelu nachází také tzv. terminátor BNC, jehož úkolem je odstranit odrazy od signálu přenášeného kabelem.

2 typy:

Existují dva typy koaxiálních kabelů: tenký koaxiální kabel a silný koaxiální kabel. Rozdíly mezi oběma druhy jsou následující:

TYP	TLOUŠŤKA	DÉLKA MAX	SÍŤOVÝ STANDARD	MAXIMÁLNÍ KAPACITA
TENKÝ	5 mm	185 M	10base-2	10 Mb/s
TLUSTÝ	10 mm	500 M	10base-5	10 Mb/s

Stojí za zmínku, že koaxiální kabel se již při výstavbě nových sítí nepoužívá. Bylo nahrazeno účinnějšími řešeními, jako je kroucená dvojlinka a optické vlákno.

4.3. Kroucená dvojlinka

1. Konstrukce:

- 8 měděných vodičů spletených do 4 párů,

- Vnější obal.

Je zakončen konektorem RJ45, známým také jako 8P8C.

V závislosti na typu krouceného páru jsou k dispozici také ochranné fólie a stínění, které chrání kabel před nežádoucími prvky, jež mohou ovlivnit přenos dat, například elektromagnetickými vlnami.

2. Typy kroucené dvojlinky:

- UTP - nestíněná kroucená dvojlinka,

- FTP - stíněný kroucený pár,

- STP - stíněný kabel s kroucenou dvojlinkou.

V praxi se můžeme setkat s různými variantami výše uvedených typů, z nichž nejdůležitější jsou:

- U/UTP - nestíněná kroucená dvojlinka

- F/UTP - lanko

- U/FTP - kroucený pár s každým párem v samostatném stínění,

- F/UTP - kroucená dvojlinka s krouceným párem s každým párem v samostatné fólii a navíc celý svazek také ve fólii.

- S/FTP - kroucený pár s každým párem v samostatném fóliovém stínění a navíc celý svazek v síťovém stínění.

Nejoblíbenějším materiálem používaným pro stínění kroucené dvojlinky je polyesterová fólie pokrytá vrstvou hliníku a mědi.

Typ krouceného kabelu, který je třeba zvolit pro konstrukci sítě, závisí na místě, kde je síť provozována, a na úrovni elektromagnetického rušení v dané lokalitě. V malých lokálních sítích, ať už ve škole nebo v domácnosti, se nejčastěji používá základní typ UTP, protože je pro tak malou síť dostačující a je také nejlevnějším typem krouceného páru.

3. Kategorie kroucených párů

Kromě typů kroucené dvojlinky existují třídy, které mimo jiné definují síťové standardy, v nichž je lze použít.

KATEGORIE	**SÍŤOVÝ STANDARD**
3	Ethernet 10Base-T
5/5e	FastEthernet 100Base-TX GigabitEthernet 1000Base-T
6	GigabitEthernet 1000Base-T
6a	10-GigabitEthernet 10GBase-T
7	10-GigabitEthernet 10GBase-T

4. Technické parametry

- Útlum signálu - je poměr výstupního a vstupního napětí, vyjádřený jako v decibelech [dB].

- Šíření signálu - Jedná se o rychlost elektrického impulsu vzhledem k rychlosti světla, vyjádřenou v procentech [%].

- Odpor - Jedná se o odpor vodiče vůči proudu vyjádřený v ohmech [Ω].

- Near Crosstalk (NEXT) - jedná se o rušení v dané sadě způsobené přenosem dat v sousední sadě.

Z hlediska instalace je důležitým parametrem také poloměr ohybu kabelu, což je u většiny řešení čtyřnásobek jeho vnějšího průměru.

4.4. Optický kabel

Zcela odlišný od dříve popsaného přenosového média je optický kabel, a to díky odlišným materiálům použitým na jádro. V případě koaxiálního kabelu a krouceného páru je jádro nebo vodič měděný, zatímco v případě optických kabelů se jedná o skleněná vlákna. Použití skleněných vláken jako základního stavebního materiálu vyžaduje také různé typy přenosových signálů. V případě měděných médií je to elektrický proud, v případě optických vláken světlo, nejčastěji infračervené.

1. Struktura:

- Jádro - má vyšší index lomu,

- Povlak - má nižší index lomu,

- Povlak na ochranu pláště,

- Vyztužující nátěr pro ochranu jádra při montáži,

- Vnější povrchová úprava.

Najdeme zde také následující typy konektorů:

- LC

- MT - RJ

- MU

- DIN

2. Typy optických vláken:

Stejně jako u mědi a optických vláken můžeme diskutovat o různých typech tohoto média. Nejběžnější dělení je na jednovidová a mnohovidová optická vlákna.

V případě jednovidových optických vláken prochází skleněným jádrem pouze jeden paprsek světla, což vede k tzv. jevu rozmazání signálu, tj. útlumu signálu.

Tento typ optických vláken umožňuje přenášet signály na velké vzdálenosti bez zesilovacího zařízení.

V mnohovidových optických vláknech je větší část paprsku přenášena jádrem, což vede k vyššímu stupni rozmazání signálu ve srovnání s jednovidovými optickými vlákny. Je to proto, že každý paprsek vyslaný jádrem musí projít jinou cestou od odesílatele k přijímači.

Proto se mnohovidová vlákna používají na krátké vzdálenosti do několika kilometrů.

Dalším rozdílem mezi jednovidovým a mnohovidovým optickým vláknem je průměr použitého jádra. U jednovidových optických vláken je to 8 až 10 mikrometrů [µm], zatímco u mnohovidových optických vláken je to 50 nebo 62,5 mikrometru.

4.5. Shrnutí

Měděné sítě

VÝHODY	NEVÝHODY
Levně koupit	**Krátké vzdálenosti mezi uzly sítě**
Jednoduchá diagnostika a oprava závad	**Náchylnost k elektromagnetickému rušení**
Bezproblémová montáž a instalace	**Pomalejší než optická vlákna**

Optická média

VÝHODY	NEVÝHODY
Rozhodně rychleji	**Složitá montáž a instalace**
Prakticky imunní vůči elektromagnetickému rušení	**Rozhodně dražší nákup kvůli potřebnému vybavení**
Přenáší data na velké vzdálenosti	**Rozmazání signálu**

Bezdrátová média

Pro bezdrátová média se používá několik řešení, ale pouze jedno z nich, rádiové vlny, se skutečně používá. Toto médium využívá k přenosu dat známá technologie Wi-Fi.

Rádiové vlny jsou elektromagnetické záření v rozsahu frekvencí od 3 Hz do přibližně 3 THz. Zdroje rádiových vln mohou být přírodní nebo umělé, například vysílání mobilních rádiových stanic. Jejich hlavním účelem je přenášet informace a v případě telekomunikací data. Existuje několik typů rádiových vln, pro přenos dat se používají dlouhé, střední, krátké a ultrakrátké vlny.

Při diskusi o rádiových vlnách je třeba zmínit standardy používané v bezdrátových sítích. Jsou důležité pro výběr správného směrovače Wi-Fi.

STANDARD	FREKVENCE	MAXIMÁLNÍ PROPUSTNOST
802.11a	5 GHz	54 Mb/s
802.11b	2,4 GHz	11 Mb/s
802.11g	2,4 GHz	54 Mb/s
802.11n	2,4 GHz | 5 GHz	150 Mb/s | 600 Mb/s
802.11ac	5 GHz	Několik Gb/s

5. Typy počítačových sítí

Počítačové sítě lze dělit různými způsoby s ohledem na různá kritéria. Základním standardem pro dělení sítí je dělení podle oblasti, ve které síť působí, takže dělení podle oblasti (pokrytí) sítě je následující:

Lokální síť (LAN) - síť pokrývající nejmenší oblast, například ateliér, školu nebo několik školních budov. Pokud používáte více počítačů nebo jeden počítač, objeví se u vás doma také síť LAN.

Metropolitní síť (MAN - Metropolitan Area Network) - síť pokrývající oblast větší než jedna místnost nebo budova. Síť MAN se rozkládá na území města nebo metropolitní oblasti.

Rozsáhlá síť (WAN - Wide Area Network) - rozsáhlá síť kombinující sítě LAN a MAN.

Kromě regionálních norem lze sítě dělit také podle jejich architektury. Rozlišujeme sítě s architekturou klient-server a peer-to-peer.

V architektuře klient-server existuje alespoň jeden počítač, který slouží uživatelům sítě (jedná se o servery), a mnoho počítačů, které využívají služeb serveru (jedná se o klienty). Architekturu klient-server používáme při procházení webu, odesílání e-mailů nebo práci s databázemi.

Jiná situace je u architektury peer-to-peer, známé také jako Peer2Peer (P2P).

V tomto případě službu neposkytuje jeden nebo více počítačů, ale více počítačů se stejnými právy. Každý počítač v síti může současně používat a sdílet prostředky. Při používání služeb pro sdílení souborů, jako je BitTorrent, používáme architekturu peer-to-peer.

5.1. Topologii sítě

Topologii sítě dělíme na fyzickou, která určuje, jak jsou zařízení navzájem propojena, a logické, které popisují způsob přenosu dat mezi zařízeními. Každá počítačová síť, i ta nejmenší, má fyzickou a logickou topologii, která určuje, jak jsou zařízení navzájem propojena a jak se přenášejí data.

Topologie počítačové sítě

Definuje vztahy mezi zařízeními v síti, spojení mezi nimi a způsob toku dat.

5.2. Fyzické topologie

Fyzické topologie sítí zahrnují:

- Topologie sběrnice (Bus),

- Topologie kruhu (Ring),

- Topologie hvězdy (Star).

Jedná se o základní topologie, které jsou základem pro budování rozšířených hvězdicových a síťových topologií ve velkých sítích.

Fyzická topologie sběrnice

Topologie sběrnice se vyznačuje tím, že všechna zařízení jsou připojena ke společnému přenosovému médiu. Běžným přenosovým médiem v této topologii je koaxiální kabel. Nevýhodou této topologie je nízká propustnost (do 10 Mb/s).

Tato topologie se používá k vytvoření místní sítě. Záměrně zde používám slovo "byl", protože se již běžně nepoužívá. Kromě nízké propustnosti je také velmi náchylný k výpadkům sítě. Když se koaxiální kabel přeruší, přestane fungovat celá síť. Nespornou výhodou této topologie jsou nízké náklady na realizaci, protože není třeba stovek metrů kabelů ani žádného mezilehlého zařízení.

Fyzická topologie kruhu

V kruhové topologii je každé zařízení připojeno ke dvěma sousedním zařízením a tvoří uzavřený kruh. Podobně jako sběrnicová topologie nevyžaduje tato konstrukce velké množství kabelů a dalšího vybavení.

Kromě toho lze použít různá přenosová média, od koaxiálního kabelu přes měděnou kroucenou dvojlinku až po optický kabel. Nevýhodou této topologie je, že přerušení média nebo výpadek jednoho z počítačů může narušit celou síť. Aby se tomu zabránilo, používají se tzv. dvojité kroužky, tj. zdvojnásobení počtu spojení mezi zařízeními. Taková topologie se pak nazývá dvojitá kruhová topologie.

Fyzická topologie hvězdy

V topologii hvězdy jsou zařízení připojena k centrálnímu bodu, tj. přístupovému bodu sítě. Dříve se tento bod používal jako rozbočovač, nyní se používá přepínač. Jedná se o nejběžnější topologii v lokálních sítích, protože se snadno navrhuje, vytváří a škáluje, je odolná proti chybám a snadno se spravuje.

Další výhodou je, že může být vytvořen pomocí různých přenosových médií, jako je měděná kroucená dvojlinka, optický kabel nebo rádiové vlny (WLAN). Významnou nevýhodou však mohou být náklady na výstavbu, protože je zapotřebí další vybavení (přepínače) a mnoho metrů kabelů.

5.3. Logické topologie

Topologie logické sítě zahrnuje:

- peer to peer,

- předat token,

- vícenásobný přístup.

Logická topologie bod-bod

V topologii bod-bod se data přenášejí pouze z jednoho zařízení do druhého. Tato zařízení mohou být vzájemně propojena přímo, např. počítač s přepínačem, nebo nepřímo na velké vzdálenosti pomocí zprostředkujícího zařízení, např. propojením dvou směrovačů vzdálených od sebe několik kilometrů.

V obou případech můžeme hovořit o logických spojeních typu bod-bod. Jedná se o logickou topologii, která se často používá v sítích LAN s fyzickou topologií hvězdy.

Logická topologie s předáváním tokenů

V topologii token passing jsou data síťovým zařízením předávána postupně. Zařízení, které obdrží dávku dat, ji analyzuje, aby zjistilo, zda na ni ukazuje. Pokud data nejsou určena pro něj, předá je sousednímu zařízení. Tímto způsobem všechna zařízení přenášejí data mezi zdrojovým a cílovým zařízením.

Logická topologie vícenásobného přístupu

Topologie s více přístupy (někdy také nazývaná topologie vysílání nebo logická sběrnice) umožňuje zařízením v síti komunikovat prostřednictvím jediného fyzického přenosového média. V počátečních fázích vývoje, kdy se rozbočovače ještě používaly jako přístupové body sítě, se používal hlavně u fyzických topologií sběrnice a hvězdy.

Každé zařízení v této topologii vidí data odeslaná po síti, která jsou odesílána všem zařízením, ale pouze konkrétní zařízení, kterému jsou data adresována, je může interpretovat. Protože zařízení v síti sdílejí společné médium, je nutné zavést mechanismy pro řízení přístupu k tomuto médiu, kterými jsou: CSMA/CD, CSMA/CA a token pass.

Metoda přístupu k propojení (síti)

Metoda CSMA/CD, metoda detekce kolizí, zahrnuje sledování stavu linky. Pokud zařízení, které má zahájit přenos, zjistí, že je linka nečinná, zahájí takový přenos. Pokud během přenosu zjistí, že jiné zařízení v síti také odesílá svá data, přenos se přeruší. Po chvíli přenos zopakujte. Tento mechanismus používají starší verze sítě Ethernet.

CSMA/CA, metoda zamezení kolizí, také zahrnuje sledování stavu linky, ale zjišťuje, že nosná, tj. zařízení, kde je přenosové médium nečinné, začíná vysíláním svého záměru před zahájením přenosu. Tento mechanismus existuje v bezdrátových sítích.

Metoda přenosu pomocí tokenu zahrnuje odeslání speciálního kusu dat zvaného token nebo značka ze zařízení do zařízení, jehož držení iniciuje přenos.

6. Modely vrstev ISO/OSI a TCP/IP

Vzájemná komunikace zařízení v počítačové síti se skládá z několika fází a několika komponent. Každý z nich je stejně důležitý, protože každý plní úkoly potřebné pro správnou komunikaci. Tyto kroky jsou definovány tzv. hierarchickým modelem. Každý, kdo zná vrstevnatý model, ví, že jeho pochopení je základem pro další znalosti a dovednosti v oblasti počítačových sítí.

Existují dva vrstevnaté modely, model protokolu TCP/IP a referenční model ISO/OSI.

Na jedné straně jsou si podobné, na druhé straně každý model komunikuje trochu jinak. Než si však tyto dva modely rozebereme a vysvětlíme rozdíly mezi nimi, řekneme vám proč byste je měli používat, k čemu se používají a jaké jsou výhody jejich používání.

Rozdělení síťového komunikačního procesu do vrstev má mnoho výhod, z nichž nejdůležitější jsou:

- jednodušší definice komunikačních pravidel a zásad (jedná se o komunikační protokoly),

- možnost práce se síťovým hardwarem a softwarem od různých výrobců,

- snazší pochopení možností celého komunikačního procesu,

- schopnost řídit proces komunikace.

Než se data ze zdrojového zařízení dostanou do koncového zařízení, musí urazit dlouhou cestu, během níž jsou nejprve řádně označena, tagována, popsána specifickými informacemi, které umožňují jejich identifikaci, a poté přenášena mezi mnoha zprostředkujícími zařízeními, dokud se nedostanou k příjemci, který je musí následně přeložit.

Bez takového modelu, který rozděluje komunikaci na menší, srozumitelnější a lépe zvládnutelné části, by bylo možné komunikaci a definuje úkoly, které je třeba provést na každé vrstvě, bude obtížné správně řídit síťovou komunikaci, protože množství řešení a technologií vytváří nekontrolovaně velký chaos. Představte si situaci, v níž neexistuje žádná takováto tvorba, žádná pravidla popisující komunikaci, a každý výrobce hardwaru a softwaru vytváří svůj vlastní nezávislý systém.

Samozřejmě, že v řešení jedné společnosti bude komunikace velmi efektivní a rychlá, ale řešení dvou různých společností mohou být vzájemně nekompatibilní. V praxi používáme síťový hardware a software od různých firem, a to díky rozdělení na samostatné vrstvy s pravidly a úkoly popisujícími jejich fungování. Tato pravidla a úkoly jsou pro všechny stejné, ale každá společnost, každý výrobce, ať už hardwaru nebo softwaru, je může implementovat po svém.

Typickým příkladem jsou operační systémy. Někteří uživatelé používají systém Windows, někteří distribuce Linuxu a někteří MacOS. Každý z těchto systémů je jiný a každý z nich provádí webové úlohy jiným způsobem, ale v konečném důsledku v každém z těchto systémů bude webová stránka nebo e-mail vypadat stejně nebo alespoň podobně. Proto jsou některé z nejdůležitějších výhod použití hierarchického modelu patří:

- řízení procesu síťové komunikace,

- definovat její pravidla a úkoly,

- schopnost spolupráce na úrovni hardwaru a softwaru mezi síťovými produkty různých výrobců,

- a kontrolovat správnost komunikace.

Nyní, když známe účel hierarchických modelů, přejděme k diskusi o jejich nejdůležitějších vlastnostech. Oba modely vznikly již dávno v 70. letech minulého století, ale jsou stále aktuální a používají se dodnes. Prvním je model TCP/IP, známý jako model protokolu. Každá z jeho vrstev provádí specifické úkoly pomocí specifických protokolů. Na druhé straně modely ISO/OSI, známé jako referenční modely, se častěji používají pro analýzu s cílem lépe pochopit komunikační procesy probíhající v síti a jsou modely pro návrh síťových řešení, a to jak hardwarových, tak softwarových.

V případě modelu TCP/IP rozlišujeme 4 vrstvy, a to aplikační, transportní, internetovou a přístupovou síťovou.

Aplikační vrstva umožňuje uživatelům využívat síťové služby, jako je síť, e-mail, sdílení souborů, připojení k terminálu a zasílání rychlých zpráv. Svým studentům vždy říkám, že tato vrstva je nejblíže uživateli, protože nám umožňuje plně využít výhod moderních webových služeb. Například když sedíme u počítače a spustíme webový prohlížeč, používáme webu na úrovni aplikační vrstvy.

Pod ní se nachází **transportní vrstva**, jejímž hlavním úkolem je efektivní komunikace mezi zařízeními. V této vrstvě jsou data rozdělena na menší části, a následně doplněna o další informace, které umožňují její distribuci do příslušné aplikace v cílovém zařízení a její připojení k cílovému zařízení v systému ve správném pořadí.

Pak je tu i**nternetová vrstva**, jejímž hlavním úkolem je najít nejkratší a nejrychlejší cestu k cílovému zařízení přes síť WAN, podobně jako GPS v autě, ale také používá logické adresy (IP adresy) pro adresování dat.

Nakonec tu máme **vrstvu pro přístup k síti**, která kóduje data jako čisté bity (nuly) a jedniček) a přenáší je na přenosové médium a adresuje je, tentokrát prostřednictvím fyzické adresy (MAC adresa).

Model ISO/OSI se skládá ze 7 vrstev (aplikační, prezentační, relační, transportní, síťové, datové a fyzické).

Na vrcholu tohoto modelu můžeme rozlišit **aplikační vrstvu**, která zde funguje velmi podobně jako v modelu TCP/IP v tom smyslu, že umožňuje koncovým uživatelům sítě používat síťové aplikace.

Dále je zde **prezentační vrstva**, která aplikační vrstvě sděluje informace o použitém formátu dat, např. informuje, které typy souborů budou přenášeny, a je zodpovědná za správné kódování dat ve zdrojovém zařízení a dekódování v zařízení přenosovém.

Pod ní se nachází **vrstva relací**, která spravuje relace uživatelů prostřednictvím například webové stránky nebo videokomunikace.

Ještě o krok dále máme **transportní vrstvu**, která je opět úplně stejná jako transportní vrstva v modelu TCP/IP a v obou případech je funkce této vrstvy naprosto stejná.

Dále je zde **síťová vrstva**, která je ekvivalentem internetové vrstvy modelu TCP/IP, tj. velmi podobné funkce, jako je adresování a určení nejlepší cesty pro přenos dat.

Následuje **vrstva datového spoje**, jejímž hlavním úkolem je řídit přístup k přenosovému médiu a adresovat data, ale tentokrát je přenášet mezi hostiteli v síti LAN.

Nakonec **fyzická vrstva** zakóduje data do čistých bitů (jedniček a nul) a přenese je přes přenosové médium do příslušného zařízení.

Oba modely jsou si velmi podobné. Výsledný rozdíl je patrný v horních vrstvách, v případě modelu ISO/OSI je rozdělen do 3 vrstev, zatímco v případě modelu TCP/IP plní stejnou funkci pouze jedna vrstva. Vrstvy jsou vidět s podobným rozdílem, že v modelu ISO/OSI máme dvě oddělené vrstvy datového spoje a fyzické vrstvy, zatímco v případě modelu TCP/IP existuje pouze jedna přístupová vrstva sítě.

7. Proces komunikace

Podívejme se nyní na proces komunikace pomocí modelu TCP/IP. Jak jsem již zmínil, tento model popisuje sadu operačních protokolů, které tvoří tzv. protokol, někdy označovaný jako zásobník protokolů. Odkud se vzal název? Vysvětlil jsem, že když chceme zobrazit webovou stránku, aplikační vrstva nejprve použije protokol HTTP, pak na transportní vrstvě použijeme protokol z této vrstvy, jako je TCP nebo UDP, a pak na internetové vrstvě protokol IP ve vrstvě přístupu k síti, jako je standard Ethernet. Komunikace je založena na souboru protokolů, které na sebe navazují. Správnost lze zaručit pouze v případě, že se pro komunikaci používá celý zásobník protokolů.

Uživatel sítě nejprve vytvoří data v aplikační vrstvě, může to být dotaz na webový server nebo může psát zprávy do messengeru. Data se pak posílají dolů po zásobníku, nejprve do transportní vrstvy, kde se rozdělí na menší části, a poté do internetové vrstvy, kde je jim přidělena adresa, která umožňuje odesílání dat přes síť WAN. Poté přejdou do vrstvy přístupu k síti a jsou jim opět přiřazeny adresy, tentokrát adresy zařízení v místní síti. Nakonec jsou data vložena do přenosového média a přes prostředníka odeslána do koncového zařízení, kde projdou zásobníkem, znovu se sestaví a jsou předána aplikační vrstvě.

Zapamatovat si!

Proces přenosu dat ze zdroje do cíle přenáší data proudící přes vrstvy na zdrojovém zařízení, která jsou následně zakódována a odeslána přes přenosové médium do cílového zařízení, kde se data místo toho dostanou na zásobník.

Než se pustíme do procesu komunikace, musíme si položit ještě jednu velmi důležitou otázku. Abychom zajistili, že se data dostanou ke správným hostitelům a aplikacím a zůstanou jim předána v co možná nezměněné podobě, říkáme tomu kontrolní informace.

Tyto informace se přidávají ve třech vrstvách. Transportní vrstva přidává čísla aplikačních portů (aplikační port na zdrojovém hostiteli a aplikační port na cílovém hostiteli), internetová nebo síťová vrstva IP adresu (včetně zdrojového a cílového hostitele), síťová nebo datová vrstva MAC adresu (zdrojový hostitel) a směrovač místní sítě). Celý proces procházení vrstev v zásobníku, jejich rozdělování na menší části a přidávání řídicích informací (tj. dalších dat) se nazývá zapouzdření. Samozřejmě existuje i opačný proces odstranění těchto dodatečných informací z cílového zařízení, který se nazývá dekapsulace.

Zapamatovat si!

Data procházejí vrstvami na zdrojovém zařízení a jsou obklopena informacemi, které identifikují aplikaci a cílové zařízení, zatímco opačný proces, kdy data procházejí vrstvami a odstraňují tyto dodatečné informace na cílovém hostiteli, je dekapsulace.

Přidáním těchto kontrolních informací do každé vrstvy zvlášť by se mírně změnila struktura vrstev, což je logické, protože do dat přidáváme některé informace, které tam dříve nebyly. Proto se mění i pojmenování datových souborů. Obvykle se data odesílaná po síti nazývají datové jednotky protokolu (PDU), ale s přechodem mezi vrstvami se jejich názvy mění, takže: Na aplikační vrstvě označujeme PDU jednoduše jako data. Později na transportní vrstvě budeme PDU označovat jako segmenty nebo datagramy v závislosti na protokolu použitém na této vrstvě. PDU na internetové vrstvě je již paket a na přístupové vrstvě sítě budeme mít rámec. Stejnou nomenklaturu budeme používat i při analýze komunikace podle modelu ISO/OSI.

8. Diskuse o používání vrstev

Nyní je čas podrobněji se seznámit s procesem komunikace založené na vrstvách. Probereme to na příkladu odeslání e-mailu. Původně uživatelé internetu vytvářeli e-maily pomocí e-mailových programů nebo webových prohlížečů. Aplikační vrstva tato data správně zakóduje a předá je transportní vrstvě.

Tato vrstva rozděluje data na menší části, segmenty, které se snáze posílají po síti. Je to podobné, jako když chceme přemístit obrovský roh z jednoho místa na druhé, ale těžko ho přemístíme celý, protože se nevejde ani do dveří, takže ho rozebereme, místo abychom to zkombinovali s kompletním přemístěním. přidává také kontrolní informace, které nám umožní později sestavit segmenty na koncovém zařízení ve správném pořadí (i když ne vždy se přidávají, záleží na protokolu použitém v této vrstvě), ale hlavně přidává také číslo portu aplikace (port aplikace na serveru a port na klientovi), což je informace, která nám umožní později určit, že se jedná o e-mail a ne o webovou stránku. O aplikačních portech si povíme více, až budeme probírat funkce a protokoly aplikační a transportní vrstvy.

Tyto segmenty jsou poté přeneseny na internetovou vrstvu, kde jsou jim přiděleny IP adresy - odesílajícímu a přijímajícímu zařízení. Tento proces slouží k tomu, aby směrovač (tj. zprostředkující zařízení mezi odesílatelem a příjemcem zprávy) věděl, kam má zprávu odeslat. Od tohoto okamžiku je náš segment adresován paketem.

Paket pak přejde do přístupové vrstvy sítě, kde se vytvoří rámec a uvede se fyzická adresa odesílajícího zařízení a fyzická adresa směrovače, ke kterému je připojen počítač, jemuž zprávu posíláme. S touto adresou se pak rámec dostane k tomuto směrovači, který jej odešle do sítě WAN.

Před samotným přenosem je však rámec zakódován do bitů a předán přes směrovač do cílového zařízení.

Po přijetí těchto bitů cílovým hostitelem proběhne proces zpětné zapouzdření a dekapsulace, při kterém jsou rámce převedeny na pakety, pakety jsou převedeny na segmenty a transportní vrstva je znovu sestaví ve správném pořadí. Po dokončení tohoto procesu se data odešlou do aplikační vrstvy, kde se zobrazí zpráva. Pokud chceme zobrazit webovou stránku nebo odeslat soubor přes Internet, bude komunikační proces podobný, jen se pro odesílání webových stránek nebo souborů místo odesílání a přijímání e-mailů použijí jiné protokoly aplikační vrstvy.

Na závěr důležitá poznámka - komunikační proces mezi zařízeními, o kterém zde hovoříme, je zjednodušený a nazýváme ho smlouva. Proč? No, protože jsme vynechali proces odesílání dat mezi zprostředkujícími zařízeními (tj. směrovači). Proces směrování, tj. přenos dat mezi směrovači v rozsáhlé síti a možnost použití různých přenosových médií v procesu od odesílatele k příjemci, je rozsáhlá a složitá problematika, kterou se nyní nebudeme zabývat. Samozřejmě se jedná o nesmírně důležitou fázi komunikace a my se jí určitě budeme věnovat, ale pouze pokud nám to naše znalosti a dovednosti v oblasti počítačových sítí dovolí.

Nyní už každý z vás ví, jak vypadá komunikační proces v modelu vrstveného protokolu TCP/IP, který je velmi podobný referenčnímu modelu ISO/OSI. Pokud tedy budete požádáni (např. učitelem při testu), abyste popsali komunikační proces na základě modelu ISO/OSI, neměli byste mít problém.

9. Síťové adresování

Nyní si objasníme velmi důležitou otázku, a to adresování v síti. Možná jste si všimli, že tato otázka se při probírání komunikačního procesu objevuje třikrát, protože informace týkající se adres nebo čísel se sčítají do tří vrstev.

Tentokrát však začněme od spodní části zásobníku a podívejme se, že přístupová vrstva sítě modelu TCP/IP a vrstva datového spoje modelu ISO/OSI přinesly koncept fyzických adres. Ptáte se, jaká je tato fyzická adresa. Fyzická adresa, známá také jako adresa MAC, je 48bitové šestnáctkové číslo zakódované na síťové kartě koncového zařízení nebo počítače. Tato adresa může mít tvar: 28-80-23-D6-BE-14, která je uvedena ve fázi vytváření karty. Skládá se ze dvou stejných částí, z nichž první je identifikátor výrobce a druhá je identifikátor karty.

Všechny tyto hexadecimální kódy se používají k nalezení hostitele v místní síti, LAN, je tato adresa, fyzická adresa zdrojového hostitele a směrovače v místní síti, brány spojující naši místní síť a WAN, v procesu zapouzdření TCP/síť v přístupové vrstvě modelu IP a vrstvě datového spoje modelu ISO/OSI.

Postupujeme-li dále, máme internetovou vrstvu modelu TCP/IP a síťovou vrstvu modelu ISO/OSI. V těchto vrstvách se během zapouzdření přidávají IP adresy, nazývané také logické adresy. Tyto adresy jsou IP adresa odesílajícího počítače a IP adresa přijímajícího počítače. Nebudu se zde zabývat podrobnostmi konstrukce, použití a výpočtu IP adres, protože na našem kanálu již existuje díl (klikněte pro vstup), který je celý věnován IP adresám, a řeknu jen, že tyto adresy jsou umístěny v různých sítích pro přenos dat Hostitelé jsou obvykle geograficky vzdáleni stovky kilometrů.

Nakonec tu máme transportní vrstvu, která nepoužívá adresování pro zjišťování hostitelů jako předchozí vrstvy, ale místo toho používá čísla portů pro přiřazení dat konkrétním aplikacím v operačním systému. Nezapomeňte, že dnešní počítače umožňují současný běh více aplikací. Současně můžeme prohlížeč používat k surfování po internetu, poslechu internetového rádia, odesílání a přijímání e-mailů a dokonce i k hraní online her. Pokud nejsou aplikace rozděleny, pokud nejsou na transportní vrstvě přiřazena čísla portů, která by umožňovala identifikaci konkrétních síťových služeb, může se stát, že se během hraní na nižších úrovních v textových editorech objeví na obrazovce příchozí e-maily V rychlých zprávách se objeví zprávy instant messaging. Podívejte se, jak je to všechno promyšlené, logicky uspořádané, bez šance, a proto mám tak rád počítačové sítě.

9.1. Shrnutí

V počítačových sítích se pro usnadnění popisu a řízení různých fází komunikace a pro standardizaci používá vrstvený model, aby byly hardware a software od různých výrobců vzájemně kompatibilní. Komunikace v síti probíhá podle pravidel a zásad známých jako přijetí komunikačních protokolů. Proces síťové komunikace zahrnuje předávání dat po zásobníku zdrojového zařízení, jejich kódování do bitů a odeslání do cílového zařízení, kde jsou data předána a interpretována v cílovém zařízení. Na každé vrstvě jsou data opatřena řídicími informacemi, čísly portů a logickými a fyzickými adresami, které jsou následně zakódovány a odeslány příjemci. Proces toku dat směrem dolů po zásobníku a přenosu řídicích informací a adres se nazývá zapouzdření, zatímco u koncových zařízení se tento proces, kdy data putují po zásobníku nahoru, nazývá dekapsulace.

10. Protokoly aplikační vrstvy

10.1. Protokol HTTP

Když spustíme webový prohlížeč, program pro rychlé zasílání zpráv nebo sdílení souborů, tvoří tyto aplikace komunikační rozhraní mezi počítačovou sítí a uživatelem. Samotný aplikační software, tedy počítačový program, samozřejmě k efektivní komunikaci nestačí, protože k tomu jsou zapotřebí výše uvedené komunikační protokoly, které jsou však v těchto programech implementovány. Příkladem protokolu aplikační vrstvy je pravděpodobně jeden z nejoblíbenějších protokolů HTTP, který je implementován ve webových prohlížečích a stejně jako všechny programy pro rychlé zasílání zpráv a další programy komunikující přes web implementuje také odpovídající protokol.

Když do prohlížeče zadáme adresu webové stránky, tzv. URL (Uniform Resource Locator), a po stisknutí klávesy Enter se náš prohlížeč spojí se serverem, kde je stránka uložena, a vyžádá si konkrétní zdroj - většinou se jedná o soubory obsahující stránky s obsahem. Pokud má server k dispozici požadovaný zdroj, odešle jeho obsah prohlížeči, který interpretuje kód HTML, z něhož je stránka složena, a zobrazí jeho obsah uživateli. Ve skutečnosti je tento proces poněkud komplikovaný. Jako příklad uveďme webovou adresu:

http://www.cybersecurity.pl/fundamentals.html

Po zadání a potvrzení prohlížeč nejprve zkontroluje typ protokolu, poté název internetové domény a nakonec zváží název konkrétního souboru. Později náš prohlížeč zavolá server DNS, aby změnil mnemotechnický název (tj. cybersecurity.co.uk) na IP adresu serveru, kde je webová stránka uložena.

Prohlížeč, který zná tuto adresu, odešle na server požadavek na přístup k souboru tomijerry.html umístěnému v doméně alamakota.pl. Pokud má server k dispozici zdroj v odpovědi, odešle příslušnou zprávu s obsahem požadovaného souboru. Obsah tohoto souboru, kód HTML, je interpretován prohlížečem a zobrazen jako webová stránka.

Protokol HTTP pracuje standardně na portu 80 a definuje několik základních typů zpráv, tj. požadavků na komunikaci mezi klientem a webovým serverem, z nichž nejdůležitější jsou: GET a POST.

10.2. Metoda GET

GET se používá k vyžádání konkrétní webové stránky ze serveru. Jeho syntaxe vypadá takto:

GET /fundamentals.html HTTP/1.1

Kromě názvu požadovaného prostředku obsahuje také verzi použitého protokolu. Když server obdrží takovou zprávu, takový požadavek, odpoví klientovi příslušnou zprávou (s níže uvedenými hlavičkami) a požadovaným prostředkem:

HTTP/1.1 200 OK/fundamentals.html

Požadavek GET obsahuje také následující informace: název hostitele (např. wp.pl), název prohlížeče, který požadavek odeslal, typy souborů akceptované prohlížečem a preferovaný jazyk nebo kódování znaků stránky. Odpověď serveru obsahuje tyto informace: čas serveru, název serverové aplikace (např. APACHE) nebo čas vypršení platnosti dokumentu.

Pokud webový server z nějakého důvodu nemůže prostředek odeslat zpět, odešle zpět chybovou zprávu, například 404 oznamující, že požadovaný prostředek nebyl nalezen, nebo 403 oznamující, že přístup k prostředku je zakázán. Vybrané zprávy a chybové kódy jsou uvedeny v následující tabulce.

Kód chyby klienta:

Kód / Popis / Význam

400 Bad Request Server nemohl zpracovat požadavek z důvodu chyby klienta.

401 Neautorizované požadavky Požadavky na zdroje, které vyžadují ověření.

403 Forbidden Server rozumí požadavku, ale konfigurace zabezpečení mu brání vrátit požadovaný prostředek.

404 Not Found Server nemohl najít zdroj na zadané adrese URL.

405 Metoda není povolena Metoda obsažená v požadavku není pro uvedený prostředek povolena.

406 Nepřijatelné Požadovaný prostředek nemůže vrátit odpověď, kterou může klient zpracovat.

407 Vyžaduje se ověření proxy serveru Vyžaduje se ověření proxy serveru

408 Request timeout Request timeout elapsed - klient neodeslal požadavek na server ve stanoveném časovém období.

409 Konflikt Požadavek nebylo možné dokončit z důvodu konfliktu s aktuálním stavem prostředku.

411 Požadovaná délka - server odmítl dokončit požadavek kvůli chybějící hlavičce Content-Length v požadavku.

415 Nepodporovaný typ média Neznámý způsob požadavku - server odmítl přijmout požadavek, protože syntaxe byla pro server nesrozumitelná.

Kód chyby serveru:

Kód / Popis / Význam

500 Internal Server Error Interní chyba serveru - server narazil na problém, který mu zabránil dokončit požadavek.

501 Not Implemented Server nemá schopnosti požadované pro požadavek.

502 Invalid Gateway Error Server, který funguje jako brána nebo prostředník, obdržel špatnou odpověď od hostitelského serveru a nemohl dokončit požadavek klienta.

503 Služba nedostupná Služba nedostupná - server v současné době nemůže dokončit požadavek klienta z důvodu přetížení.

504 Překročen časový limit brány - server, který funguje jako brána nebo zprostředkovatel, neobdržel odpověď od zadaného serveru HTTP, FTP, LDAP atd. ve stanoveném čase nebo je ke zpracování požadavku vyžadován server DNS.

505 HTTP Version Not Supported Unsupported - server nepodporuje nebo odmítá podporovat verzi HTTP uvedenou klientem.

10.3. Metoda POST

Dalším typem zprávy je zpráva POST, která se používá k odesílání dat na server. Například když je na stránce formulář, který odesílá data na server, například registrační formulář, data, která do něj vložíme, se odešlou pomocí zprávy POST.

Přestože je protokol HTTP velmi populární a pravděpodobně nejpoužívanější ze všech protokolů aplikační vrstvy, není bezpečný. Metoda POST odesílá data na server v prostém textu. Pokud je přenos mezi klientem a serverem zachycen, je možné přečíst informace, které chcete odeslat na server.

To je velmi nebezpečné, a proto dnes většina webových stránek může některé informace odesílat na server, např. ty stránky, které vyžadují přihlášení, již používají protokol HTTPS, který šifruje komunikaci mezi klientem a serverem a běží na portu 443.

Další typy zpráv, které mohou klienti posílat webovému serveru, jsou:

Odstranění požadavku na prostředek ze serveru

Hlavička požaduje od serveru prostředky ve formě hlaviček.

Žádost o propojení vytváří vztahy mezi existujícími zdroji

OPTIONS Požadavek serveru na identifikaci podporovaných metod.

Put požádá server o přijetí souboru od klienta.

Trace požádá server o vrácení hlaviček zprávy odeslané klientem.

10.4. Elektronická pošta

E-mail používá dva protokoly aplikační vrstvy, které spolupracují. Jeden slouží k odesílání pošty, což je protokol SMTP, a druhý k přijímání zpráv, což je protokol POP3. Dnes lze IMAP používat také k přijímání e-mailů. Tyto protokoly úzce souvisejí s aplikacemi, procesy běžícími na klientských počítačích a serverech, které vytvářejí a přijímají zprávy. Jedná se o procesy MUA (Mail User Agent), MTA (Mail Transfer Agent) a MDA (Mail Delivery Agent).Proces MUA běží na klientském počítači a ostatní dva procesy na poštovním serveru.

Zjednodušený postup odesílání e-mailů pomocí proxy serveru je následující:

1. uživatel vytvoří e-mailovou zprávu a pomocí procesu MUA ji předá poštovnímu serveru a procesu MTA běžícímu na tomto serveru.

2. tento proces analyzuje záhlaví zprávy, včetně. k určení příjemce zprávy a kontroluje, zda je uživatel, na kterého zpráva směřuje, v jeho seznamu uživatelů.

3. pokud ano, předá zprávu procesu MDA, který je zodpovědný za její doručení příslušnému příjemci.

4. pokud příjemce zprávy nemá účet na daném serveru, proces MTA předá zprávu procesu MTA na jiném serveru, kde se nachází uživatelský účet.

5. server předá zprávu procesu MDA, který ji doručí určenému příjemci.

V následující tabulce jsou uvedeny porty, na kterých pracuje e-mailový protokol.

Protokol	**Číslo portu**
IMAP	143
POP3	110
SMTP	25
Šifrovaný IMAP	993
Šifrovaný POP3	995
Šifrovaný SMTP	465 nebo 587

10.5. Protokol FTP

Třetí, stejně oblíbenou webovou službou je možnost odesílání a přijímání souborů prostřednictvím protokolu FTP (File Transfer Protocol). Služba je také komunikačním protokolem, když chceme nahrát soubory webové stránky na webový server nebo chceme jednoduše nahrát nějaké soubory na server a sdílet je s ostatními uživateli. K provedení operace nahrávání souborů na server nebo stahování prostředků ze serveru musíme použít klienta FTP a taková služba musí být samozřejmě spuštěna i na serveru. Klienti FTP jsou k dispozici v každém operačním systému, například prostřednictvím příkazového řádku, což je sice nepohodlné, ale funguje to.

Pokud používáte FTP pouze ke stahování souborů, můžete tak bezpečně činit pomocí webového prohlížeče. Většina, ne-li všechny populární prohlížeče mají vestavěné klienty FTP.

Pokud však chcete nahrávat soubory na server, doporučujeme použít specializované programy, jako je FileZilla nebo WinSCP - jsou zdarma a lze je snadno stáhnout z webu.

Klient FTP WinSCP

Při použití tohoto protokolu musí být pro správnou komunikaci mezi klientem a serverem navázána dvě spojení. První připojení slouží pouze k odesílání příkazů a zpráv a nazývá se řídicí připojení (běží na portu 21), zatímco druhé připojení běží na portu 20 a slouží k přenosu souborů na server a ze serveru. K ochraně přístupu k serveru FTP se používá autentizace uživatele, která je naprosto stejná jako při přihlašování k profilům nebo e-mailům na sociálních sítích, ale někdy, když je zdroj k dispozici širšímu publiku, je takzvaným uživatelům umožněn anonymní přístup, a proto není vyžadována autorizace. Toto řešení by mělo být použito pouze v případě, že uživatel může stahovat data ze serveru. Nahrávání souborů, tj. jejich umístění na server, je vždy přístupné pouze uživatelům s přihlašovacím jménem a heslem.

10.6. Protokol SSH

Běžně používaným protokolem aplikační vrstvy je protokol pro vzdálenou správu hostitele známý jako SSH (Secure Shell). Pro neprofesionály v oblasti informačních technologií nemá tento název velký význam, protože se nejedná o protokol, webové stránky nebo e-mail, který by používali "běžní jedlíci chleba". Správci jej používají ke správě serverů, které se často nacházejí v různých geografických lokalitách, ne nutně na jejich pracovišti. Používají ji například také lidé, kteří si koupili servery VPS, a proto je spravují. Tento protokol je odvozen od jiného protokolu pro vzdálený přístup, protokolu TELNET, a je pravděpodobně jeho lepší verzí. Proč? Protože je TELNET mimochodem pravděpodobně nejstarším protokolem na aplikační vrstvě, nešifruje komunikaci mezi klientem a serverem, zprávy se posílají v prostém textu, takže je možné komunikaci zachytit a zajímat se, v jaké relaci se informace posílají. Podle něj je to nepřijatelná situace, a proto je hostitel spravován vzdáleně pomocí šifrovaného protokolu SSH.

Výchozím algoritmem pro šifrování komunikace je RSA, ale k šifrování dat lze použít i o něco slabší algoritmus DSA. Během instalace serveru SSH se vytvoří dvojice klíčů - veřejný a soukromý klíč serveru - které se používají k šifrování a dešifrování komunikace. Když se klient poprvé připojí k serveru, uloží veřejný klíč serveru do souboru known_hosts na disku.

Poté vytvoří tzv. klíč relace, který se používá k šifrování veškeré komunikace. Klíč relace je zašifrován veřejným klíčem, který byl předtím přijat od serveru a odeslán zpět. Od tohoto okamžiku je veškerá komunikace šifrována klíčem relace.

Ve výchozím nastavení běží SSH na portu 22. PUTTY je jeden z nejoblíbenějších klientských programů pro používání SSH, je zdarma, lze jej stáhnout z webu a nevyžaduje instalaci. Chcete-li se vzdáleně připojit k hostiteli, jednoduše jej spusťte, zadejte název hostitele nebo jeho IP adresu, vyberte SSH, pokud není ve výchozím nastavení vybráno, a klikněte na tlačítko Otevřít. Pokud se ke vzdálenému hostiteli připojujete poprvé, potvrďte, že se chcete připojit a můžeme jej spravovat na dálku.

10.7. Protokol DNS

DNS je protokol, služba, která překládá lidsky čitelné názvy domén na IP adresy zařízení na internetu. Představte si situaci, kdy DNS neexistuje, ale my chceme v prohlížeči zobrazit své oblíbené webové stránky. Místo názvu domény musíme zadat IP adresu, tj. například adresu ve slovním tvaru: 212.56.93.112. Pro většinu z nás to není problém, některá čísla si lze zapamatovat. Na druhou stranu je na internetu mnoho webových stránek a je obtížné zapamatovat si mnoho číselných adres. Navíc je snadné udělat v takových digitálních záznamech chybu a ve světě internetu může taková malá chyba vést k jiné stránce, než jsme očekávali.

To je jedna strana mince a druhá strana je, že IP adresa serveru se nemusí měnit příliš často. Když naše webové stránky změní IP adresu a služba DNS nefunguje, musíme se adresu znovu naučit a zapamatovat si ji. Systém DNS tento problém řeší, protože tuto adresu změní ve své databázi záznamů a přiřadí ji názvu domény. Pro nás uživatele je pak jedno, jaká je IP adresa webu, důležité je, že známe adresu, název domény a že se nemění.

DNS je služba, která funguje v architektuře klient-server, ale klienty zde nepovažujeme za počítačové programy, jako jsou prohlížeče nebo programy pro sdílení souborů. V tomto počítači je spuštěna pouze systémová služba DNS Resolver, která obsluhuje všechny aplikace v klientských počítačích, jejichž názvy je třeba změnit. Při konfiguraci síťového zařízení nebo jen počítače bychom měli zadat dvě adresy serverů DNS, aby v případě, že jeden z nich nekomunikuje, fungoval druhý jako náhrada názvu.

Servery DNS ukládají nejrůznější záznamy, včetně záznamů A a AAAA obsahujících adresy koncových zařízení a záznamů MX, které se starají o výměnu pošty, protože je důležité si uvědomit, že systém DNS nepřevádí pouze doménové adresy na IP adresy pro webové stránky, ale vztahuje se také na e-mailový server. Výměna jmen pro mě vypadá takto:

1. klient odešle dotaz na server DNS, který zkontroluje, zda záznam existuje v jeho databázi.

2. pokud ano, přeloží název na IP adresu a odešle ji zpět klientovi:

3. pokud ne, kontaktuje jiné servery, aby se daný záznam nacházel v jejich databázi:

Odesílání dotazů na jiné servery ohledně serveru DNS, který záznam ve své databázi nenašel, může vést k velkému síťovému provozu, což je matoucí situace. Aby se zabránilo nadměrnému a zbytečnému síťovému provozu, když jiný server najde záznam a odešle jej serveru přiřazenému našemu zařízení, uloží tento server záznam do mezipaměti, takže v budoucnu nebudete muset pro stejnou adresu odkazovat na jiný server. To jistě urychlí pozdější změny názvů, protože naše servery DNS již nebudou vyhledávat záznamy na jiných serverech, ale názvy okamžitě nahradí. Podobně služby DNS v osobních počítačích ukládají dříve přeložené názvy. To lze ověřit zadáním příkazu ipconfig /displaydns v počítači se systémem Windows. Poté zjistíme, která mapování jsou uložena v mezipaměti služby DNS našeho počítače.

10.8. Hierarchie DNS

Hierarchie serverů DNS má podobu obráceného stromu, na jehož vrcholu je kořenový server DNS nejvyšší úrovně. Server nejvyšší úrovně ukládá informace o tom, jak se dostat na server nejvyšší úrovně, který zase ukládá informace o tom, jak se dostat na server druhé úrovně atd. Domény nejvyšší úrovně určují zemi (.pl.de nebo .uk) nebo typ organizace (.org .com nebo .gov).

V příkladu adresy, jako je Pocztowy.wp.pl, rozlišujeme mezi doménou nejvyšší úrovně (.pl), dále doménou druhé úrovně (wp.pl) a nakonec doménou třetí úrovně (Pocztowy.wp.pl Samozřejmě ne všechny adresy musí obsahovat co nejvíce úrovní domén, nejen domény nejvyšší a druhé úrovně, jako jsou wp.pl, pasja-informatyki.pl, szkola.pl.

10.9. Protokol DHCP

Stejně jako dříve zmíněný protokol DNS je i protokol DHCP protokolem, který funguje spíše jako služba než jako program nebo aplikace. Protokol DHCP umožňuje počítačům připojujícím se k síti získávat IP adresy, masky podsítí, adresy brány a serveru DNS a další nastavení z předem nakonfigurovaného fondu adres. Server DHCP může být nakonfigurován v samostatném počítači a bude představovat samostatné zařízení v síti, které bude přidělovat IP adresy klientským počítačům, nebo může běžet na stávajícím serveru jako samostatná služba, samostatný proces.

V současné době nám router v naší domácnosti umožňuje nastavit i takovou službu. Přidělování adres klientským počítačům prostřednictvím služby DHCP (tzv. dynamické přidělování) je pro správce velmi pohodlné řešení, zejména v rozsáhlých sítích, kde se často objevují nové počítače a jejich uživatelé. V síti se 100, 200 nebo 500 počítači a velkým počtem mobilních zařízení by pouhá konfigurace IP adres byla zdlouhavá a hlavně časově náročná.

Samozřejmě ne všechna zařízení v síti mohou získat adresy tímto způsobem, protože některá z nich, jako jsou aplikační servery, databáze, ověřování uživatelů, síťové tiskárny nebo směrovače, by měla a musí mít adresy přidělené staticky, tj. ručně. Proč? Protože služba DHCP nakonfigurovaná na serveru ne vždy trvale přidělí počítači danou IP adresu. Takovou adresu pronajme pouze na dobu určenou při konfiguraci DHCP, třeba na hodiny, dny, ale ne trvale, i když i z toho existují výjimky, které vám řeknu při konfiguraci konkrétního serveru DHCP.

Zakázaný stroj vrátí pronajatou adresu, která je vrácena do fondu. Tuto adresu si pak může pronajmout jiné zařízení. Pokud si server, směrovač nebo síťová tiskárna tyto adresy pronajme, může se stát, že je bude muset po určité době vrátit do fondu a není zaručeno, že stejnou adresu opět obdrží. Klientské počítače, které komunikují s jakýmkoli serverem nebo jiným důležitým zařízením běžícím v síti, se na něj odkazují pomocí jeho IP adresy, pokud se IP adresa často mění, některé služby pro uživatele v místní síti nemusí být po určitou dobu k dispozici, zejména ve firmě Vše další je nepřijatelné.

Aby počítač se systémem Windows získal adresu ze serveru DHCP, musí být v konfiguraci sítě vybrána možnost "Získat IP adresu automaticky".

10.10. Seznam protokolů

Protokoly aplikační vrstvy popsané v této části představují pouze malou část celkového seznamu dostupných protokolů aplikační vrstvy. V počítačové síti existuje mnoho dalších služeb, z nichž každá běží na jiném protokolu. Je těžké je zde vyjmenovat, proto jsou uvedeny ty nejoblíbenější a nejčastěji používané. Zájemce o hlubší zkoumání tématu komunikačních protokolů aplikační vrstvy odkazuji na literaturu. Následující tabulka obsahuje sadu oblíbených protokolů aplikační vrstvy a čísla jejich portů. Jsou jistě užitečné pro kontrolu před vyšetřením nebo odbornými testy.

Protokol	Popis	Port
HTTP	Hypertextový přenosový protokol	80
HTTPS	Šifrovaný protokol HTTP pomocí protokolů SSL nebo TLS	443
POP3	Protokol přijímání pošty	110 (šifrovaný 995)
IMAP	Protokol pro příjem pošty pro správu složek v poštovní schránce	143 (šifrovaný 993)
SMTP	Protokol odesílání pošty	25 (šifrovaný 465 lub 587)
FTP	Protokol přenosu souborů	21 (příkazy) i 20 (soubory)
FTPS	Šifrovaný protokol FTP	990
TELNET	Protokol připojení terminálu	23
SSH	Šifrovaný protokol připojení terminálu	22
DNS	Protokol pro změnu názvů domén na IP adresy	53
DHCP	Protokol pro automatickou konfiguraci hostitelů v síti	67 i 68 (IPv6 – 546 i 547)
LDAP	Protokol adresářových služeb (např. AD ve WS)	389 (šifrovaný 639)
SNMP	Protokol konfigurace síťového zařízení	161
MySQL	Systém správy databází	3306
PostgreSQL	Systém správy databází	5432

11. Úkoly transportní vrstvy

Transportní nebo přenosová vrstva (tyto názvy lze zaměňovat) je velmi důležitou součástí komunikačního procesu. Mezi nejdůležitější úkoly této vrstvy patří:

- navazovat a zpracovávat připojení (relace) mezi hostiteli,

- sledovat připojení mezi hostiteli,

- Rozdělte data na menší části,

- Identifikace jednotlivých aplikací,

- Řízení toku dat,

- Zpětný přenos v případě ztráty dat.

Sledování připojení, což jsou konverzace mezi hostiteli, umožňuje více aplikacím odesílat a přijímat data současně. Na jednom počítači můžeme kontrolovat poštu, používat elektronické bankovnictví nebo komunikovat s přáteli. V tuto chvíli se nám zdá přirozené, že je vlastně těžké si představit situaci bez této možnosti, ale je třeba připomenout, že je to možné díky dopravní vrstvě.

Možnost používat více služeb najednou zahrnuje také rozdělení dat, tj. jejich rozdělení na menší části. To umožňuje efektivnější komunikaci, protože se nepřenáší velké množství dat současně. Nebýt segmentace, mohla by data přijímat vždy jen jedna aplikace a ostatní používané aplikace by musely čekat, až na ně přijde řada. Jak vidíte na obrázku níže, segmenty se odesílají střídavě, střídavě se odesílají segmenty webových stránek, e-mailové segmenty, segmenty instant messengeru atd. Celý proces střídání přenosu více aplikačních segmentů se nazývá multiplexování.

Dalším důležitým úkolem nebo funkcí transportní vrstvy je přenos dat do vlastní aplikace. Každá aplikace má svůj vlastní identifikátor, který ji jednoznačně definuje. Tento identifikátor je číslo portu aplikace.

Je přiřazen segmentu nebo datagramu během zapouzdření na transportní vrstvě a zaručuje doručení dat konkrétní aplikaci.

Stejně jako IP adresy jsou čísla portů přidělována organizací IANA (Internet Assigned Numbers Authority), která čísla portů rozděluje do tří skupin:

Název skupiny portů	Rozsah číslování	Aplikace
Dobře známé (ang. well knows)	0 – 1023	Služby a aplikace serveru
Registrováné (ang. registered)	1024 – 49151	Uživatelské služby a aplikace
Dynamické (ang. dynamic)	49152 – 65535	Náhodně vybrané pro uživatelské aplikace

Dobře známé porty, tj. porty 0 až 1023, jsou registrovány pro služby a konkrétní serverové aplikace, např. webové servery mají výchozí port 80 a servery POP3 port 110. Sada aplikací se známými porty, včetně protokolů transportní vrstvy, jak je uvedeno níže.

Protokol aplikační vrstvy	Číslo portu	Protokol transportní vrstvy
HTTP	80	TCP
HTTPS	443	TCP
POP3	110 (šifrované 995)	TCP
IMAP	143 (šifrované 993)	TCP
SMTP	25 (šifrované 465 nebo 587)	TCP
FTP	21 (příkazy) i 20 (soubory)	TCP
FTPS	990	TCP
TELNET	23	TCP
SSH	22	TCP
DNS	53	TCP lub UDP
DHCP	67 i 68 (IPv6 – 546 i 547)	UDP

LDAP	389 (šifrované 639)	TCP lub UDP
SNMP	161	UDP

Druhou skupinu, registrované porty, používají aplikace nainstalované v počítači uživatele. Pokud například nainstalujeme do počítače aplikaci systému pro správu databáze MySQL, bude spuštěna na portu 3306. Třetí a poslední skupina, dynamické číslo portu, je náhodně přiděleno klientské aplikaci, např. když klient odešle na server požadavek na sdílení webové stránky, server ve výchozím nastavení přijme požadavek na portu 80, ale klient obdrží požadavek od serveru. Příchozí odpověď nebude odeslána na port 80, protože ten je vyhrazen pro proces webového serveru, ale na náhodný počet portů přidělených z fondu dynamických portů.

Na stejném čísle portu nemůže běžet více aplikací. Jakmile je aplikace spuštěna na portu 53 (DNS), není možné, aby na tomto portu byla spuštěna jiná aplikace.

Pokud již víme, co je port aplikace, představíme si další pojem. To by byla zásuvka.

S pojmem zásuvky jste se již setkali při výuce počítačové techniky při probírání základních desek a procesorů a objevuje se také v počítačových sítích. Zásuvka je kombinací IP adresy a čísla portu:

192.168.20.20:80

Zásuvka jednoznačně identifikuje konkrétní proces běžící na zařízení, takže například když náš prohlížeč zavolá webový server, aby zobrazil webovou stránku, budou požadavky serveru odeslány do jeho zásuvky, tedy procesu (aplikaci webového serveru).

11.1. Záhlaví protokolu TCP

Protokol TCP je komplexní protokol orientovaný na spojení, jehož cílem je zajistit spolehlivý přenos dat a řízení toku. Při zapouzdření se do hlavičky TCP přidává až 20 bajtů řídicích dat, což je však nutné pro spolehlivost protokolu TCP. Mezi aplikace využívající tento protokol patří webové prohlížeče, e-mailoví klienti a programy pro přenos souborů. Režim segmentu TCP si můžete prohlédnout níže. Čísla v závorkách označují počet bitů vyhrazených pro dané pole.

<table>
<tr><td colspan="3">BIT (0)</td><td>BIT (15) BIT (16)</td><td>BIT (31)</td></tr>
<tr><td colspan="3">Zdrojový port (16)</td><td colspan="2">Cílový port (16)</td></tr>
<tr><td colspan="5">Sekvenční číslo (32)</td></tr>
<tr><td colspan="5">Číslo potvrzení (32)</td></tr>
<tr><td>Délka záhlaví (4)</td><td>Rezervováno (6)</td><td>Bity kódu (příznaky) (6)</td><td colspan="2">Okno (16)</td></tr>
<tr><td colspan="3">Kontrolní součet (16)</td><td colspan="2">Indikátor naléhavosti (16)</td></tr>
<tr><td colspan="5">Možnosti (0 nebo 32)</td></tr>
<tr><td colspan="5">Data aplikační vrstvy (proměnná délka)</td></tr>
</table>

- Zdrojový port - port aplikace odesílající data.

- Cílový port - port aplikace, do které jsou data odesílána.

- Pořadové číslo - číslo posledního bajtu v segmentu.

- Číslo potvrzení - číslo dalšího bajtu, který příjemce očekává.

- Délka - délka celého segmentu TCP.

- Kódové bity (příznaky) - kontrolní informace o segmentu.

- Okno - množství dat, které lze přenést bez potvrzení.

- Kontrolní součet - slouží k ověření přenášených dat.

- Indikátor převzetí služeb při selhání - používá se pouze v případě, že je nastaven příznak URG.

11.2. Třístupňové sladění

Protokol TCP je spojovací protokol, což znamená, že než může zdrojový hostitel odeslat jakákoli data cílovému hostiteli, musí být mezi nimi navázáno spojení. Tato kombinace se nazývá třícestné podání ruky. Zdrojový hostitel, tj. klient, odešle segment obsahující příznak SYN (SYN je příznak synchronizace sériového čísla) a segment obsahuje také náhodné sériové číslo klienta (nazývané také ISN, SEQ=100), které se použije pro následné sloučené datové fragmenty.

Po přijetí tohoto segmentu je cílový hostitel, tj. server, informován, že si s ním klient přeje navázat spojení. V odpovědi server odešle segment s nastavenými příznaky SYN a ACK (příznak ACK informuje klienta, že server přijal předchozí segment), sekvenční číslo přijaté od klienta se zvýší o 1 (ACK = 101) a jeho náhodné sekvenční číslo (SEQ = 300).

Nakonec klient odešle segment zpět na server s nastaveným příznakem ACK a potvrdí přijetí předchozí zprávy s pořadovým číslem serveru zvýšeným o 1 (SEQ=101, ACK=301). Tím se proces připojení dokončí a data se správně přenesou. Níže je uveden třístupňový proces odsouhlasení.

Teprve po navázání spojení TCP se serverem může klient odeslat příslušná data, například požadavek na webovou stránku nebo soubor.

Po odeslání všech dat je třeba relaci uzavřít. Klient pak odešle serveru segment s příznakem FIN, kterým informuje server o svém záměru uzavřít relaci, a ten odpoví potvrzovacím segmentem s příznakem ACK, že takový segment obdržel. Server pak rovněž odešle segment s příznakem FIN a klient odpoví potvrzovacím segmentem s příznakem ACK. Tím dojde k uzavření relace TCP.

Vlajka	**Aplikace**
URG	Označuje existenci pole indikátoru naléhavosti v záhlaví (urgent)
ACK	Označuje existenci pole s číslem potvrzení v záhlaví. (acknowledgment)
PSH	Vynucený přenos paketů (push)
RST	Opětovné navázání spojení (reset)
SYN	Synchronizace sekvenčních čísel
FIN	Konec dat od odesílatele

11.3. Okno TCP

Spolehlivost doručení dat v rámci relace TCP závisí na tom, zda klient odešle potvrzení o přijetí dříve odeslaných dat. Než může server odeslat klientovi další část dat, musí obdržet toto potvrzení o přijetí. To někdy způsobuje zpoždění v doručování segmentů, protože nejsou odesílány nepřetržitě. Tyto problémy jsou však přijatelné, pokud je vyžadována spolehlivost komunikace.

Předpokládáme-li, že 1000 bajtů dat je odesláno v segmentu s pořadovým číslem 1, klient po přijetí 1 části dat odešle serveru segment s potvrzovacím číslem 1001. Další bajt, počínaje bajtem 1001. Když server odešle dalších 1000 bajtů, číslo přijatého potvrzení bude 2001, další číslo bude 3001, další 4001 atd.

Samozřejmě, že ve skutečnosti, když hostitel musí pokaždé potvrdit příjem tak malého množství dat, může to způsobit velké přetížení odkazu, např. doba načítání stránky může být dlouhá. Proto je odesláno více dat a zpětná vazba je potvrzena. Množství dat, které může server odeslat, než obdrží potvrzení od klienta, se nazývá velikost okna, v tomto případě 3000 bajtů.

Tato velikost je uvedena v záhlaví segmentu TCP a kromě toho, že určuje, kolik dat lze odeslat bez potvrzení, umožňuje řídit tok dat mezi zařízeními. Pokud klient při příjmu dat narazí na zablokování a dojde ke ztrátě segmentu, může zařízení odeslat serveru informaci o zmenšení velikosti tohoto okna, tedy množství dat, které lze přijmout bez potvrzení, čímž se přenos zpomalí, ale zabrání se ztrátě segmentu. Po určité době se velikost okna vrátí na původní velikost. Změna velikosti okna během přenosu se nazývá dynamické okno nebo posuvné okno.

11.4. Protokol UDP

Dalším protokolem, který implementuje některé funkce transportní vrstvy, je protokol UDP. V tomto případě je to však mnohem jednodušší, protože protokol neimplementuje žádný mechanismus, který by zaručoval spolehlivost doručení dat nebo řízení toku.

Protokol UDP je jednoduchý protokol bez spojení a jeho největší výhodou je nízká režie řídicích dat přidaných během zapouzdření. Protokol UDP přidává do datagramu pouze 8 bajtů řídicích dat. Záhlaví datagramu UDP vypadá takto:

BIT (0)	**BIT (15) BIT (16)**	**BIT (31)**
Zdrojový port (16)	Cílový port (16)	
Délka (16)	Kontrolní součet (16)	
Délka aplikační vrstvy (proměnná délka)		

- Zdrojový port - určuje port aplikace, ze kterého mají být data odeslána.

- Cílový port - určuje port aplikace, na který mají být data odeslána.

- Length - 16-bitové pole, které určuje délku celého datagramu UDP.

- Kontrolní součet - 16-bitové pole sloužící k ověření platnosti odesílaných dat.

UDP bez spojení znamená, že zdrojový hostitel před zahájením komunikace neodesílá žádné informace pro navázání spojení s cílovým hostitelem. Obecně platí, že pokud chce zdrojové zařízení zahájit přenos, chce odeslat právě dokončená data bez předchozí dohody.

Pokud bychom to přirovnali ke komunikaci mezi lidmi, pro protokol TCP by to vypadalo asi takto: Hej, Tome, soustřeď se, protože se s tebou chystám mluvit a teprve až dostanu tuhle zprávu, začne normální konverzace, samozřejmě jen pokud Tom odpoví: OK, začnu poslouchat. V případě UDP to Toma neupozornilo, že se chystám začít mu sdělovat něco důležitého, prostě jsem začal konverzaci.

Mezi aplikace nebo služby využívající tento přenosový protokol patří DNS, DHCP, telefonie VoIP a streamování videa.

Proč právě tyto? Odpověď je jednoduchá, tyto aplikace upřednostňují rychlost před spolehlivostí komunikace, respektive potřebou přijímat všechna přenášená data. Představte si situaci, kdy sledujeme videopřenos nebo hrajeme hru s přáteli, například CS. Je obtížné soutěžit ve hře nebo cokoli sledovat, když se balíčky opozdí.

Někdo by se mohl zeptat: ale kde se bere to zpoždění? Například segmenty TCP jsou mnohem větší než datagramy UDP a TCP musí potvrzovat doručená data, takže se jich po síti posílá větší množství než v případě UDP.

U aplikací využívajících tento konkrétní protokol lze tolerovat, že někdy může dojít ke ztrátě nebo poškození paketů. V případě služeb DNS se v případě ztráty datagramu dotaz jednoduše znovu odešle na server DNS a není tragédií, pokud datagram během relace nedorazí, protože zprávy lze vždy opakovat. U aplikací využívajících protokol TCP již není ztráta nebo záměna přípustná. Datagramy jsou přijímány v pořadí, v jakém byly přijaty, a pokud je datagramů více, je povinností konkrétní aplikace zajistit jejich správné sestavení.

11.5. Příkaz NETSTAT

Jak mohu zobrazit připojení našeho počítače k různým serverům v systému Windows? K tomu můžeme použít program Wireshark, pomocí kterého můžeme zkontrolovat vše, co prochází naší síťovou kartou, a také příkaz NETSTAT v konzoli systému Windows. Po zadání můžeme sledovat, jaká aktivní připojení máme. Na výstupu tohoto příkazu se zobrazí typ protokolu transportní vrstvy použitý pro připojení, socket mého počítače, tj. IP adresa s číslem portu, socket serveru, ke kterému jsme připojeni, a stav připojení.

Programy lze volat s různými argumenty, jejichž seznam a popis se zobrazí po zadání příkazu netstat /help.

Těchto připojení je hodně, a to proto, že jednak používám systém Windows 10, o kterém je známo, že téměř neustále něco odesílá na servery společnosti Microsoft, a kromě toho mám nastavenou synchronizaci s cloudovými službami a je zde antivirový program, který se také připojuje na její servery. Jak tedy zjistíme, ke kterým službám je náš počítač připojen? Stačí spustit příkaz netstat -f a zkopírovat název domény (PPM -> Tag -> Vybrat název domény -> CTRL + C nebo PPM -> Kopírovat).

Vlastníka domény můžeme zjistit prostřednictvím whois.domaintools.com a jeho vyhledávače. Stačí vložit zkopírovaný název domény.

12. Úlohy a protokoly síťové vrstvy

Síťová vrstva (model ISO/OSI - vrstva 3), známá také jako internetová vrstva, přijímá fragmentovaná data z transportní vrstvy a poté provádí operace umožňující přenos paketů po síti. Mezi tyto operace patří:

- adresování dat pomocí IP adres;

- zapouzdření dat, což je přiřazení dalších informací požadovaných použitým protokolem síťové vrstvy;

- směrování, což je výběr nejlepší trasy pro paket;

- dekapsulace, která tyto dodatečné informace odstraní, jakmile paket dorazí do svého cíle.

Víme, že síťová komunikace se řídí určitými pravidly, tzv. komunikačním protokolem. Víme také, že každá vrstva používá svůj vlastní protokol, nezávislý na ostatních. Síťová vrstva, kde se také objevují, se neliší. Nejběžnějším komunikačním protokolem pro tuto vrstvu je IPv4. Nejdůležitějším důvodem pro jeho použití je to, že se jedná o otevřený protokol. To znamená, že nepatří žádné společnosti nebo firmě, takže může komunikovat mezi zařízeními různých výrobců. Již se řídí protokolem IPv6, který je rovněž otevřený.

V současné době používá tyto protokoly souběžně mnoho výrobců zařízení a softwaru. Možná, že v budoucnu IPv6 zcela nahradí IPv4, ale nemyslím si, že je to příliš brzy. Samozřejmě existují i proprietární protokoly, jako je protokol IPX společnosti Novell, která se specializuje na vývoj síťových operačních systémů, nebo protokol AppleTalk vyvinutý společností Apple. S jistotou však lze říci, že IPv4 je zdaleka nejpoužívanějším protokolem síťové vrstvy.

12.1. Protokol IPv4

Protokol IPv4 je navržen tak, že během zapouzdřování není třeba přidávat mnoho řídicích dat. Poskytuje pouze základní funkce potřebné k přenosu paketů ze zdroje do cíle. Je bez připojení, což znamená, že před odesláním dat nenavazuje spojení, a funguje na principu "nejlepšího úsilí", což znamená, že nepoužívá řízení toku ani potvrzení o doručení dat jako protokol TCP, ale dělá vše pro to, aby byla komunikace efektivní. Je to také protokol nezávislý na médiu, což znamená, že data lze přenášet mezi hostiteli bez ohledu na použité médium.

Vždyť v jedné síti můžeme používat kroucenou dvojlinku, v jiné optická vlákna a ve třetí rádiové vlny. Protokol IP funguje v každé síti úplně stejně. Problém, který může nastat při přenosu dat přes různá média, je maximální velikost paketu, což je hodnota MTU (Maximum Transmission Unit), pokud je paket příliš velký, směrovače připojené k síti jej rozdělí na menší části. Tento proces se nazývá fragmentace, což je další termín z našeho internetového slovníku.

Abychom pochopili, jak IPv4 funguje a jak se pakety přenášejí přes Internet, použiji k vysvětlení jeho fungování příklad paketu odeslaného mojí tetou ze Spojených států. Balíček se skládal ze 3 lepenkových krabic spojených dohromady. Teta napsala adresu dárku a poslala ji kurýrní společnosti. Při odesílání balíku se vzdává dalších možností, jako je potvrzení o přijetí nebo sledování. Pracovník společnosti před vydáním zásilky označí karton místem určení a zpáteční adresou. Spolu s desítkami dalších zásilek je autem převezen do přístavu, kde je zabalen do kontejneru a následně přeplaven přes oceán.

V cílovém přístavu se kontejnery vybalí, zásilky se roztřídí a poté se autem převezou do různých měst a místních sběrných míst. Z místa vyzvednutí autem má být zásilka doručena na adresu, ale ukáže se, že tři spojené kartony jsou příliš velké na to, aby je bylo možné přepravit na vozíku, a tak je kurýr rozdělí na jednotlivé kartony a doručí vám je v této podobě. Protože si vaše teta nevybrala další možnosti, kurýrní společnost jí nevystavila potvrzení. Můžete to udělat sami, např. zavolat tetě a poděkovat jí 🙂

Převod na IP komunikaci by vypadal následovně:

- zásilka je odeslána bez předchozího oznámení příjemci - máme režim bez spojení;

- během procesu zapouzdření je přiřazena zdrojová a cílová adresa.

- v našem případě je adresa domova příjemce adresou cílovou a adresa domova tety je adresou zpáteční;

- zásilka neobsahovala mnoho kontrolních údajů, které by mohly zpomalit komunikaci - proto se teta vzdala další možnosti, potvrzení a sledování zásilky;

- zásilky se na místo určení dostávají prostřednictvím optických vláken, kroucených párů a rádiových vln - protože zásilky jsou doručovány různými dopravními prostředky: loděmi, velkými auty, malými auty;

- balík je příliš velký na to, aby mohl být poslán celý po jedné síti, a proto je roztříštěn - tj. balík je na určitém místě rozdělen tak, aby mohl být přepraven v malém autě;

- protokol IP nezaslal potvrzení o přijetí balíku - stejně jako společnost neujistila mou tetu, že balíček dorazil.

Jako každý komunikační protokol má i IPv4 standardizované hlavičky pro přidání řídicích informací. Příklad typické hlavičky IPv4 je uveden níže.

<table>
<tr><td>Verze</td><td>IHL</td><td>Typ služby</td><td colspan="2">Délka balení</td></tr>
<tr><td colspan="3">Identifikace</td><td>Vlajka</td><td>Přesunutí fragmentu</td></tr>
<tr><td>TTL</td><td colspan="2">Protokol</td><td colspan="2">Kontrolní součet záhlaví</td></tr>
<tr><td colspan="5">Zdrojová adresa</td></tr>
<tr><td colspan="5">Cílová adresa</td></tr>
<tr><td colspan="3">Možnosti</td><td colspan="2">Náplň</td></tr>
</table>

- cílová IP adresa - IP adresa zařízení, na které jsou data směrována;

- zdrojová IP adresa - IP adresa zařízení, které odesílá data;

- Time to Live (TTL) - 8bitové pole udávající zbývající dobu životnosti paketu. Hodnota TTL se snižuje nejméně o 1 při každém průchodu paketu směrovačem (tj. po každém skoku). Pokud hodnota dosáhne 0, směrovač paket zahodí a odstraní jej ze síťového datového toku. Tento mechanismus zabraňuje nekonečnému přenosu paketů, které nemohou dosáhnout svého cíle, mezi tzv. směrovači. Pokud jsou povoleny směrovací smyčky, bude síť přetížena pakety, které nikdy nedorazí do cíle. Snižování hodnoty TTL na každém skoku zajistí, že nakonec dosáhne hodnoty 0, a pakety s polem TTL 0 budou zahozeny.

- Protokol - tato 8bitová hodnota identifikuje použitý protokol vyšší (transportní) vrstvy, například UDP nebo TCP.

- Type of Service (ToS) - obsahuje 8bitovou hodnotu, která určuje prioritu každého paketu.

- Fragment Offset - pole používané při rekonstrukci paketů rozdělených směrovači. Určuje pořadí, v jakém mají být jednotlivé pakety uspořádány při rekonstrukci.

- Příznak More Fragments (MF) - Jeden bit používaný spolu s polem Fragment Offset k rozdělení a rekonstrukci paketů. Nastavení příznaku MF znamená, že fragment není posledním fragmentem v paketu. Když přijímající hostitel zaznamená příchozí paket s nastavenou hodnotou MF = 1, zkontroluje pole Fragment Offset, aby mohl fragment umístit při rekonstrukci paketu. Pokud přijímající hostitel zjistí, že příchozí paket má nastavenou hodnotu MF = 0 a nenulovou hodnotu v poli fragment offset, použije tento fragment jako poslední blok rekonstruovaného paketu.

- Příznak DF (Don't Fragment) - Jediný bit, který, pokud je nastaven, znamená, že fragmentace paketů není povolena. Fragmentace paketů není povolena, pokud je nastaven příznak DF.

- Version - obsahuje číslo verze protokolu IP (v tomto případě IPv4).

- Délka hlavičky (IHL) - určuje velikost hlavičky paketu.

- Délka paketu - toto pole udává celkovou velikost paketu v bajtech, včetně délky paketu, včetně záhlaví a dat.

- Identifikace - toto pole slouží k jednoznačné identifikaci fragmentu rozděleného paketu IP.

- Kontrolní součet záhlaví - toto pole slouží ke kontrole chyb v záhlaví paketu.

- OPTIONS - jedná se o prostor v záhlaví IPv4 pro další pole pro podporu dalších služeb. Používá se však jen zřídka.

12.2. Adresování IPv4

Jedním z klíčových úkolů síťové vrstvy je adresování. Adresování v sítích IP je velmi podobné adresování, které používáme my lidé. Mechanismus adresování se samozřejmě liší pouze na logické úrovni. Hostitelé v síti jsou sdruženi do skupin, což usnadňuje správu a adresování.

Stejně jako lidé žijeme v určitých městských ulicích. Díky tomu se výše uvedená zásilka mé americké tety dostane k příjemci bez problémů. Nejprve trajektem do Polska, pak kamionem do vašeho města a pak menším autem na ulici a číslo domu. To je velmi podobné adresování hostitele. Pakety odesílané mezi sítěmi nejprve dorazí do sítě, ke které hostitel patří, a poté jsou odeslány konkrétnímu hostiteli. Tento typ adresování se nazývá hierarchické adresování, protože nejprve se načtou obecné informace, což je v případě přenosu dat síťová adresa, a teprve poté konkrétní informace, což je IP adresa konkrétního hostitele.

V počítačové síti mohou hostitelé mezi sebou komunikovat třemi způsoby:

- použít jeden přenos;

- prostřednictvím více misí;

- prostřednictvím vysílání.

Nejběžnější je přenos Unicast, který se používá pro typické spojení mezi dvěma hostiteli. Když například klient odešle požadavek na server, použije k tomu jediný přenos vysílání.

Použití vícesměrového vysílání může výrazně snížit spotřebu šířky pásma sítě, protože jeden paket není odeslán více hostitelům jako u jednosměrového vysílání, ale je odeslán jeden paket, který může dosáhnout více příjemců současně.

Směrovače mohou používat vícesměrové vysílání k výměně směrovacích informací a distribuci softwaru. Při vícesměrovém přenosu se používá speciální skupina adres, tzv. skupinové adresy, a v protokolu IPv4 je to rozsah uvedený níže:

224.0.0.0 až 239.255.255.255

Vysílání zase odešle paket všem hostitelům v dané síti. Používá se přitom speciální adresa, tzv. broadcastová adresa, takže v paketech IP nejsou uloženy adresy všech hostitelů v síti. Je tedy technicky nemožné použít jedno a dvě vysílání, například když není známa adresa konkrétního zařízení. Tento typ přenosu se nejčastěji používá v místních sítích a vysílání se zřídkakdy používá ke komunikaci s hostiteli mimo danou místní síť.

V celém fondu adres IPv4 existují různé skupiny adres známé jako účelové adresy. Jedná se o adresy, které se nepoužívají pro komunikaci WAN. Mezi tyto speciální adresy patří takzvané zpětné adresy. Adresa zpětné smyčky není nic jiného než vlastní adresa. kromě platné adresy IP používané pro komunikaci je každému počítači v síti přidělena také vlastní adresa, nejčastěji 127.0.0.1. Každá adresa ve fondu se navíc používá k ověření konfigurace protokolu IPv4 na hostiteli.

Dalším speciálním typem adresy je adresa místního odkazu. Tyto typy adres se používají v případech, kdy má hostitel získat IP adresu ze serveru DHCP, ale z nějakého důvodu není adresa k dispozici. Hostitel pak získá adresu z místního fondu linkových adres. Přenosy dat pomocí těchto adres mohou probíhat pouze v místní síti, kde jsou spuštěna data hostitele. Existuje také poslední sada speciálních adres, adresy TEST-NET. Stejně jako lokálně připojené adresy se používají pouze pro komunikaci v místní síti pro vzdělávací účely. Lze je použít v dokumentaci nebo v příkladech, například v online kurzech. Neměly by se však používat trvale. Speciální rozsahy adres jsou uvedeny v následující tabulce:

Rozsah adres	Název
127.0.0.1 – 127.255.255.254	Zpětná smyčka (Loopback)
169.254.0.1 – 169.254.255.254	Místní propojení (Local-Link)
192.0.2.0 – 192.0.2.254	Vzdělávání (Test-Net)

12.3. Testování síťové vrstvy

Každý operační systém implementuje programy, které umožňují testovat síťovou vrstvu. Jedním z nich je program PING, který se používá k testování spojení mezi hostiteli. Tento název je k dispozici v systému Windows a různých distribucích Linuxu. Druhým je program TRACERT, který se používá k testování směrování mezi zdrojovým a cílovým hostitelem. V systémech s jádrem Linux se stejný program nazývá TRACEROUTE.

Protokol PING používá jiný protokol síťové vrstvy, ICMP, k odeslání datagramu echo request a čekání na odpověď. Po přijetí odpovědi se zobrazí čas, který uplynul od odeslání požadavku do přijetí zpětné vazby. K testování lze použít PING:

- Tzv. lokální zásobník, tj. ověření správnosti instalace protokolu IP v počítači, stačí zadat příkaz PING v konzoli systému Windows a použít jednu z adres zpětné vazby, tj. v rozsahu 127.0.0.1 až 127.255.255.254:

- Je navázáno spojení s hostitelem v místní síti, pak místo adresy zpětné smyčky zadejte adresu hostitele v místní síti (např. 192.168.0.1):

- Připojení k hostiteli ve vzdálené síti. Pokud chcete zkontrolovat komunikaci se serverem, na kterém je stránka uložena, můžete zde místo IP adresy zadat název domény, tj. facebook.com:

Někdy se může stát, že na požadavek echo odeslaný programem PING neobdržíme odpověď, i když vzdálená síť funguje a komunikuje správně. Je to proto, že někteří správci sítí z bezpečnostních důvodů omezují nebo zcela zabraňují vkládání datagramů ICMP do svých sítí.

Další částí testování síťové vrstvy je zkoumání směrování paketů od zdrojového hostitele k cílovému hostiteli. Tisíce směrovačů pracují v rozsáhlé síti a vytvářejí takzvaný Internet, spojení mezi místními sítěmi rozesetými po celém světě.

Pro kontrolu, přes které směrovače je paket odeslán, např. z počítače na webový server, použijeme TRACERT pro Windows nebo TRACEROUTE pro Linux. Fungují úplně stejně a stejně jako PING používají protokol ICMP protokol a zprávy echo. Chcete-li provést test, zadejte do konzoly příkaz TRACERT a adresu cílového hostitele. Může to být IP adresa nebo doménová adresa, pokud chcete otestovat směrování na konkrétního hostitele, například wp.pl.

13. Úkoly vrstvy datového spoje

Hlavní a zásadní úlohou vrstvy datového spoje je poskytovat vyšším vrstvám přístup k přenosovému médiu. Data, která se při průchodu vrstvami pohybují po zásobníku dolů, musí být v určitém okamžiku doručena na médium, přes které se dostanou do svého cíle, přijímajícího hostitele. To je hlavní funkce vrstvy datového spoje: ukládá data z vyšších vrstev na médium.

Síťová vrstva, o které jsme hovořili v předchozí části tohoto kurzu, zahrnovala segmenty s adresami IP, které byly přijaty z transportní vrstvy během procesu zapouzdření a vytvořily pakety. Tyto pakety přicházejí do vrstvy datového spoje před odesláním cílovému hostiteli a poté procházejí vrstvou datového spoje do přenosového média. Ještě předtím však pakety obdrží další kontrolní informace, tentokrát fyzickou adresu zařízení, 48bitovou adresu MAC.

Z paketů se pak stanou rámce, které vstupují do média a jsou dále přenášeny k cílovému hostiteli. Adresa MAC je přiřazena při výrobě karty a uložena v paměti ROM. Paměť ROM je určena pouze pro čtení, takže není možné měnit přiřazené adresy na úrovni karty nebo hardwaru. Tyto adresy však lze změnit na úrovni systému zařízení, například v operačním systému. Někdy správci provádějí takové změny na úrovni systému, např. když nechtějí znovu konfigurovat síťový hardware, např. když do sítě přijde nový počítač.

Samotná vrstva datového spoje je prostředníkem mezi přenosovým médiem a síťovým softwarem. V případě koncových zařízení, tj. počítačů, serverů nebo telefonů, se jedná o jedinou vrstvu implementovanou nejen v softwarové, ale také v hardwarové oblasti. Fyzickou reprezentací vrstvy datových spojů je síťová karta, kterou instalujeme do počítače. Tyto karty představují rozhraní mezi síťovým softwarem a přenosovým médiem. Protože vrstva datového spoje pracuje na dvou úrovních, na úrovni hardwaru a softwaru, jsou její funkce a úkoly rovněž rozděleny do dvou menších podvrstev:

- LLC (Logical Link Control),

- MAC (Media Access Control).

Podvrstva LLC obsahuje informace o používaném protokolu síťové vrstvy, takže různé protokoly síťové vrstvy, například IPv4, IPv6 nebo IPX, mohou používat stejné přenosové médium a síťovou kartu a její funkce v počítači vykonává ovladač síťové karty. Na druhé straně podvrstva MAC definuje pravidla přístupu k médiu a vykonává adresovací funkce. Metoda MAC byla popsána v prvním díle tohoto seriálu.

Souhrnně lze říci, že vrstva datového spoje:

- přijímat data ze síťové vrstvy,

- vytvářet rámce, které lze přenášet přes médium,

- poskytuje fyzickou adresu rámce,

- Odpovídá za řízení přístupu k médiu.

Tato vrstva je implementována v koncových zařízeních, jako jsou počítače, ale také ve směrovačích a přepínačích.

Rámec a komunikace ve vrstvě datového spoje

Existuje mnoho řešení a mnoho síťových standardů pro implementaci funkcí na vrstvě 2. Máme standardy Ethernetu, máme bezdrátové sítě a nakonec máme mnoho síťových protokolů, které fungují v sítích WAN, jako je Frame Relay. Neexistuje tedy nic takového jako univerzální rámec. Každá síťová norma má svou vlastní strukturu, která je specifická pro konkrétní řešení. Shrneme-li toto téma, můžeme předpokládat, že typický rámec druhé úrovně se skládá ze tří hlavních částí:

Nadpis	Data	Zápatí
Adresy MAC **zdroj a cíl** **signál pro spuštění rámce**	pakety vrstvy síťová/internetová vrstva	signál konce snímku **kontrolní součet**

Nyní sledujme proces komunikace mezi zařízeními se zaměřením na funkce vrstvy datového spoje. Předpokládejme, že náš počítač odešle požadavek na webový server ve vzdálené síti.

Data pro odeslání takového požadavku jsou již zapouzdřena do jednoho paketu s číslem portu aplikace a logickou adresou, tj. IP adresou počítače a serveru.

Před vstupem paketu do přenosového média musí vrstva datového spoje vytvořit rámec s příslušnými adresami MAC odesílatele a příjemce rámce. V případě adresy MAC odesílatele je věc jasná, jedná se pouze o adresu MAC počítače, ale co adresa cílového hostitele? Pokud počítač a webový server nejsou ve stejné síti a nelze určit adresu MAC jeho síťové karty, je to technicky nemožné. Proč? Protože adresy MAC se používají pouze pro komunikaci v rámci sítě a nikdy mimo ni. Proto bude v poli rámce obsahujícím cílovou adresu MAC uložena adresa MAC rozhraní směrovače, ke kterému je náš počítač připojen.

Rámec je odeslán přes přenosové médium do prvního směrovače. Ten po přijetí rámce tento rámec dekapsuluje, aby mohl přečíst IP adresu zařízení, na které paket směřuje. IP adresy nelze číst přímo z rámců 2. vrstvy, proto je nutná dekapsulace. Po přečtení adresy IP z paketu (jakmile je rámec dekapsulován, data se opět stanou paketem) ji porovnejte se záznamem ve směrovací tabulce a najděte položku, která označuje, že síť serveru je směrována přes jiné směrovače.

Poté vytvoří nový rámec, jehož zdrojovou adresou bude adresa MAC rozhraní, které se připojuje k druhému směrovači, a cílovou adresou MAC tohoto směrovače.

Rámec pak projde médiem k druhému směrovači, který jej opět zapouzdří a přečte z paketu IP adresu. Zjistí, že příjemcem dat je zařízení pracující v síti, které je k němu přímo připojeno, takže proces zapouzdření provedený druhým směrovačem proběhne znovu, tentokrát do pole MAC adresa zadá adresu MAC svého druhého směrovače. Jako zdrojová adresa se použije rozhraní a jako cílová adresa MAC adresa adresního serveru.

Takto připravené snímky se přenesou na server, který je rovněž dekapsuluje. Tentokrát se však jedná o zařízení, na které data směřují, takže data kompletně dekapsuluje, tj. dodatečně přečte číslo portu aplikace, aby mohla data odeslat příslušné konkrétní aplikaci, v tomto případě webové službě.

Webová služba poté připraví data odpovědi. Data jdou nejprve do transportní vrstvy, kde je jim přiřazeno číslo portu aplikace, poté do síťové vrstvy, kde vytvoří paket s příslušnou IP adresou, a nakonec do vrstvy datového spoje, kde je z paketu připraven rámec označený adresami MAC serveru a směrovače pro připojený server.

Odpověď je poté předána médiu, které je následně odesláno klientovi. Během tohoto procesu prochází dvěma směrovači, které provádějí dekapsulaci a rekapsulaci, a protože musí přečíst IP adresu, mohou předat odpověď. Odpověď nakonec patří klientovi. Tím se data rozbalí a prohlížeč může zobrazit webovou stránku.

13.1. Protokol ARP

Když jako uživatelé sítě přenášíme data z jednoho zařízení do druhého, známe IP adresu nebo název domény zařízení, abychom mohli takové přenosy provádět. Ještě horší jsou adresy MAC, na jejichž základě my uživatelé sítě neurčujeme příjemce dat, to se děje mimo nás. Počítačové sítě založené na protokolu IPv4 používají k získání informací o MAC adrese konkrétního zařízení protokol ARP (Address Resolution Protocol).

ARP je mechanismus, který umožňuje mapování logických (tj. IP) adres na fyzické (tj. MAC) adresy. Předpokládejme, že počítač, který chce odeslat data jinému zařízení, zná jeho IP adresu, ale nezná jeho MAC adresu. Aby počítač odesílající data tuto adresu znal, vytvoří rámec ARP broadcast a před odesláním zadaných dat jej rozešle všem zařízením ve stejné síti. V poli zdrojové adresy rámce je uložena adresa počítače, který rámec připravil, a v poli cílové adresy je uložena vysílaná adresa MAC: FF-FF-FF-FF-FF-FF.

Každé zařízení, které rámec přijme, jej dekapsuluje do paketu a zkontroluje, zda je adresa IP v cílovém poli jeho adresou. Pokud cílová IP adresa není jeho vlastní, paket ignoruje; pokud je to jeho IP adresa, vytvoří nový rámec s uloženou MAC adresou a odešle jej k přenosu.

Počítač vysílající rámec vysílání nyní zná fyzickou adresu zařízení, se kterým chce komunikovat, a může zahájit komunikaci. Informace o mapování IP na MAC jsou uloženy v tabulce ARP každého zařízení pro pozdější použití. Ve výchozím nastavení systému Windows tyto záznamy trvají maximálně 10 minut a poté jsou odstraněny. Chcete-li zobrazit tabulku ARP, spusťte z konzoly příkaz arp -a. Jak vidíte, je zde několik záznamů, což znamená, že v posledních 10 minutách došlo ke komunikaci mezi mým počítačem a jiným zařízením.

13.2. Ethernet

Práce na tomto standardu se datují do 70. let 20. století, kdy se jedna z největších technologických společností Xerox rozhodla navrhnout otevřený standard síťové komunikace, který by sloužil lidem po mnoho let. Koncem 70. let 20. století vyvinula standard pro lokální sítě a stala se předlohou pro Ethernet. Ethernet je dnes standardem, který lze nalézt ve většině lokálních počítačových sítí na celém světě, a díky svým mnoha výhodám se stal standardem i pro městské sítě a v některých případech i pro rozsáhlé sítě.

Ethernet je kompletní sada síťových řešení implementovaných na vrstvě datového spoje i na fyzické vrstvě. Na vývoj této technologie v současné době dohlíží IEEE (Institute of Electrical and Electronics Engineers), který její standard zveřejnil v roce 1985 a popisuje jej pod čísly 802.2 a 802.3. Standard 802.2 zahrnuje funkce související s podvrstvou LLC, která souvisí s podvrstvou MAC a fyzickou vrstvou modelu OSI.

K úspěchu řešení založených na Ethernetu přispívá mnoho faktorů, mezi něž patří:

- snadné nasazení,

- spolehlivost,

- schopnost přizpůsobit se novým technologiím,

- náklady na implementaci jsou relativně nízké.

13.3. Vývoj sítě Ethernet

Probereme nyní vývoj sítě Ethernet. Původní verze standardu, nazývané tlusté sítě (tzv. tlustý Ethernet) a tenké sítě (tzv. tenký Ethernet), měly ve srovnání s dnešními možnostmi jen málo funkcí. Starší verze fungují na měděném přenosovém médiu (koaxiální kabel). Používají fyzickou topologii sběrnice, která se vyznačuje tím, že všechna zařízení jsou připojena ke společnému médiu. Řešení vyžaduje řízení přístupu k médiu, které je implementováno pomocí přístupu CSMA/CD.

Po mnoha letech používání řešení založených na topologii sběrnice jako přenosového média se ukazuje, že toto řešení již není dostatečně účinné. Rychlý růst sítě vede ke stále vyšším nárokům uživatelů na šířku pásma a spolehlivost. Místo koaxiálních kabelů se hojně používají kroucená dvojlinka, kabely UTP a nové topologie. Objevily se hvězdicové topologie, stejné, jaké se používají dnes, ale místo přepínačů se jako centrální bod sítě používají rozbočovače. O přepínačích tehdy nikdo neslyšel.

Použití rozbočovačů do jisté míry zlepšilo výkon počítačových sítí, ale brzy se ukázalo, že ani toto řešení není ideální. Základní vlastností rozbočovače je, že přenáší data do všech zařízení, která jsou k němu připojena. Funguje to takto, počítač, který chce odeslat data jinému zařízení, komunikuje prostřednictvím rozbočovače. Ten naopak není tak chytrý, aby přenášel data do příslušného zařízení, ale jednoduše je posílá všem připojeným zařízením.

Pouze zařízení, kterým jsou data zasílána, analyzují adresování, aby určila, zda jsou příjemci. Pokud nejsou příjemci, údaje ignorují, a pokud jsou, interpretují je.

Tento typ řešení znamená, že ačkoli fyzická topologie je hvězdicová, logicky je podobná topologii používané v předchozí generaci sítě Ethernet. I zde se používá metoda přístupu ke spoji založená na CSMA/CD, která se stala neefektivní v důsledku rychlého růstu sítě. Každý rozbočovač navíc vytváří tzv. kolizní doménu.

Čím více zařízení je k rozbočovači připojeno, tím větší je kolizní doména, a čím větší je kolizní doména, tím větší je pravděpodobnost kolizí, což omezuje propustnost a vytváří požadavky na časté opakované přenosy dat. Více kolizí není jediným problémem spojeným s používáním rozbočovačů. Mezi další nevýhody těchto zařízení patří omezená škálovatelnost a zvýšené zpoždění při přenosu dat, mimo jiné díky výše zmíněným otřesům.

Snahy o odstranění nedostatků Ethernetu založeného na rozbočovačích pokračovaly v průběhu let až do vynálezu inteligentního síťového zařízení zvaného přepínač, který vyřešil problémy, jež trápily dřívější verze Ethernetu.

Přepínače v počítačových sítích se používají dodnes a nic nenasvědčuje tomu, že by se to mělo v dohledné době změnit. Proč jsou tato zařízení tak oblíbená a proč jsou tak chytrá? Na rozdíl od rozbočovače neodesílá přepínač data všem zařízením, která jsou k němu připojena, ale pouze konkrétnímu zařízení, pro které jsou data určena, čímž samozřejmě obchází vysílání, jako je například dříve zmíněný přenos ARP. Mezi portem přepínače, ke kterému je zařízení připojeno, a samotným zařízením existuje logická topologie bod-bod. Data odeslaná do konkrétního zařízení jsou odesílána pouze do něj.

Použití přepínače téměř zcela eliminuje riziko kolizí, protože zařízení mezi sebou nemusí soupeřit o přístup k médiu. Zároveň je omezena velikost kolizní domény, protože takovou doménu tvoří pouze porty přepínače a k němu připojená zařízení. Výhod přepínačů je mnohem více. Každé zařízení připojené k portu přepínače má k dispozici vyhrazenou šířku pásma. Pokud například přepínač nabízí přenosovou rychlost 100 Mb/s, bude tato šířka pásma k dispozici každému zařízení, které je k němu připojeno.

V případě rozbočovače je tato šířka pásma sdílena mezi všemi zařízeními. Pomocí přepínače lze data přenášet i v plně duplexním režimu, což znamená, že připojená zařízení mohou přijímat a odesílat data současně.

V současné době se používá několik verzí standardu Ethernet. Nejpopulárnější z nich je standard nabízející nominální propustnost až 100 Mb/s, známý jako standard FastEthernet. Přenos v tomto standardu probíhá pouze po 2 měděných párech namísto 4 kroucených párů. Jedná se o běžné řešení používané v mnoha počítačových sítích.

Ve většině případů splňuje požadavky počítačových sítí.

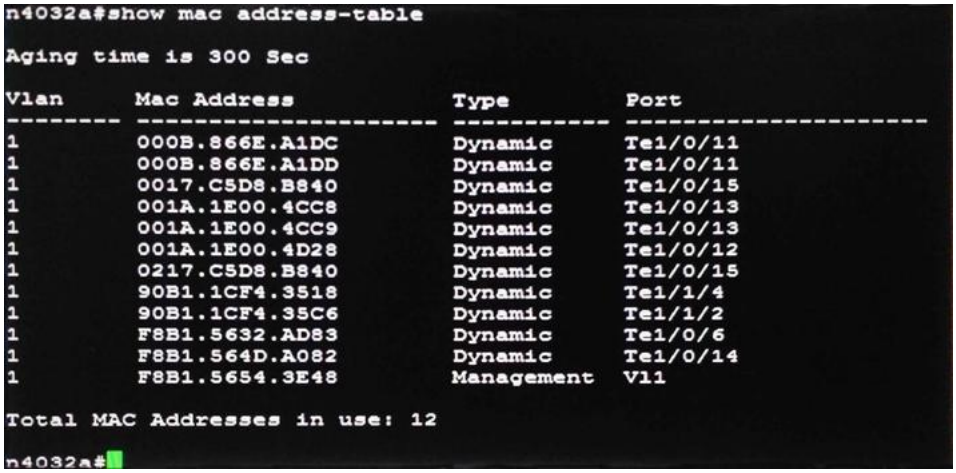
Standard Gigabit Ethernet lze použít v případě, že se požadavky na šířku pásma sítě zvyšují s množstvím přenášených dat. Nominálně poskytuje propustnost 1 Gb/s. Při použití standardu 1000BASE-T se pro přenos používají všechny měděné kroucené páry. Tato verze Ethernetu se používá ve velkých místních sítích, které používají VoIP a přenášet velké množství různých typů médií.

Pomocí standardu Ethernet lze data přenášet také po optických vláknech, v takovém případě se standard gigabitového Ethernetu nazývá 1000BASE-SX nebo LX. Existují také standardy Ethernetu, které umožňují komunikaci rychlostí 10 nebo dokonce 100 Gb/s. Používají se hlavně v metropolitních a rozsáhlých sítích, protože jejich implementace je velmi nákladná a málokdo si může dovolit používat tento typ řešení v místní síti. V následující tabulce jsou uvedeny nejrozšířenější verze standardů Ethernet a přenosové médium, které používají:

Standard Ethernet	Maximální propustnost	Použité přenosové médium	Maximální vzdálenost
100BASE-TX (fastEthernet)	100 Mb/s	UTP (kat. 5/5e)	100 m.
100BASE-FX (fastEthernet)	100 Mb/s	Optická vlákna (single/multi-mode)	400/2000 m.
100BASE-T (gigabitEthernet)	1 Gb/s	UTP (kat. 5e)	100 m.

100BASE-TX (gigabitEthernet)	1 Gb/s	UTP (kat. 6)	100 m.
100BASE-SX (gigabitEthernet)	1 Gb/s		550 m.
100BASE-LX (gigabitEthernet)	1 Gb/s	Jednovidové optické vlákno	2000 m.
10GBASE-T (10gigabitEthernet)	10 Gb/s	UTP (kat. 6/7)	100 m.
10GBASE-LX4 (10gigabitEthernet)	10 Gb/s	Jednovidové/vícevidové optické vlákno	300/10000 m.

Výše popsané přepínače používají k přenosu dat mezi zařízeními připojenými k portům přepínače adresy MAC. Každý přepínač má něco, čemu se říká tabulka adres MAC. Nejedná se o nic jiného než o soubor informací, které určují, které zařízení, respektive MAC adresa kterého zařízení, je připojeno k určitému portu.



Záznamy v takové tabulce jsou přidávány dynamicky, nikoli správcem. Přepínač načte informace uložené v tabulce během procesu učení. Přepínač z přijatého rámce přečte zdrojovou adresu MAC, přidá ji do své tabulky a přiřadí číslo portu, na kterém rámec přijal. Pokud naopak neví, komu má takový rámec poslat, protože v tabulce MAC adres příjemce není žádný záznam, nastane proces zvaný zahlcení.

To lze přirovnat k vysílání, protože rámec je odeslán všem zařízením kromě odesílatele. Zařízení, kterému není rámec adresován, jej zahodí, zatímco přijímající zařízení odpoví a odešle rámec přepínači. Přepínač přečte z rámce adresu MAC odesílatele a uloží ji do své tabulky. Celý proces učení a zaplavování je zobrazen ve výukovém videu.

Rámec Ethernetu

Vzhledem k tomu, že standard Ethernet pracuje na druhé vrstvě modelu OSI, můžete hádat, že vytváří také své rámy. Samozřejmě ano, Ethernet zapouzdřuje svůj vlastní rámec, který se nazývá ethernetový rámec. Níže si můžete prohlédnout příklad rámečku:

Velikost pole v bytech	**7**	**1**	**6**	**6**	**2**	**46 - 1500**	**4**
Název pole	Preambule	Značka začátku snímku	Adresa MAC příjemce	Adresa MAC odesílatele	Délka/typ	Data a plnění	Řídicí kód rámce (FCS)

- Preambule a značka začátku rámce - tato pole slouží k informování cílového zařízení, že je připraveno přijímat rámce;

- Cílová adresa MAC, což je fyzická adresa příjemce rámce;

- Zdrojová adresa MAC, což je fyzická adresa odesílajícího hostitele;

- Délka/Typ - pole délka určuje velikost rámce, zatímco typ určuje protokol používaný vyššími vrstvami, z nichž nejběžnější je IPv4;

- Data - jedná se o paket přijatý ze síťové vrstvy. Minimální velikost tohoto pole musí být 46 bajtů a maximální velikost musí být 1500 bajtů. Pokud je paket menší než 46 bajtů, je doplněn náhodnými daty, aby se velikost celého rámce zvětšila na požadované minimum, což je maximálně 64 bajtů.

- Kontrolní kód rámce - pole obsahující kontrolní součet rámce, který slouží k detekci případných chyb rámce. Zařízení odesílající data vypočítá kontrolní součet a vloží jej do rámce, příjemce dat po přijetí dat rovněž vypočítá kontrolní součet; pokud jsou oba kontrolní součty správné, je rámec přijat, pokud se liší, je rámec považován za poškozený a odmítnut.

Celková velikost rámce může být až 1518 bajtů (při výpočtu velikosti rámce se nezohledňuje preambule a začátek signálu rámce). K dispozici je také rámec Ethernet s maximální délkou 1522 bajtů. Takové rámce se používají ve virtuálních sítích LAN, v tzv. VLAN.

14. Základní otázky komunikace VoIP

Klíčové definice

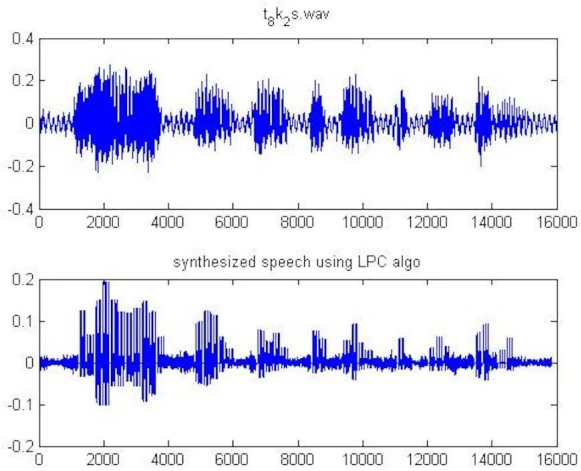
VoIP - https://pl.wikipedia.org/wiki/Voice_over_Internet_Protocol
PBX - https://pl.wikipedia.org/wiki/PBX
Kodek - https://pl.wikipedia.org/wiki/Kodek
SIP - https://pl.wikipedia.org/wiki/Session_Initiation_Protocol

Co je VoIP?

VoIP je zkratka pro Voice over Internet Protocol. Jedná se o technologii, která umožňuje odesílat a přijímat zvuk prostřednictvím počítačové sítě, a používá se k uskutečňování "telefonních hovorů" v reálném čase.

Přestože se technologie VoIP stala v posledním desetiletí velmi populární, její historie začala téměř před 100 lety ve výzkumném ústavu Bell Labs.
V roce 1938 vytvořil Homer Dudley, inženýr ze společnosti Bell Labs, první elektronický syntezátor řeči, známý jako Vocoder. Koncepce fungování byla podobná dnešnímu paketovému přenosu (IP), který zaznamenává hlasové vzorky na jednom telefonu a přehrává je na druhém. Stejná technologie se dnes používá nejen v telefonii VoIP, ale také v kochleárních implantátech.

Bez počítačové sítě není možné volat přes Internet. Historie počítačových sítí začíná v roce 1969 v americké vládní agentuře Advanced Research Project Agency. Práce agentury vedla k vývoji síťového protokolu TCP/IP a ke spuštění první počítačové sítě ARPANET. Tato síť formálně fungovala až do roku 1990.
V roce 1973 vytvořili Bob McAuley, Ed Hofstetter a Charlie Radar na MIT první hlasový paket přenášený přes ARPANET.

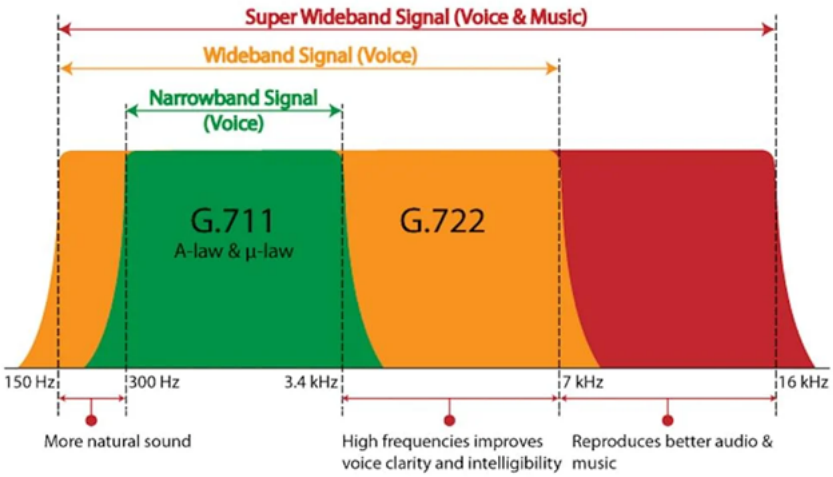


(Zdroj:: https://www.mathworks.com/matlabcentral/fileexchange/13529-speech-compression-using-linear-predictive-coding)

Tento přenos hlasu byl umožněn díky technologii LPC neboli lineárnímu prediktivnímu kódování, která je základem moderní technologie VoIP. LPC je technika analýzy řeči, která se opírá o lineární prediktivní model pro zpracování a resyntézu komprimovaných digitálních forem hlasových a řečových signálů.

V té době nebylo možné ARPANET používat soukromě. Prvním "technickým" kyberzločincem byl Leonard Kleinrock, který v roce 1973 poslal přes ARPANET zprávu o svém ztraceném elektrickém holicím strojku.

V roce 1974 mezi sebou společnosti Lincoln Lab a Culler Harrison Inc. úspěšně přenesly testovací hlasové datové pakety. V roce 1976 uskutečnily společnosti Culler Harrison a Lincoln Labs telekonferenci prostřednictvím LPC. V roce 1982 dosáhli významného pokroku a použili LPC pro připojení přes místní kabelovou síť, mobilní paketovou síť a rozhraní s PSTN (Public Switched Telephone Network).



Rysunek 2: Pierwszy szerokopasmowy kodek audio

(Zdroj obrázku: https://www.gl.com/newsletter/g722-wideband-audio-codec-support-across-tdm-voip-platforms-newsletter.html)
V roce 1988 schválila ITU-T širokopásmový zvukový kodek G.722, program, který umožňuje převádět zvuk do "digitálního" jazyka a po přenosu po síti jej převádět zpět na zvukový signál. Kodek G.722 nabízí ve srovnání se svými předchůdci výrazně lepší kvalitu řeči. G.722 nabízí rychlost přenosu dat až 64 kb/s, takže je ideální pro komunikaci VoIP - zejména v místních sítích (LAN).

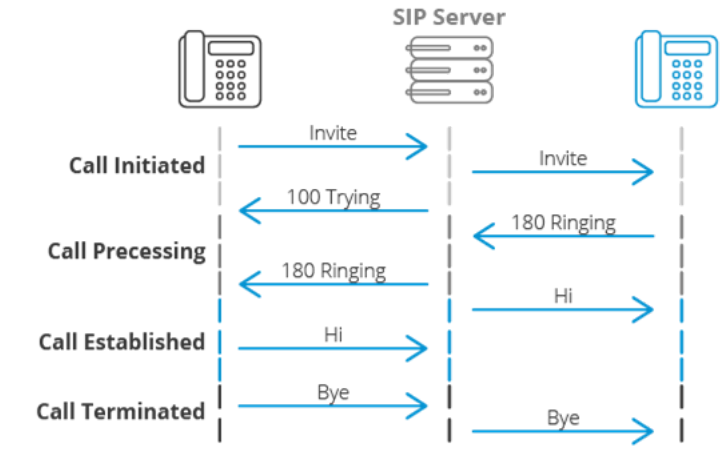
V roce 1989 vytvořil vývojář Brian C. Wiles systém RASCAL, první systém, který úspěšně přenášel hlas po sítích Ethernet - první aplikaci VoIP.

V roce 1991 John Walker ze společnosti Autodesk napsal a vydal NetFone, později známý jako Speak Freely, první softwarový telefon VoIP.

V roce 1993 se objevil první videokonferenční systém Teleport. Vývojáři Teleportu byli David Allen a Herold Williams, kteří svůj produkt prodali společnosti Hilton Hotels.

První komerční aplikací VoIP se v roce 1995 stal program VocalTec Internet Phone. Program používal protokol H.323, požadavky byly procesor 486, 8 MB RAM, 16bitová zvuková karta a připojení k internetu SLLP nebo PPP. VocalTec byl v případě mezinárodních a meziměstských hovorů levnější než klasické telefonní hovory.

V roce 1996 byl vyvinut protokol SIP (Session Initiation Protocol). První verze protokolu SIP obsahovala pouze jeden příkaz - "uskutečnit hovor" - ale v roce 1999 byly možnosti protokolu SIP rozšířeny na šest příkazů.

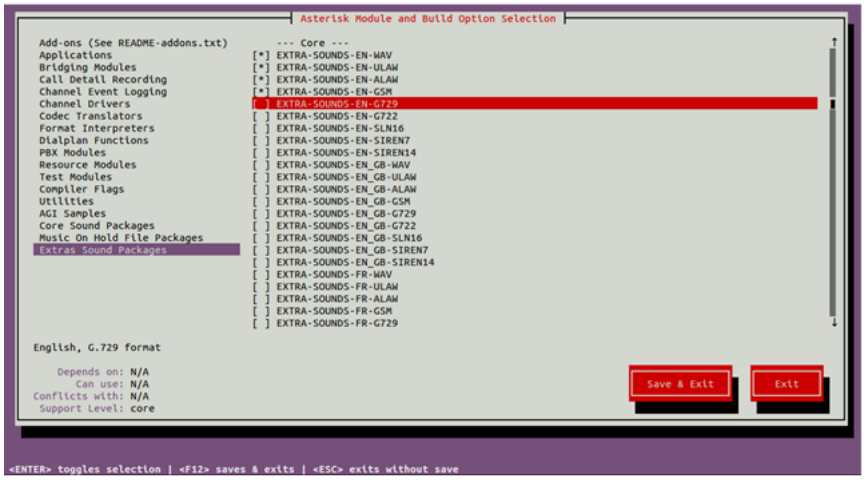


Rysunek 3: Protokól SIP

(Zdroj obrázku: https://www.3cx.pl/voip-sip/sip/)

Protokol SIP se stal preferovaným protokolem pro mobilní telefonii VoIP.

V roce 1999 se Mark Spencer rozhodl naprogramovat vlastní systém IP-PBX, program, který funguje jako telefonní ústředna, a nazval jej Asterisk. Asterisk je program s otevřeným zdrojovým kódem, který si rychle získal popularitu a dodnes jej vyvíjejí a vylepšují tisíce vývojářů.



Rysunek 4: Instalacja asterix w systemie Linux

(Zdroj obrázku: https://www.howtoforge.com/how-to-install-asterisk-17-on-ubuntu-2004/)

V roce 2003 vznikl Skype, který se brzy stal nejpoužívanějším hlasovým komunikátorem. Postupem času se Skype vyvinul ve videokomunikátor s možností přenosu souborů. Dnes ji vlastní společnost Microsoft.

V roce 2006 byla spuštěna první mobilní aplikace VoIP Truphone pro uživatele telefonů Nokia, iPhone, Android a Blackberry. Aplikace používá protokol SIP k uskutečňování hovorů přes internetové připojení, nikoli přes mobilní sítě.

V letech 2011 až 2015 došlo v USA k velkému nárůstu popularity telefonie VoIP. V celosvětovém měřítku se zvýšil počet poskytovatelů VoIP, což podpořilo konkurenci a vedlo nebo již vedlo k vytlačení starších telefonních systémů.

Pandemie COVID v roce 2020 změnila v mnoha odvětvích ekonomiky ze dne na den charakter práce na dálku. Sjednocená komunikace založená na technologii VoIP umožňuje týmům pracovat na dálku a kontaktovat zákazníky prostřednictvím různých kanálů, včetně videohovorů, mobilních aplikací, konferenčních hovorů, týmových textových zpráv a hlasové pošty.

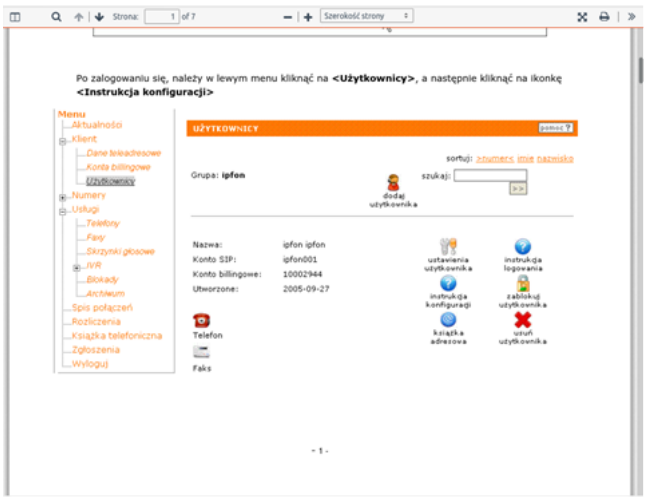
Mezi nejoblíbenější softwarové aplikace využívající technologii VoIP patří: Microsoft Teams (výchozí messenger pro operační systém MS Windiows11), Google Meet, Zoom.

VoIP pro domácnosti, VoIP pro firmy

Řešení VoIP pro domácí uživatele

Domácí uživatelé jsou ti, kteří obvykle potřebují jedno telefonní číslo.

Chcete-li si zřídit veřejné telefonní číslo PSTN s předvolbou státu a oblasti (města), musíte se zaregistrovat u poskytovatele služeb VoIP. Poskytovatel VoIP vám při registraci vytvoří účet SIP - přihlašovací jméno a heslo a sdělí vám, jak SIP nakonfigurovat. Po získání informací o účtu se můžeme přihlásit k ústředně a používat telefonii VoIP v aplikacích pro mobilní telefony, v aplikacích nainstalovaných v operačních systémech Microsoft, Apple, Linux nebo konečně v telefonech VoIP.



Rysunek 5: Przykład uzyskania danych logowania do konta SIP

(Zdroj obrázku: https://docplayer.pl/64633184-Uzyskanie-nazwy-i-hasla-konta-sip.html)

Řešení VoIP pro firmy

Pro správu více telefonů VoIP ve firmě je nutné zřídit pobočkovou ústřednu. Ústředna může být buď fyzické zařízení instalované v prostorách společnosti, nebo virtuální ústředna (software poskytovaný společností prodávající telefonní služby).

V případě virtuální pobočkové ústředny musí pevné telefony zaměstnanců společnosti podporovat VoIP. Náklady na telefon VoIP jsou srovnatelné s náklady na klasický telefon, takže pro nové firemní prostory se telefon VoIP jeví jako nejlepší volba.

Společnosti s tradičními linkami PSTN a sluchátky mohou zůstat u přidělených telefonních čísel dvěma způsoby:

- nákup pobočkové ústředny VoIP s moduly PSTN/ISDN bez nutnosti výměny telefonů,
- přenos čísel do virtuální pobočkové ústředny a nahrazení telefonů telefony s podporou VoIP.

Přehled aplikací VoIP

Aplikace související s VoIP lze rozdělit na:

- klient - nainstalovaný na telefonech/počítačích koncových uživatelů VoIP.
- serverové aplikace - instalované na běžných serverech nebo vyhrazených pobočkových ústřednách.

Klientské aplikace

Moderní technologie mobilních telefonů je založena na digitální technologii, takže zvuk je přenášen prostřednictvím kodeku.

V současných chytrých telefonech je přidání čísla VoIP možné bez instalace dalšího softwaru. V nastavení systému Android nebo iOS můžeme zadat údaje o účtu SIP a používat telefonování VoIP. Existuje také mnoho aplikací VoIP, které poskytují další funkce (např. sdílený adresář atd.). Při výběru způsobu používání telefonie VoIP je nejlepší řídit se doporučeními poskytovatele služby VoIP. Poskytovatelé služeb mají často vlastní aplikaci určenou pro využívání služeb VoIP.

Na stolních počítačích, noteboocích nebo tabletech bez možnosti připojení k mobilní síti můžeme používat VoIP přes internet. Stačí tedy připojit notebook k síti Wi-Fi a nainstalovat aplikaci VoIP, abyste mohli telefonovat.

Existuje mnoho populárních aplikací, které umožňují telefonní připojení VoIP k veřejné komutované telefonní síti (PSTN) : Microsoft Teams, ZOIPER, Blink, Zoom atd. Seznam klientských aplikací VoIP můžeme sledovat na adrese: https://en.wikipedia.org/wiki/List_of_SIP_software ;

Serverové aplikace

Server SIP spravuje volání v síti, přijímá požadavky klientů VoIP na navázání a ukončení volání.

Nejoblíbenějším open source serverem SIP je Asterix (https://www.asterisk.org). Chcete-li ve firmě provozovat Asterix, musíte mít nainstalovaný server s operačním systémem Linux. V distribucích Linuxu, které obsahují server Asterix, jsou k dispozici balíčky deduplikačního softwaru. Nejlepší způsob instalace serveru Asterix je stažení speciálně připravené distribuce Linuxu - freePBX (https://www.freepbx.org/downloads/). Asterix má mnoho funkcí moderní telefonie, mimo jiné: SMS, hudba při čekání/připojení, hlasová schránka.

15. Výkonnost sítě. Seznámení se s metodami snižování síťového provozu.

Faktory ovlivňující výkonnost počítačové sítě

Výkonnost počítačové sítě ovlivňují:

Pasivní části počítačové sítě, což jsou části počítačové sítě, které slouží pouze k přenosu dat mezi aktivními síťovými zařízeními. Mezi pasivní části počítačové sítě patří: měděné kabely, optické kabely, síťové zásuvky a rozvodné panely.

Aktivní zařízení jsou části počítačové sítě, které přenášejí/přijímají informace nebo slouží k přenosu/rozšíření dat v počítačové síti. Mezi aktivní zařízení patří: síťové karty, přepínače, síťové zesilovače/opakovače.

Elektromagnetické rušení, které ovlivňuje bezdrátový přenos a měděné kabely (kroucené páry).

15.1. Kvalita kroucené dvojlinky

Kroucená dvojlinka přenáší informace ve formě elektrických impulsů. Kroucená dvojlinka obsahuje 8 měděných žil (vodičů) potažených izolací. Pro lepší přenos dat jsou vodiče zkrouceny do párů. Rychlost a kvalitu přenosu dat ve formě elektrických impulsů nejvíce ovlivňuje elektromagnetické rušení.

Kvalitu zpracování kroucených kabelů ovlivňují:

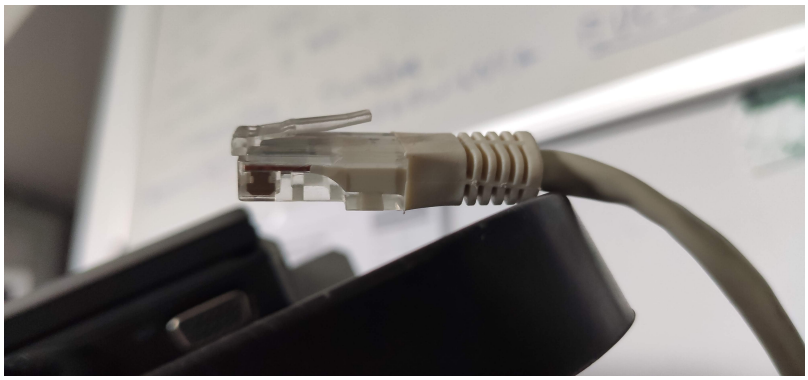
- kvalita zpracování měděného vodiče, tj. čistota kovu, zachované rozměry profilu.
- kvalitu a množství izolace.

V závislosti na množství izolace a použitých metodách stínění (ochrana proti rušení) se kroucená dvojlinka definuje podle kategorie 1 až 8 a typu stínění: U - nestíněný, F - stíněný fólií, S - stíněný síťkou, SF - stíněný fólií a síťkou. Vyšší kategorie kabelu zajišťuje rychlejší přenos dat, například: kategorie 5 UTP, ScTP, STP zajišťuje přenos až 1 Gb/s; kategorie 6 UTP, ScTP, STP - 10 Gb/s.

Síťové kabely jsou zakončeny konektory RJ45. Kvalita použitého materiálu a stínění RJ45 má samozřejmě vliv na přenos dat.

Příklady poškození kroucené dvojlinky

Ve videu 1 vidíme kabel kategorie 6 vyrobený v továrně na specializované výrobní lince. Kabel vložený do zásuvky si zachovává své vlastnosti a koncovka RJ45 funguje správně i po opakovaném připojení počítače. Ochrana proti nežádoucímu vypadnutí kabelu funguje správně - je slyšet charakteristické cvaknutí. Kabel také nelze vytáhnout bez uvolnění ochrany. Tento stav kabelu zaručuje správný přenos dat.



Na obrázku je kvalitní síťový kabel se správnou zástrčkou RJ45.

Video 2 ukazuje kabel vyrobený svépomocí s použitím špatné zástrčky RJ45. Špatná kvalita plastu vede k poškození ochrany. Toto poškození znamená, že kabel může vypadnout ze zásuvky - přenos dat se přeruší.

Video 3 - kroucen

Video 4 - kabel kategorie 5e. Ze zástrčky RJ45 vypadla vnější izolace. Příslušné páry vodičů musí být zkroucené, aby se neutralizovalo rušení při přenosu signálu. V tomto případě není zajištěno správné zkroucení párů.

15.2. Optická vlákna

Optická vlákna přenášejí informace ve formě světelných pulzů. Díky jevu úplného vnitřního odrazu je světlo proudící uvnitř optického vlákna zachyceno. Proto je možné přenášet informace na mnohem větší vzdálenost beze ztrát než u měděných kabelů.

Světlo, které prochází optickým vláknem, je zeslabeno. Protože dosud nebyla vynalezena metoda, která by umožnila vyrobit dokonale odrazivé optické vlákno, dochází k úbytku optického výkonu. V současné době jsou optické kabely schopny přenášet informace na maximální vzdálenost přibližně 100 km beze ztrát. Díky použití optických zesilovačů na určité vzdálenosti můžeme prostřednictvím optických sítí propojit velmi vzdálená místa.

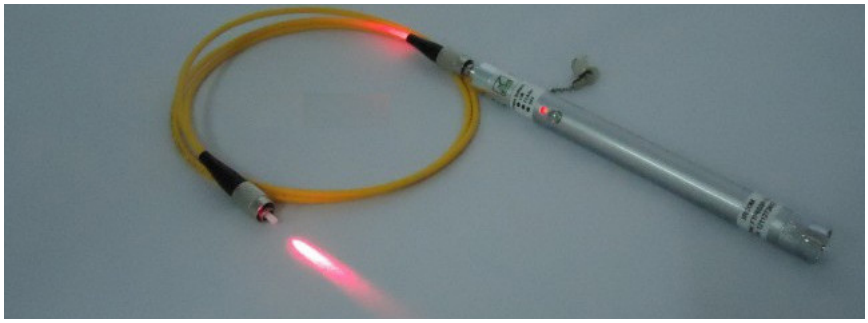
Kvalita optických sítí je ovlivněna především kvalitou práce při jejich pokládce. Pozornost je třeba věnovat:

- maximální poloměr ohybu kabelu - v závislosti na normě je poloměr ohybu: 30, 10 7,5 mm,
- kvalita řezacího zařízení - po řezání nesmí být okraj optického vlákna roztřepený,
- kvalita svářečky

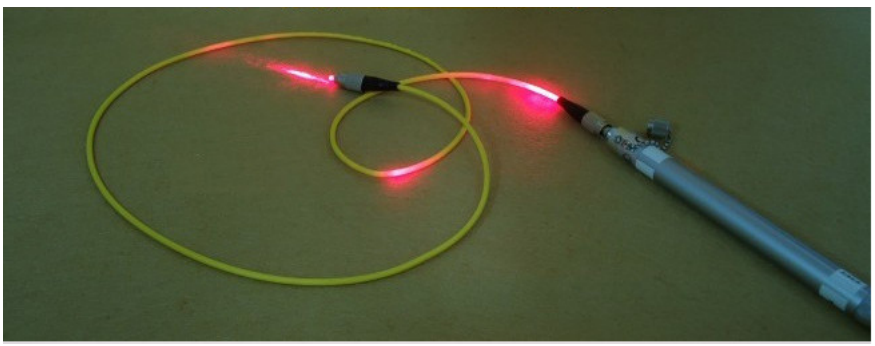
Příklady závad

Jedním ze způsobů testování optického vlákna je použití vizuálního lokátoru poškození:

- Optické vlákno normální



- optické vlákno vadné



K výše uvedenému poškození došlo pravděpodobně překročením poloměru ohybu optického vlákna.

15.3. Síťové přepínače, síťové karty

Síťový přepínač je zařízení pro přenos dat mezi hostiteli v počítačových sítích. Hostitel je jakékoli zařízení připojené k počítačové síti - notebook, tiskárna, televizor atd.

Největší vliv na výkon sítě má přepínač. Propustnost portů vyjádřená v bitech za sekundu (100 Mbit/s, 10 Gbit/s), tj. kolik dat lze do přepínače odeslat za maximálně jednu časovou jednotku, je nejdůležitějším faktorem určujícím výkon počítačové sítě.

Přepínač zpracovává více připojení mezi hostiteli současně, proto je důležité věnovat pozornost parametrům, jako je množství paměti, rychlost procesoru a propustnost. (Přepínací kapacita systému, propustnost systému).

Příklad přepínače

Síťové karty jsou zařízení, která umožňují připojení hostitele k počítačové síti. Základním parametrem síťové karty je rychlost odesílání a příjmu dat vyjádřená v bitech za sekundu (100Mbit/s, 1Gbit/s atd.). Při připojování hostitele k přepínači je třeba mít na paměti, že výkon sítě bude odpovídat zařízení s nejnižší propustností - příklad 100Mb/s přepínač + 1000Mb/s síťová karta dává maximální propustnost 100Mb/s.

15.4. Testy výkonnosti sítě

Rušení sítě

Ke ztrátě dat v důsledku elektromagnetického rušení může docházet jak v bezdrátových sítích, tak v sítích využívajících měděné kabely. Elektrické sítě, zařízení napájená vysokými proudy produkují elektromagnetické záření.

Pokud se jakákoli část sítě WiFi nachází v blízkosti zařízení, jako je elektrický vlak nebo tramvaj, lze očekávat rušení přenosu dat.

Síťové kabely vyrobené z mědi jsou podobně ovlivněny elektromagnetickým zářením. Sítě, kde jsou kabely UTP umístěny příliš blízko elektrických kabelů, mohou být vystaveny elektromagnetickému rušení.

Pokud se v dané lokalitě očekává elektromagnetické rušení, použijte jako nosič dat optická vlákna, která jsou vůči elektromagnetickému záření odolná.

Testy výkonnosti počítačové sítě

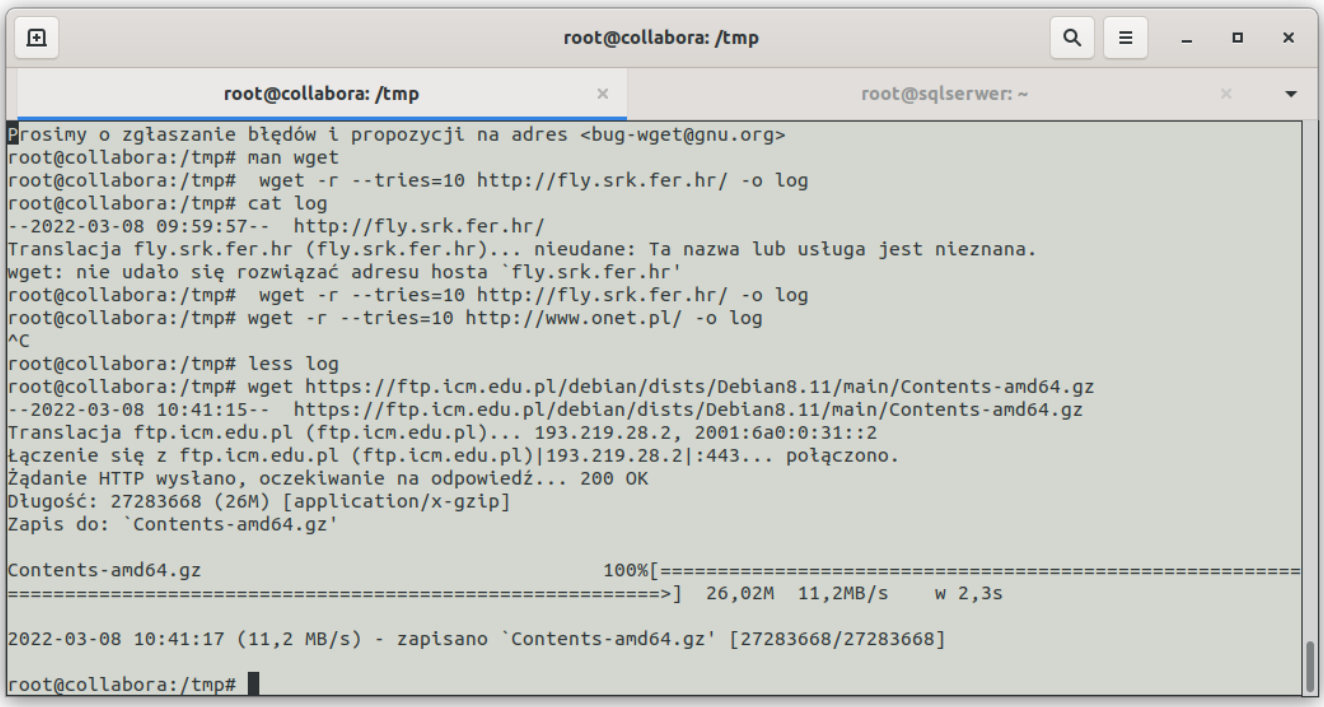
Výkonnost počítačové sítě spočívá v určení propustnosti, tj. množství informací, které můžeme studovanou sítí odeslat za určitý čas. Nejjednodušší způsob, jak určit výkonnost sítě, je tedy stáhnout/odeslat určitý objem dat a změřit čas, který to zabere.

Výsledky testu výkonnosti sítě mohou být zkresleny dalšími faktory, které nejsou přímo součástí počítačové sítě. Při odesílání nebo stahování dat je důležité mít na paměti, že je třeba je číst a zapisovat na disk. Pokud má pevný disk počítače maximální rychlost čtení/zápisu nižší než rychlost sítě, výsledek testu propustnosti nezobrazí výkon sítě, ale pouze výsledek čtení/zápisu dat na pevném disku. V tomto případě můžeme říci, že takzvaným "úzkým hrdlem" našeho počítačového systému je pevný disk. Dalším častým faktorem, který snižuje výkon sítě, jsou limity rychlosti stahování uplatňované na serverech pro sdílení souborů. Protože poskytovatelé stahování musí zajistit, aby mělo ke stahovaným souborům přístup co nejvíce klientů, nemohou při stahování umožnit dosažení maximální rychlosti stahování pouze jednomu klientovi. Souborové servery dělí maximální rychlost odesílání ze serveru ke klientovi předpokládaným počtem klientů za dané časové období, takže při stahování souboru přes internet s propustností například 300 Mb/s je maximální přenos například 10 Mb/s.

Pro testování propustnosti sítě můžeme použít libovolný program, který stahuje/odesílá data. Pro získání spolehlivých výsledků je však třeba jej opakovat mnohokrát v různých dnech a časech. Test výkonu můžeme provést pomocí programů, jako je wget, ping, nebo pomocí webových stránek k tomu určených: speeedtest.net, www.nperf.com.

wget

Program wget je konzolový program, který se nejčastěji používá v prostředí Linux. V systému MS Windows od verze 10 lze snadno "nainstalovat" Linux pomocí technologie WSL (Windows Subsystem for Linux). Chcete-li provést test šířky pásma sítě pomocí programu wget, zadejte v konzole (textovém terminálu) následující příkaz: wget https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz , tento příkaz spustí stahování z internetové adresy: https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz. Jak vidíme na obrázku níže, získáme následující informace: 26 MB bylo staženo rychlostí 11,2 MB/s za 2,3 sekundy.



(Obrázek 1. Test rychlosti sítě pomocí programu wget)

Pomocí programu wget můžeme provést více testů současně, např.:

wget -r --tries=10 http://www.onet.pl/ -o log

Zde provádíme rekurzivní stahování (-r) obsahu www.onet.pl , pokusy o stažení se opakují desetkrát, výsledky se zaznamenávají do souboru protokolu. Výsledky uložené v souboru protokolu ukazují čas a rychlost přenosu z webové stránky.

ping

Dalším konzolovým programem dostupným v různých operačních systémech je ping.

Příklad testu výkonnosti sítě pomocí příkazu ping:

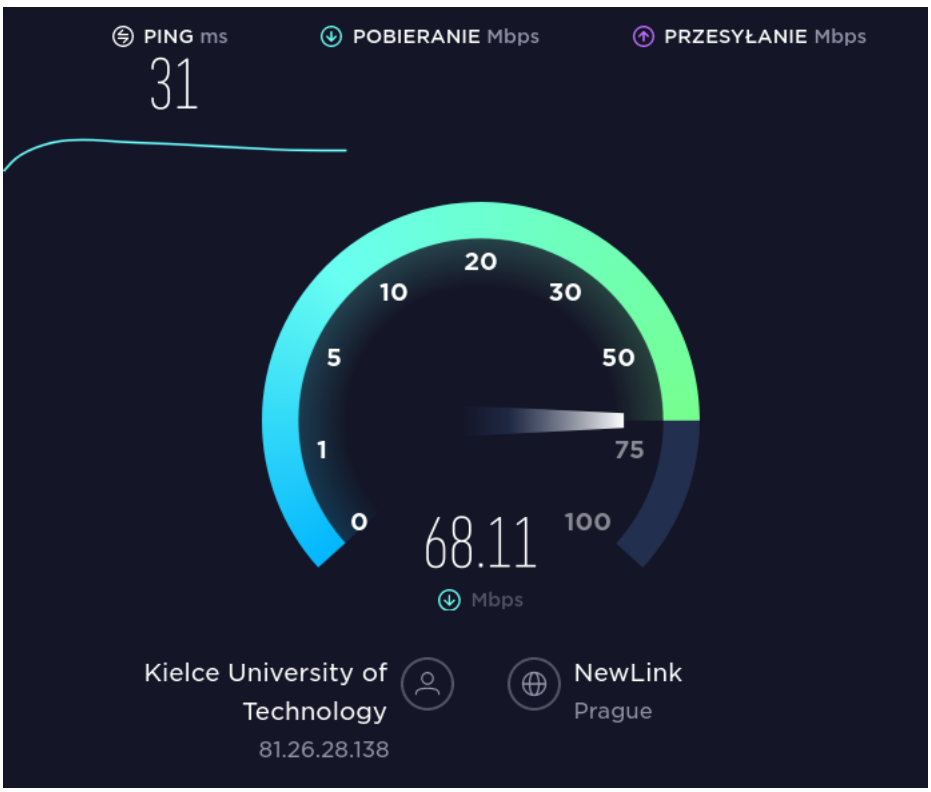
```
ping wp.pl
PING wp.pl (212.77.98.9) 56(84) bytes of data.
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=1 ttl=55 time=16.0 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=2 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=3 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=4 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=5 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=6 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=7 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=8 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=9 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=10 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=11 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=12 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=13 ttl=55 time=15.2 ms

--- wp.pl ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12015ms
rtt min/avg/max/mdev = 15.185/15.307/16.032/0.212 ms
```

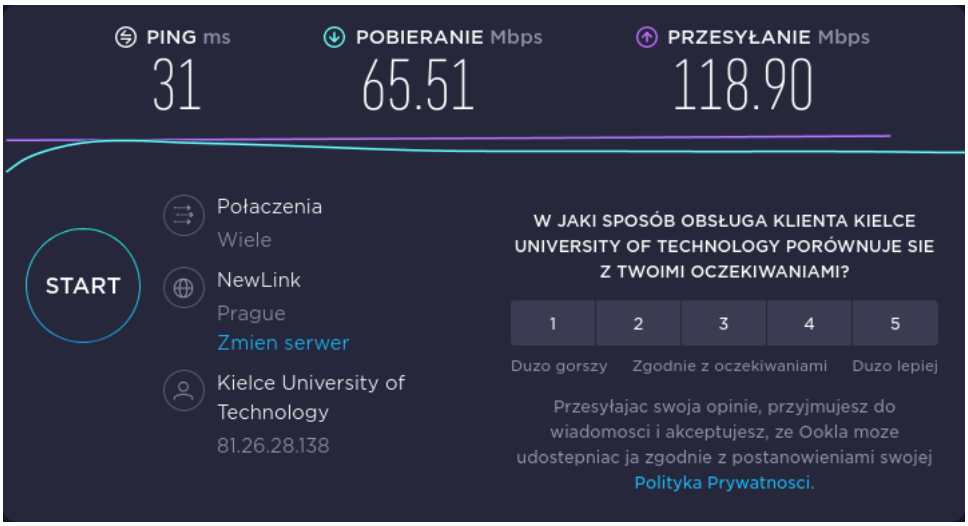
Ve výše uvedeném příkladu byl serveru s adresou www.wp.pl 13krát odeslán paket ICMP Echo Request a stejný počet odpovědí (ICMP Echo Reply) byl přijat. Poslední řádek příkladu (min/avg/max/mdev = 15,185/15,307/16,032/0,212 ms) obsahuje výsledek testu rychlosti průchodu paketu sítí - čím nižší je doba odezvy, tím je naše síť efektivnější.

speedtest.net

Existují také webové aplikace pro testování rychlosti stahování a nahrávání. Na adrese https://www.speedtest.net můžeme provést test zobrazující jak hodnotu PING, tak rychlost stahování a odesílání. Níže uvedené obrázky ukazují snímky obrazovky z testu nahrávání internetu mezi sítí v Kielcích (Polsko) a sítí v Praze (Česká republika).



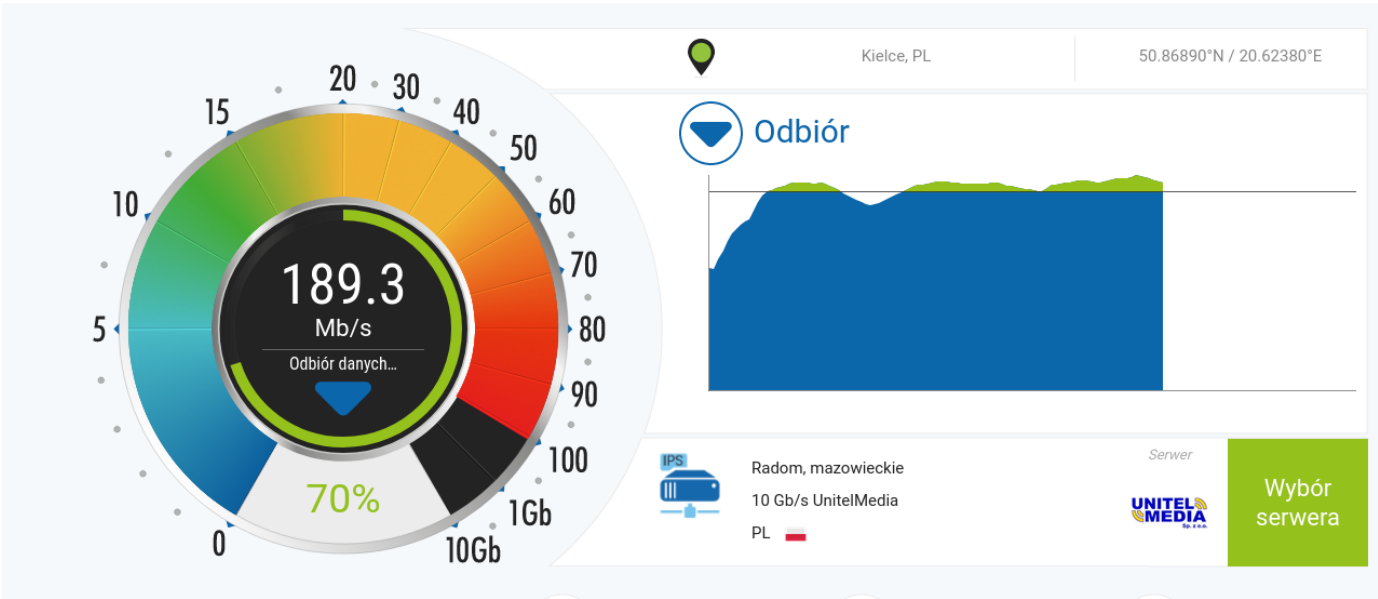
Obrázek 2. Test rychlosti sítě pomocí speedtest.net



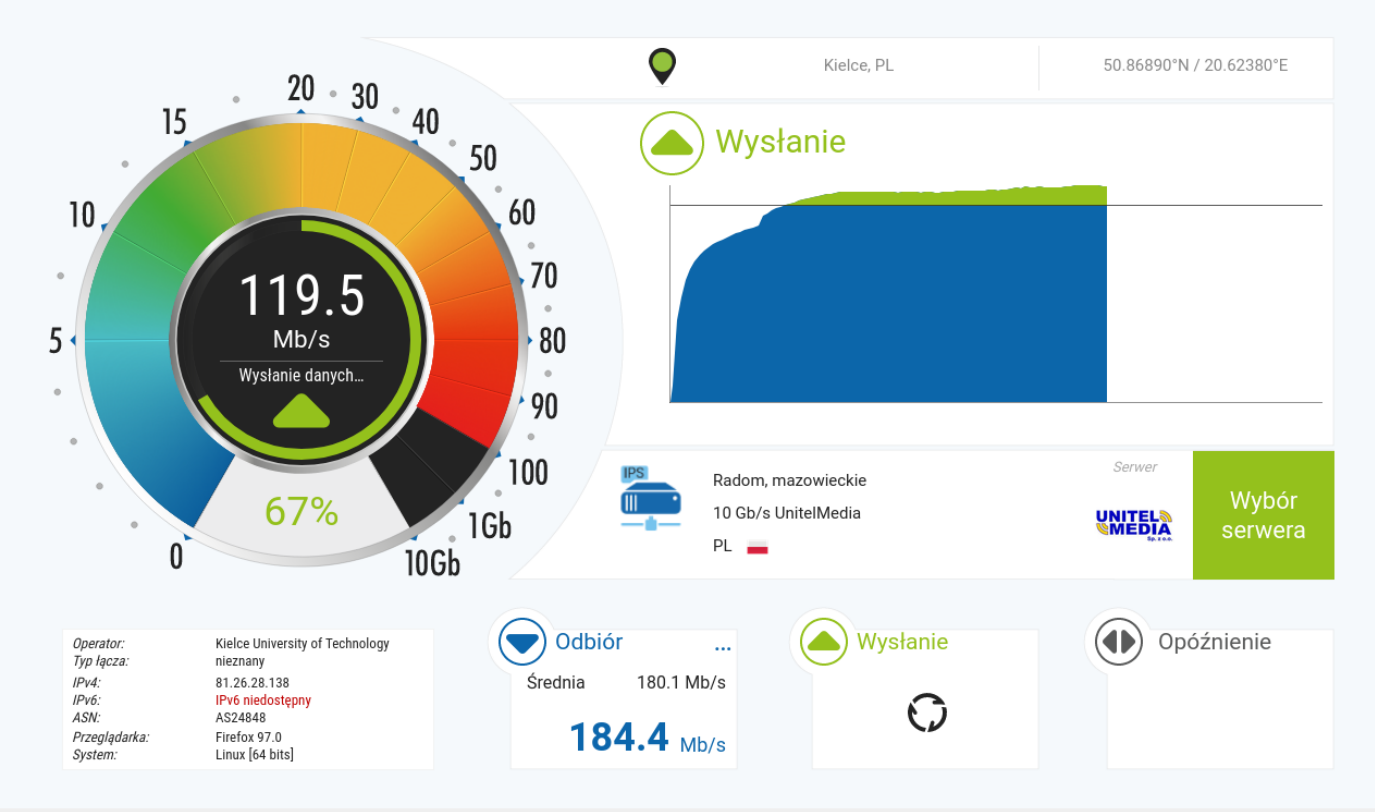
Obrázek 3. Výsledek testu sítě pomocí speedtest.net

www.nperf.com

Webová aplikace npref.com je podobná aplikaci speedtest.net. Výsledky jsou rovněž prezentovány v atraktivní grafické podobě.



Obrázek 4: Test rychlosti sítě s www.nperf.com



Obrázek 5: Test rychlosti sítě s www.nperf.com

15.5. Omezení síťového provozu na příkladu "domácího" směrovače

Směrovač připojuje domácí (firemní) síť k internetu. Na směrovači můžeme omezit rychlost, zakázat přístup k internetu místním hostitelům. Výluky a omezení provozu mohou být trvalé nebo aktivované na určitou dobu.

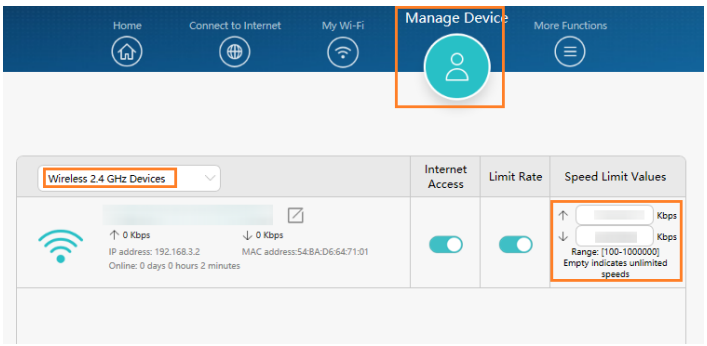
V "domácím" směrovači, tj. levném zařízení určeném pro obsluhu sítě sestávající z několika až několika desítek hostitelů, můžeme zakázat přístup a omezit rychlost stahování a odesílání. Možnosti omezení síťového provozu samozřejmě závisí na modelu směrovače.

Účelem zavedení omezení přenosové rychlosti je ochrana před poklesem rychlosti stahování nebo odesílání na klíčových hostitelích v naší domácí síti. Pokud například předpokládáme, že náš notebook, na kterém pracujeme na dálku, by měl mít během telekonference stabilní připojení k internetu, zavedli bychom omezení rychlosti pro všechna ostatní zařízení.

Příklad povolení omezení rychlosti v routeru Wi-Fi Huawey:

Připojte počítač/telefon ke směrovači Wi-Fi (na výrobním štítku na spodní straně směrovače zjistěte výchozí název Wi-Fi bez hesla) nebo připojte počítač k portu LAN směrovače pomocí kabelu Ethernet. Zadejte výchozí IP adresu do adresního řádku prohlížeče a přihlaste se na stránku webové správy (zkontrolujte výchozí IP adresu na výrobním štítku na spodní straně směrovače).

Klikněte na možnost Spravovat zařízení, vyberte telefon nebo počítač, pro který chcete nastavit limit, povolte možnost Omezit rychlost a kliknutím na ikonu v části Hodnoty omezení rychlosti nastavte maximální rychlost odesílání a stahování.



Obrázek - Obrazovka konfigurace zařízení, zdroj: https://consumer.huawei.com/en/support/content/en-us15806295/ ;

15.6. Základní testování počítačových sítí

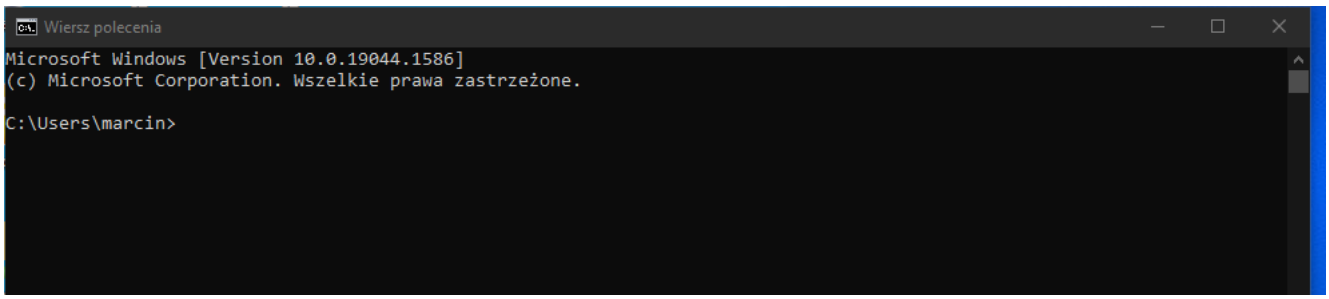
Testy počítačových sítí v prostředí MS Windows a UNIX-Like pomocí programů:

- ping
- tracert
- telnet
- nc
- wget

Všechny výše uvedené programy se spouštějí zadáním příkazu do terminálu/příkazového řádku.

V operačním systému Linux s grafickým prostředím / macOS je třeba spustit terminál, aby bylo možné provádět příkazy zadané z klávesnice. Příkazy se zadávají v okně terminálu.

V operačním systému MS Windows je pro spuštění příkazu zadaného z klávesnice nutné spustit příkazový řádek. Chcete-li spustit příkazový řádek v systému Windows 10/11, klikněte na tlačítko "Start" a do vyhledávacího okna zadejte cmd.



15.7. ping

Popis programu ping

Program ping slouží k diagnostice síťových připojení. Používáme ji ke kontrole kvality spojení mezi počítači, které odesílají požadavky a posílají zpět odpověď.

Ping odpoví na následující otázky:

- Existuje mezi počítači spojení?
- Jaká je doba odezvy odeslaného paketu?

Spusťte program v příkazovém řádku MS Windows (terminál Linux/Mac). Do příkazového řádku zadejte: ping [IP nebo název] a potvrďte stisknutím klávesy Enter.

Příklad fungování programu ping v systému Linux:

```
ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.364 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.274 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.433 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.545 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=64 time=0.380 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=64 time=0.284 ms
64 bytes from 10.10.10.1: icmp_seq=7 ttl=64 time=0.477 ms
64 bytes from 10.10.10.1: icmp_seq=8 ttl=64 time=0.257 ms
^C
--- 10.10.10.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7154ms
rtt min/avg/max/mdev = 0.257/0.376/0.545/0.099 ms
```

Ve výše uvedeném příkladu byl 8krát odeslán paket ICMP Echo Request a stejný počet odpovědí (ICMP Echo Reply) byl přijat. Pakety byly odeslány z počítače s IP 10.10.10.2 na počítač s IP 10.10.10.1. Průměrná doba odezvy byla 0,376 milisekundy.

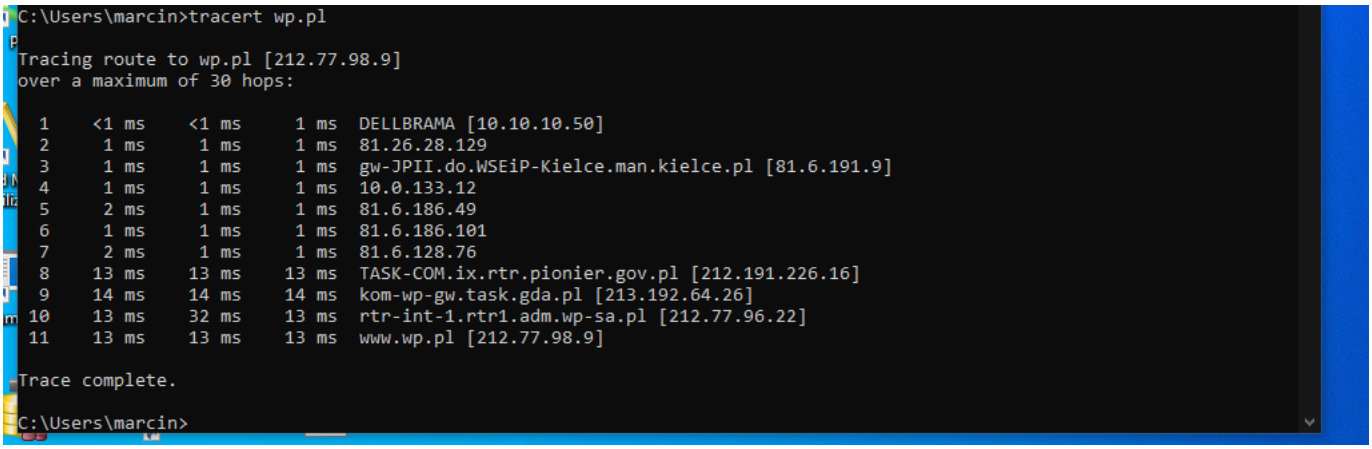
15.8. tracert

Tracert je program pro určení směrování (trasy) paketů v síti IP tracert (MS Windows) / traceroute (Linux/macOS).

Funkce Tracert/traceroute vrátí seznam po sobě jdoucích směrovačů na trase k cílovému počítači v síti.

Čím delší je trasa - čím větší je počet směrovačů - tím obtížnější je komunikovat s cílovým počítačem v síti. Pokud je na naší trase špatně nakonfigurovaný směrovač, budeme mít ztížený přístup k danému počítači (pomalé načítání webových stránek, chyby při stahování souborů, špatná kvalita internetového rádia atd.).

Příklad zkoumání trasy z prostor univerzity na server wp.pl:



Ve výše uvedeném příkladu vidíme 11 uzlů (směrovačů).

15.9. telnet

Telnet je program, který se používá k připojení ke vzdálenému serveru. Telnet je instalován na počítačích serverové třídy, ale je také široce používán na všech typech síťových zařízení (např. přepínače, AccessPoint).

Pomocí telnetu můžete zkontrolovat, zda je na vzdáleném počítači spuštěna určitá služba, např. SMTP nebo HTTP.

Chcete-li zkontrolovat připojení mezi klientským počítačem a serverem v příkazovém řádku (terminálu), zadejte příkaz:

telnet [adresa testovaného serveru] [zadaný port služby]

Pokud chcete zjistit, zda je v počítači www.nasa.gov funkční server STMP a zda se k němu budete moci připojit z počítače a odesílat poštu, zadejte příkaz:

telnet www.nasa.gov 25

kde 25 je číslo portu TCP, na kterém služba SMTP (odesílající poštu) naslouchá.

15.10. nc

Netcat (nc) je příkaz spouštěný v terminálu. Je k dispozici v systémech Linux a macOS Lze jej použít k testování provozu více portů TCP na vzdáleném serveru současně.

Příklad:

v linuxovém terminálu zadám:

nc -z -v 10.10.10.1 22

Příkaz vrátí výsledek:

Connection to 10.10.10.1 22 port [tcp/ssh] succeeded! (Připojení k portu 10.10.10.1 22 [tcp/ssh] úspěšné!)

To znamená úspěšné připojení k hostiteli 10.10.10.1 na portu TCP 22.

15.11. wget

Wget je konzolový program, který slouží ke stahování souborů. Wget vrací rychlost stahování, takže získáme informace o výkonu našeho internetového připojení.

Příklad:

V terminálu zadám:

wget https://download.moodle.org/download.php/direct/stable311/moodle-latest-311.tgz -O moodle-latest-311.tgz

To znamená, že budu stahovat soubor ze serveru https://download.moodle.org, stažený soubor uložím pod názvem **moodle-latest-311.tgz**.

Po zadání příkazu v terminálu vrátí wget následující informace:

--2022-03-31 11:31:57-- https://download.moodle.org/download.php/direct/stable311/moodle-latest-311.tgz
Resolving download.moodle.org (download.moodle.org)... 104.22.64.81, 104.22.65.81, 172.67.26.233, ...
Connecting to download.moodle.org (download.moodle.org)|104.22.64.81|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 60212386 (57M) [application/g-zip]
Saving to: 'moodle-latest-311.tgz'

moodle-latest-311.tgz 100%
[===>]
57,42M 11,0MB/s in 5,2s

2022-03-31 11:32:03 (11,1 MB/s) - 'moodle-latest-311.tgz' saved [60212386/60212386]

Vidíme, jakou rychlostí byl soubor stažen - 11,0 MB/s.