# 17. HTTP, HTTPS, POP3 a IMAP

## Teoretická část

**Vysvětlete a popište webové protokoly http a HTTPS**. **Vysvětlete a popište emailové protokoly POP3, SMTP a IMAP. Vysvětlete zabezpečení používaná v HTTPS a SSL. Popište skladbu hypertextového odkazu.**

## Praktická část

1. **Předveďte a vysvětlete použití hypertextových odkazů v internetu včetně https.**
2. V úloze WIN7 předveďte nastavení pošty a vysvětlete možnosti.

## Doplňující otázky

1. **Přiřaďte porty ke službám: 443, 143, 25, 110, 80.**

# Webové protokoly

## http

**HTTP (Hypertext Transfer Protocol)** je [internetový](https://cs.wikipedia.org/wiki/Internet) [protokol](https://cs.wikipedia.org/wiki/Protokol_(informatika)) určený pro **výměnu** [**hypertextových**](https://cs.wikipedia.org/wiki/Hypertext)**dokumentů** ve formátu [HTML](https://cs.wikipedia.org/wiki/HyperText_Markup_Language). Používá obvykle port [**TCP**](https://cs.wikipedia.org/wiki/Transmission_Control_Protocol)**/80.**

Protokol funguje způsobem dotaz - odpověď. Uživatel (pomocí programu, obvykle [internetového prohlížeče](https://cs.wikipedia.org/wiki/Internetov%C3%BD_prohl%C3%AD%C5%BEe%C4%8D)) pošle [serveru](https://cs.wikipedia.org/wiki/Webov%C3%BD_server) dotaz ve formě čistého textu, obsahujícího označení požadovaného dokumentu, informace o schopnostech prohlížeče apod. Server poté odpoví pomocí několika řádků textu popisujících výsledek dotazu (zda se dokument podařilo najít, jakého typu dokument je atd.), za kterými následují data samotného požadovaného dokumentu.

Pokud uživatel bude mít po chvíli další dotaz na stejný server (např. proto, že uživatel v dokumentu kliknul na hypertextový odkaz), bude se jednat o další, nezávislý dotaz a odpověď. Z hlediska serveru nelze poznat, jestli tento druhý dotaz jakkoli souvisí s předchozím. Kvůli této vlastnosti se protokolu HTTP říká bezestavový protokol – protokol neumí uchovávat stav komunikace, dotazy spolu nemají souvislost. Tato vlastnost je nepříjemná pro implementaci složitějších procesů přes HTTP (např. internetový obchod potřebuje uchovávat informaci o identitě zákazníka, o obsahu jeho „nákupního košíku“ apod.). K tomuto účelu byl protokol HTTP rozšířen o tzv. [HTTP cookies](https://cs.wikipedia.org/wiki/HTTP_cookie), které umožňují serveru uchovávat si informace o stavu spojení na počítači uživatele.

## HTTPS

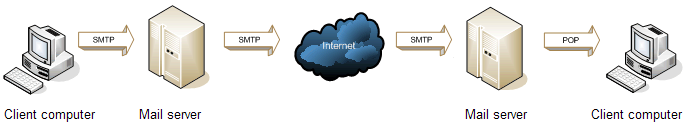
**HTTPS (Hypertext Transfer Protocol Secure)** je v [informatice](https://cs.wikipedia.org/wiki/Informatika) nadstavba síťového [protokolu](https://cs.wikipedia.org/wiki/Protokol_(informatika)) [HTTP](https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol), která umožňuje **zabezpečit spojení** mezi klientem (např. webovým prohlížečem) a serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany. HTTPS používá protokol HTTP, přičemž přenášená **data jsou šifrována pomocí**[**SSL**](https://cs.wikipedia.org/wiki/Secure_Sockets_Layer) nebo [TLS](https://cs.wikipedia.org/wiki/TLS) a standardní [port](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_port) na straně serveru je **443.**

**Protokol HTTPS využívá**[**asymetrické šifrování**](https://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie). Obě strany si před zahájením komunikace vygenerují pár klíčů (privátní a veřejný). Při zahájení komunikace si vymění veřejné klíče, které by obě strany měly ověřit pomocí jiného komunikačního kanálu.

Za certifikáty vydané certifikačními autoritami, které mají svůj veřejný klíč v úložišti, které je dodáváno s webovým prohlížečem, je nutné platit

# Co to je Mail Server?

**Mailový server** (Poštovní server) je server, který **dohlíží na emaily a doručuje je skrze síť**, nejčastěji skrze Internet. Mail Server muže přijmout emaily od klientů a doručit je jiným Mailovým serverům. Mailový server doručuje emaily také klientským počítačům. Klientský počítač je počítač, kde čtete emaily, kupříkladu firemní nebo domácí počítač. Nebo také mobilní zařízení, smartphone. Vše pomocí protokolů, jako je SMTP, POP3, IMAP.



**Mail server** neboli poštovní server je **role na serveru**, která se stará o emailovou stránku vaší společnosti.

**Potřebujeme HW server**, na kterém běží **OS** (Windows Server 2008/Windows Server 2012, Linux, atd.). Dále je zapotřebí **mít nastavený DNS** systém a přistupování z internetu/intranetu. V případě firmy **doménu Emailového serveru**. Dále **Databázi účtů (Active Directory)**. Emaily se musí někam ukládat – **Uložiště**, v nejlepším případě zajištěné redundantní spojení pomocí **RAID**. Mít nastavený **MX Záznam** **u providera** vašeho internetu. Poslední co je třeba, mít **Administrátorský účet na serveru**.

# Emailové protokoly

## SMTP

**SMTP (Simple Mail Transfer Protocol )** je [internetový](https://cs.wikipedia.org/wiki/Internet) [protokol](https://cs.wikipedia.org/wiki/Protokol_(informatika)) určený pro **přenos zpráv elektronické pošty (**[**e-mailů**](https://cs.wikipedia.org/wiki/E-mail)**) mezi**[**přepravci elektronické pošty**](https://cs.wikipedia.org/wiki/Mail_Transfer_Agent)**(MTA)**. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů [POP3](https://cs.wikipedia.org/wiki/POP3) nebo [IMAP](https://cs.wikipedia.org/wiki/Internet_Message_Access_Protocol). Jedná se o jednu z nejstarších aplikací. SMTP funguje nad protokolem [TCP](https://cs.wikipedia.org/wiki/TCP), používá port **TCP/25.**

**Ve zkratce:** **SMTP protokol se zabývá Uploadem (Posílání) emailů. Buď od Klienta k Serveru, nebo od Serveru k Serveru.**

## POP3

**POP (Post Office Protocol)** je internetový [protokol](https://cs.wikipedia.org/wiki/Protokol_(informatika)), který **se používá pro stahování** [**emailových zpráv**](https://cs.wikipedia.org/wiki/E-mail)**ze vzdáleného**[**serveru**](https://cs.wikipedia.org/wiki/Server)**na**[**klienta**](https://cs.wikipedia.org/wiki/Klient_(po%C4%8D%C3%ADta%C4%8De)). Jedná se o aplikační protokol pracující přes [TCP](https://cs.wikipedia.org/wiki/TCP)/[IP](https://cs.wikipedia.org/wiki/Internet_Protocol) připojení. V současnosti je používána zejména třetí verze (POP3).

**Ze vzdáleného**[**serveru**](https://cs.wikipedia.org/wiki/Server)**se stáhnou všechny zprávy, třeba i ty, které uživatel číst nechce**, nebo [spam](https://cs.wikipedia.org/wiki/Spam) (pokud ho již nefiltruje poštovní server). Většina POP3 serverů sice umožňuje **stáhnout pouze hlavičky zpráv** (a následně vybrat zprávy, které se stáhnou celé), ale podpora v klientech vesměs chybí. **Tuto nevýhodu může odstranit protokol**[**IMAP**](https://cs.wikipedia.org/wiki/Internet_Message_Access_Protocol), který pracuje se zprávami přímo na serveru.

**Ve zkratce: POP3 protokol se využívá, pokuď potřebujeme stáhnout E-mail z Mail Serveru na klientský počítač.**

## IMAP

**IMAP (Internet Message Access Protocol)** je [internetový](https://cs.wikipedia.org/wiki/Internet) [protokol](https://cs.wikipedia.org/wiki/Protokol_(informatika)) **pro vzdálený přístup k**[**e-mailové**](https://cs.wikipedia.org/wiki/E-mail)**schránce prostřednictvím**[**e-mailového klienta**](https://cs.wikipedia.org/wiki/E-mailov%C3%BD_klient). IMAP nabízí oproti jednodušší alternativě [POP3](https://cs.wikipedia.org/wiki/Post_Office_Protocol) pokročilé možnosti vzdálené správy (**práce se složkami** a přesouvání zpráv mezi nimi, prohledávání **na straně**[**serveru**](https://cs.wikipedia.org/wiki/Server) a podobně) a práci v tzv. on-line i off-line režimu.

Protokol IMAP umožňuje trvalé (tzv. on-line) připojení k e-mailové schránce. Díky tomu je možné s celou poštovní schránkou plně pracovat z libovolného místa. **Všechny zprávy a složky jsou uloženy na poštovním**[**serveru**](https://cs.wikipedia.org/wiki/Server)**a na počítač se stahují jen nezbytné informace**, takže při zobrazení složky se stáhnou jen záhlaví zpráv a jejich obsah až v případě, že zprávu chce uživatel přečíst. U jednotlivých zpráv se uchovává jejich stav (nepřečtená, přečtená, důležitá), uživatel může zprávy přesouvat mezi složkami, složky vytvářet, mazat, prohledávat na straně serveru apod. Protokol umožňuje současné připojení více [klientů](https://cs.wikipedia.org/wiki/Klient_(po%C4%8D%C3%ADta%C4%8De)) zároveň.

**Ve zkratce: IMAP dovoluje uživateli pracovat s Emaily přímo na Serveru. Emaily se nemusí stahovat do klientského PC.**

### Architektura Pošty

Doručování elektronické pošty po Internetu se účastní tři druhy programů:

* [**MUA**](https://cs.wikipedia.org/wiki/Mail_User_Agent) - Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
* [**MTA**](https://cs.wikipedia.org/wiki/Mail_Transfer_Agent) - Mail Transfer Agent, [server](https://cs.wikipedia.org/wiki/Server), který se stará o doručování zprávy na cílový systém adresáta
* [**MDA**](https://cs.wikipedia.org/wiki/Mail_Delivery_Agent) - Mail Delivery Agent, [program](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_program) pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.)

## Vysvětlete zabezpečení používaná v HTTPS a SSL

**Protokol HTTPS** využívá [asymetrické šifrování](https://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie). Obě strany si před zahájením komunikace vygenerují pár klíčů (privátní a veřejný). Při zahájení komunikace si vymění veřejné klíče, které by obě strany měly ověřit pomocí jiného komunikačního kanálu. Ověření může proběhnout kontrolou [výtahu](https://cs.wikipedia.org/wiki/Ha%C5%A1ovac%C3%AD_funkce) (otisk, hash) veřejného klíče u protistrany například pomocí telefonu nebo lze použít princip přenosu důvěry, kdy nám protistrana předá veřejný klíč, který je [digitálně podepsaný](https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis) (nejlépe certifikační autoritou, které důvěřujeme a jejíž veřejný klíč máme v důvěryhodném úložišti. Digitální certifikáty jsou základním kamenem zabezpečení poskytovaného protokoly SSL/TLS.

**Secure Sockets Layer**, SSL (doslova vrstva bezpečných [socketů](https://cs.wikipedia.org/wiki/Socket" \o "Socket)) je [protokol](https://cs.wikipedia.org/wiki/Protokol_(informatika)), resp. vrstva vložená mezi vrstvu transportní (např. [TCP/IP](https://cs.wikipedia.org/wiki/TCP/IP)) a aplikační (např. [HTTP](https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol)), která poskytuje zabezpečení komunikace [šifrováním](https://cs.wikipedia.org/wiki/Kryptografie) a [autentizaci](https://cs.wikipedia.org/wiki/Autentizace) komunikujících stran.

## Popište skladbu hypertextového odkazu

**Například URL adresa:** [**https://www.seznam.cz/**](https://www.seznam.cz/)

**HTTPS** – Protokol využívaný k přenosu dat mezi serverem a klientem

**WWW -** World Wide Web je souhrnné označení pro celou řadu služeb provozovaných prostřednictvím sítě Internet

**SEZNAM** – Doména druhého řádu

**CZ** – Doména nejvyššího řádu

# Přiřaďte porty ke službám: 443, 143, 25, 110, 80

443 – HTTPS

143 – IMAP

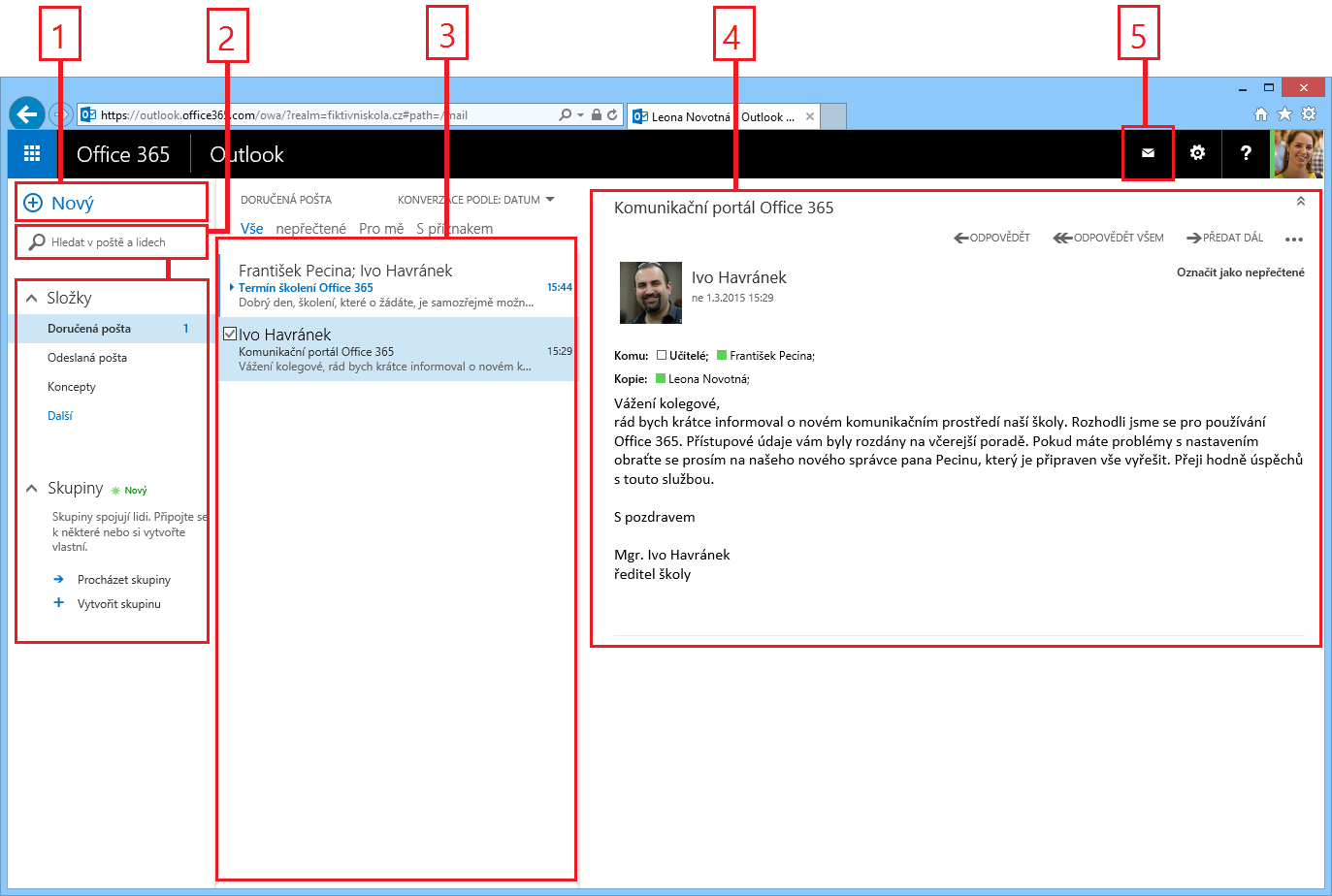
25 – SMTP

110 – POP3

80 – HTTP

# V úloze WIN7 předveďte nastavení pošty a vysvětlete možnosti.

Předpokládám, že půjde o Outlook



1. V levém horním rohu se nachází tlačítko “**Nový**”, slouží pro vytvoření nového emailu.
2. První sloupec obsahuje také jednotlivé **složky emailové schránky**. Uživatel si může snadno [zobrazit složky](https://napoveda.skolnilogin.cz/trvale-zobrazovani-vsech-slozek/), které ho zajímají. Nesmíme zapomenout ani na vyhledávací pole výše.
3. Zde se zobrazují **emaily ze zvolené složky**. Můžeme pracovat s jejich **řazením** pomocí rozklikávacího seznamu “Konverzace podle”
4. **Podokno pro čtení** umožňuje zobrazení samotného emailu. Prohlížený email je v prostředním sloupci vždy graficky zvýrazněn (modré podbarvení).
5. Tento **symbol** upozorňuje na novou **příchozí poštu**.