Inovace bakalářského studijního oboru Aplikovaná chemie

http://aplchem.upol.cz

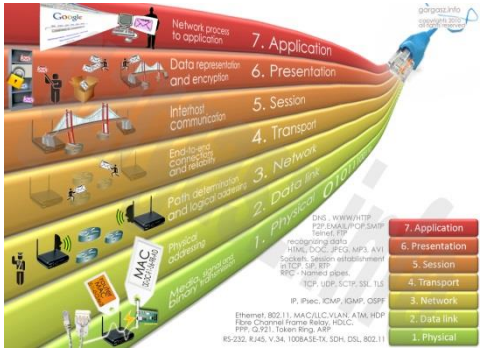
CZ.1.07/2.2.00/15.0247

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Internet a zdroje

Opakování

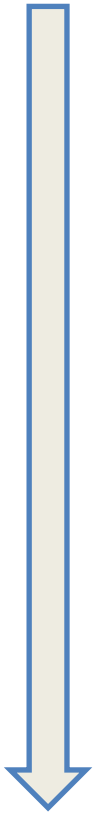


Síťové vrstvy

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Síťové vrstvy



Fyzická vrstva

- Lan, router, switch, WLAN AP, Bluetooth, WiMax, IRDA, RJ 45

Síťová vrstva

- IP (Internet Protocol)

Transportní vrstva

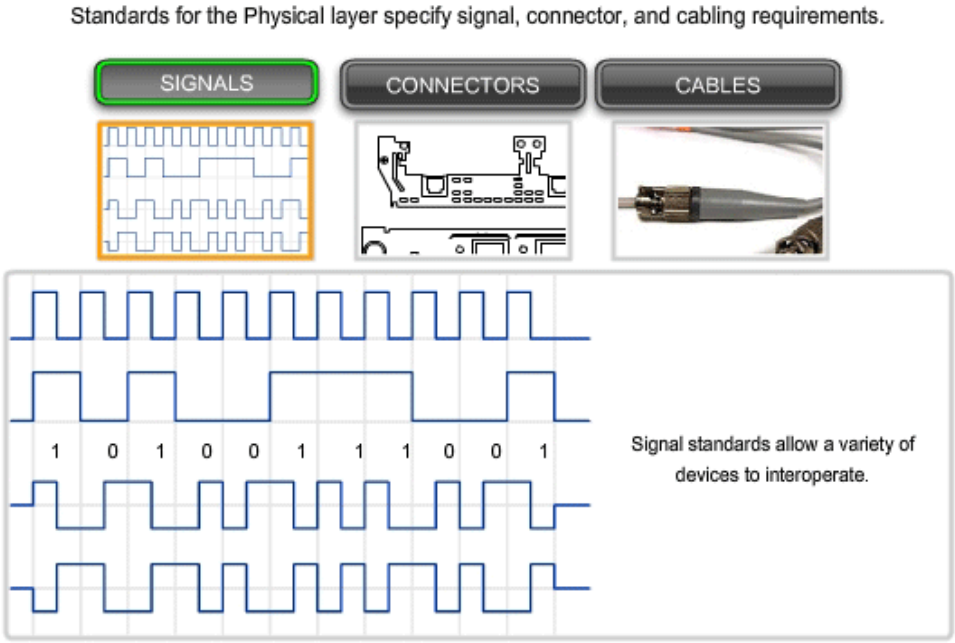
- TCP (Transmission Control Protocol), UDP (User Datagram Protocol)

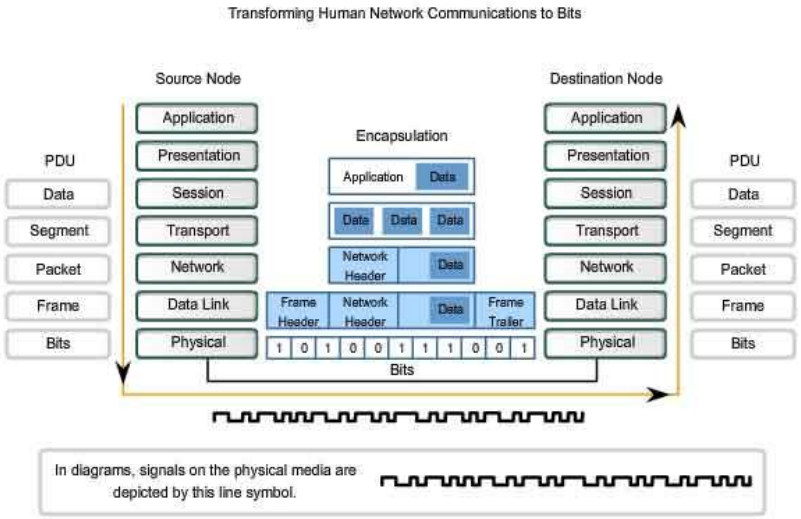
Aplikační vrstva

- DHCP, DNS, SMTP, SSH, FTP, ...

Fyzická vrstva (Physical layer)

- **První vrstva** modelu vrstvové síťové architektury (**OSI** model)
- **Převod proudů bitů na signál (např. elektrický) a naopak**
- **Typické zařízení – HUB, kabely**
- Aktivace, udržování + rušení fyzického spoje
- Protokoly fyzické vrstvy stanovují **elektrické vlastnosti rozhraní** (napěťové úrovně, průběhy, kmitočty, modulace, rychlosti, elektrické vlastnosti kabelů) a **mechanické vlastnosti** (tvary, velikosti a zapojení konektorů).

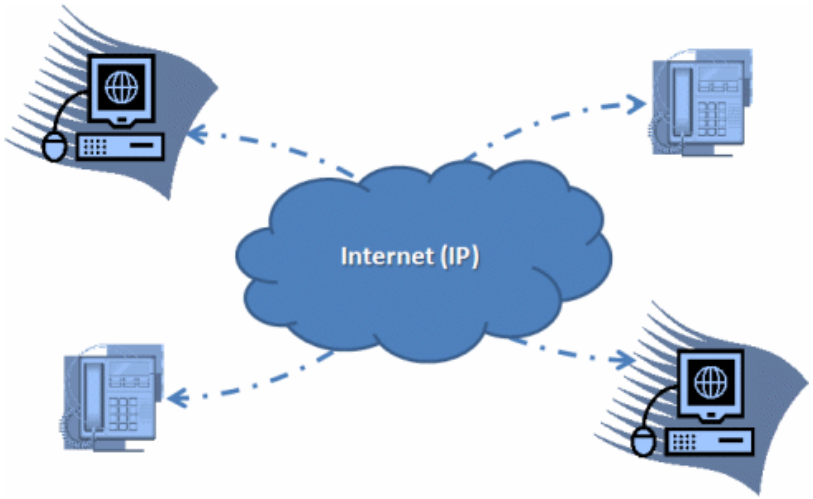


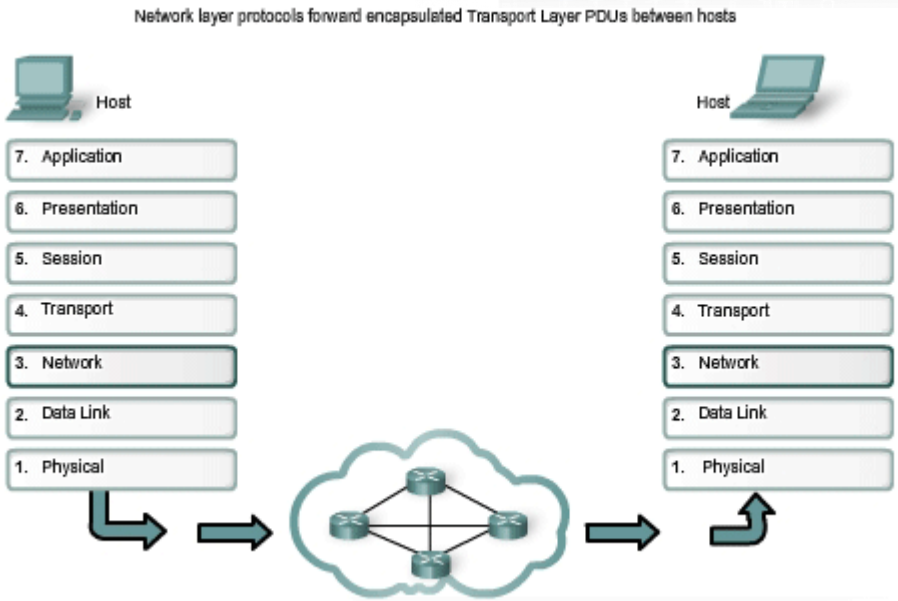


Síťová vrstva (Network Layer)

- **Třetí vrstva** modelu vrstvové síťové architektury (**OSI** model)
- Směrování v sítí + síťové adresování
- spojení mezi systémy, které spolu přímo nesousedí.
- Nejzmámější protokol – **I**nternet **P**rotocol (**IP protocol**)

router

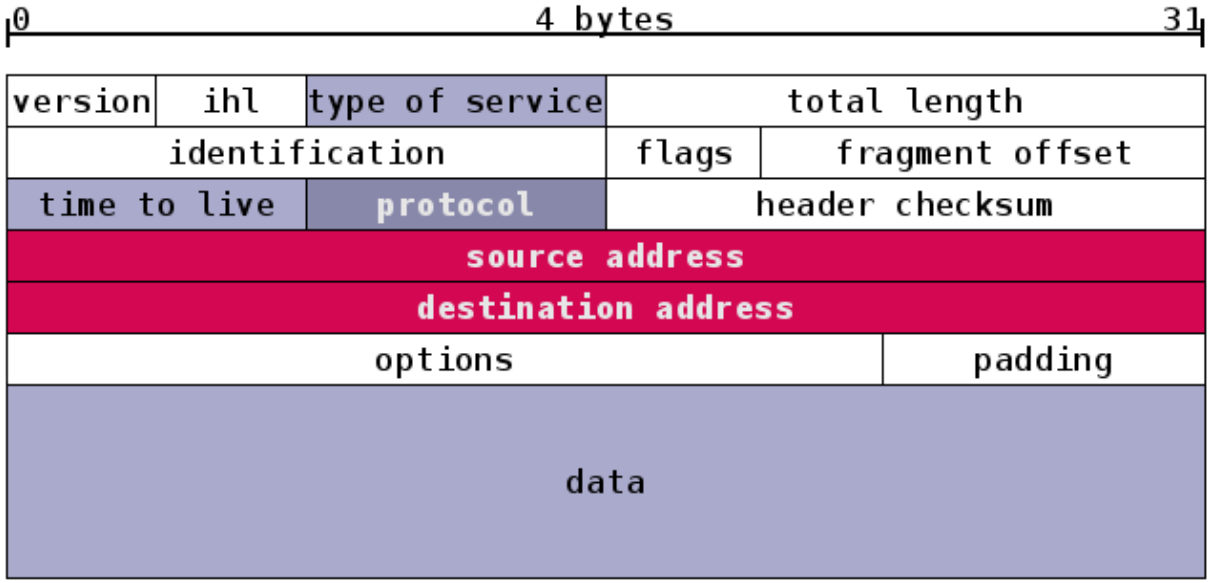




Síťová vrstva (Network Layer)

- Úkolem **IP** protokolu je zajistit samotný přenos dat.
- Data jsou dělena do malých balíčků – **pakety („letters“)**.
- Každý paket se skládá z hlavičky (informace o adresátovi, délce života paketu, šifrování apod.) a z těla, které obsahuje konkrétní informaci

IPv4 paket



- **Každá IP adresa v rámci jedné sítě se může vyskytovat pouze jednou**

Síťová vrstva (Network Layer)

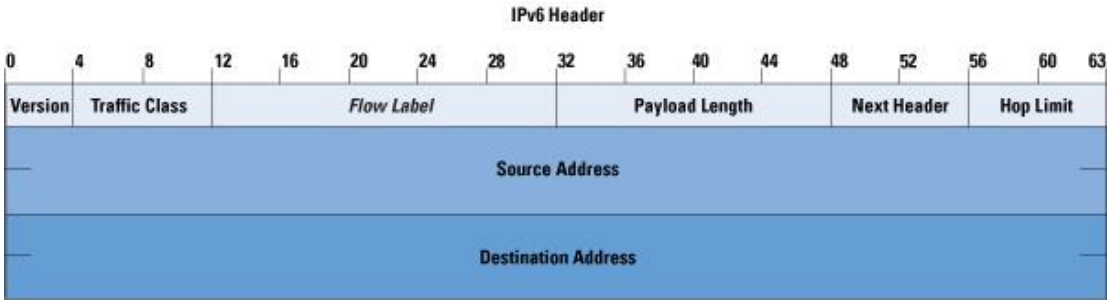
Verze protokolu IP

IPv4

- Internet protokol verze 4
- **32 bitové adresy**
- cca 4 miliardy různých IP adres, dnes nedostačující

IPv6

- Internet protokol verze 6
- **128 bitové adresy**
- podpora bezpečnosti
- podpora pro mobilní zařízení
- fragmentace paketů – rozdělování
- není zpětně kompatibilní s IPv4
- snadnější automatická konfigurace (NDP – Neighbor discovery protocol)

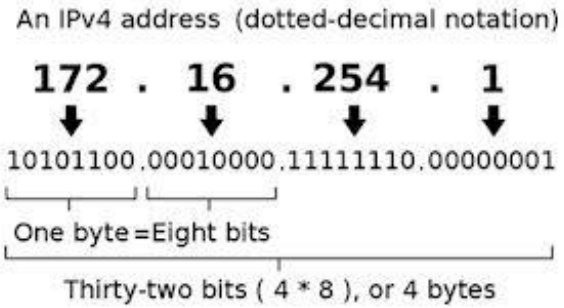


Síťová vrstva (Network Layer)

Adresy v IPv4

32 bitové číslo, oddělené tečkami – 192.168.20.1

Počet adres: 2^{32} = 4 294 967 296



Struktura IP adresy:

adresa sítě	adresa podsítě	adresa počítače

Maska podsítě:

32 bitové číslo – v binárním tvaru obsahuje jedničky tam, kde se vyskytuje síť a podsíť. Nuly se vyskytují na místě, kde se nachází počítač

Třída	1. bajt	minimum	maximum	maska podsítě
A	0–127	0.0.0.0	127.255.255.255	255.0.0.0
B	128–191	128.0.0.0	191.255.255.255	255.255.0.0
C	192–223	192.0.0.0	223.255.255.255	255.255.255.0
D	224–239	224.0.0.0	239.255.255.255	255.255.255.255
E	240–255	240.0.0.0	255.255.255.255	—

Síťová vrstva (Network Layer)

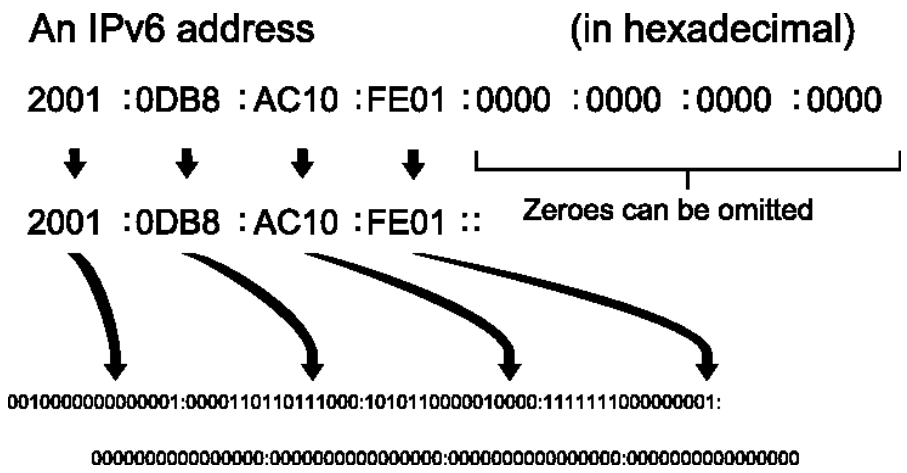
Adresy v IPv6

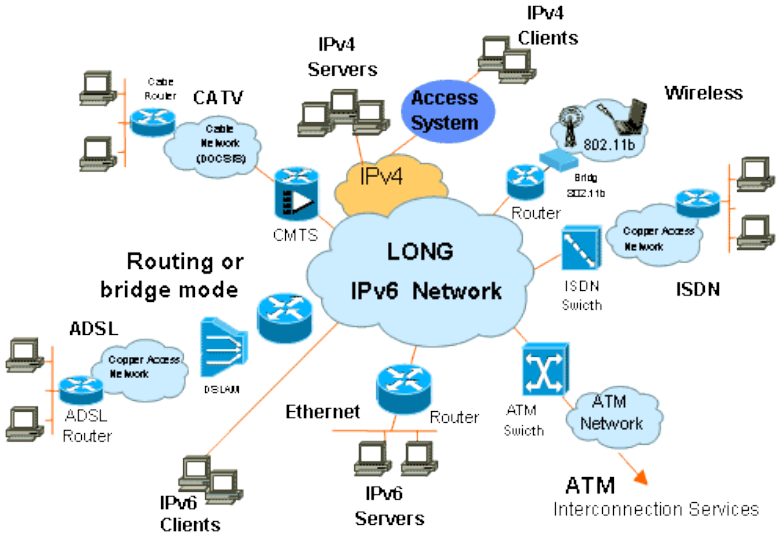
128 bitové číslo

Počet adres: $2^{128} \approx 3 \times 10^{38}$ (6×10^{23} IP adres na 1 m² zemského povrchu)

Formát:

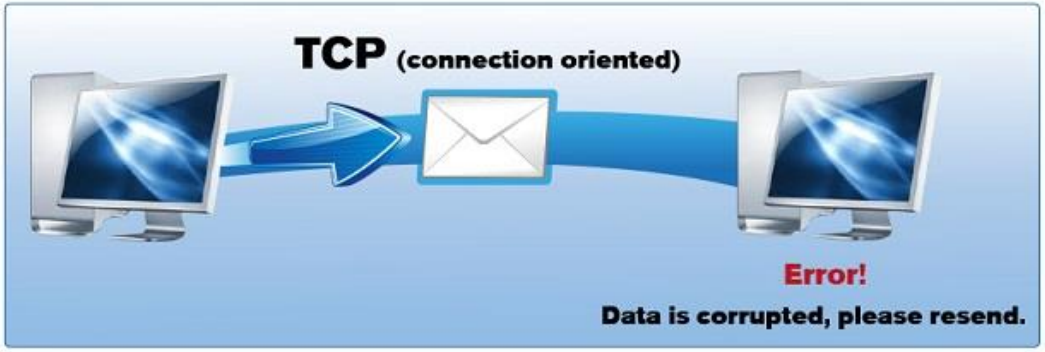
8 skupin po 4 hexadecimálních číslicích: 2001:0718:1c01:0016:0214:22ff:fec9:0ca5

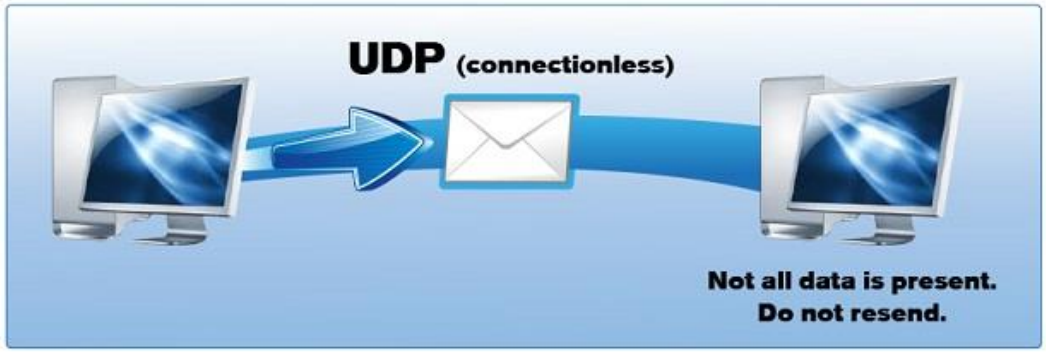




Transportní vrstva (Transport Layer)

- **Čtvrtá vrstva** modelu vrstvové síťové architektury (**OSI** model)
- přenos dat mezi koncovými uzly
- Vrstva nabízí spojově (**TCP**) a nespojově orientované (**UDP**) protokoly





TCP a UDP

TCP je spojově orientovaný protokol.

- spolehlivost – TCP používá potvrzování o přijetí, opětovné posílání a překročení časového limitu. Pokud se jakákoliv data ztratí po cestě, server si je opětovně vyžádá. U TCP nejsou žádná ztracená data, jen pokud několikrát po sobě vyprší časový limit, tak je celé spojení ukončeno.
- zachování pořadí – Pokud pakety dorazí ve špatném pořadí, TCP vrstva příjemce se postará o to, aby se některá data pozdržela a finálně je předala správně seřazená.
- vyšší režie – TCP protokol potřebuje např. tři pakety pro otevření spojení, umožňuje to však zaručit spolehlivost celého spojení.

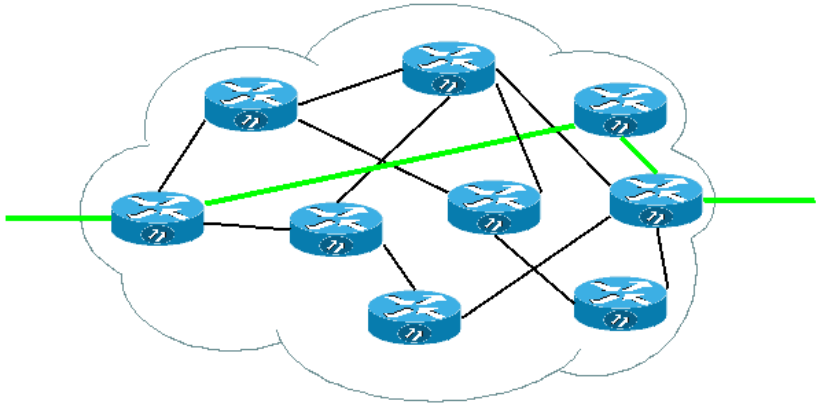
UDP je jednodušší protokol založený na odesílání nezávislých zpráv.

- bez záruky – Protokol neumožňuje ověřit, jestli data došla zamýšlenému příjemci. Datagram se může po cestě ztratit. UDP nemá žádné potvrzování, přeposílání ani časové limity. V případě potřeby musí uvedené problémy řešit vyšší vrstva.
- nezachovává pořadí – Při odeslání dvou zpráv jednomu příjemci nelze předvídat, v jakém pořadí budou doručeny.
- jednoduchost – Nižší režie než u TCP (není zde řazení, žádné sledování spojení atd.).

Routing

Routing = určování cest v počítačových sítích

- Úkol routingu: doručení datového paketu určenému adresátovi (hledání co nejefektivnější cesty)
- Neřeší celou cestu paketu, řeší vždy jen jeden krok → komu předat paket jako dalšímu
- Routing je základním úkolem síťové vrstvy



Ikona routingu

Routovací algoritmy a prokoly

Routovací (směrovací) algoritmy: zajišťují vznik a životaschopnost routovací tabulky

Dvě základní skupiny:

- Statické algoritmy → routovací tabulka se nemění, je dána konfigurací počítače; změny se provádějí ručně → koncové stanice nebo routery v malých sítích (LAN)
- Dynamické algoritmy průběžně reagují na změny v síti → změnám přizpůsobují routovací tabulky
  - Podle způsobu výměny informací se dělí na: centralizované; izolované; distribuované a hierarchické

Při zadefinování přesných pravidel → vznik směrovacího protokolu

Routovací algoritmy dynamické

1) Centralizované: routery posílají informaci do jednoho routovacího centra → centrum sestaví mapu sítě, spočítá z ní routovací tabulky a rozešle je routerům

- **Výhody:** díky kompletní mapě sítě určení globálně optimální tabulky
- **Nevýhody:** špatně škáluje (na linkách, které vedou do centra se kumulují zprávy o stavu sítě a odesílané tabulky) + problém se synchronizací tabulek (routery blíže centru je dostávají dříve)

2) Izolované: nikdo nikomu neposílá informace o stavu sítě, každý router se rozhoduje sám → použití záplavového algoritmu

- **Nevýhody:** vznik cyklů v síti
- **Řešení:** omezení životnosti paketu × protokol OSPF

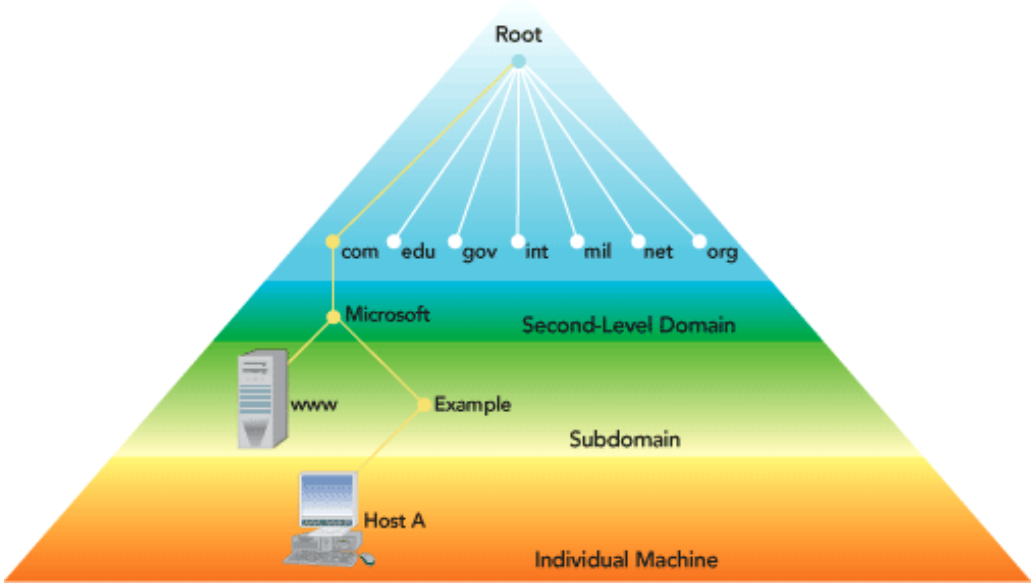
3) Distribuované: standardní přístup ke směrování v Internetu

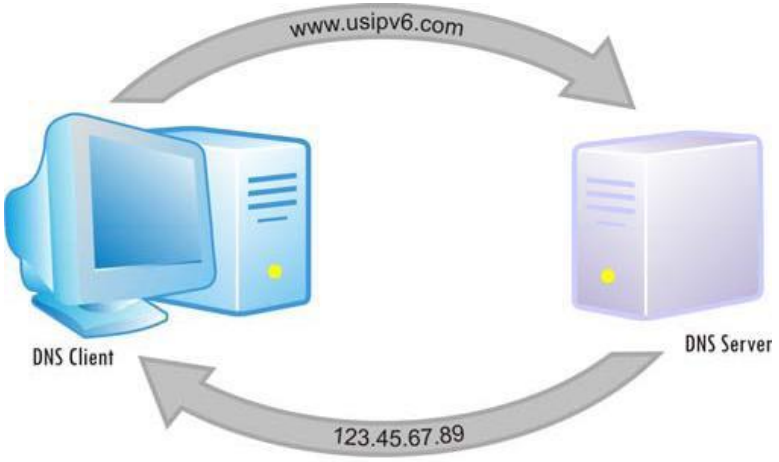
4) Hierarchické: řeší problém rozsáhlých sítí → autonomní oblast dělí na menší samostatné oblasti

DNS

DNS (Domain Name System)

- hierarchický systém doménových jmen, který je realizován servery DNS a protokolem DNS
- Vzájemné převody doménových jmen a IP adres
- Subdomény mohou mít až 63 znaků a skládat se mohou až do celkové délky doménového jména 255 znaků





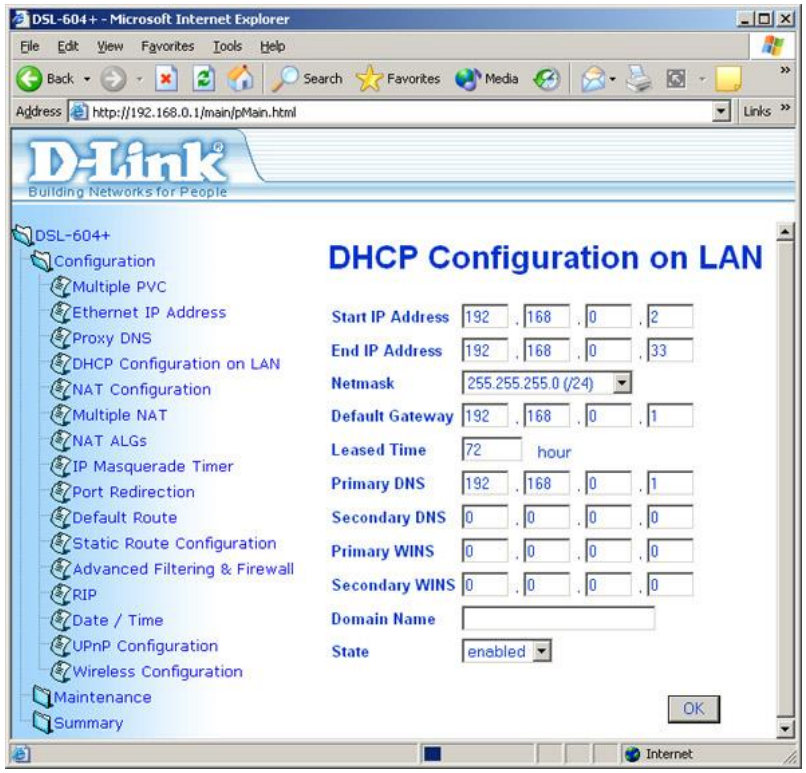
DHCP

DHCP (Dynamic Host Configuration Protocol)

- automatická konfiguraci počítačů připojených do počítačové sítě
- zjednodušuje a centralizuje správu počítačové sítě (přidávání PC, hromadné změny parametrů apod.)

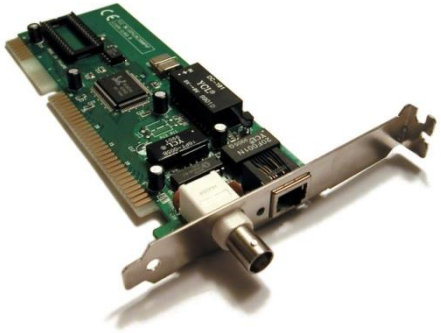
DHCP parametry:

- IP adresa
- maska sítě
- implicitní brána (anglicky *default gateway*)
- DNS server (seznam jedné nebo více IP adres DNS serverů)
- a další údaje, např. servery pro NTP, WINS, …



Hardware

- Síťová karta




- Propojovací média (kabely atd.)

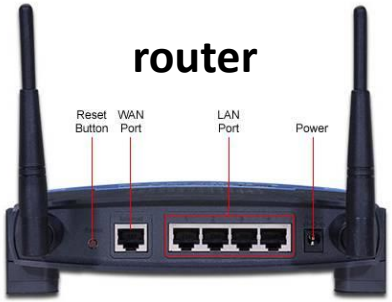


Hardware

- **Prostředky pro fyzickou vrstvu:**
  - Repeatery (opakovače), zesilovače, huby (rozbočovače)

- **Prostředky pro linkovou vrstvu:**
  - Bridges (mosty), Switch

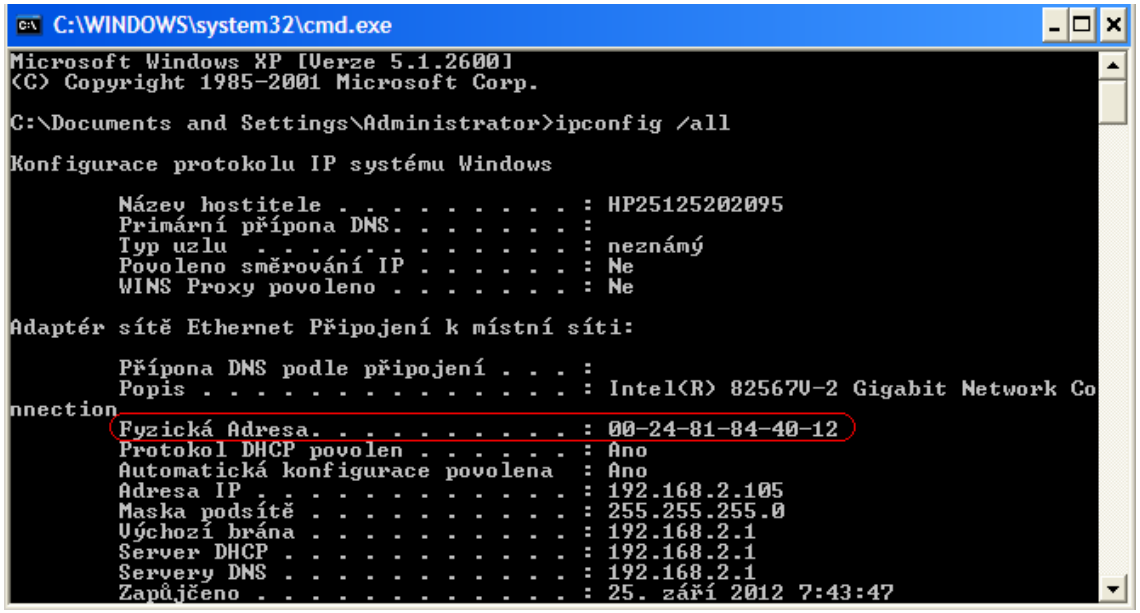
- **Prostředky pro síťovou vrstvu:**
  - Routery



- **Prostředky pro vyšší vrstvy:**
  - Gateway (brána)

Hardware

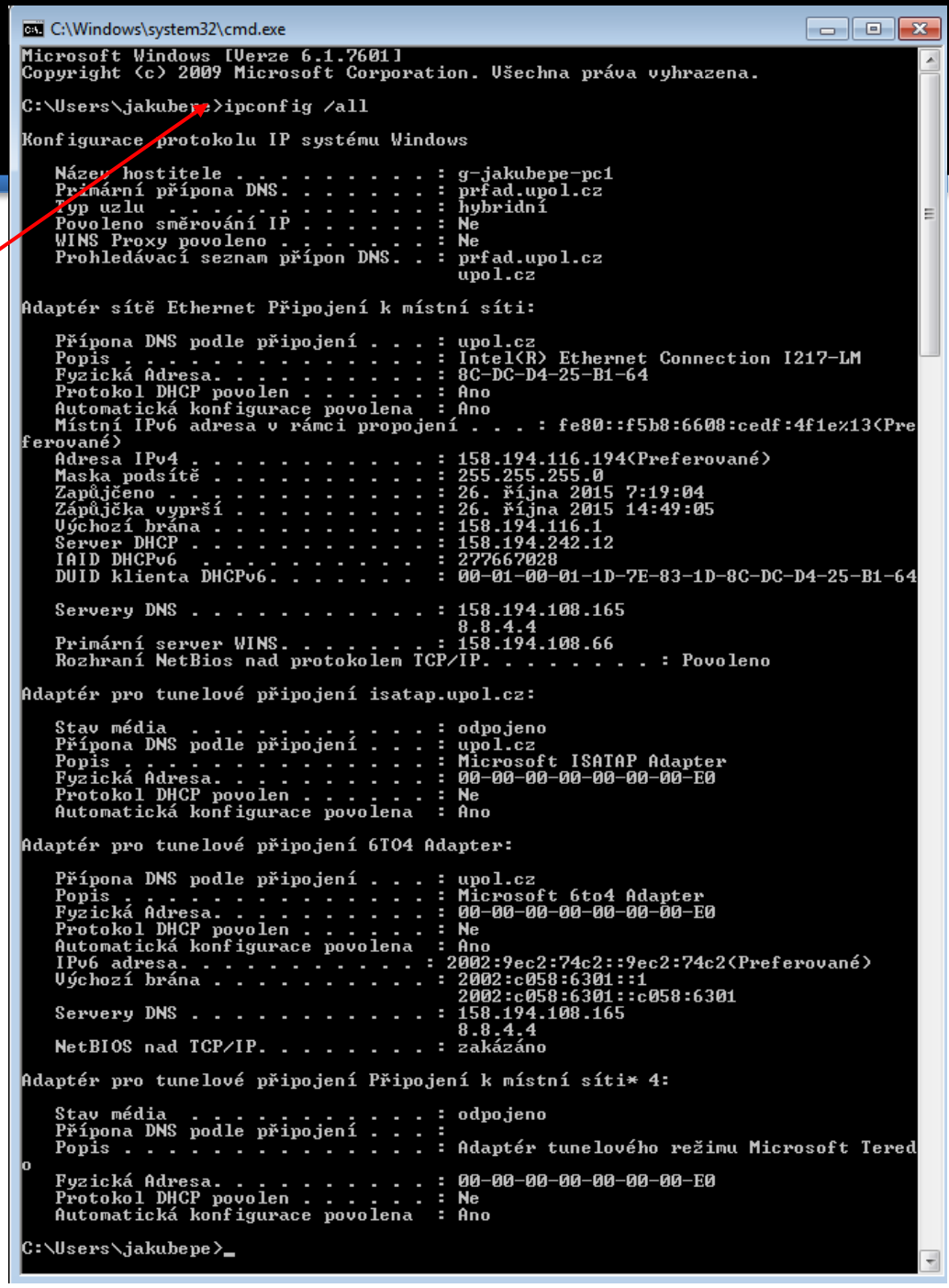
- Síťová karta (**N**etwork **I**nterface **C**ontroller – **NIC)**
  - Slot: PCI, PCI-e (notebooky: externě přes PCMCIA) × integrovaná
  - **MAC adresa** = Fyzická (Hardwarová) adresa unikátní 48-bitový identifikátor karty daný výrobcem



Hardware

- Síťová karta – testování provozu
  - Utility:

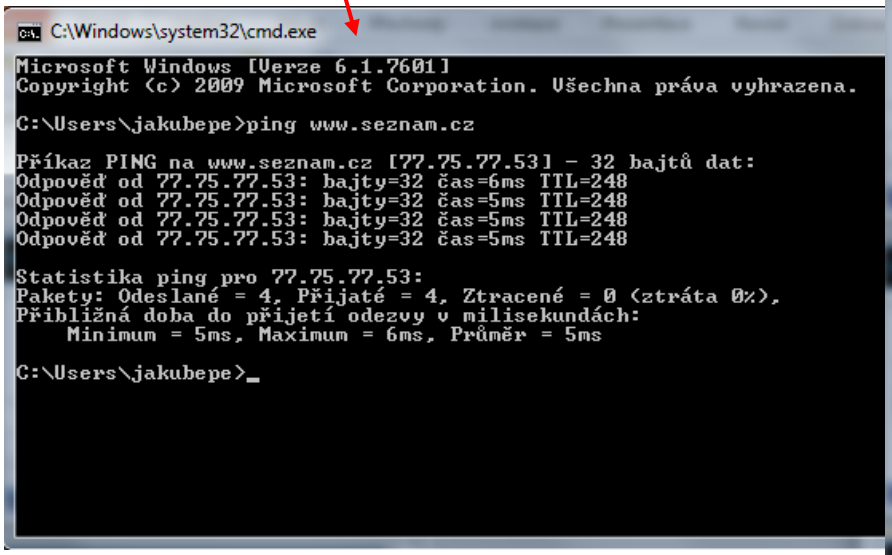
    ipconfig

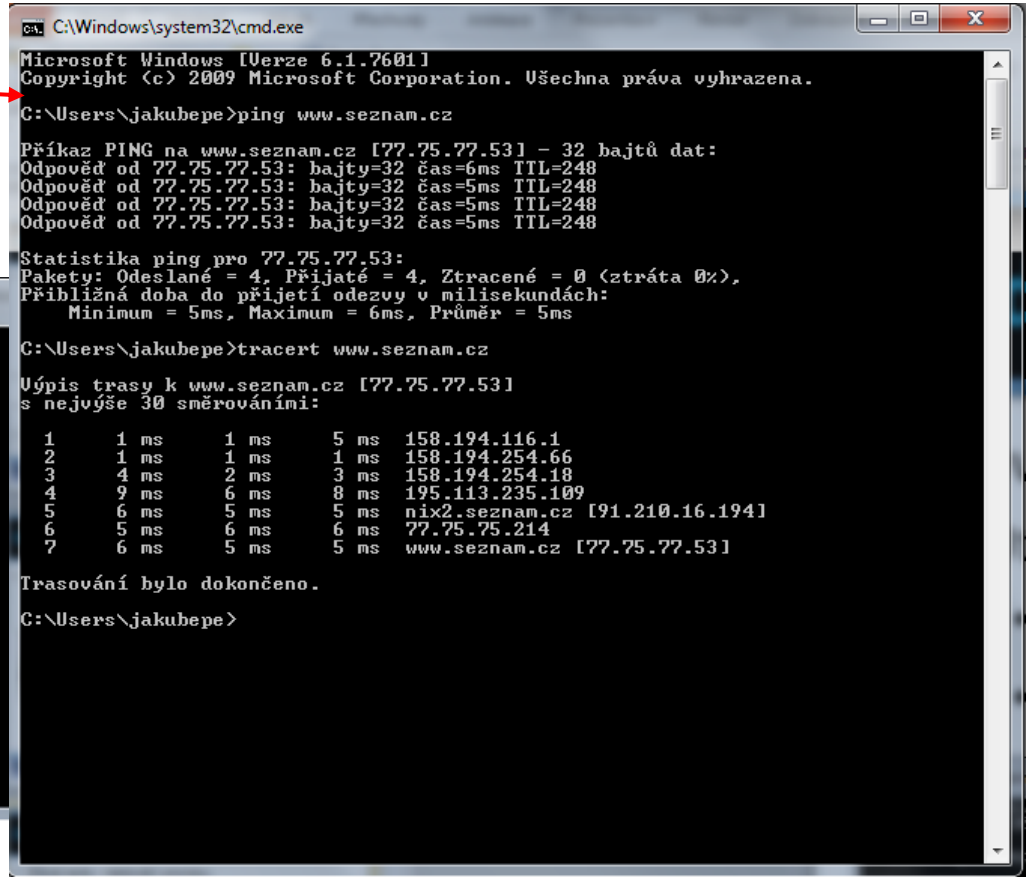


Hardware

- Síťová karta – testování provozu
  - Utility:

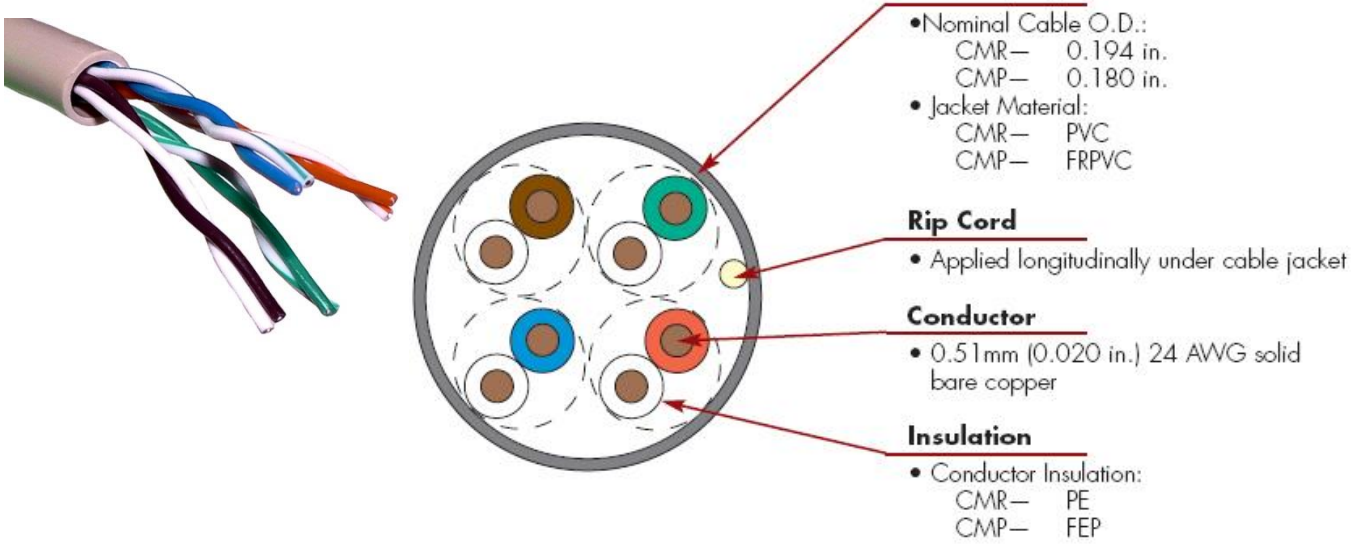
ping × tracert

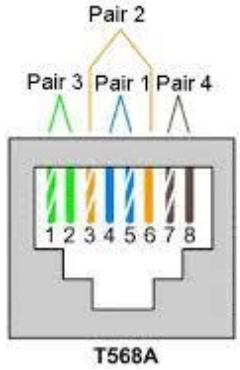


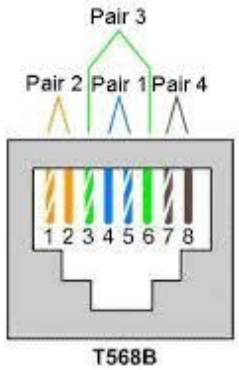


Hardware

- **Kroucená dvojlinka**
  - Tvořena páry vodičů, které jsou pravidelně kroucené a které se dále kroutí mezi sebou
  - Oba vodiče jsou rovnocenné – symetrické vedení
  - Přenášený signál lze vyjádřit jako rozdíl potenciálů obou vodičů
  - Kroucení vodičů ⇨ zlepšení elektrických vlastností kabelu (snižuje se interakce dvoulinky s jejím okolím, tj. je omezeno vyzařování elmag. záření do okolí i jeho příjem z okolí)

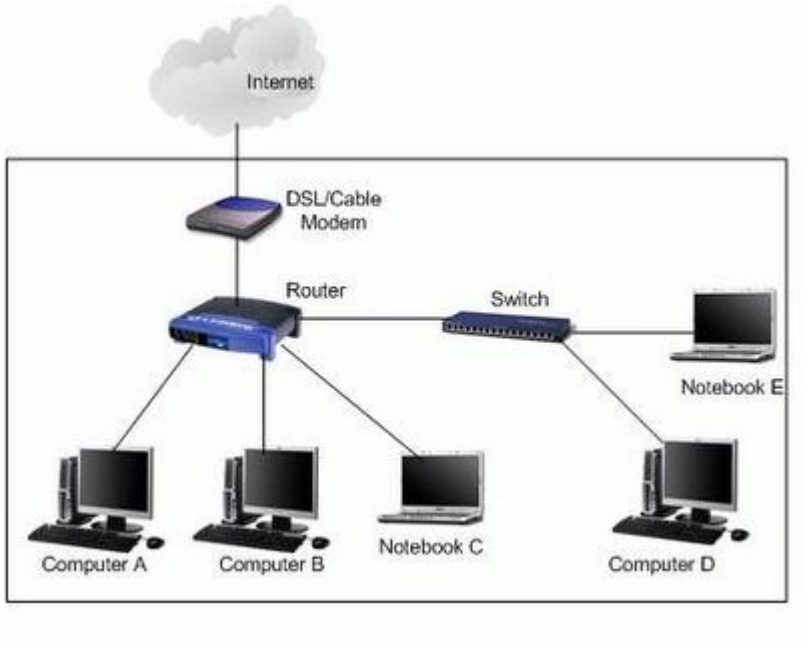






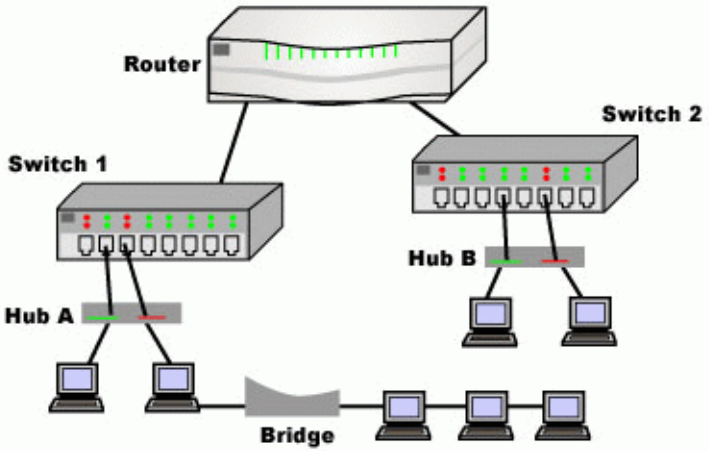
Router vs. switch

- **Router**
  - Procesem routování posílá pakety směrem k cíli → tj. spojuje dvě sítě a přenáší mezi nimi data
  - **Využití protokolu IP**
- **Switch**
  - Propojuje jednotlivé segmenty sítě → tj. propojuje počítače v rámci místní sítě
  - Výrazně jednodušší než router
  - **Využití systému MAC adres**



Hub, repeater, gateway, bridge

- **Hub** (rozbočovač) – základní prvek sítí s hvězdicovitou topologií
  - Veškerá data, která přijdou na port, zkopíruje na všechny ostatní porty → přetěžování
  - Zastaralá technologie – nahrazována switchem
- **Repeater** (opakovač) – přijímá zkreslený (zeslabený, zašuměný) signál → opravený a zesílený ho posílá dále
- **Gateway** (brána) – vzájemně propojuje nekompatibilní sítě (případně zařízení)
- **Bridge** (most) – propojení kabelových segmentů v rámci sítě → zamezení přetěžování
  - Spojení segmentů různých fyzických vrstev

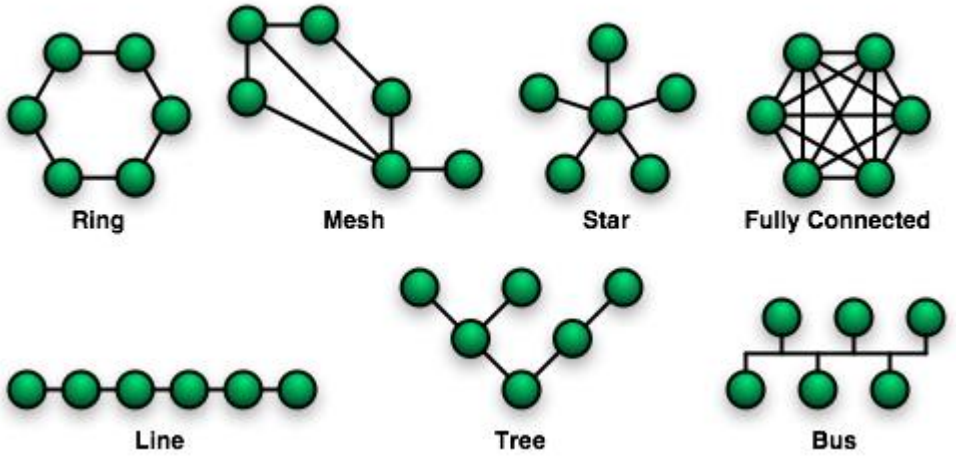


Topologie sítí

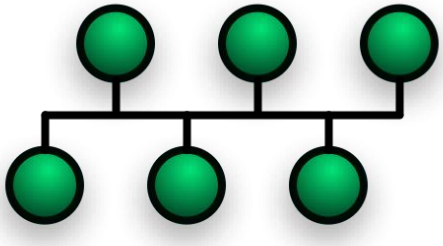
Topologie sítí a jejich popis:

1. **Fyzická topologie** reálná konstrukce sítě
2. **Logická topologie** se vztahuje k tomu, jak jsou data v síti přenášena a kudy protékají z jednoho zařízení do druhého. Nemusí nutně kopírovat fyzické schéma sítě.
3. **Signálová topologie** mapuje skutečné propojení mezi uzly v síti sledováním, kudy signál prochází.

Ukázky fyzické topologie



Topologie sítí – fyzická topologie

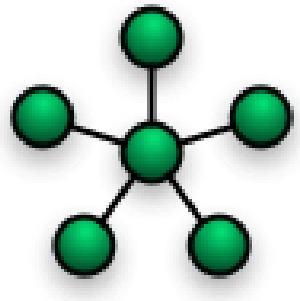


Výhody:

- Snadná realizace a snadné rozšíření již stávající sítě.
- Nevyžaduje tolik kabeláže jako např. hvězdicová topologie.
- Vhodná pro malé nebo dočasné sítě, které nevyžadují velké rychlosti přenosu.

Nevýhody:

- Nesnadné odstraňování závad.
- Omezená délka kabelu a také počtu stanic.
- Pokud nastane nějaký problém s kabelem, celá síť přestane fungovat.
- Výkon celé sítě rapidně klesá při větších počtech stanic nebo při velkém provozu.



Výhody:

- Funguje i po kolizi jednoho/více počítačů
- Dobrá výkonnost v porovnání se sběrnicovou topologií. Nedochází ke kolizím mezi pakety
- Snadno se nastavuje a rozšiřuje
- Závady se dají snadno nalézt

Nevýhody:

- Potřeba extra hardware v porovnání se sběrnicovou topologií.
- V případě selhání centrálního síťového prvku přestane fungovat celá síť.

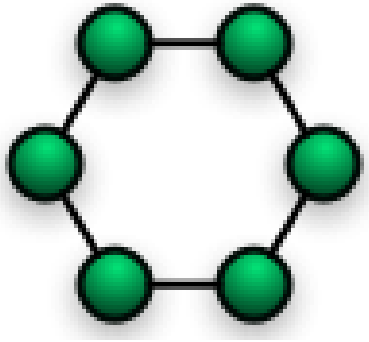
Topologie sítí – fyzická topologie

Výhody:

- přenos dat je relativně jednoduchý, protože pakety se posílají jedním směrem
- nevznikají kolize
- minimální zpoždění (v bitech podle počtu uzlů)
- průchodnost sítě je z výše uvedených důvodů ze všech ostatních topologií nejvyšší

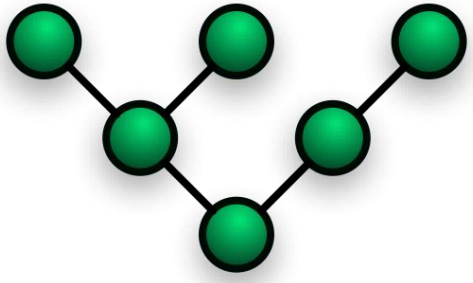
Nevýhody:

- data musí projít přes všechny členy kruhu, což zvyšuje riziko poruchy
- přerušením kruhu vzniká problém (Při vyřazeni jedné stanice další stanice přestávají pracovat)
- při přidání nového uzlu je nutné dočasně kruh přerušit



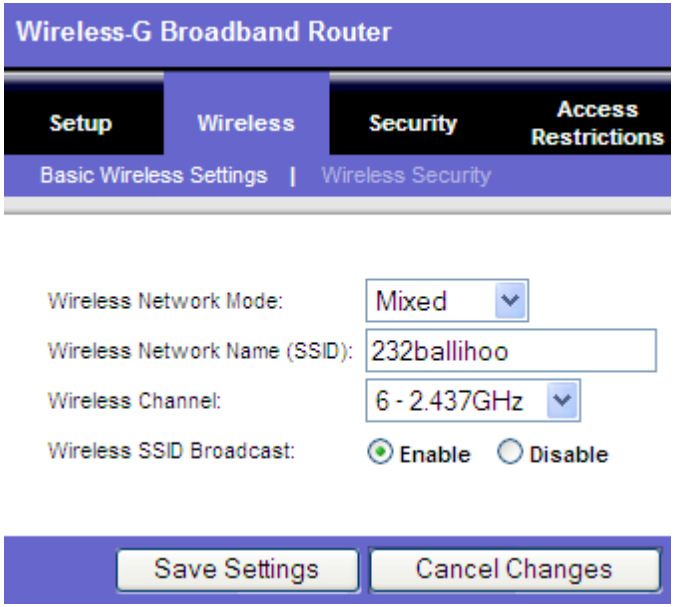
Výhody:

- Pokud selže jeden aktivní síťový prvek, ostatní části sítě mohou dále pokračovat.
- Snižuje se potřebné množství kabelů.
- Zvýšení bezpečnosti - zvyšuje se obtížnost odposlouchávání síťové komunikace.



WIFI a její struktura

- **Identifikátor SSID** (Service Set Identifier) – řetězec až 32 ASCII znaků, pravidelně vysílán jako broadcast
- **Ad-hoc sítě** – propojení dvou klientů (peer-to-peer), identifikace probíhá pomocí SSID
  - Vhodné pro malé sítě (krátká vzdálenost)
- **Infrastrukturní sítě** – jeden nebo více AP (access pointů), které vysílají své SSID



WIFI a bezpečnost

Aktivace šifrování a autentizace!

- Blokace SSID (nejprimitivnější)
- Kontrola MAC adres (filtrace na základě seznamu povolených MAC adres)
- Autentizace pomocí protokolu **IEEE 802.1X**
  - Použití **WEP** (Wired Equivalent Privacy) klíčů (symetrické šifrování) – WEP, WEP+, WEP2
  - Použití **WPA** (Wi-Fi Protected Access) – využití WEP klíčů s dynamickou výměnou
  - Použití **WPA2** – zapojení AES šifrování

Technické zázemí

Výměna zpráv pomocí programu MTA (MUA)

↓

protokolem **SMTP** (**S**imple **M**ail **T**ransfer **P**rotokol)

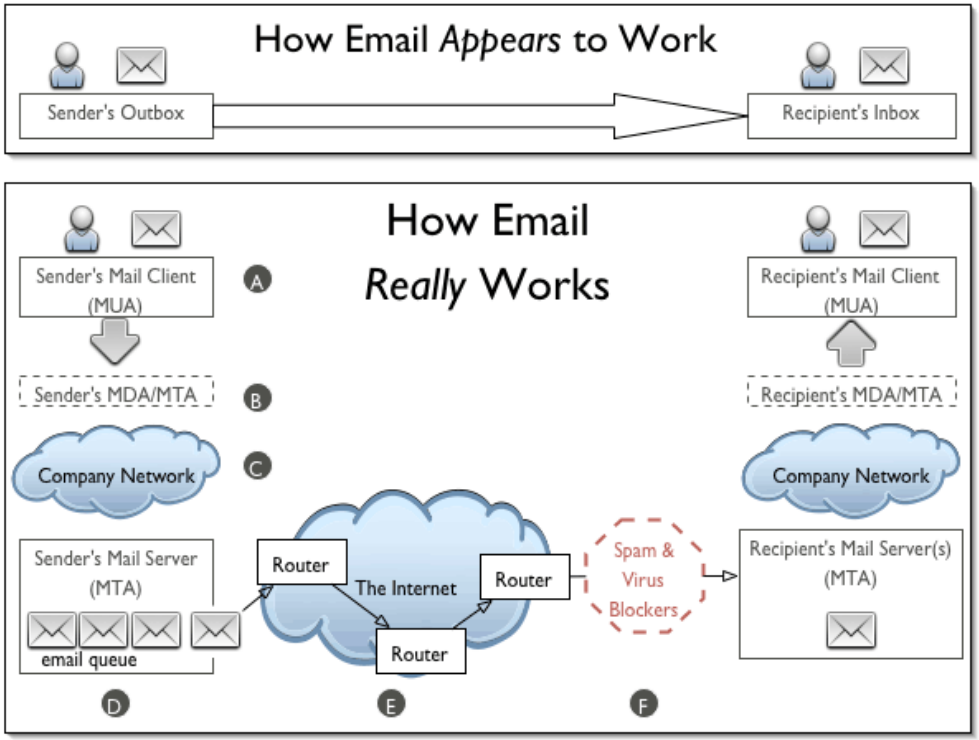
↓

Stahování zpráv z poštovního serveru pomocí **POP** × **IMAP**

↓

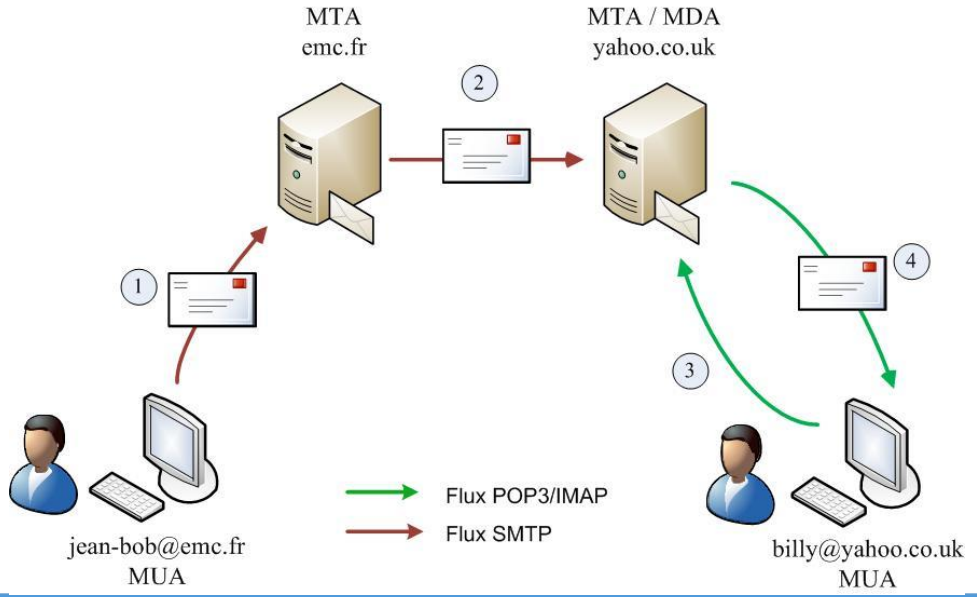
Prohlížení mailu

mailový klient vs. **web**



SMTP – Simple Mail Transfer Protocol

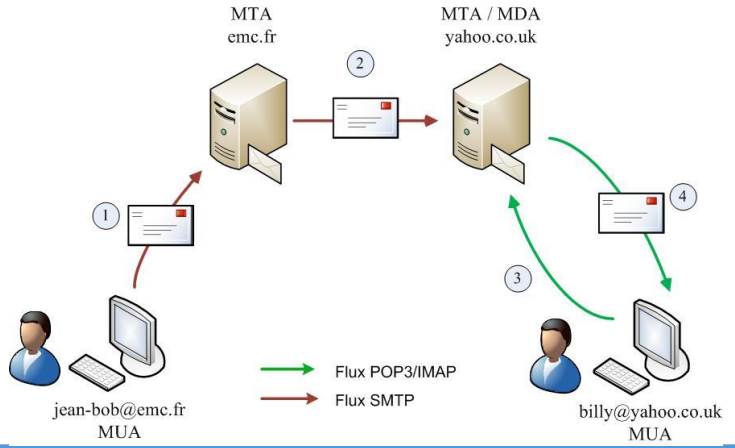
- Protokol určený pro přenos e-mailů mezi přepravci elektronické pošty (**MTA**)
- Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem
- Zpráva je doručena do poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů **POP3** nebo **IMAP**



MTA, MDA, MUA...

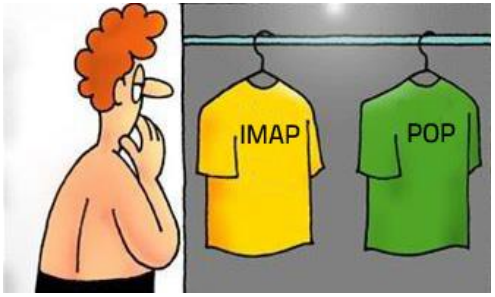
Architektura pošty

- **MUA** – Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
- **MTA** – Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta
- **MDA** – Mail Delivery Agent, 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.)



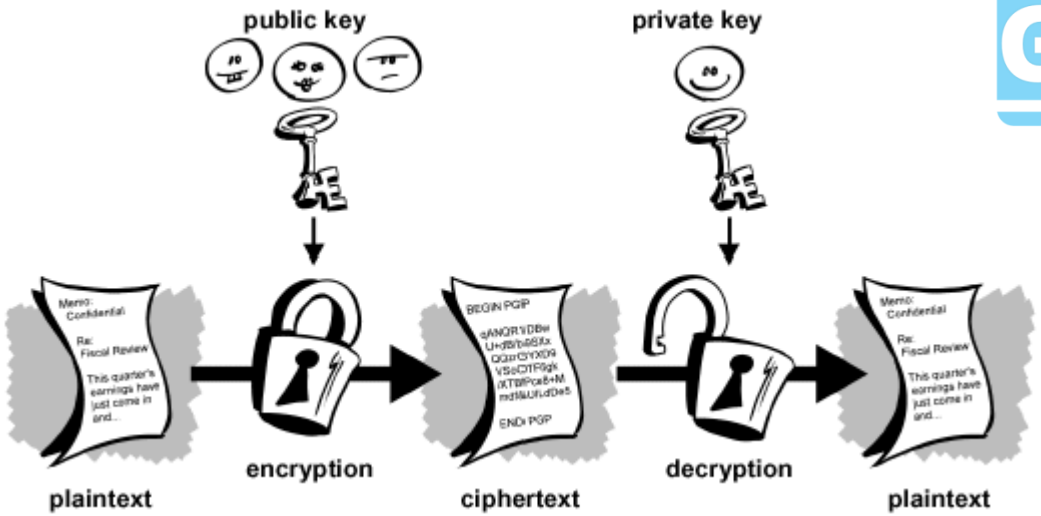
POP3 vs. IMAP

- **POP3** (**P**ost **O**ffice **P**rotocol version **3**)
  - Pracuje pouze v **off-line** režimu (port 110)
  - Protokol POP3 dovoluje připojení pouze jednoho uživatele ke schránce
- **IMAP** (**I**nternet **M**essage **A**ccess **P**rotocol)
  - umí pracovat v tzv. **on-line** i **off-line** režimu (port 143)
  - pokročilé možnosti vzdálené správy (práce se složkami apod.)
  - IMAP dovoluje současné připojení více uživatelů k jedné schránce
  - využití příznaků → přehled o stavu zprávy (jestli byla přečtena, smazána atd.)
  - podpora více schránek na serveru



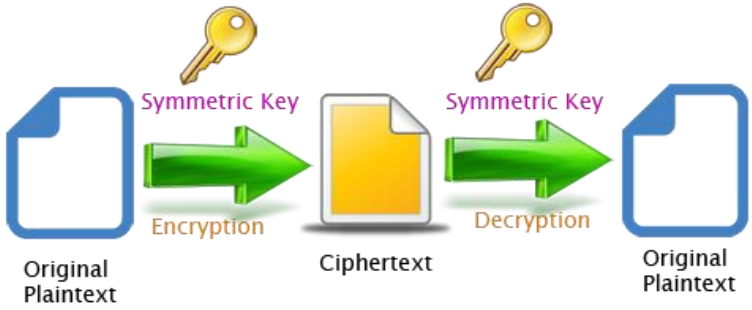
E-mail a bezpečnost

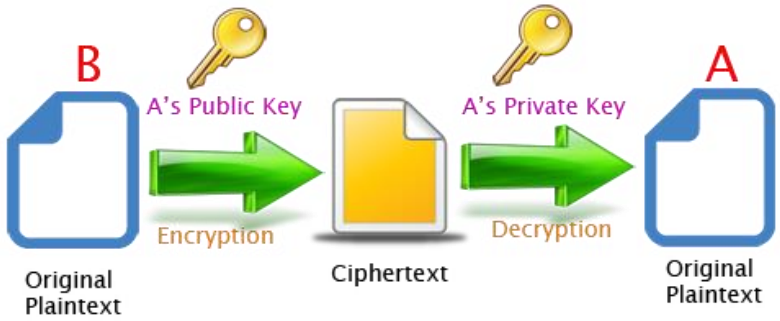
- e-mailové zprávy obecně nejsou šifrované
- Nutnost tvorby kopií e-mailů + Nutnost zapojení šifrování
  - **S/MIME**
  - **PEM**
  - **PGP**
  - **GPG**
  - VPN
  - TOR



S/MIME, PEM, PGP, GPG

- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**
  - Šifrování zpráv + digitální podpis
  - Obsah zprávy – symetrická šifra
  - Klíč se následně šifruje asymetricky
  - Autentizace: otisk zprávy + digitální podpis
- **PEM (Privacy-Enhanced Mail)**
  - Obsah zprávy – symetrická šifra
  - Klíč se následně šifruje asymetricky
- **PGP (Pretty Good Privacy)**
  - Obsah zprávy – symetrická bloková šifra (náhodně generovaný klíč: 128 bit)
  - Klíč se následně šifruje asymetricky
  - Autentizace: digitální podpis
- **GPG (GNU Privacy Guard)**
  - Open alternativa k PGP

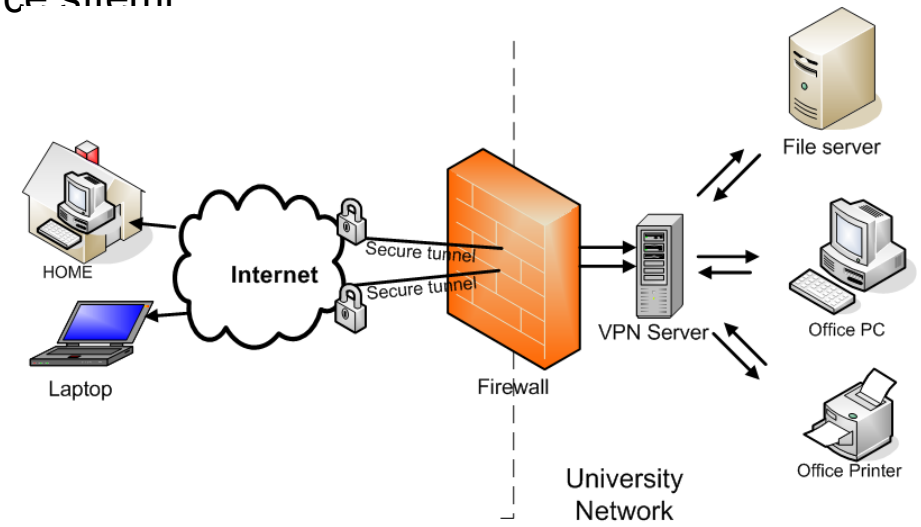




VPN

VPN (virtual private network)

- Propojení PC prostřednictvím nedůvěryhodné sítě (Internet)
  - bezpečné spojení mezi dvěma či více sítěmi
- využití dig. podpisů + šifrování



Aplikace:

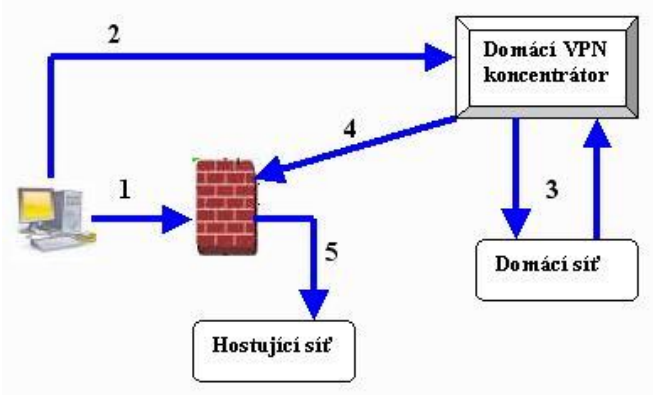
1. Zprovoznit VPN server
2. Připojit PC k Internetu
3. Připojit klienty k VPN serveru

Úloha VPN serveru:

1. Síťová brána (zprostředkovává spojení)
2. Šifrování komunikace

Princip fungování:

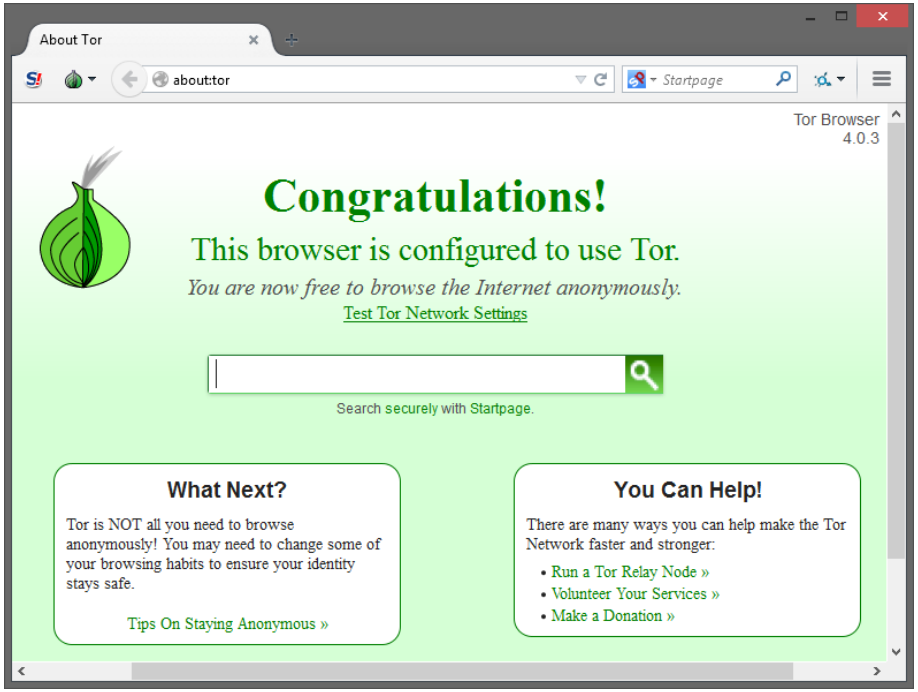
1. Uživatele blokuje firewall
2. proto se hlásí na Domácí VPN koncentrátor
3. Který ověří jeho důvěryhodnost (domácí síť)
4. Pokud je známý, povolí komunikaci
5. A konečně se může připojit do hostující sítě

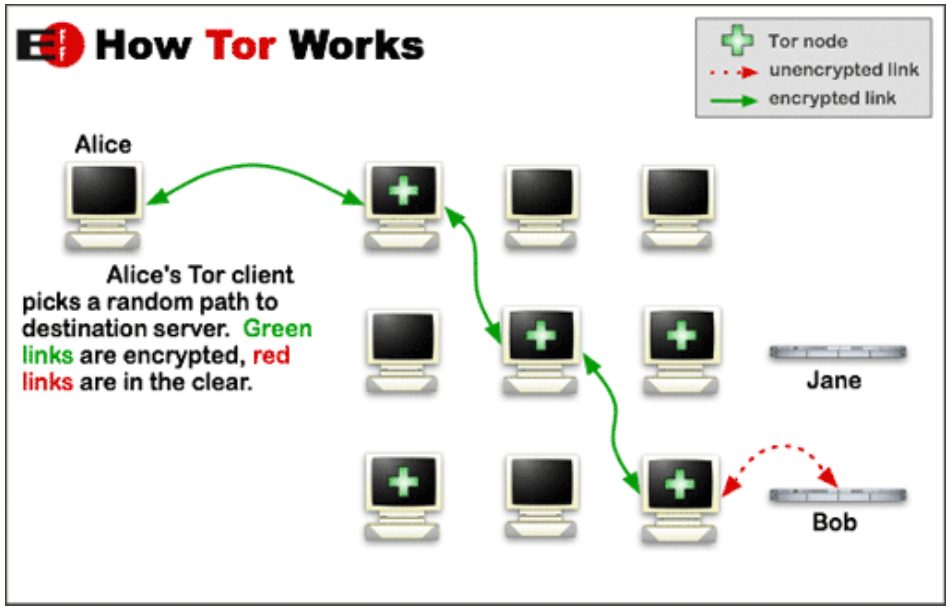


TOR

TOR (**T**he **O**nion **R**outing)

- Softwarový systém zajišťující anonymitu
- Open Source
- Ochrana osobních údajů
- Ochrana obchodní aktivit



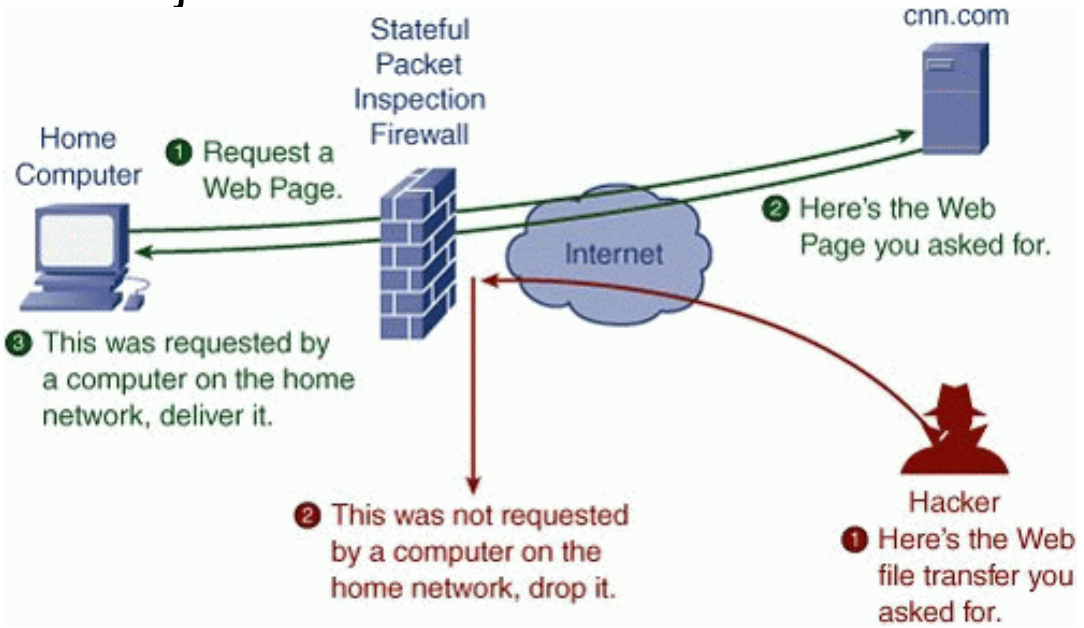


Firewall

- síťové zařízení/aplikace, sloužící k řízení a zabezpečení síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
- **Zjednodušeně:** kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje

Rozdělení firewallů:

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS



Firewall – podrobněji

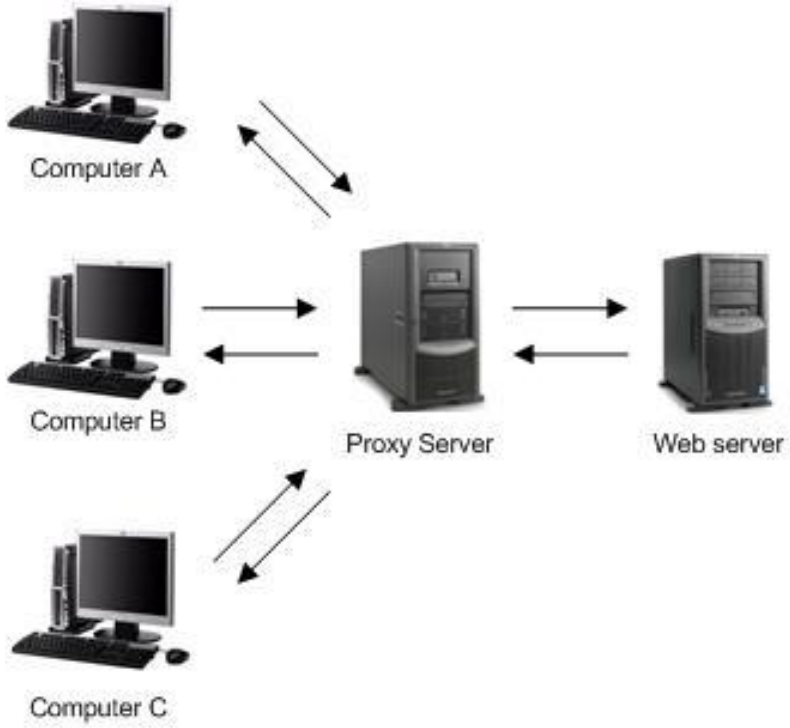
Paketové filtry: Nejjednodušší a nejstarší forma firewallování

- pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket
- **Výhoda:** vysoká rychlost zpracování (vysokorychlostní přenosy velkých množství dat)

Aplikační brány (Proxy firewally):

- **Průběh komunikace →**

klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi



Firewall – podrobněji 2

Stavové paketové filtry:

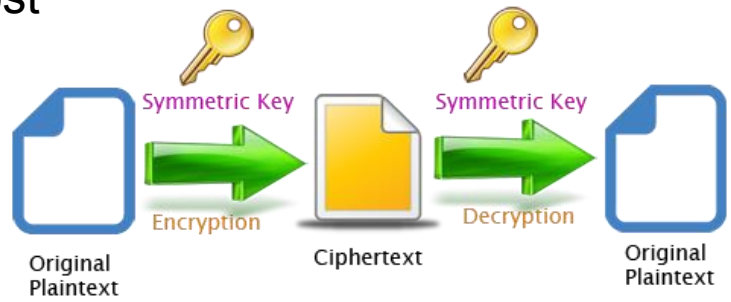
- kontrola jako u paketových filtrů + ukládaní informací o povolených spojeních → usnadnění rozhodnutí zda pakety pustit nebo ne
- Výhody:
  - urychlení zpracování paketů již povolených spojení
  - nastavení směru navazování spojení → firewall sám povolí odpovědní pakety
  - Vysoká rychlost, relativně solidní úroveň zabezpečení (je horší než u Aplikační brány), jednoduchá konfigurace
- Příklady:
  - Komerční: Cisco PIX, Cisco IOS Firewall
  - Free: `iptables` v linuxovém jádře a `ipfw` v *BSD

Základy moderního šifrování

Symetrická kryptografie

→ šifrovací algoritmus používá k šifrování i dešifrování jediný klíč

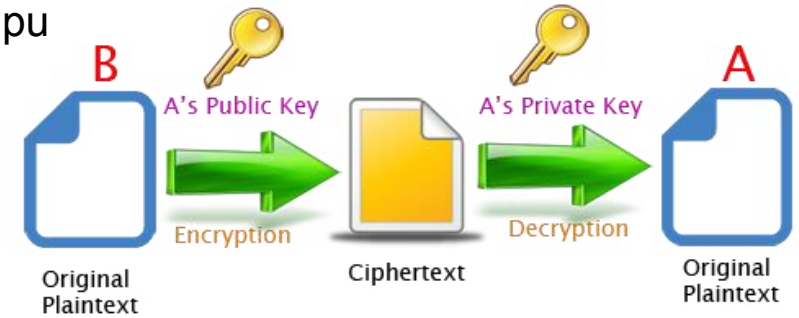
- Výhoda: nízká výpočetní náročnost
- Nevýhoda: nutnost sdílení tajného klíče
- **Rozdělení:**
  - Blokové šifry → rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost (AES, Blowfish, DES atd.)
  - Proudové šifry → zpracovávají otevřený text po jednotlivých bitech (FISH, RC4)



Základy moderního šifrování

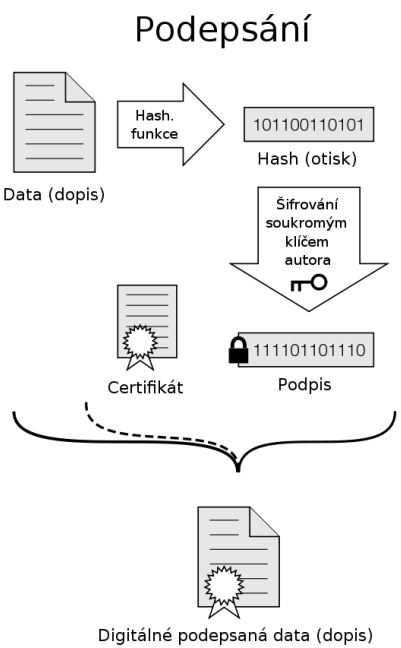
Asymetrická kryptografie

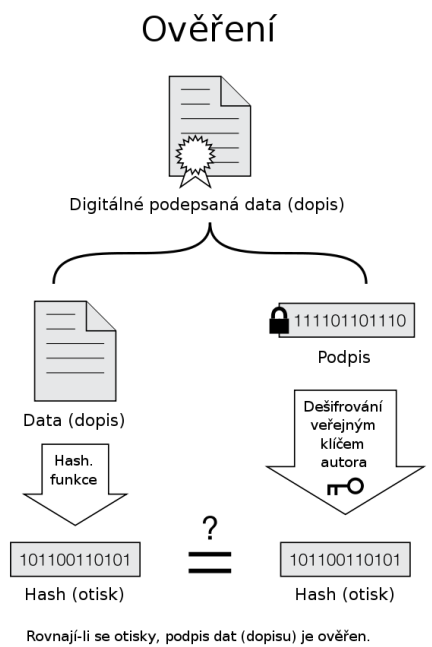
- pro šifrování a dešifrování používají odlišné klíče (využití i u elektronického (digitálního) podpisu)
- Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče:
  - šifrovací klíč je veřejný, majitel klíče ho volně uveřejní
  - dešifrovací klíč je soukromý, majitel jej drží v tajnosti
- Mechanismy funkce
  - Asymetrická kryptografie je založena na tzv. jednocestných funkcích → operace, které lze snadno provést pouze v jednom směru
  - ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup (např. násobení)
  - rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný



Digitální podpis

- Elektronický podpis jsou elektronické identifikační údaje autora (odesílatele), které jsou připojené k elektronického dokumentu
- **Zaručený elektronický podpis dokumentu zajišťuje:**
  - **autenticitu** – lze ověřit původnost (identitu subjektu, kterému patří elektronický podpis)
  - **integritu** – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není úmyslně či neúmyslně poškozen
  - **nepopiratelnost** – autor nemůže tvrdit, že podepsaný elektronický dokument nevytvořil (např. nemůže se zříct vytvoření a odeslání výhružného dopisu)
  - může obsahovat **časové razítko,** které prokazuje datum a čas podepsání dokumentu





zaručený elektronický podpis – zákon č. 227/2000 Sb., o elektronickém podpisu

Certifikáty a jejich využití

- Využití při ověření veřejného klíče (viz asymetrické šifrování)
- Certifikát definuje vazbu uživatel–klíč a definuje délku trvání této vazby
- Certifikáty vydává certifikační autorita – certifikační servery,
  - např. Microsoft
  - U nás certifikační autorita (www.ca.cz) nebo CA Czechia (www.caczechia.cz)
- Certifikát musí obsahovat:
  - Identifikátor algoritmu certifikační služby
  - Jméno autority, která certifikát vydala
  - Dobu platnosti certifikátu
  - Informace o veřejném klíči