

# Počítačové sítě

přednášky

*Jan Outrata*

říjen–prosinec 2010 (aktualizace září–prosinec 2013)

Tyto slajdy byly jako výukové a studijní materiály vytvořeny za podpory grantu FRVŠ 1358/2010/F1a.

# Fragmentace

- linkové rámce mají omezenou velikost (jeden až dva, max. jednotky kB), maximální velikost dat v rámci = **MTU (Maximum Transfer Unit)**, např. u Ethernetu II 1500 B
- IP paket může být ale dlouhý až 64 kB → **fragmentace paketu**
- pokud je fragmentace zakázána (bitem DF v záhlaví IP paketu):
  - paket je zahozen (pokud nejde jinou linkou) a odesilateli je to signalizováno pomocí ICMP typu 3, kód 4 – využití v algoritmu zjištění nejmenší MTU na cestě k uzlu (**Path MTU Discovery, PMTUD**)
  - později byla tato signalizace doplněna o možnost informace o MTU linky (2 B proměnné části záhlaví ICMP paketu)
- zvyšuje režii přenosu dat → OS se snaží vytvářet pakety délky ≤ MTU, aby nebylo fragmentace potřeba

**CVIČENÍ:** zjištění nejmenší MTU k uzlu pomocí programu ping se zakázáním fragmentace a nastavením velikosti paketu (algoritmus PMTUD)

# Fragmentace

- = dělení IP paketu na fragmenty o celkové délce  $\leq$  MTU linky, RFC 791
- **fragment** = samostatný **IP paket** se stejnou hlavičkou jako původní paket (s **identifikací fragmentu**), až na položky:
  - celková délka = délka fragmentu ( $\leq$  MTU)
  - **posunutí fragmentu** – offset dat fragmentu v datové části původního paketu, tj. kolik dat původního paketu je v předchozích fragmentech, v jednotkách 8B
  - **indikaci dalších fragmentů** (bit MF příznaků) – poslední fragment nemá nastavenou

Obrázek: Obrázek průvodce 144→145(5)

# Fragmentace

- **skládání fragmentů** (se stejnou identifikací fragmentu a protokolem vyšší vrstvy) do původního paketu provádí **pouze příjemce paketu!** – nikdo jiný nemusí mít všechny fragmenty
- pokud příjemce nemůže paket sestavit, protože v určené době nemá všechny fragmenty (protože např. první byl na cestě odfiltrován, např. podle adresy vyššího protokolu), signalizuje to příjemci pomocí ICMP typu 11, kód 1
- mechanismus umožňuje dále fragmentovat i fragmenty, směrovači na cestě

**CVIČENÍ:** zachytávání a inspekce IP fragmentů generovaných např. programem ping s nastavením velikosti paketu

# Volitelné položky IP záhlaví

- max. 40 B za povinnými položkami IP paketu

Obrázek: Obrázek průvodce 145→146(5)

- bit kopírovat znamená kopírování položek do všech fragmentů, jinak jen prvního
- číslo volby specifikuje typ volitelné položky, 0 pro poslední položku, 1 pro výplň záhlaví na násobek 4 B
- **zaznamenávej směrovače** (číslo 7): každý směrovač na cestě k příjemci zapíše IP adresu svého výstupního rozhraní (max. 9), příjemce je může zopakovat v odpovědi s touto volbou
- **zaznamenávej čas** (68): každý směrovač na cestě k příjemci zapíše čas (v ms od poslední půlnoci UTC, 4B) nebo čas a IP adresu svého výstupního rozhraní (8B, max. 4)

# Volitelné položky IP záhlaví

- **explicitní směrování** (131, 137): explicitní zadání směrovačů, přes které má paket jít, **striktní** = zadání všech, směrovače upravují adresu příjemce paketu na adresu následujícího směrovače, z bezpečnostních důvodů (průnik do privátní sítě) bývají pakety s touto položkou na směrovačích **filtrvány**
- **upozornění pro směrovač** (148): informace pro směrovače na cestě k cílovému směrovači, že v paketu mohou být informace (ohledně směrování) užitečné i ně
  - některé volby jsou implementované v programu ping

**CVIČENÍ:** zachytávání a inspekce IP paketů s volitelnými položkami v záhlaví generovaných např. programem ping

# Protokoly ARP a RARP

## ARP (Address Resolution Protocol)

- odchozí IP paket se vkládá do linkového rámce (např. Ethernet), jak se zjistí linková adresa příjemce? → **protokol ARP** (RFC 826)
- **zjištění linkové adresy** příjemce ze znalosti jeho IP adresy
- uzel vyšle **ARP paket žádosti** obsahující IP adresu příjemce na všesměrovou linkovou adresu a příjemce odpoví **ARP paketem odpovědi** (přímo odesilateli)
- ARP paket se vkládá přímo do linkového rámce, NE do IP paketu – **ARP je protokol nezávislý na IP**

# Protokoly ARP a RARP

## ARP (Address Resolution Protocol)

Obrázek: Obrázek průvodce 154

- **ARP paket:**

- typ linkového protokolu: číslo použitého linkového protokolu, např. 1 pro Ethernet II, 6 pro Ethernet podle IEEE 802.3 (viz IANA)
- typ síťového protokolu: stejná čísla jako v poli Protokol u linkového rámce, např. 0x800 pro IP
- HS a PS: délka linkové a síťové adresy
- operace: 1 pro ARP žádost, 2 pro ARP odpověď
  - linková adresa příjemce je v ARP žádosti nulová
  - v ARP odpovědi jsou oproti žádosti adresy prohozeny



# Protokoly ARP a RARP

## ARP (Address Resolution Protocol)

### • ARP cache

- = **tabulka síťová adresa – linková adresa**, naplněná staticky (manuálně) nebo dynamicky z přichozících linkových rámců se síťovými pakety a ARP odpovědí
- použita při zjišťování linkové adresy k síťové adrese
- omezená doba uchování dynamických položek (nepoužitých např. 2 minuty, maximální např. 10 minut), parametr OS
- pro manipulaci slouží program `arp`

### • proxy ARP

- ARP pakety se nesměrují (přísně vzato ARP není síťový protokol), **ARP** funguje **v rámci lokální sítě** (v dosahu linkového protokolu)
- = **konfigurace směrovače**, kdy v odpovědi na ARP dotaz se síťovou adresou za směrovačem uvede směrovač jako linkovou adresu příjemce svoji linkovou adresu
- ⇒ automatické nastavení směrování pro uzly v lokální síti přes směrovač

**CVIČENÍ:** zobrazení a manipulace s ARP cache, zachytávání a inspekce ARP paketů (po vymazání ARP cache)

# Protokoly ARP a RARP

## RARP (Reverse ARP)

- = **zjištění síťové adresy** odesílatele ze znalosti své linkové adresy
- dříve použití u bezdiskových stanic bootovaných po síti, které žádají o svoji síťovou adresu na základě linkové, tu přidělí a v odpovědi sdělí **RARP server**
- stejný paket jako u ARP, pole operace: 3 pro RARP žádost, 4 pro RARP odpověď
- dnes překonán aplikačním protokolem **DHCP**

# Protokol IGMP (IP multicast)

- = služební protokol IP k **šíření IP paketů na skupinové adresy (IP multicast)** s více příjemci **v rámci lokální sítě** (TTL=1)
- IP multicast výrazně snižuje síťový provoz a zátěž odesílatele
- několik verzí, zde verze 2 (RFC 2236)
- pro každou skupinovou adresu udržuje směrovač lokální sítě **skupinu členů** (uzlů) a pokud je nějaká skupina neprázdná, směrovač šíří multicast pakety s adresou skupiny zvenku dovnitř lokální sítě
- uzel (aplikace na něm) požadující příjem multicast paketů vyšle **IGMP paket** s požadavkem na členství ve skupině dané skupinovou adresou

Obrázek: Obrázek průvodce 158

# Protokol IGMP (IP multicast)

- **IGMP paket** obsažen v IP paketu:
  - typ: dotaz směrovače na členství ve skupině (11), požadavek na členství ve skupině (16), opuštění skupiny (17)
  - **MRT (Maximum Response Time)**: pouze u typu 11, čas (v desetinách s), do kterého se musí uzly znovu přihlásit do skupiny, jinak jsou vyřazeni
  - **skupinová IP adresa**: nula u dotazu typu 11 (adresuje všechny skupiny), jinak z **třídy D**, rozsah **224.0.0.0/24** je pro vyhrazené účely (např. 224.0.0.1 je všeobecná pro všechny uzly, 224.0.0.2 pro všechny směrovače atd.)
- více směrovačů na lokální síti: dva režimy směrovače – **dotazovač** (posílá dotazy) a **posluchač** (dotazovač, který se přepnul, pokud detekoval v lokální síti dotazy směrovače s vyšší adresou, jen poslouchá)

# Protokol IGMP (IP multicast)

## Mapování síťových na skupinové linkové adresy

- „mapování“ jednoznačných IP adres (unicast) → ARP, mapování všesměrové → všesměrová linková adresa
- síťová karta zpracovává (v normálním, ne promiskuitním, režimu) pouze jí adresované a všesměrové rámce, navíc pak **skupinové rámce**, o které **zažádá síťová vrstva**
- Ethernet:
  - skupinová MAC adresa: nejnižší bit prvního bytu = 1
  - první tři byty MAC adresy pro výrobce – IANA má 00:00:5E, polovina jejího rozsahu pro **skupinové adresy**, prefix **01:00:5E**
  - = **nejednoznačné mapování** 28 bitů skupinové IP adresy do 23 bitů skupinové MAC adresy: IP adresy lišící se pouze v nevyšších 5 bitech (po prefixu skupinových adres), např. 224.0.1.1 a 225.0.1.1, mapovány na stejné linkové adresy

Obrázek: Obrázek průvodce 162

⇒ pakety s nechtěnou IP adresou musí odfiltrovat síťová vrstva

# IP multicast

## IP multicast mimo lokální síť (v Internetu)

- šíření multicast paketů Internetem od odesílatele k příjemcům ve více lokálních sítích – poměrně **složitá záležitost**, cíl **zamezit nekontrolovanému lavinovitému duplikování paketů** v Internetu
- **úpravy směrovacích protokolů** pro výměnu směrovacích informací mezi směrovači – protokoly např. **DVMRP, MOSPF, MBGP**
- problémy se škálovatelností (počty příjemců v milionech), **aktivní výzkum**
- dříve experiment s **MBONE (Multicast Backbone)** = vybrané směrovače („jádro Internetu“) zabezpečující šíření multicast paketů pomocí tunelů
- dnes protokoly **PIM (Protocol Independent Multicast)** konstruuující **distribuční strom multicastu** (pro každou skupinovou adresu), varianty Sparse Mode (SM), Source Specific Mode (SSM), Bidirectional Mode
- využití v **distribuci multimediálního obsahu (streaming)**, neobecně jako způsob přenosu libovolných dat v Internetu

# Protokol IP verze 6 (IPv6)

- ~ “**IP nové generace**”, **IPng**, vyvíjen od roku 1991, 1995 RFC-1883, dnes RFC-2460 (základ + přidružená RFC)
- odstraňuje **nedostatky IPv4**: řešení problému adresace, dynamické konfigurace, podpory bezpečnosti, mobility uzlů, multimédií aj.
- = nejen **zvětšení IP adresy, nový pohled na IP paket** (revize):
  - zjednodušení záhlaví – přesun málo využívaných základních položek do (zřetězených) volitelných: pro směrování, fragmentaci, autentizaci aj.
  - (bezstavová) **automatická konfigurace uzlů**
  - bezpečnost – **autentizace a šifrování** na úrovni síťové vrstvy
  - podpora **mobility uzlů** – se snahou o zachování TCP spojení při přechodu uzlu ze sítě do sítě (!)
  - podpora multimédií – třídy dat (včetně real-time komunikace), směrování toku a ne jednotlivých paketů
  - ...

# Protokol IP verze 6 (IPv6)

## IPv6 paket

Obrázek: Obrázek průvodce 196→208(5)

- = 40 B základní záhlaví + nepovinná rozšíření různé délky, data, max. 64 kB, ale možnost rozsáhlého paketu v rozšířeních
- **třída dat**: specifikace priority dat pro rozhodování o zahození paketu při zahlcení sítě, hodnoty 0 až 7 pro klasický provoz (datové přenosy, pošta, interaktivní atd.), 8 až 15 pro přenosy v reálném čase (multimédia)



# Protokol IP verze 6 (IPv6)

## IPv6 paket

- **identifikace toku dat:** spolu s adresou odesilatele jednoznačně identifikuje datový tok, pro potřeby **směrování** – řešení směrování jen u prvního paketu toku, ne u každého (na základě jen adresy příjemce u IPv4), nebo k **zajištění šířky pásma** – prioritní FIFO paketů na směrovači místo obyčejné (jako u IPv4), protokol RSVP
- **další záhlaví:** typ následujícího záhlaví **nepovinného rozšíření IPv6** (včetně typu 59 pro žádné) nebo protokolu vyšší vrstvy, např. TCP (6), UDP (17), IP (v IP, 4)
- **počet hopů:** ~ TTL u IPv4, k zahazování zatoulaných paketů nebo k nalezení nejkratší cesty (zvyšování TTL, obdoba traceroute)

# Protokol IP verze 6 (IPv6)

## IP adresa

- délka 16 B (128 b), tři typy:
  - jednoznačná síťového rozhraní (unicast)
  - skupinová (multicast) – zvláštní případ všeobecná (broadcast)
  - skupinová **anycast** = paket doručen jen nejbližšímu z adresátů skupiny, adresy z rozsahu unicast adres, např. subnet-router, DNS query anycast
- notace zápisu s až čtveřicemi šestnáctkovými číslic oddělenými dvojtečkou, např. **2001:718:1401:50:0:0:0:0d**, nebo častěji zkrácená pomocí zdvojené dvojtečky (pouze jednou, nahrazuje sekvenci 0), např. **2001:718:1401:50::0d**, nebo i s posledními čtyřmi byty v notaci adresy IPv4 (tzv. kompatibilní adresy), např. **FE80::158.194.80.13**
- notace sítě spolu s maskou (**prefix**): prefix adresy pro síť/počet 1 v (binární) masce

# Protokol IP verze 6 (IPv6)

## IP adresa

- **rozdělení na poloviny** (RFC 2373, 2450): adresa sítě (64 b) a adresa uzlu (rozhraní, 64 b)
- **adresa sítě**: obdobně jako u IPv4, **globální prefix** (45 b za prvními třemi bity) pro Internet Registry a autonomní systémy, např. pro RIPE 2001:0600::/29 až 2001:07F8::/29, dále poskytovatele (supersítě) a organizace (sítě), pak pro subsítě (16 b)

Obrázek: Obrázek průvodce 214→227(5)

- globálně jednoznačné (unicast) adresy pro Internet: (zatím) **2000::/3**, bloky /23 až /12 pro Internet Registry

# Protokol IP verze 6 (IPv6)

## IP adresa

Obrázek: Obrázek průvodce 215→227(5)

- **adresa rozhraní:** vlastní, podle **IEEE EUI-64** = **MAC adresa** podle IEEE 802, kde doprostřed se vloží **0xFFFE** a nastavení druhého bitu prvního byte, např. pro 00:02:B3:BF:30:EA je 202:B3FF:FEBF:30EA, náhodně dynamicky generovaná (**Privacy Extensions**)
- **bezstavová autokonfigurace, SLAAC:** adresa rozhraní podle IEEE EUI-64 nebo náhodná „samopřidělená“ na základě **oznámení směrovače (router advertisement, RA)** s adresou sítě (prefixem), obdoba 169.254.0.0/16 u IPv4, zabezpečení RA Guard, SEND (asymetrická kryptografie, šifrovaná adresa), access listy na přepínači
- **DHCPv6:** bezstavové – SLAAC + další info (DNS servery na LAN, domény apod.) z DHCP serveru, stavové – jako DHCP pro IPv4, ale ne výchozí brána LAN (sic!), identifikace uzlu pomocí DUID místo MAC rozhraní – pro uzel, nezávislost na MAC, 3 typy, zabezpečení DHCP Snooping

# Protokol IP verze 6 (IPv6)

**IP adresa** – speciální adresy:

- celá 0: nspecifikovaná, rozhraní ještě nebyla přidělena adresa
- ::1/128: **loopback**
- FE80::/10: automatické v rámci lokální sítě nebo linkově propojených sousedů (**link-local** unicast), nesměrují se, adresa rozhraní automaticky „samopřidělená“ podle IEEE EUI-64, pro objevování sousedů (viz dále), oznámení směrovače, směrovací protokoly aj.
- FC00::/7: unikátní (síťová adresa, prefix, z data a MAC rozhraní) v rámci organizace (**unique-local** unicast), použití u intranetu, nesměrují se, dříve FEC0::/10 – privátní v rámci organizace (**site-local** unicast), obdoba vyhrazených rozsahů u IPv4 (10.0.0.0/8 atd.)
- FF00::/8: skupinové adresy (**multicast**), první 4 bity z druhého byte specifikují rozsah skupiny, např. 1 v rámci uzlu, 2 lokální sítě, 5,8 organizace, E globální, vyhrazené adresy, např. FF02::1 pro všechny uzly = **broadcast**

# Protokol IP verze 6 (IPv6)

**IP adresa** – speciální adresy:

- **přechodové z IPv4**: tunelovací (IPv6 v IPv4) 2002:AB:CD::/16 **6to4** – pro IPv4 ( $A.B.C.D$ )<sub>16</sub> adresu rozhraní, 6to4 relay směrovač (např. NIC.cz) na anycast adrese 192.88.99.1, **ISATAP** – relay ve firemní síti (v DNS), **Tunnel Broker** – veřejný relay (HE, SixXS), 2001::/32 **Teredo** – pro uzly za NAT, UDP zapouzdření, veřejný Teredo server (např. Microsoft), mapování ::FFFF:a.b.c.d na IPv4 a.b.c.d. (**SIIT**, virtuální IPv4 rozhraní), překlady IPv6 (např. 64:FF9B::/96) na IPv4 **NAT64 & DNS64**, aj.
- 2001:db8::/32: pro dokumentace (obdobné i u IPv4)
- ...

# Protokol IP verze 6 (IPv6)

## Nepovinná rozšíření

Obrázek: Obrázek průvodce 199→211(5)

- **záhlaví rozšíření:** typ následujícího záhlaví (tvoří řetězec použitých položek na rozdíl od všech u IPv4), délka záhlaví, data
- **informace pro směrovače** (typ 0): informace = volby (pole typ, délka, hodnota, např. rozsáhlý paket délky až 4 GB, typ 194)
- **směrovací informace** (43): **explicitní směrování, hop-by-hop** – pole počet směrovačů, maska striktního směrování (bit = 1 = sousední směrovač), adresy směrovačů a příjemce, 2007 zrušeno

# Protokol IP verze 6 (IPv6)

## Nepovinná rozšíření

- **záhlaví fragmentu** (44): fragmentovat může pouze odesílatel (na rozdíl od IPv4, algoritmus PMTUD), pole posunutí fragmentu (hodnota v jednotkách 8B), indikace dalších fragmentů, identifikace fragmentu
- **autentizace** (51, protokol AH) a **bezpečnost/šifrování** (50, ESP): integrita a autentizace (místo kontrolního součtu, MD5 ze sdíleného tajemství a paketu), šifrování odesílatelem nebo směrovači, použití v IPSec, poslední záhlaví
- uspořádání od těch pro směrovače po ty pro koncový uzel



# Protokol IP verze 6 (IPv6)

## Protokol ICMP verze 6

- = nepovinné rozšíření IP záhlaví, typ 58, RFC 2463
- stejně jako u IPv4 pro **signalizaci** chybových stavů a **diagnostiku**
- pole typ, kód, kontrolní součet a tělo
- např. echo (žádost, odpověď), čas vypršel, nedoručitelný paket (není směr, adresa, administrativně), změň směrování, žádost+odpověď o směrování apod.
- **Neighbor discovery protokol, NDP**: objevování sousedů ~ překlad IPv6 adresy na linkovou adresu (místo ARP a RARP u IPv4) = žádost a oznámení o linkové adrese (neighbor solicitation a advertisement), žádost o a oznámení směrovače (router solicitation a advertisement) – adresa sítě (prefix) a výchozí brány LAN (nově i DNS serverů), povolení SLAAC, aj., zasílaná na skupinovou adresu LAN (speciální FF02::1:FF00:0/104)

**CVIČENÍ:** zachytávání a inspekce IPv6 paketů, zjištění IPv6 adresy síťového rozhraní

# Bezpečnost protokolu IP

## IPv4

- **neřeší**, naopak např. některé volitelné položky (explicitní směrování) mohou být nebezpečné
- pouze kontrolní součet záhlaví – snadné přepočítat po modifikaci paketu
- útoky: podvržení IP adresy odesílatele a příjemce (**IP spoofing**), zahlcení sítě (např. flood ping) a odepření služby (**Denial of Service, DoS**)
- řešení: **filtrace** (některých ICMP paketů, paketů s volitelnými položkami atd.), **šifrování** – privátní sítě (intranet, s překladem adres), DHCP Snooping aj.

## IPv6 – útoky + řešení jako u IPv4

- autentizace (protokol AH) a šifrování (protokol ESP) v dalších záhlavích → **IPSec**
- zabezpečení autokonfigurace – SEND

# Bezpečnost protokolu IP

## Firewall

- oddělení vnitřní sítě (intranetu) od vnější (Internetu), ochrana systému uzlu před sítí
- služby: **filtrace provozu**, kontrola adres, překlad adres (NAT) – na základě IP záhlaví (a dále záhlaví vyšších protokolů), aplikační brána (proxy, protokol SOCKS), logování a detekce útoků (IDS, IPS)
- provozován na hraničních směrovačích (bráně) mezi sítěmi nebo na klientských počítačích
- nastavení pravidel (fitračních aj.) OS nebo pomocí aplikačního programu
- **demilitarizovaná zóna (DMZ)** – část sítě s počítači dostupnými z vnitřní (chráněné) i vnější sítě, např. aplikační (proxy) servery

# Bezpečnost protokolu IP

## Překlad adres (**Network Address Translation, NAT**) (RFC 1631)

- = překlad IP adres paketů z vnitřní sítě (intranetu) na IP adresy vnější sítě (Internetu) a naopak
- **SNAT (Source NAT)** = překlad IP adresy odesílatele, **DNAT (Destination NAT)** = překlad IP adresy příjemce
- poskytuje skrytí vnitřní sítě, využití také při spojení více intranetů se stejným rozsahem adres
- provozován na hraničních směrovačích (bráně) mezi sítěmi, typicky v rámci firewallu
- **maškaráda** = SNAT na IP adresu hraničního směrovače ve vnější síti, překlad i (zdrojového) portu transportní vrstvy (**NAPT (Network Address and Port Translation)**)
- zasahuje i do vyšších vrstev, transportní (překlad portů) i aplikační (porozumění aplikačnímu protokolu)

# Bezpečnost protokolu IP

## IPSec (Internet Protocol Security) (RFC 2401 – 2412)

- původně v rámci prací na IPv6 (jeho povinná součást), backportován i pro IPv4
- = zabezpečení komunikace mezi počítači (koncovými síťovými rozhraními) na úrovni síťové vrstvy ⇒ **bezpečná síť**
- = **autentizace** komunikujících rozhraní a **šifrování** IP paketů
  - poměrně komplikovaný protokol, závislý na architektuře TCP/IP
  - funkce: správa šifrovacích klíčů (certifikační autority, autentizace (digitální podpis, hashe), šifrování (DES, RSA))
- záhlaví IPSec mezi záhlavím IP a daty paketu, položky pro autentizaci (AH) a šifrování (ESP), viz IPv6, dále protokoly pro výměnu klíčů **ISAKMP** a **IKEY**
- režimy:
  - transportní – šifrování datové části IP paketu, mezi koncovými uzly
  - tunelovací – tunelování IP sítě v IP síti, zapouzdření šifrovaných IP paketů do nových IP paketů (IPSec over IP), tunel mezi směrovači nebo vzdáleným uzlem a hraničním směrovačem sítě

# Sítě WAN na bázi IP

- původní představa WAN jako propojení LAN pomocí směrovačů a pronajatých okruhů ATM nebo Frame Relay přestala stačit
- páteřní sítě přímo na bázi IP, **homogenní IP síť**
- **IP over Fiber** = přenos IP prostřednictvím optických sítí, varianty
  - systém **SONET/SDH** – převod el. signálů na optické, IP over ATM (vysoká režie, 622 Mb/s), IP over SONET/SDH (IP pakety v PPP rámcích v kontejneru SONET/SDH, synchronní přenos, 155 Mb/s)
  - **IP over DWDM** (případně ještě se SONET/SDH) – transparentní přenos paketů bez převodu signálu a formátování do rámců, až 10 Gb/s, kombinace s MPLS (MPΛS)
- **virtuální privátní sítě (VPN)**: virtuální IP síť v rozlehlé IP síti
- **MPLS**: přepínané IP sítě místo hop-by-hop sítí (se směrovači), na základě tzv. návěští po definované cestě (zaručení atributy spojení, QoS, VPN atd.)
- **QoS**: zabezpečení kvality přenosu pomocí rezervace zdrojů/upřednostnění paketů (InetServ/DiffServ), protokol RSVP

# Virtuální privátní síť (VPN)

- = privátní síť virtuálně v rozlehlé transportní síti (Internetu), často jako propojení (privátních) sítí nebo uzlu a (privátní) sítě, nahrazuje pronajaté telekomunikační okruhy
- privátní adresace – nutno řešit oddělení privátních sítí např. pomocí filtrace a NAT

## → tunelování

- = zapouzdření paketů nebo celých rámců vnitřní sítě do paketů transportní sítě
  - vytváření **tunelů** = (dvoubodových) logických spojení mezi uzly virtuální sítě, propojení do transportní sítě = **VPN gateway**
  - zabezpečení tunelů a oddělení sítí: autentizace, šifrování
- tunelování linkové vrstvy (zapouzdřování rámců): protokoly **PPTP**, **L2TP** (PPP rámce v IP, Frame Relay, ATM, autentizace, šifrování, komprese, vícebodové tunely)
- tunelování síťové vrstvy (zapouzdřování paketů): **IP over IP**, protokoly **GRE** (původní, dvoubodové tunely) a **IPSec**
  - oddělení IP sítí – např. přepínání, MPLS (MPΛS)