# Úvod

## Komunikace obecně

* Atributy komunikace
  + Identifikace
  + Metoda komunikace
  + Jazyk komunikace
  + Rychlost komunikace
  + Procesní řízení
    - Začátek, požadavky, odpovědi, konec
* Typy komunikace
  + Běžná
  + Telekomunikace
    - Zabudována pravidla
    - Řízení vnitřní sítí
      * Včetně koncových zařízení
    - Funguje na principu přepojovaných okruhů
      * Při výpadku jedné stanice se spojení rozpadne
    - Příklady: telefonní síť
  + Počítačová síť
    - Volně dostupné
    - Řízení komunikace probíhá na koncových zařízeních
    - Síť zabezpečuje pouze přenos
    - Funguje na principu předávání paketů
      * Každý paket si volí jinou cestu
  + Konvergovaná síť
    - Propojení telekomunikací a počítačových sítí

# Počítačové sítě

## Úvod

* Vznik počítačových sítí
  + Původně izolované systémy (např. univerzity v USA)
  + Později point-to-point propojení
  + Dnes LAN propojeny do WAN
* Dělení sítí (pouze terminologické)
  + LAN
    - Sdílení v rámci lokální sítě
    - Jednotné řízení a vlastnictví
  + WAN
    - Vzdálený přístup, komunikace
    - Mnoho vlastníků → distribuované řízení
  + Dále MAN, GAN, RAN…
* Veřejné a privátní sítě
  + Většina LAN je privátních
  + Propojení privátních sítí pomocí VPN
* Historie internetu
  + 1969 – APRANET
    - Provoz na univerzitách v USA
  + 1974 – termín „Internet“
  + 1983 – začátek TCP/IP

## Požadavky

* Bezpečnost
  + Nové kritérium – dříve nebylo nutné
  + Ověřování
    - Identity
    - Správnosti obsahu
  + Metody
    - Ověřování uživatelů a přístupová práva
    - Inspekce dat
    - Kryptografie
* Rozšiřitelnost
* Kvalita služeb
  + Přenosové parametry sítě
    - Zpoždění (*latence, delay*)
    - Pravidelnost doručování (*jitter*)
    - Ztrátovost dat
    - Šířka pásma (*bandwidth, „*rychlost*“*)
  + Různé služby mají různé požadavky na jednotlivé parametry
  + Implementace
    - Klasifikace dat podle „významnosti“
    - Lze upřednostňovat kvalitu nebo rychlost

## Modely

* Síťový model
  + Určuje počet a strukturu vrstev
  + Rozdělení práce mezi vrstvy
* Síťová architektura
  + Zahrnuje síťový model
  + Navíc komunikační technologie
  + Konkrétní služby a protokoly
* OSI (Open Systems Interconnection)
  + Síťový model
  + Vhodný pro výuku (jinak nepraktický)
  + Vrstvy
    - Fyzická – fyzický přenos (bitů) mezi uzly
    - Linková – přenos datových rámců mezi uzly
    - Síťová – směrování mezi sítěmi
    - Transportní – end-to-end přenos datových bloků
    - Relační – řízení dialogu mezi koncovými uzly
    - Prezenční – datové konverze pro aplikace
    - Aplikační – komunikace mezi programy
  + Standardy OSI
    - X.400 (Message Handling System)
    - X.500 (Directory Access Protocol)
* TCP/IP
  + Účelový, z praxe
  + Vrstvy
    - Linková – Ethernet, Wi-Fi
    - Síťová – IP
    - Transportní – TCP, UDP
    - Aplikační – FTP, HTTP, SMTP, DNS, SIP

## Služby

* Spojové služby
  + Obdoba telefonního spojení
  + Spolehlivé doručení dat
  + Jednoduchá aplikační implementace
    - Nemožnost řídit komunikaci
  + V TCP/IP používá TCP
* Nespojové služby
  + Obdoba poštovního spojení
  + Nezaručené spojení
  + Kontrolu dat musí provádět aplikace
  + V TCP/IP používá UDP
* Aplikační modely
  + Klient-server
    - Klient zná pevnou adresu serveru
    - Klient navazuje komunikaci, zadává požadavky
    - Server obvykle obsluhuje více klientů
    - Tok dat
      * Server → klient: download
      * Klient → server: upload
    - Příklady: DNS, WWW, SMTP
  + Peer-to-peer (P2P)
    - Partneři neznají pevné adresy
    - Každý je zároveň klientem i serverem
    - Nejsou vyhraněné role
    - Příklady: Napster, Gnutella, BitTorrent
* Adresování počítačů
  + Linková vrstva (HW)
    - MAC adresa
  + Síťová vrstva (SW)
    - IP adresa
  + Aplikační vrstva
    - Doménová adresa
* Správa domén
  + Domény prvního řádu
    - Spravuje ICAAN (Internet Corporation for Assigned Names and Numbers)
    - Technické (.arpa)
    - Rezortní (.com, .org, .gov)
    - Kódy zemí (.cz, .us)
  + Domény druhého řádu
    - V ČR CZ.NIC, sdružení ISP
  + Domény nižších řádů
    - Spravuje vlastník
* IP adresy
  + Každý koncový uzel musí mnít svou IP adresu
  + Verze
    - IPv4 (32 bity)
    - IPv6 (128 bitů)
  + Veřejné adresy přiděluje ISP
  + Adresy v LAN přiřazuje centrální uzel
    - Pevné nebo dynamické
* Port
  + 16bitové číslo identifikující proces který zpracovává konkrétní pakety
  + V podstatě adresa aplikace, služby
  + Příklady
    - 21/TCP – FTP
    - 22/TCP – SSH
    - 25/TCP – SMTP
    - 53/\* – DNS
    - 80/TCP – HTTP
    - 443/TCP – HTTPS
    - 5060/\* – SIP
* Socket
  + Celá adresa koncového uzlu komunikačního kanálu
  + Formát <IP adresa, port>
* NAT (Network Adress Translation)
  + Překlad adres
  + Obecný princip, kdy lokální síť používá privátní adresy a ven se představuje veřejnými adresami
* Adresování služeb
  + URI (Uniform Resource Identifier)
    - Jednotný systém odkazů
    - Možnost jednoho klienta pro více služeb
    - URL (Uniform Resource Location)
    - URN (Uniform Resource Name)
    - Struktura URI:
      * schéma:[//] autorita [cesta] [?dotaz] [#fragment] autorita = [jméno[:heslo]@]adresa[:port]
    - Příklad:
      * <ftp://sunsite.mff.cuni.cz/Net/RFC?ID=43#Local>
* Multiplexing (zapouzdření)
  + Různé komunikační kanály na jedné vrstvě využívají stejný kanál na nižší vrstvě

## Bezpečnost

* Autentizace
  + Proces ověření identity
  + Pozor – autorizace je vymezení rozsahu služeb pro autentizovaný subjekt
  + Lokální autentizace
    - Heslo, PIN
    - HW klíč, token
    - Biometrie
  + Vzdálená autentizace
    - Systém OTP
    - Speciální protokoly (SASL)
    - Autentizační protokol a server (LDAP, Kerberos)
* OTP (One Time Password)
  + Obecně mechanizmy pro nepředvídatelnou textovou autentizaci uživatele
  + Uživatel obdrží od serveru časově omezený token
* Symetrické šifrování
  + Při šifrování a dešifrování používají stejný klíč
  + Rychlé, vhodné na velká data
  + Nevýhoda v nutnosti distribuce klíče
  + Příklady: DES, RC4
* Asymetrické šifrování
  + Pro šifrování a dešifrování se používá pár navzájem různých klíčů
  + Použití jednocestné funkce
    - Např. násobení vs. rozklad na prvočinitele
  + Příklady: RSA, DSA
  + Není nutné distribuovat privátní klíč
  + Nevýhodou pomalé algoritmy
* Hashovací funkce
  + Z jedinečného vstupu vytvoří jedinečný výstup → hash
  + Nalezení textu se shodným hashem je obtížné
  + Využití v kry
  + Příklady: CRC, MD5
* Proces šifrování dat
  + Volný text
    - Zašifrován symetricky náhodným klíčem
  + Klíč asymetricky zašifrován veřejným klíčem příjemce
  + Posílá se symetricky zašifrovaný a asymetricky zašifrovaný klíč
  + Příjemce rozšifruje klíč pomocí privátního klíče
  + Pak rozšifruje text
* Proces elektronického podpisu
  + Volný text se zaheshuje
  + Hash se asymetricky zašifruje pomocí privátního klíče odesílatele
  + Posílá se volný text a zašifrovaný hash
  + Rozšifrováním hashe veřejným klíčem získá příjemce původní hash
  + Může zaheshovat text stejnou funkcí a oba hashe porovnat
* Autenticita veřejných klíčů
  + Nutnost ověřit majitele veřejného klíče (tj. toho, komu chci zprávu poslat)
  + Autenticitu ověřuje třetí strana a připojuje svůj podpis
* Certifikát
  + Certifikát je veřejný klíč společně s identifikací vlastníka a podpisem vydavatele
    - Vydavatel je obvykle certifikační autorita (CA)
  + Struktura certifikátu
    - Certifikát
      * Verze certifikátu
      * Sériové číslo certifikátu
      * Vydavatel
      * Doba platnosti
      * Vlastník veřejného klíče
      * Informace o veřejném klíči vlastníka (algoritmus a klíč)
    - Algoritmus pro elektronický podpis
    - Elektronický podpis
* SSL (Secure Socket Layer) ~ TLS (Transport Layer Security)
  + Mezivrstva mezi transportní a aplikační vrstvou (tj. např. mezi TCP/IP a HTTP(S))
  + Umožňuje autentizaci a šifrování
  + Využívá jej HTTPS
  + Princip
    - Klient pošle požadavek na SSL spojení
    - Server pošle odpověď a certifikát
    - Klient ověří certifikát serveru a vygeneruje základ šifrovacího klíče
    - Ten zašifruje veřejným klíčem serveru a pošle mu ho
    - Ze základu oba vygenerují primární šifrovací klíč
    - Potvrdí si, že jejich klíče souhlasí

# Aplikační vrstva

## Úvod

* Vlastnosti
  + Průběh dialogu na obou stranách
  + Formát zpráv (textový/binární, struktura)
  + Typy zpráv (požadavky a odpovědi)
  + Interakce s transportní vrstvou

## DNS (Domain Name System)

* Vlastnosti
  + Klient-sever aplikace pro překlad jmen na adres
  + Binární protokol
  + Port 53
  + TCP i UDP
    - Dotazy do 512B přes UDP
* DNS Záznam
  + Vlastnosti
    - Název
    - Platnost (TTL)
    - Typ a data
  + Typy záznamů

|  |  |  |
| --- | --- | --- |
| **Typ** | **Jméno** | **Data** |
| SOA | Jméno domény | Obecné informace o doméně |
| NS | Jméno domény | Jméno DNS serveru domény |
| A | Jméno počítače | IPv4 adresa |
| AAAA | Jméno počítače | IPv6 adresa |
| PTR | Reverzní jméno počítače | Doménové jméno počítače |
| CNAME | Alias | Kanonické jméno počítače |
| MX | Jméno domény/počítače | Jméno poštovního serveru a jeho priorita |

* + Příklad záznamu
    - ns.cuni.cz. 3600 IN A 195.113.19.78
* DNS servery
  + Typy serverů
    - Primární – spravují záznamy o doméně
    - Sekundární – stahuje a uchovává kopii primárních serverů (průběžně nebo na výzvu)
    - Caching-only – udržují nevyřešené dotazy po dobu platnosti
  + Každá doména musím mít alespoň jeden primární server
  + Data mezi DNS servery se předávají pomocí TCP
* Bezpečnost DNS
  + Útočník může do odpovědi serveru přidat falešné údaje o doméně
  + Existuje DNSSEC
    - Na bázi podepisovacího klíče domény
    - Komplikované, nepříliš rozšířené
* Diagnostika DNS
  + Program nslookup
    - Příkazy: set type, server, name, IPadr, ls, exit
* DNS dotaz
  + Dotaz  
    ID: n   
    FLAGS: Recursion Desired   
    QUERY: www.cuni.cz. IN A
  + Odpověď  
    ID: n  
    FLAGS: Authoritative Answer  
    QUERY: www.cuni.cz. IN A  
    ANSWER: www.cuni.cz. IN CNAME tarantula  
     tarantula IN A 195.113.89.35  
    AUTHORITY: cuni.cz. IN NS golias  
    ADDITIONAL: golias IN A 195.113.0.2

## FTP (File Transfer Protocol)

* Vlastnosti
  + Jeden z nejstarších protokolů
  + Dříve hojně využíván
  + Dnes spíše pro anonymní přístup
    - Otevřený přenos hesla – nebezpečné
* Kódy odpovědí
  + 1xx – předběžná kladná odpověď
  + 2xx – definitivní kladná odpověď
  + 3xx – neúplná kladná odpověď
  + 4xx – dočasná záporná odpověď
  + 5xx – trvalá záporná odpověď
* Průběh spojení
  + Řídící spojení
    - Vyřizuje požadavky klienta a odpovědi serveru
  + Vedlejší datová spojení
    - Pro každý datový přenos se otvírá nové TCP spojení, které se poté zase uzavře
  + Aktivní spojení
    - Navazuje jej server
    - Používá port 20 (ftp-data)
    - Příkaz PORT s IP a portem klienta
  + Pasivní spojení
    - Zahajuje jej klient
    - Klient posílá příkaz PASV – požadavek na IP a port, kam se může připojit
  + Výpis dat pak proběhne příkazem LIST
* Aplikace pro FTP
  + WWW prohlížeče
  + Správci souborů
  + Řádková příkaz ftp
* Příkazy FPT
  + Navazování realce: open, user
  + Ukončování relace: close, quit, bye
  + Vzdálené příkazy: cd, pwd, ls, dir
  + Práce se soubory: delete, rname, mkdir, rmdir
  + Přenos souborů: get, put
  + Další: prompt, hash, status,…

## SMTP (Simple Mail Transfer Protocol)

* Vlastnosti
  + Port 25
* Elektronická pošta
  + Obecná služba nezávislá na internetu
* Princip SMTP
  + Přímé doručení na cílový SMTP server
    - Možné například v LAN
  + Nepřímé
    - Přes jiný server v lokální síti (mail forwarder)
    - E-mail pak putuje sítí a přes MTA (mail transfer agent) se postupně dostane až k cílovému serveru
    - Pokud je cílový server nedostupný, lze do hlavičky mailu přidat MX (mail-exchanger)
      * MX může přijímat maily za původní server
* Poštovní program
  + Dvě možnosti připojení k mailboxu
    - Přímo na MTA server
      * Nebezpečné pro server
    - Přes protokol POP nebo IMAP
* Soubory a diakritika v poště
  + Původně pouze ASCII znaky
  + Později nahrazeno UUENCODE
    - Binarní
  + Dnes MIME (Multipurpose Internet Mail Extension)
    - Dnes široké využití, například také v HTTP
    - Podporuje tedy nonASCII znaky v těle a někdy i v hlavičce
    - Dělí se na hlavičku a tělo
      * Hlavička
        + Typ dokumentu, znaková sada. Kódování, název souboru, způsob zpracování
      * Tělo jako samotný obsah
    - Podporuje kódování Base64 nebo Quoted-Printable
      * Base64 – vychází z UUENCODE
        + Převádí binární data ta tisknutelné znaky
        + Zakóduje tři byty na čtyři znaky ASCII (nárust o 33%)
      * Quoted-Printable
        + Zachovává ASCII znaky
        + nonASCII znaky kóduje jako „=HH“, kde HH je hexadecimální hodnota znaku
* Bezpečnost pošty
  + Maily nejsou šifrované
  + „Odesílatel“ je pouze informace v hlavičce – lze ji změnit
  + Poštovní server by měl posílat maily lokálních uživatelů komukoliv, ostatní maily pouze lokálním uživatelům
    - Jinak tzv. open-relay – hrozba šíření spamu
* Blokace spamu
  + Grey-listing
    - Spamové automaty nekontrolují, zda byl mail doručen
    - Server proto zkusí první pokus o přijetí mailu odmítnout a vrátí odpověď 450
    - Regulérní mail server se pokusí o odeslání znovu → mail dorazí se zpožděním
    - Pokud se nepokusí o nové odeslání, je server zařazen na „gray-list“
  + (DKIM) DomainKeys Identified Mail
    - Server mail a jeho hlavičky podepíše předtím, než je pošle
  + Antispam
    - Heuristika → Riziko špatného zařazení

## POP (Post Office Protocol)

* Vlastnosti
  + Protokol pro přístup uživatelů k poštovní schránce
  + Aktuální verze je 3
  + Port 110
* Nevýhody
  + Plaintextový
  + Otevřené posílání hesla
  + Maily je nutné stahovat celé
  + Nepodporuje adresáře
  + Dnes často doplněn o TLS

## IMAP (Internet Message Access Protocol)

* Vlastnosti
  + Port 143
    - Nebo 993 pro šiforování
  + Nástupce POP
* Výhody
  + Zabudovaná možnost šifrovaného spojení
  + Podpora více schránek
  + Možnost stáhnout jen část mailu
  + Možnost vyhledávat na serveru
  + Podpora paralelních příkazů

## WWW

* Vlastnosti
  + Distribuovaná hypertextová databáze
  + Základní jednotkou je hypertextová stránka
  + Jazyk HTML
  + Statické a dynamické dokumenty
* Hypertext
  + Jeho předchůdcem Gopher (distribuovaná databáze)
  + Systém souborů navzájem propojených odkazy
* HTML (Hypertext Markup Language)
  + Systém značek
  + Předchůdcem XML

## HTTP(S)

* Vlastnosti
  + Port 80
  + Formát zprávy
    - Příkaz
    - Hlavičky
    - Tělo dokumentu
* HTTP v.1
  + Jeden požadavek – jeden dokument/obrázek
  + Nezávislé požadavky
  + Po jednom spojení může postupně putovat více požadavků
* HTTP v.2
  + Binární protokol
  + Vlastní streamy nad jedním TCP spojení
  + Server může klientovi podstrčit data, která bude možná potřebovat (aniž by o ně žádal)
* Kódy odpovědí
  + 1xx – informativní odpověď
  + 2xx – kladná odpověď
  + 3xx – přesměrování
  + 4xx – chyba na straně klienta
  + 5xx – chyba na straně serveru
* Metody http
  + GET – načte dokument
  + HEAD
  + POST – předá parametry a načte dokument
  + PUT – předá dokument
  + DELETE – mazání
  + CONNCET – vytvoření spojení
* Cookies
  + Server si do nich ukládá stav komunikace (tj. data o uživateli)

## Telnet

* Vlastnosti
  + Přihlašování na vzdálené počítače
  + Port 23
  + Uživatel pracuje s NVT (Network Virtual Terminal)
  + Otevřený přenos dat

## SSH (Secure shell)

* Vlastnosti
  + Podpora terminálu, přenosu souborů
  + Ověřování serveru
  + Šifrované
  + Od v.2 podpora více paralelních kanálů
  + Zpřístupnění souborového systému
* Bezpečnost SSH
  + Klient ověřuje server pomocí klíče (potvrzuje uživatel) nebo certifikátu
  + Server ověřuje klienta pomocí hesla, OTP nebo veřejným klíčem

## VoIP (Voice over IP)

* Vlastnosti
  + Obecná technologie přenosu hlasu po IP
  + Lze realizovat různými způsoby
    - H323
    - SIP
    - Skype (používá HTTP)
* Problémy
  + Digitalizace hlasu
  + Nalezení partnera
  + Propojení s telefonní sítí

### H.323

* Vlastnosti
  + Komplexní řešení multimediální komunikace od ITU
  + Binární
  + Zahrnuje řadu dílčích protokolů
  + Složité
  + Dnes nahrazováno SIP

### SIP

* Vlastnosti
  + Náhrada H.323
  + Port 5060
  + Řeší pouze vyhledání partnera a navázání spojení
  + Neřeší přenos data
    - Obvykle doplněn protokolem RTP/RTCP

## Sdílení souborového systému

### NFS (Network File System)

* Vlastnosti
  + Pro UNIX
  + Formát odkazu: server:cesta
  + Pro autentizaci využívá Kerberos
* SMB (Server Message Block)
  + Propojení UNIX a Windows
  + Autentizace pomocí uživatelského jména a hesla
  + Formát odkazu: \\server\cesta

## NTP (Network Time Protocol)

* Vlastnosti
  + Synchronizace času mezi uzly sítě
  + Stejné timestampy souborů
  + Porovnávání času událostí na různých počítačích
  + Klient kontaktuje servery v konfiguraci
  + Problém s latencí sítě
* Stratum
  + Zdroje s přesným časem
  + Primární stroj – Stratum 0
    - Od něj potom Stratum 1, 2, 3, …
    - Se „vzdáleností“ klesá přesnost

## DHCP (Dynamic Host Configuration Protocol)

* BOOTP
  + Předchůdce
  + Sloužil pro konfiguraci bezdisketových stanic
  + Princip
    - Klient pošle (všem) svou MAC adresu síťové karty
    - Server mu pošle zpět jeho jméno a IP adresu
  + Nahrazen DHCP
* Vlastnosti DHCP
  + DUP
  + Klient port 68
  + Server port 67
  + Podporuje dynamické přidělování adres
    - Možnost časově omezit platnost adresy
  + Umožnuje kooperaci více serverů
* Průběh komunikace
  + Klient pošle boreadcastový požadavek DHCPDISCOVER
  + Server pošle několik DHCPOFFER: SRV=10.0.0.1, IP=10.1.1.1 s adresou serveru a volnými adresami
  + Klient odpovídá DHCPREQUEST: SRV=10.0.0.1, IP=10.1.1.1 s adresou, kterou vybere
    - Obvykle vybírá adresu, kterou používal v poslední době nebo podle délky pronájmu
  + Server potvrdí klientovi, že je adresa volná DHCPACK
  + V polovině uplynuté doby klient znovu posílá DHCPREQUEST
    - Pokud je adresa stále volná, začíná mu nová doba pronájmu
    - Pokud už není volná, tak v 7/8 uplynuté doby pronájmu si klient vyžádá broadcastem novou adresu

# Transportní vrstva

## TCP/IP

* TCP (Transmission Control Protocol)
  + Spojové služby
  + Klient naváže spojení a data tečou ve formě streamu
  + Relaci řídí TCP, nikoliv aplikace
  + Komplikované
  + Pomalejší, ale bezztrátové → „spolehlivý“
  + Paket

|  |  |  |
| --- | --- | --- |
| Source port | | Destination port |
| Sequence number | | |
| Acknowledgement Number | | |
| Data offset | Flags | Window |
| Checksum | | Urgentpointer |
| Options | | |
| Data | | |

* + - Příjemce potvrzuje přijetí paketu příznakem ACK (pole flags)
      * Pokud je to možné, pošle ho s jinými daty
      * Odesilatel nemusí nutně na AKC čekat, posílá více paketů a až když ACK po delší době nedorazí, situaci řeší
        + Časové okno, resp. ve velikosti odeslatelných dat → pole window
        + Situaci řeší tak, že posílá nepřijaté pakety znovu
    - Příznaky
      * SYN – inicializace „Sequence number“
      * ACK – potvrzuje přijetí paketu (krom posledního)
      * PSH – informuje příjemce, že obdržel kompletní blok a má ho předat aplikaci
      * FIN – odesílatel zavírá svou stranu spojení
      * RST – odesilatel odmítá přijmout spojení
      * URG – paket obsahuje urgentní data, jejich adresa je v „Urgent Pointer“
* UDP (User Datagram Protocol)
  + Nespojové služby
  + Neexistuje relace, data se posílají jako nezávislé zprávy
    - Relaci si může vytvářet aplikace
  + Jednoduché
  + Pravidelný tok dat, riziko ztrátovosti → „nespolehlivý“
  + Datagram

|  |  |
| --- | --- |
| Source port | Destination port |
| Legth | Checksum |
| Data | |

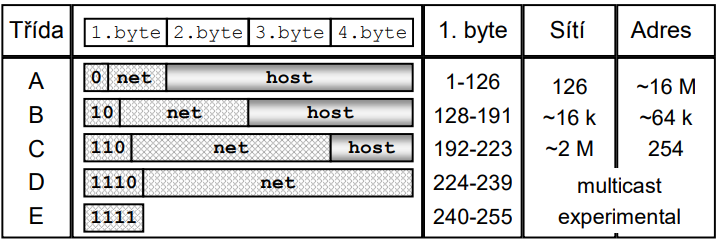
# Síťová vrstva

## IP (Internet Protocol)

* Vlastnosti
  + Používá se v TCP/IP na síťové vrstvě
  + Nespojovaná služba
  + Nespolehlivý protokol
  + Nezávislá na médiu
* Adresy
  + Obsahují část s adresou sítě a část s adresou uzlu
  + IPv4: 4 byty
  + IPv6: 16 bytů
* Přidělování adres
  + Centrální: IANA
* Struktura IPv4 datagramu

|  |  |  |  |
| --- | --- | --- | --- |
| Header length | Service Type | Packet Length | |
| Fragment Identification | | Flags | Fragment Offset |
| Time-to-live | Protocol | Header Checksum | Verze |
| Source IP Address | | | |
| Destination IP Address | | | |
| Options | | Padding | |
| Data | | | |

* Třídy IPv4 adres



* Speciální IPv4 adresy
  + Výchozí zdrojová adresa - 0.0.0.0/8
  + Loopback - 127.0.0.1/8
    - Pokud klient i server běží na stejném počítači
  + Adresa sítě - <adresa sítě>.<samé nuly>
  + Network broadcast - <adresa sítě>.<samé jedničky>
    - Všem v dané síti
  + Limited broadcast - 255.255.255.255
  + Privátní adresy 10.0.0.0/8, 172.16-31.0.0/16, 192.168.\*.0/24
    - Ve výjimečných případech mohou opustit vlastní síť
  + Link-local adresy
    - Nesmí opustit privátní síť
* Subnetting
  + Rozdělení sítě na podsítě
  + Síťová maska obsahuje 1 tam, kde je adresa podsítě v části alokované pro hosta
  + Dnes se často používá jen formát s / za IP adresou, ke se uvádí počet bitů masky
* IPv6
  + 16bytové adresy
  + Speciální IPv6 adresy
    - Loopback - ::1/128
    - Link-Scope - fe80::/10, dříve link-local
    - Unique-Local - fc00::/7, dříve privátní IPv4 adresy
    - Multicast a unicast
    - Chybějí broadcastové

## Směrování

* Princip
  + Směrování by měla umět každá stanice v TCP/IP síti
  + V každém sítovém zařízení je směrovací tabulka
    - V tabulce je uveden „gateway“ (směr), „destination“ (cíl) a „mask“ (maska)
    - Maska vyjadřuje „uvažovanou část“ adresy cíle
  + Typy záznamů
    - Přímé – přímo připojené sítě
      * Loopback
    - Nepřímé – LAN podsítě
    - Default – ISP
  + Vznik záznamu
    - Implicitní – automaticky po přiřazení adresy rozhraní
    - Explicitní – „ručně“ zadán příkazem
    - Dynamický – v průběhu práce od partnerů v síti
* Směrovací algoritmus
  + Najdi ve směrovací tabulce všechny vyhovující záznamy
    - Neexistují → „No route to host“
    - Jinak z vyhovujících záznamů vyber ten s nejširší maskou
      * Pokud je to můj PC, vrať
      * Pokud je to požadavek do mojí sítě, předej
      * Pokud je to požadavek ven, pošli na „default“ ISP
* Konfigurace sítě
  + UNIX
    - ipconfig – nastavení adresy síťového rozhraní
    - route – změna routovací tabulky
    - dhcpclient – automatická konfigurace pomocí DHCP
* Diagnostika směrování
  + route print – výpis směrovací tabulky
  + tracert – kontrola cesty
* Statické řízení směrovacích tabulek
  + Cesty se nastavují při startu podle konfigurace
  + Bezpečné, jednoduché
  + Nepružné, problémy se subnettingem
* Dynamické řízení směrovacích tabulek
  + Routery si navzájem vyměňují informace o síti pomocí routovacího protokolu
    - Stanice jej mohou číst
  + Pružné, samoopravitelnost, samoúdržba
* Distance vector protokoly
  + Uzel má u záznamů ve směrovací tabulce i „vzdálenosti“
    - Tu průběžně sdílí s ostatními
  + Výhody
    - Jednoduché
  + Nevýhody
    - Pomalá reakce na chyby
    - Metrika špatně zohledňuje vlastnosti linek
    - Chyba ve výpočtu jednoho routeru ovlivňuje celou síť
* Link state protokoly
  + Každý router zná mapu celé sítě
  + Routery si navzájem sdělují stav svých linek a podle toho si každý modifikuje svoji mapu sítě
  + Výhody
    - Adaptabilní
    - Každý počítá sám za sebe
    - Výměna dat probíhá pouze při změnách
  + Nevýhody
    - Náročné na paměť a CPU
* Autonomní systémy
  + Definice: blok sítí se společnou routovací politikou
  + Směrování v rámci WAN
* IP filtrování
  + Základem bezpečnostní politiky
  + Ve skutečnosti probíhá na transportní vrstvě
  + Typy konfigurace
    - Přísná konfigurace
      * Ven vybrané, dovnitř nic
    - Obvyklá konfigurace
      * Ven vše, dovnitř nic
  + Problém, pokud chceme vystavit část sítě ven (např. http server)
    - Obvykle řešeno vymezením DMZ (demilitarized zone)
* Proxy server
  + Kontroluje provoz určitého protokolu
  + Transparentní varianta
    - SW na routeru zachytí požadavek, uloží si ho a provede jej sám prostřednictvím proxy serveru
    - Odpověď pak přepošle původnímu žadateli
  + Netransparentní varianta
    - Klienty je třeba nakonfigurovat, aby neposílali požadavky přímo, ale na proxy server
      * Lze i po síti
  + Významný bezpečnostní a výkonnostní prvek
    - Umožňuje kontrolovat aktivitu klientů
    - Umožňuje omezit objem provozu

## ICMP (Internet Control Message Protocol)

* Vlastnosti
  + Typy zpráv
    - Echo, Echo reply – testování dosažitelnosti
      * Příkaz ping
    - Time Exceeded – vypršel TTL
    - Redirect – výzva ke změně v routovací tabulce
      * Pokud moje stanice neví o jiné sítí, router jí na ni vrátí redirect
    - Destination Unreachable – nelze doručit paket

## TTL (Time to live)

* Vlasnosti
  + Ochrana před zacyklením
  + Udává se v počtu hopů, který paket nesmí překročit
    - TTL = 0 → Time Exceeded

## RIP (Routing Information Protocol)

* Vlastnosti
  + Metrikou je počet routerů v cestě
  + Rozsah sítě je omezen na 15 hopů, 16 je „nekonečno“
  + Pro výpočet nejkratších cest používá Bellman-Fordův algoritmus
  + Aktuální verze podporuje subnetting
  + Nepoužitelný pro velké dynamické sítě

## OSPF (Open Shortest Path First)

* Vlastnosti
  + Nejrozšířenější link-state interní routovací protokol
  + Využívá Dijkstrův algoritmus k nalezení nejkratší cesty
  + Využívá hierarchický model sítě
* Metrika
  + Konfigurovatelná
  + Implicitně součet cen na cestě, kde cena je „šířka pásma“

## BGP (Border Gateway Protocol)

* Vlastnosti
  + Externí routovací protokol
  + Zajišťuje ohodnocení cesta a eliminaci smyček

## ARP (Adress Resolution Protocol)

* Vlastnosti
  + Spojovací článek mezi síťovou a linkovou vrstvou
  + Umožňuje uzlům v sítí přiřazovat MAC adresy k IP adresám
  + Neznámé adresy zjišťuje boradcastovou výzvou
    - Ukládají se na uzlu do ARP cache
    - Odpovídající si nejprve zapíše tazatele do svojí ARP tabulky
  + Výpis arp tabulky arp -a

# Linková vrstva

* Vlastnosti
  + Dělení na dvě podvrstvy
    - LLC (Logical Link Control)
      * Umožňuje různým protokolům síťové vrstvy přistupovat ke stejnému médiu
        + Tj. multiplexing
    - MAC (Media Access Control)
      * Řídí adresaci uzlů a přístup k médiu: kdo, kdy a jak může data odesílat a jak je přijímat
  + TCP/IP se touto vrstvou nezabývá
  + Síťový segment (fyzická síť)
    - Množina uzlů sdílející stejné médium
* Datová jednotka (frame)
  + Liší se podle použitého média
  + Obecně obsahuje synchronizační pole, hlavičku, datové pole a patičku

## Topologie sítí

* Způsoby řízení přístupu k médiu
  + Multipoint
    - Deterministický
      * Autorita určuje, kdo smí kdy vysílat
    - Nedeterministický
      * Každý může kdykoliv vysílat
      * Nutné řešit kolize
      * Například u Ethernetu
  + Point to point
    - Halfduplexní linka
      * „Jeden drát“ – nutné řešit kolize
    - Fulldupelxní
      * „Dva dráty“ – bez kolizí
* Řešení kolizí
  + CSMA (Carrier Sense with Multiple Access)
    - Uzel poslouchá „nosnou“, a pokud není volno, čeká
  + CSMA/CD (Collision Detection)
    - Ethernet
    - Během vysílání uzel současně detekuje případnou kolizi
    - Při kolizi stanice zastaví vysílání, upozorní ostatní, počká určitou náhodnou dobu a pokus opakuje
      * Obvykle se exponenciálně prodlužuje interval čekání
  + CSMA/CA (Collision Avoidance)
    - Když je volná nosná, vysílá se celý rámec a čeká se na ACK
    - Pokud není volná nosná nebo nedorazí ACK, zahájí se exponenciální čekání

## Ethernet

* Historie
  + Vznik ve firmě Xeron
  + Sedmdesátá léta
* Vlastnosti
  + Vůdčí technologie pro lokální sítě
    - Pružný, přizpůsobivý
  + Řízení přístupu metodou CSMA/CD
  + Adresy
    - 3 byty prefix, 3 byty adresa
* Rámce

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Destination MAC address | Source MAC address | Type | DATA | FCS |

* Virtuální sítě (VLAN)
  + Prostředek, jak po jedné fyzické síti provozovat více nezávislých lokálních sítí
  + Sítě jsou označeny 12bitovým identifikátorem (VLANID)
  + Ethernetový rámec se prodlouží o 32 bitů dlouhý tag

## CRC (Cyclic Redundancy Check)

* Vlastnosti
  + Hashovací funkce široce používaná pro kontrolu konzistence dat
  + Posloupnost bitů je považována za koeficienty polynomu
    - Ten se vydělí charakteristickým polynomem
    - Zbytek po dělení se převede na bity → hash
  + Účinný (n-bitový)
    - Detekuje 100% chyby s lichým počtem bytů a chyby kratší než n bitů

## WiFi

* Vlastnosti
  + Bezdrátová síť, jiný název: WLAN (wireless LAN)
  + Mnoho různých variant pod souhrnným označením IEEE 802.11 (802.11a, b, g, n, y,...)
  + Psáma 2,4GHz a 5 GHz
  + Struktura
    - Ad-hoc peer-to-peer
    - Infrastruktura přístupových bodů
  + SSID – identifikátor sítě
  + Problém – zabezpečnení

# Fyzická vrstva

* Vlastnosti
  + Přenos dat pro konkrétním fyzickém médiu
* Typy přenosu
  + Analogový přenos
    - Každé možné hodnotě přiřazujeme jinou
  + Digitální přenos
    - Příchozí hodnoty ohodnocujeme na základě intervalu, do kterého spadají
* Baseband vs. broadband
  + Baseband přenáší přímo signál a kóduje ho
  + Broadband přenáší základní signál a moduluje ho (fázi, amplitudu, frekvenci)

## UTP (Nestíněná kroucená dvoulinka)

* Vlastnosti
  + 4 páry Cu vodičů navzájem pravidelně zakroucené
    - Zakroucení snižuje vyzařování i příjem elektromagnetického záření
    - 100Mb Ethernet používá jen dva páry
  + Konektor RJ 45

## Optická vlákna

* Vlastnosti
  + Signál se šíří jako viditelné světlo vláknem z SiO2
  + Vysoké frekvence, velká šířka přenosového pásma
  + Minimální rušení
  + Drahé, náročná manipulace
* Typy vláken
  + Jednovidová (singlemode)
    - Svítí se laserem → jeden paprsek, větší dosah, šířka pásma
  + Vícevidová (multimode)
    - Svítí se LED

## Segmentace sítě

* Repeater (hub, rozbočovač)
  + Spojuje segmenty na fyzické vrstvě
  + Řeší větší dosah, neřeší propustnost
* Bridge (switch)
  + Řeší propustnost
* Spanning Tree Algoritmus
  + Problémy u sítí, jejíchž graf je cyklický
  + Nutné najít kostru sítě