MPKS

① Komunikační sítě, topologie, modely (ISO/OSI, TCP/IP), funkce vrstev.

- **komunikace**
  - spojovaná (~telefon, stavová), nespojovaná (datagramy, bez spojení)
  - spolehlivá, nespolehlivá - poslaná data opatřována/zahazována
  - přepojování okruhů (TDM, kvalita), paketů (statistický MX, proměnné zpoždění)
- **topologie**
  - všesměrové šíření: sběrnice (multipoint), rádiový spoj
  - spoje bod-bod: hvězda, kruh, strom, obecná topologie

ISO/OSI	TCP/IP	funkce
aplikační	aplikační	aplikace
prezentační		kódování, lokalizace
relační		šifrování
transportní	transportní	spolehlivý, spojovaný přenos (TCP/UDP)
síťová	síťová	přenos paketů přes směrovače
linková	síťového rozhraní	přenos rámců, synchronizace, přístup k médiu
fyzická		kódování, modulace, média, kanálový

MPKS

② Aplikace HTTP, FTP, SMTP, DNS

- **HTTP**
  - neperzistivní HTTP/1.0 (2RTT/objekt, režie OS na každé spojení)
  - perzistivní HTTP/1.1 (bez/s překrýváním - pipelining - zda čeká na odpovědi)
  - fce GET, POST, HEAD; kódy odpovědí
  - stavová komunikace - cookies
- **FTP**
  - režim aktivní (spojení otevírá server), pasivní (klient)
- **SMTP**
  - přenos, typ. 7bit, kódování Quoted-printable, Base64 (@ MIME)
  - protokoly POP3, IMAP
- **DNS**
  - distribuovaná databáze, jméno ⇔ adresa
  - TLD servery, root servery, autoritativní DNS servery pro každou doménu
  - rekurzivní dotaz (NS odpoví výsledek), iterační dotaz (NS odpoví jiný NS)
  - reverzní záznamy

MPKS

③ Protokolová rodina TCP/IP: TCP (navazování spojení, řízení toku), UDP, IP (směrování, fragmentace, adresy, NAT/PAT)

- UDP: pakety se mohou ztratit, přijít mimo pořadí; bez spojení, nestavové, malé hlavičky, broadcast, nespolehlivé
- principy spolehlivého přenosu: Stop-and-Wait, plovoucí okno
- TCP (v hlavičce čísla SEQ, ACK, příznaky ACK, RST, SYN, FIN)
  - navázání: SYN → SYN+ACK → ACK, ukončení: FIN → FIN+ACK → ACK
  - řízení toku pomocí RcvWindow, CongWin; mechanismy: AIMD (+1, /2), „pomalý" start, zotavení po ztrátě a timeoutu; rychlost ~ CongWin / RTT
- IP
  - směrování: určení cesty paketu, předání
  - fragmentace: malé MTU ⇒ rozdělení; spojeno až u příjemce
  - adresace (v4): 32 bitů + síť, dříve třídy A,B,C,D, nyní CIDR (zvl. maska sítě) ⇒ agregace adres (zmenšení směrovacích tabulek)
  - NAT/PAT – překlad na interní adresy, na síťové vrstvě
  - směrovací algoritmy: Link-State (OSPF), Distance Vector (RIP), hierarchické (BGP)

MPKS

④ Přenosová média: kabeláž pro LAN, optická vlákna – základní vlastnosti

- kapacita kanálu bez šumu (Nyquist) $C = 2B\log_2 M$, se šumem (Shannon) $C = B\log_2(1+S/N)$
- kabel TP: přeslechy, terminální šum, více párů, (stínění), levný
  - provedení UTP, FTP, S-STP; drát/lanko
  - kategorie 3, 5, 5e  , 6e  , 7f 
- optická vlákna: bez přeslechů, min. šum, ≈100 km bez opakovače
  - mnohovidová: LAN, 50 μm, 1 dB/km, omezení disperzí na $B \cdot L \approx 1$ GHz·km
  - jednovidová: MAN/WAN, 9 μm, 0,25 dB/km, $B \cdot L \approx 100$ GHz·km, (D)WDM

MPKS

⑤ Lokální počítačové sítě, přístupové metody (Aloha, CSMA, CSMA/CD, CSMA/CA)

- LAN: vysoké rychlosti, náhodný provoz, malá rozlehlost
- varianty přístupu: řízené (Token Ring), neřízené (Ethernet); centralizované/distribuované
- Aloha: náhodný přístup s potvrzováním; slotted Aloha – synchronizace na rámec
- CSMA: nepersistivní (při det. vysílání se odmlčí na náhodnou dobu), persistivní (čeká na konec vysílání) – Ethernet
- CSMA/CD: analogová detekce kolize ⇒ vysílám jam signálu + pauza
- CSMA/CA: u bezdrátů, může implementovat RTS/CTS
- kolizní doména – část sítě, kde může vzniknout kolize; délka segmentu omezena požadavkem max. doby zjištění informace o kolizi.

MPKS

⑥ Ethernet: princip, varianty – 100M, 1G, 10G, aktivní prvky, VLAN, PoE, topologie, protokol Spanning Tree, strukturovaná kabeláž

- dříve CSMA/CD, dnes PtP; MAC adresa 6B (3B výrobce, 3B ID)
- rámec 46 až 1500B dat + 26B hlavičel a CRC
- 100BASE-TX, -FX: UTP cat. 5/optika, 100m, 100Mbit/s; pár pro každý směr, modulace PAM5x5, kódování 4B5B a MLT-3
- 1000BASE-SX, -LX (optika 8B10B), -T (4 páry cat 5e, 5PAM)
- 10GBASE: plně duplexní, jen PtP; -S, -L, -E (laser); -T (cat 7 ⇒ 100m)
- aktivní prvky
  - hub (fyzická vrstva, spojení segmentů, kolizní doména)
  - switch (transparentní bez adresy)
  - router (síťová vrstva, viditelný)
- VLAN: log. rozdělení přepínače (dle portů, MAC, dynamicky), tagování v hlavičce
- PoE: 48V/15W, varianta A (střídy trafo), B (nevyužité páry kabelu)
- Spanning Tree – zabraňuje vzniku smyček, přepínače si posílají po několika sekundách informace; nadbytečné porty vypnuté
- strukturovaná kabeláž (topologie, vzdálenosti, kabely, konektory) – horizontální, vertikální
- topologie: typicky síť homogenní, centrálním prvkem směrovač

MPKS

⑦ Multimediální aplikace: základní požadavky, protokoly RTP a SIP, služby VoIP, metody zajištění kvality služby v sítích IP

- citlivé na zpoždění a jitter, tolerují ztrátu (opak datových přenosů)
- RTP - nadstavba UDP (+sekvenční číslo, čas), nemá QoS, řídicí protokol RTCP (pravidelné reporty)
- SIP - formát podobný HTTP, data po RTP, dyn. vazba IP adresa ⇔ tel. číslo
- VoIP: telekomunikační H.323, internetový SIP, proprietární Skype
- zajištění QoS:
  - předimenzování sítě (LAN)
  - FIFO, zahazování při plné frontě
  - Leaky Bucket - limituje velikost dávky a průměrnou rychlost
  - IntServ - rezervace zdrojů, protokol RSVP, výkonově náročné
  - DiffServ - klasifikace paketu na vstupu sítě, uvnitř dle přidělené priority

MPKS

⑧ Bezpečnost síťového provozu: základy kryptografie (symetrická, s veřejným klíčem, blokové a proudové šifry), autentizace, integrita - MD5, SHA, certifikáty, protokoly SSL, IPSec.

- šifrování
  - symetrické blokové: DES (64b bloky, trojitá 3-DES, řetězení; novější AES)
  - proudové symetrické - PN posloupnosti: RC4 (WEP, SSL)
  - nesymetrické - s veřejným klíčem: RSA (veřejný klíč - šifrování $c = m^e \bmod n$, soukromý klíč - dešifrování $m = c^d \bmod n$)
- autentizace - prokázání identity protistrany: symetrická kryptografie, kryptografie s veřejným klíčem
- hašovací funkce MD5 (128b kontrolní součet, možnosti kolizí), SHA-1 (slabý), SHA-2
- distribuce klíčů: symetrická (přes prostředníka KDC), s veřejným klíčem (podpis certifikační autority CA)
- SSL: vrstva pro TCP, autentizace serveru + šifrování; certifikátem serveru (veřejným klíčem) šifrován hlavní klíč, server ho dešifruje a použije ke komunikaci
- IPSec: pro TCP i UDP, dva protokoly AH (autentizace, integrita), ESP (navíc šifrování - zapouzdření utajeného paketu)

MPKS

⑨ Management: protokol SNMP, databáze MIB.

- Zařízení obsahují spravované objekty, struktura uložena v MIB – Management Information Base
- modul → objekt → datový typ
- pojmenování objektů – hierarchické, OID (Object ID)
- komunikace UDP, request/response mód, trap mód; manažer↔agent
- SNMPv1, v2: otevřený přenos, bez zabezpečení
- SNMPv3: šifrování, autentizace

MPKS

⑩ Vysokorychlostní sítě, technika MPLS, MPλS, fotonické sítě

- sítě ATM (Asynchronous Transfer Mode)
  - přepojování paketů
  - rámec 53B = 5B hlavička + 48B data
  - třídy Constant/Variable/Available/Unspecified Bit Rate
- technologie xDSL (Digital Subscriber Line)
- MPLS (Multiprotocol Label Switching)
  - detekce proudu paketů, přenášení stejnou cestou ⇒ spojovaná komunikace
  - Edge Router detekuje proud, značí pakety nálepkou
  - pakety přepínány stabilní cestou podle nálepek – rychlejší
- MPλS (Lambda Switching)
  - integrace MPLS pro DWDM
  - nálepka = vlnová délka, čisté pro optické sítě
- optická pojítka – do 1Gb/s, do 2km; FSO – transparentní kanál – opalovač na fyzické vrstvě