**Zkouškové otázky**

1. Klasifikace (LAN/MAN/WAN) a služby sítí
2. Referenční model ISO OSI a architektura TCP/IP
3. Strukturovaná kabeláž a opakovač
4. Ethernet (přepínaný)
5. Wi-Fi a Bluetooth
6. Modem, sítě xDSL a GSM, protokol PPP
7. Protokol IP(v4): paket, adresa a síťová maska, lokální síť
8. Protokol IP(v4): směrování
9. Protokol IP(v4): IP fragmentace, protokoly ICMP a (R)ARP
10. Protokol IP: IPv4 multicast, IPv6
11. Transportní protokoly: transportní služby a protokol UDP,port,segment/datagram
12. Protokol TCP: navázání a ukončení TCP spojení
13. Protokol TCP: řízení toku dat, zpoždění odpovědi a posuvné okno,řešení zahlcení sítě
14. Systém DNS: jmenné služby, architektura, domény a zóny
15. Systém DNS: řešitel a jmenný server, překlad jména
16. Systém DNS: protokol (operace Query), záznamy/věty
17. Systém DNS: DNSSec, diagnostika, delegace a registrace domén,Internet Registry
18. Protokol DHCP a směrovací protokoly
19. Elektronická pošta (architektura, zpráva, protokoly)
20. Protokoly HTTP a FTP
21. Bezpečnost sítí (napříč vrstvami, útoky, firewall, NA(P)T, IPSec,VPN, SSL/TLS, proxy)

**1. Klasifikace (LAN/MAN/WAN) a služby sítí**

* Klasifikace podle rozlehlosti sítí
  + LAN (Local Area Network)
    - Omezeny rozsahem (jednotky km, nejčastěji v budově, nebo komplexu budov)
    - Často virtuální
    - od 10Mb/s do 1Gb/s
  + MAN (Metropolitan Area Network)
    - Propojení a prodloužení několika LAN
    - V rámci měst(a)
  + WAN (Wide Area Network)
    - Páteřní sítě, telekomunikační sítě
    - Neomezeně rozsáhlé
  + PAN (Personal Area Network)
    - Omezeny dosahem v okolí zařízení (desítky m)
    - např Bluetooth
* Služby sítí
  + Připojení k síti
  + Vzdálený přístup
  + Přenos technických prostředků (tiskárny, disky)
  + Adresářové služby
  + Elektronická pošta
  + Informační služby (www)

**2. Referenční model ISO OSI a architektura TCP/IP**

* Referenční model ISO OSI
  + Snaha o standardizaci sítí.
  + Normy pro propojení dvou zařízení
  + Nepopisuje implementaci, ale uvádí všeobecné principy sedmivrstvé síťové architektury
    - Fyzická vrstva - Přenos signálu (bitů) bez ohledu na význam bitů
    - Linková vrstva - Zajištění výměny dat mezi sousedními zařízeními v dosahu protokolu. Bity mají význam (data).
    - Síťová vrstva - Přenos mezi vzdálenými, nesousedními zařízeními. Jednotka přenosu - paket.
    - Transportní vrstva - Přenos dat mezi aplikacemi v rámci jednoho počítače. Jednotka přenosu - transportní paket (datagram). Protokoly TCP a UDP.
    - Relační vrstva - Zabezpečená organizace výměny dat mezi aplikacemi
    - Prezentační vrstva - Jednotná reprezentace (a zabezpeční) informací, v jaké se přenáší sítí a jsou dostupné aplikacím
    - Aplikační vrstva - Předepisuje aplikační formát dat
* Architektura TCP/IP
  + Použití v síti Internet (dříve ARPANET)
  + Popsána v RFC (Request For Comments) - doporučení, protokoly, konvence
  + Vyvinuta k propojení vojenských pracovišť.
  + Nedodržuje přesný ISO OSI vrstvový model - sloučení několika vrstev

**3. Strukturovaná kabeláž a opakovač**

* Propojovací kabely
  + Koaxiální kabel
  + Kroucená dvojlinka (max 100m)
    - UTP - nestíněná
    - STP - stíněná
  + Optická vlákna (dosah v řádu kilometrů nebo až desítek kilometrů)
    - Dvě vrstvy - obal a jádro
    - Princip - Jádrem se šíří světlo, které se na rozhraní jádra a obalu odráží
* Opakovač
  + Propojení několika segmentů (rozbočovač) - HUB
  + Zopakování zeslabeného vstupního signálu

**4. Ethernet (přepínaný)**

* Síť využívající switch pro propojení prvků sítě
* Switch
  + K přepínání využívá přepínací matici (tabulka fyzických portů a MAC adres)
  + Dokáže propojit sítě s ruznými rychlostmi (vyrovnávací paměť)
  + Metody přepínání
    - Store-and-Forward - Každý rámec načte do vnitřní paměti (kontroluje jeho chybovost) a podle cílové adresy přepošle na odpovídající port
    - Cut-Through - Do vnitřní paměti načítá pouze hlavičku rámce a podle cílové adresy přepošle na odpovídající port
* Sdílené přenosové médium, v daném okamžiku ho využívá jeden uzel
* Uzly samostatné, rovnocenné
* Fast Ethernet -> Gigabitový Ethernet -> 10Gigabitový Ethernet

**5. Wi-Fi a Bluetooth**

* Důvody: Mobilita, snadná použitelnost, dostupnost, ...
* Přenos dat pomocí rádiových vln
* Wi-Fi
  + Topologie
    - ad-hoc - přímá komunikace mezi stanicemi (do deseti stanic)
    - s přístupovým bodem (AP) - stanice komunikují prostřednictvím AP
    - s více přístupovými body (roaming) - AP propojeny pevnou sítí, klient se přepojuje k AP s nejlepším signálem
* Bluetooth
  + Odlišná protokolová architektura
  + Master a Slave uzly

**6. Modem, sítě xDSL a GSM, protokol PPP**

* Modem
  + Pro připojení k datové síti pomocí telefonní sítě (modulace, demodulace dat a zvuku)
* xDSL
  + Skupina technologií (např. ADSL, HDSL, SDSL) souhrnně označující se jako xDSL
  + Dosažení maximální rychlosti na telefonní lince
* GSM
  + Bezdrátová síť pro přenos hlasu (telekomunikace)
  + Území rozdělené do buněk, které obsluhuje jedna BTS (Base Transceiver Station)
  + Telefony komunikují s BTS
* PPP (Point to Point Protocol)
  + Komunikační protokol linkové vrstvy
  + Přímé spojení mezi dvěma síťovými uzly (nejčastěji na telefonní lince)

**7. Protokol IP(v4): paket, adresa a síťová maska, lokální síť**

* Paket
  + Základní jednotka přenášených dat
  + Skládá se z hlavičky, která obsahuje informace nutné pro jeho doručení a samotných dat
* Adresa a síťová maska
  + Každé rozhraní má jednu jednoznačnou adresu
  + 4B oddělené tečkami
  + Dvě části adresy - adresa sítě a adresa uzlu
  + Počet možných zařízení na síti: 2^(počet nul masky)
  + Třídy
    - A - Rozmezí: 0-126, Maska: 255.0.0.0
    - B - Rozmezí: 128-191, Maska: 255.255.0.0
    - C - Rozmezí: 192-223, Maska: 255.255.255.0 (/24)
    - D - Rozmezí: 224-239, Multicast
    - E - Rozmezí: 240-255, Původně pro experimentální účely
* Lokální síť (Intranet)
  + Intranet = lokální síť (pro informační systém), obvykle uzavřená, nebo s omezením provozu z vnější sítě dovnitř (případně ven).
  + Dynamické přidělování adres (DHCP)
  + NAT + vyhrazený rozsah adres - 10.0.0.0/8 (A), 172.16.0.0/12 (B), 192.168.0.0/16

**8. Protokol IP(v4): směrování**

* Směrování (routing) = odesílání paketů na další směrovač nebo cílový uzel
* Předávání (forwarding) = předávání paketů mezi rozhraními konkrétního směrovače
* Směrovací tabulka
* Router
  + Propojuje několik sítí
  + Řeší směrování k dalšímu routeru, nebo koncovému uzlu (next hop)
  + Předává pakety mezi síťovými rozhraními

**9. Protokol IP(v4): IP fragmentace, protokoly ICMP a (R)ARP**

* Fragmentace
  + Linkové rámce mají omezenou velikost (MTU - Maximum Transfer Unit), ale IP paket může být větší => fragmentace
  + Pokud je fragmentování zakázáno a paket překročí velikost MTU, nejspíš bude zahozen
  + Fragmet = Packet obsahující stejnou hlavičku jako původní + offset (kolik dat bylo v předchozím fragmentu) a indikaci dalšího fragmentu
  + Skládání fragmentů se provádí pouze u příjemce paketu
* ICMP (Internet Control Message Protocol) - Služební protokol pro diagnostiku a signalizaci mimořádných (chybových) stavů
* (R)ARP
  + Zjištění linkové adresy příjemce z jeho IP adresy (RARP - naopak)
  + Uzel vyšle ARP paket žádosti na všesměrovou linkovou adresu. Příjemce odpoví ARP paketem přímo odesílateli.
  + ARP cache = tabulka: | síťová adresa | linková adresa |

**10. Protokol IP: IPv4 multicast, IPv6**

* IGMP - Služební protokol k šíření IP paketů na skupinové adresy (IP multicast) s více příjemci
* IP multicast mimo lokální síť - Využití převážně pří streamování multimediálního obsahu
* IPv6
  + řešení problémů adresace, dynamické konfigurace, podpory bezpečnosti, ...
  + Adresa - 16B

**11. Transportní protokoly: transportní služby a protokol UDP,port,segment/datagram**

* Transportní služby
  + Spojová
    - Ztracená nebo poškozená data jsou znovu vyžádána - spolehlivá služba
    - Integrita dat zabezpečena kontrolním součtem
    - Zpracovává souvyslý proud uspořádaných dat od vyšší vrstvy
  + Nespojová
    - Nezaručuje doručení ani znovuzaslání ztracených nebo poškozených dat - nespolehlivá služba
    - Integrita dat zabezpečena kontrolním součtem
    - Zpracovává nesouvislé části dat od vyšší vrstvy
* Protokol UDP
  + Poskytuje nespolehlivou, nespojovou službu
  + Vyšší výkon než TCP
  + Snaha vyhnout se fragmentaci datagramů
  + Oproti TCP může být příjemcem i všesměrová IP adresa

**12. Protokol TCP: navázání a ukončení TCP spojení**

* model klient/server (TCP umožňuje i navázání spojení v obou směrech současně, ale nevyužívá se)
* Navázání spojení
  + Obě strany otevřou port. Klient v aktivní režimu, server v pasivním režimu
  + Klient odešle segment s příznakem SYN a navrhne délku přijímaných segmentů (MSS | MSS <= MTU)
  + Server odešle segment s příznaky SYN a ACK
  + Klient odešle segment s příznakem ACK
  + Nyní lze posílat data oběma směry
* Ukončení spojení
  + Strana A odešle segment s příznakem FIN (vedle ACK) - aktivní uzavření spojení
  + Strana B odešle potvrzovací segment s příznakem ACK - pasivní uzavření spojení
  + Strana B odešle segment s příznakem FIN - úplné uzavření spojení
  + Strana A odešle potvrzovací segment s příznakem ACK

**13. Protokol TCP: řízení toku dat, zpoždění odpovědi a posuvné okno,řešení zahlcení sítě**

* Řízení toku dat
  + Odesílatel
    - Má definovaný interval pro příjem potvrzovacího segmentu
    - Při ztrátě nebo poškození segmentu po vypršení intervalu, nebo příjmu tří opakovaných stejných potvrzení opakuje odeslání segmentu
    - Hodnota intervalu se dynamicky mění podle stavu sítě na základě předpokládané doby odezvy
  + Příjemce
    - Má definovaný interval pro příjem následujícího segmentu s dalšími daty v toku
    - Při neobdržení následujícího segmentu po vypršení intervalu, opakuje přijetí předchozích dat
    - Po obdržení chybějícího segmentu potvrdí příjem všech dat
* Zpoždění odpovědi
  + Výhodné u interaktivních aplikací (telnet, FTP, SSH), vyměňujících malé segmenty
  + Potvrzovaní příjmu dat ne hned, ale se zpožděním, během kterého se mohou nahromadit data k odeslání
* Posuvné okno
  + Využití při odesílání většího množství dat - zamezení zahlcení příjemce
  + Segmenty se odesílají bez potvrzování každého zvlášť až do počtu počtu odeslaných bytů rovných délce posuvného okna
  + Velikost okna navrhne příjemce při navazování spojení a je možné ji v průběhu komunikace měnit
* Řešení zahlcení sítě
  + Pokud je síť na straně příjemce pomalá, může dojít k jejímu zahlcení -> okno i na straně odesílatele
  + Okno zahlcení (CWND) - množství nepotvrzených dat jaké je možno odeslat aniž by došlo k zahlcení sítě
  + Odesílatel odesílá data do velikosti menšího z posuvného okna a okna zahlcení
  + Dvě fáze určování velikosti okna zahlacení
    - Pomalý start - Od navázání spojení se každým potvrzeným segmentem zdvojnásobuje až do a) ztráty segmentu b) velikosti posuvného okna c) hranice pravděpodobnosti zahlcení
    - Vyhýbání se zahlcení - selektivní potvrzování

**14. Systém DNS: jmenné služby, architektura, domény a zóny**

* Jmenné služby
  + Aplikace používají pro identifikaci uzlů IP adresy - pro člověka těžko zapamatovatelné
  + Uživatel pracuje s pojmenovanými uzly, jména se přeloží na IP adresu a služba pracuje s ní
* DNS
  + Systém překladu doménových jmen na IP adresy a naopak
  + Decentralizovaná distribuovaná databáze záznamů doménových jmen a IP adres
  + Decentralizovaná distribuovaná aplikační služba modelu klient/server
* Domény
  + Pojmenované, stromově hierarchické skupiny logicky sdružených uzlů v síti
  + Top-level domény - generické (com, info, net, org), sponzorované (gov, xxx), národní (cz, sk, eu),
  + Doménové jméno - tečková notace, zleva jméno uzlu postupně následované nadřazenými doménami, oddělenými tečkou
  + Rezervované domény - example, invalid, localhost, test
* Zóny
  + Část domény spravovaná jmenným serverem

**15. Systém DNS: řešitel a jmenný server, překlad jména**

* Řešitel (resolver)
  + Vyžaduje od serveru konečnou odpověď (výsledek překladu, nebo chybu - neexistující záznam)
  + Komponenta OS
  + Konfigurace IP adresy jmenných serverů
  + Kromě DNS překladu lze využít lokální soubor s ručně zadanými asociacemi jmen a IP adres
* Jmenný server
  + Spravuje záznamy pro svou zónu
  + Obsahuje seznam IP adres serverů spravujících kořenovou zónu
  + Program poskytující klientům odpověď na dotaz
  + Typy
    - Primární - Hlavní autoritativní server pro doménu/zónu
    - Sekundární - Vedlejší autoritativní server pro doménu/zónu. Pravidelně kopíruje záznamy z primárního serveru
    - Caching only - Poskytuje pouze neautoritativní odpovědi
    - Kořenový - Primární server pro kořenovou doménu/zónu. Je jich víc
    - Forwarder - Server provádějící překlad pro jiný server (v roli klienta)
  + Pro každou doménu vždy minimálně dva jmenné servery
* Překlad jména
  + Požaduje resolver nebo jmenný server (v roli klienta), poskytuje jmenný server
  + Vyřešení dotazu
    - Aplikace žádá resolver o překlad
    - Resolver prohledá cache
    - Resolver vznese dotaz na jmenný server pro místní doménu
    - Server prohledá cache
    - Server vznese dotaz na jiný jmenný server (DNS databáze je distribuovaná)

**16. Systém DNS: protokol (operace Query), záznamy/věty**

* Protokol
  + Pracuje způsobem dotaz-odpověď, služba typu klient/server
  + Základní operace - DNS Query - překlad doménového jména na IP
  + Využívá oba transportní protokoly TCP i UDP na portu 53
  + Není zcela spolehlivý - Časový interval pro odpověď, protokol UDP
* DNS Query
  + Základní operace protokolu DNS.
  + Stejný formát paketu pro dotaz i pro odpověď
  + Komprese paketu
* Záznamy/RR věty
  + Zdrojové věty - Forma dat záznamů v DNS paketech operací, forma uložení záznamů o doménových jménech, IP adresách a všech ostatních informací v textové podobě

**17. Systém DNS: DNSSec, diagnostika, delegace a registrace domén,Internet Registry**

* DNSSec
  + Zabezpečení záznamů na jmenných serverech a v DNS paketech
  + Použití elektronického podpisu
  + Nevýhody - Soukromý klíč je potřeba pro podpis každého DNS paketu se záznamy
* Diagnostika
  + Postup
    - Ověření fungování sítě - např. pomocí ping
    - Ověření konfigurace resolveru
    - Testování místních jmenných serverů - dotazy jako resolver i jako server v roli klienta
    - Kontrola a ladění konfigurace serveru
  + Nástroje: nslookup, dig, dnswalk
* Delegace a registrace domén
  + Delegace
    - Vytvoření primárního a sekundárního jmenného serveru pro doménu
    - Delegace domény v nadřazené doméně
  + Registrace
    - Registrace domény - Prostřednictvím registrátora (CZ.NIC)
    - Registrace reverzní domény
* Internet Registry
  + Organizace přidělující v internetu IP adresy, čísla autonomních systémů, jména domén, ...
  + IANA - Nejvyšší, rozděluje mezi regionální IR
  + Regionální - Spravují větší geografické oblasti rozdělené mezi lokální IR
  + Lokální - Národní IR a poskytovatelé připojení k internetu

**18. Protokol DHCP a směrovací protokoly**

* DHCP
  + Přidělení IP adresy v síti (+ IP adresy jmenných serverů)
  + Architektura klient/server
  + Port: 67, 68 TCP
* Směrovací protkoly
  + RIP - Protokol umožňující routerům komunikovat mezi sebou a reagovat na změny topologie počítačové sítě.
  + OSPF - Provádí změny v routovacích tabulkách na základě změny stavu v síti
  + BGP - Používá se pro směrování mezi autonomními systémy (množina sítí pod společnou správou)

**19. Elektronická pošta (architektura, zpráva, protokoly)**

* Mnoho aplikačních protokolů
* Architektura klient/server
* Čtení pošty
  + POP3 (110 TCP) - Pouze stahuje poštu ke klientovi.
  + IMAP4 (143 TCP) - Stahuje poštu ke klientovi a změny odesílá zpět na server
* Odesílání pošty
  + SMTP (25 TCP)
  + ESMTP
* Konference a diskusní skupiny - Protokol NNTP

**20. Protokoly HTTP a FTP**

* Architektura klient/server
* HTTP
  + Přenos hypertextových dokumentů
  + Port 80 TCP
  + URL
  + Metody dotazu GET a POST
  + Relace (session) a cookies
* FTP
  + Přenos dat mezi počítači
  + Port: 20, 21 TCP
  + Příkazový (21) a datový kanál (20)
  + Nezabezpečený (hesla v plaintextu)

**21. Bezpečnost sítí (napříč vrstvami, útoky, firewall, NA(P)T, IPSec,VPN, SSL/TLS, proxy)**

* Bezpečnost sítí
  + Není absolutně žádná ;-)
* Útoky
  + Man-in-the-Middle útok - Útočník se stane prostředníkem mezi dvěma klienty. Může komunikaci odposlouchávat, nebo ji zamezit.
  + DoS útok - Zahlcení serveru falešnými daty, aby se k němu nedostali ty skutečné
  + SYN flood útok - Útočník otevírá nová a nová spojení (které neukončuje), dokud oběti nedojdou systémové prostředky
  + Smurf útok - Útočník pošle na broadcast velké množství ICMP paketů z podvržené IP adresy (oběti). Zařízení na síti poté zahltí oběť odpovědmi.
  + Přesměrování portů - Ve chvíli, kdy je útočník MITM, může přesměrovávat porty na kterých klient se serverem komunikuje (např. HTTPS -> HTTP).
* Firewall
  + Oddělení vnitřní sítě (intranet) od vnější (internet)
  + Filtrace provozu
* NAT (Network Address Translation)
  + Překlad IP adres paketů z vnitřní sítě na IP adresy vnější sítě a naopak
  + Skrytí vnitřní sítě za jednu vnější IP adresu
* IPSec
  + Bezpečnostní rozšíření protokolu IP již na síťové vrstvě
  + Autentizace + šifrování každého paketu
* VPN (Virtual Private Network)
  + Privátní sítě v transportní síti (Internetu), často jako pro propojení privátních sítí
  + Tunelování - zabezpečené šifrováním
* SSL - Zabezpečení aplikačních protokolů (HTTP, FTP, IMAP)
* Proxy
  + Prostředník mezi klientem a serverem
  + Pokládá klientovi požadavky serveru a přitom sám vystupuje jako klient -> anonymizace skutečného klienta