Počítačové sítě a decentralizované systémy

seznam možných otázek ke zkoušce

Poslední aktualizace: 10. května 2024

Průběh zkoušky:

Zkouška je písemná, obvykle cca 4–5 otázek vybraných z níže uvedených. Součástí zkoušky je i diskuse nad tématy, z nichž byly otázky vybrány, také s ohledem na státnice.

1) Základní pojmy a nástroje:

1. Vyberte si dvě z následujících standardizačních institucí a stručně je charakterizujte: ETSI, ITU, ISO, IEEE, IETF, IEC, IAB, IANA, ANSI, EIA, TIA (čím se zabývá, příp. struktura, nejznámější „počin“ apod.).
2. ISO/OSI: vysvětlete pojmy PDU, SDU, entita v modelu ISO/OSI, SAP, IDU, ICI, primitiva SAPu, socket.

   Vysvětlete pojmy protokolová sada a protokolový zásobník. Jmenujte několik různých protokolových zásobníků běžně používaných v počítačových sítích.
3. Jaký je rozdíl mezi kódováním Manchester, 4B/5B a MLT-3? Jak funguje přenos typu baseband a broadband? Jak (obecně) funguje modulace a multiplexování? Jaký je rozdíl mezi frekvenčním, vlnovým, časovým, statistickým a kódovým multiplexem? K čemu slouží QAM a OFDM?

2) Ethernet:

1. Přístupová metoda CSMA/CD, Backoff algoritmus (obecně). Za jakých okolností se (ne)používá? Které protokoly se u Ethernetu používají na vrstvách L1 a L2 (jejích podvrstvách) a jaký vliv mají na formát rámců? Které typy rámců se tedy používají a k jakým účelům, pro jaký typ obsahu?
2. Vysvětlete zkratky 1000Base-T, 1000Base-SX/LX/CX, 10GBase-SR/LR/LRM,ER, 10GBase-T, 10Gase-W, 2.5GBase-T. Co je to MAU (transceiver)? Vyberte si jednu podvrstu vrstvy L1 závislou na médiu a jednu nezávislou na médiu a stručně charakterizujte.
3. Jak se řeší situace, kdy je třeba poslat velmi malý ethernetový rámec, menší než je spodní limit? Co je to burst mode? Jak se v plném duplexu zajišťuje, aby switch stíhal přijímat a zpracovávat příchozí data, resp. jak se řeší situace, kdy switch nestíhá přijímat?
4. Jak v Ethernetu probíhá autonegociace? Jaký je rozdíl mezi pulsy NLP a FLP?

   Jak funguje PoE? Proč jsou různé výkonové třídy (a jaké existují)?

   Co je to EFM?

   Co to jsou horizontální rozvody? Jak dlouhé mohou být přenosové cesty na různých úsecích horizontální kabeláže?

3) Další témata k lokálním sítím:

1. Jaký je rozdíl mezi deterministickou a nedeterministickou přístupovou metodou v síti? Jmenujte některou deterministickou a některou nedeterministickou a obě stručně charakterizujte.

2. Co je to VLAN? Jaký je rozdíl v členství ve skupině podle portů, podle MAC adres, na vrstvě L3, podle multicast adresy, podle politiky, VLAN s autentizací?

   K čemu slouží VLAN typu default, datová, native, management? Co je to trunk? Jaká je role protokolu IEEE 802.1Q?

3. K čemu slouží protokol STP? Co je to BPDU? Podle čeho se určuje root bridge (root switch)? Co se děje během procesu konvergence?

   Čím jsou charakteristické stavy portů forwarding, blocking, listening, learning a disabled? Co znamenají role portů root port, designated port, blocked (backup, alternate) port?

   Čím se vyznačují varianty RSTP a MSTP?

4. K čemu slouží technologie EtherChannel? Jaké vlastnosti musí mít spoje zařazené do EtherChannelu? Kolik jich maximálně může být a jak se mezi nimi dělí provoz?

   Jaký je rozdíl mezi protokoly LACP a PAgP a k čemu se v EtherChannelu využívají? Do kterých tří stavů může být nastaveno zařízení propojené v EtherChannelu vzhledem k těmto protokolům?

5. K čemu slouží SAN sítě? Vysvětlete pojem Fibre Channel. K čemu se používá, jaké jsou vlastnosti, výhody, nevýhody? Jaká kabeláž se zde používá? Jakou roli plní protokol FCP a co je to HBA? Co se konkrétně pomocí FC přenáší?

   Jaký je rozdíl mezi FC topologiemi point-to-point, switched fabric a FCoE?

   Co je to iSCSI a v čem se liší od FCoE?

4) Rozlehlé sítě a telekomunikace:

1. WAN sítě: jaká je role zařízení typu DCE a DTE? Jaká je role primárního uzlu a sekundárních uzlů v síti? Vysvětlete rozdíl mezi režimy komunikace NRM, ARM a ABM.

   Typy rámců i-frame, s-frame a u-frame: vysvětlete rozdíl mezi nimi a jejich typické využití.

2. Čím je charakteristická síť Frame Relay? K čemu u ní slouží parametry CIR a EIR? Jak s nimi souvisí příznak DE? Co je to DLCI, jak se používá? Podle čeho se přepíná provoz uvnitř FR sítě?

   Čím se vyznačuje síť ATM? Co je to VPI/VCI?

3. Čím se vyznačuje síť MPLS? Co je to label? Co je součástí MPLS záhlaví a jak je lze uspořádat do zásobníku? Kde se nachází vzhledem k ostatním záhlavím protokolové datové jednotky? Proč se někdy používá více MPLS záhlaví?

   Která zařízení se označují LSR, ELSR, P, PE, CE? Jak vypadá směrovací (přepínací) tabulka na zařízení uvnitř MPLS sítě?

   Jakou roli má protokol LDP?

4. Co je to SONET/SDH? Co je to WDM? V čem se liší CWDM, DWDM a OTN?

   Popište běžnou strukturu telefonní sítě včetně ústředen. Co je to PBX? Co znamená PSTN a POTS? Co označují pojmy CODEC a MODEM?

5. Charakterizujte protokol PPP. Popište funkcionalitu jeho vrstev NCP a LCP. Stručně charakterizujte možnosti autentizace u PPP – PAP, CHAP a EAP. Dá se PPP propojit s autentizačním serverem?

   Charakterizujte rozšíření PPP – Multilink PPP (MPPP), Tunneling PPP (PPTP). Co je to L2TP, PPPoA, PPPoE?

6. Charakterizujte ADSL. Proč jde o asymetrické spojení? Čím může být ovlivněna rychlost ADSL? Jak je rozděleno přenosové pásmo? Jaké jsou možnosti oddělení frekvencí pro upstream a downstream? Popište princip modulace DMT. Co je to agregace, jak se vypočte agregační poměr?

   Stručně charakterizujte zařízení, která se používají v síti ADSL – modem, splitter, DSLAM. Načrtněte, jak bývají tato zařízení propojena (případně co k nim bývá připojeno) a jak jsou napojena na telekomunikační a datovou síť včetně části na straně ISP (ale od ISP dále do Internetu nemusíte).

7. Charakterizujte další DSL technologie – HDSL, HDSL-2 (SHDSL), SDSL, a především VDSL. Zaměřte se rozdíly oproti ADSL a typické využití těchto technologií.

   Co je to DOCSIS? Jaké má vlastnosti ve srovnání s VDSL? Co je to CMTS?

8. Co je to FTTx? Stručně charakterizujte varianty FTTN/C/B/H. Jaký je rozdíl mezi aktivní (AON) a pasivní (PON) infrastrukturou? Co je to ONT a ONU a jakou to má spojitost s VDSL a DOCSIS?

   Co je to pobočková ústředna? Co musí mít firma k dispozici, aby si PBX zařídila? Co je to Asterisk?

5) Bezdrátové a mobilní sítě:

1. Jaký je rozdíl mezi fixní a mobilní bezdrátovou technologií? Jaký je rozdíl mezi bezlicenčním a licencovaným frekvenčním pásmem?

   Stručně popište typické vlastnosti Wi-Fi (standard a jeho nejznámější annexy, frekvenční pásma). Co je to TWT (u Wi-fi 6)?

2. Co je to Access Point? Co je to BSA, ESA, distribuční systém? Jak se AP může vypořádat se situací, kdy se k němu připojí zařízení pracující na různých standardech (například g, n, ax)?

   Charakterizujte technologii MIMO u Wi-Fi zařízení. Co je to MU-MIMO? Jaký je rozdíl mezi OFDM a OFDMA?

   Jak funguje přístupová metoda CSMA/CA s mechanismem RTS/CTS? Co je to „skrytá stanice“ a jaký problém může znamenat?

3. Jaký je hlavní rozdíl mezi MAC rámcem pro Wi-fi a MAC rámcem pro „drátový“ Ethernet – vzhledem k tomu, mezi kterými typy uzlů se Wi-fi MAC rámec posílá (zaměřte se především na adresaci)? Jaký je rozdíl mezi datovým, řídícím a management rámcem?

   AAA ve Wi-Fi – co tato zkratka znamená? Popište mechanismy WEP a WEP+IEEE 802.1x. Popište mechanismy WPA, WPA2 a WPA3 (jak to funguje, šifrování, integrita, varianty). Co je to WPS?

4. Mobilní sítě: jakou obvykle mají strukturu? Jakou roli plní základnová stanice (BTS)? Jak se tato síť napojuje na PSTN a PSDN? (nemusíte znát zkratky různých mezilehlých zařízení) Můžete načrtnout.

   Velmi stručně nastiňte rozdíly mezi GSM, CDMA, GPRS, EDGE, UMTS, HSDPA, HSUPA, HSPA. Jaký je rozdíl mezi LTE a LTE Advanced?

   Stručně charakterizujte síť IMT-2020 (5G). Co je to Sub6GHz a mmWave? Jak funguje slicing?

6) Síťová a transportní vrstva:

1. Co je to CIDR, agregace cest? K čemu slouží? Co je to CIDR blok?

   Jaký je rozdíl mezi statickým NATem a Masquerade? Co vše se v případě Masquerade eviduje? Co je to Carrier-Grade NAT (CGN)?

   Koexistence IPv4 a IPv6: vysvětlete pojmy Dual Stack, IP Tunneling a NAT/PT.

2. Správa skupin v IPv4 a IPv6: co všechno obnáší? Jaké protokoly se pro tento účel používají a jakým způsobem?

   Objevování sousedů: k čemu se používá a jaké protokoly se pro tento účel používají? Jak se používají tabulky sousedů? Co je to Solicited-node Multicast Address? Co je to DoD?

   Mechanismus objevování sousedů v IPv6 je možné zabezpečit protokolem SEND. Jak to funguje?

3. Co je to Token Bucket (na routeru)?

   Transportní vrstva: jakou roli hrají v TCP záhlaví příznaky SYN, ACK, FIN, RST, URG, PSH?

7) Decentralizované a distribuované systémy:

1. Charakterizujte pojmy centralizovaný systém, decentralizovaný systém, distribuovaný systém s důrazem na jejich odlišnosti. U každého uveďte příklad.

   Co je to bridging? Jaký je rozdíl mezi režimy Source-route bridging a Transparent bridging?

   Co je to switching? Jaký je rozdíl mezi přepínáním Store-and-Forward, Cut-Through a Fragment Free?

   Co j to routing? Co je to konvergence sítě?

2. Co je to administrativní vzdálenost (AD)? Pokud má OSPF AD=110 a RIP má AD=120, co to znamená? Proč mají statické cesty AD=1 a u čeho je AD=0?

   Co je to autonomní systém? Má každá firma svůj? Jaký je rozdíl mezi směrovacími protokoly typu interior a exterior?

3. Směrování – algoritmus vektoru vzdáleností: jaký je základní princip tohoto algoritmu? Co znamenají pojmy hold-down timer, poison reverse, split horizon?

   Charakterizujte směrovací protokoly RIP a EIGRP (verze, podpora beztřídního směrování, IPv6, způsob implementace směrovacího algoritmu, metrika, co je to DUAL).

   Charakterizujte směrovací protokol BGP (role ASN, algoritmus vektoru cest, zapouzdření BGP zpráv).

4. Směrování – algoritmus stavu spoje: jaký je základní princip tohoto algoritmu? Které tabulky algoritmus předepisuje na routeru? Jak algoritmus určuje optimální cesty (Dijkstra) a kde konkrétně se počítají?

   Charakterizujte směrovací protokol OSPF (verze, podpora beztřídního směrování, IPv6, typ směrovacího algoritmu, metrika, hierarchické směrování – oblasti, vnitřní a hraniční routery, autentizace).

5. Co to jsou jmenné služby? Co je to princip lokality? Co je to zóna, zónový soubor, doménový server, zone transfer? Jaké existují typy DNS serverů, jaká je jejich role v síti? Jmenujte alespoň dva známé DNS servery (jako software).

Co je to DNS resolver a kde ho najdeme? Jaká je role DNS cache a kde se může používat?

Jaký je rozdíl mezi rekurzivním a iterativním DNS dotazem a kde se který obvykle používá?

Co je to tabulka hostitelů? Co je to kanonické jméno? Jaké typy údajů tam jsou ke každému záznamu? K čemu slouží RR typu A, AAAA, PTR, CNAME, NS, MX, SOA a TXT?

6. Co je to DNSSEC? K čemu slouží mechanismy SPF a DKIM a jak se vztahují k RR záznamům typu TXT?

   Co je to QoS? Co se dá například garantovat? Charakterizujte IntServ a DiffServ. Co je to DSCP? Stručně charakterizujte třídy kategorií EF, AF a BE.

   Co je to *DiffServ doména*? Kde konkrétně probíhá zařazování paketu do konkrétní kategorie a jak se tento údaj používá na routerech? Jak se řeší koexistence různých typů DiffServ QoS v různých protokolech (např. IP vs. MPLS)?

7. VoIP – kam můžeme telefonovat z VoIP zařízení a k čemu slouží VoIP brána? Jak souvisí VoIP a QoS?

   Stručně charakterizujte protokoly SIP a H.323, zaměřte se na jejich funkčnost a rozdíly mezi nimi (včetně typického použití). K čemu slouží protokol RSVP? Potřebujeme při videopřenosu nějaké kodeky?

   Co je to videotelefonie a videokonference? Vyberte si dva z produktů pro videokonference a stručně charakterizujte.

8) Management a monitoring:

1. Správa sítě – co v sobě zahrnuje? Co je to NMS a jaké protokoly lze použít? Stručně charakterizujte protokol CMIP.

   K čemu slouží protokol SNMP? Jaký je rozdíl mezi jeho verzemi? Na jakém principu funguje správa pomocí SNMP? Jaké dva typy komunikace mezi agentem a správcem jsou podporovány? Co je to komunita a community name? Jak je to s bezpečností SNMP komunikace?

   Co je to MIB-II? Co je v ní evidováno a jakým způsobem? Jak se řeší adresace konkrétní položky v MIB-II? Co je to OID? Jaké typy objektů jsou uvnitř? Jak se k nim přistupuje (jak končí adresy)?

2. K čemu slouží Syslog a jakou roli plní démon syslogd? V jakém formátu jsou data (zprávy), která přijímá? Uveďte alespoň 3 různé kategorie zpráv. Co může Syslog provést s konkrétní zprávou a jak se dá určit tato akce?

   Co je to RMON a na jakém principu funguje? Jaký je vztah mezi RMON a MIB? Jaký je rozdíl mezi RMONem a SNMP a jaký je jeho přínos pro síť?

   Systém Snort – k čemu slouží, v jakých režimech může pracovat a na jakém principu funguje?

3. Co je to NetFlow a na jakém principu funguje? Co je to IPFIX? Kterými údaji je jednoznačně popsán tok? Uveďte také příklady složitějších konverzací (tj. více než jeden paket) patřících do jediného toku. Co je to Observation Point a Flow kolektor?

   Jaké výhody/nevýhody má NetFlow například oproti Snortu nebo SNMP?

4. Co je to VPN, v jakých situacích se používá, jaké jsou základní typy VPN (podle toho co konkrétně tyto tunely propojují)? Jaký je rozdíl mezi běžným tunelem a VPN? Co vše je třeba v rámci VPN řešit? S jakými problémy se můžeme setkat u VPN spojů, co je to Path MTU Discovery?

Co je to multipoint VPN?

IPSec – na jaké vrstvě pracuje? Jaký je rozdíl mezi tunelovacím a transportním režimem IPSec? Jaká existují IPSec záhlaví a jaký je mezi nimi rozdíl? K čemu slouží IKE?

5. Jakého typu jsou GRE a L2TP tunely? Srovnejte jejich vlastnosti navzájem a s IPSec tunely.

   Jaké vlastnosti má OpenVPN? Jaké vlastnosti má MPLS VPN? Jaké mají výhody a nevýhody?

   Stručně popište GRE a L2TP tunely, SSL/TLS tunely a MPLS VPN, včetně typu VPN. Na jakém principu funguje SSH, k čemu se používá a co potřebujeme ke zfunkčnění SSH na serveru a klientech (různé operační systémy)?

9) Bezpečnost:

1. Vysvětlete pojmy asset, threat, threat intelligence, APT, vulnerability, exploit, attack surface, perimeter.
2. Co je typické pro průzkumné útoky, přístupové útoky, útoky na odmítnutí služby.

   K čemu se používají ICMP útoky? Co je to eavesdropping? V čem spočívá útok typu MitM?

   Co je to IP spoofing, ARP/ND spoofing, DNS spoofing?

   Co je to hijacking? Co je to SQL Injection?

   Jak může probíhat DoS útok? Jak probíhá DDoS útok? Jaký je rozdíl mezi útokem Ping Flood a Smurf Attack?
3. Jaká je role bezpečnostních týmů? Co lze říct o zkratkách CERT a CSIRT? Může kterýkoliv bezpečnostní tým používat kteroukoliv z nich?

   Jakou roli plní týmy CSIRT.CZ a CESNET-CERTS?
4. Co je to *síťový analyzátor*, k čemu slouží? Podle čeho se rozhodujeme, kam ho umístíme? Uveďte alespoň dva známé výrobce síťových analyzátorů. Uveďte příklad některého hardwarového síťového analyzátoru (stručně charakterizujte).
5. K čemu je dobré zrcadlení provozu? Jak funguje SPAN? Co k jeho zprovoznění potřebujeme a jak se nazývají porty používané při SPANu? Jaký je rozdíl mezi local a remote SPANem?

   Co je to network tap, k čemu slouží? Jaké porty obvykle mívá, s čím se přes jaké rozhraní propojuje? Jak se řeší PoE u připojených koncových zařízení?
6. Co je to firewall, na jakém principu funguje? Do jakých oblastí je síť členěna z pohledu firewallu? Jak je to se zónami u Zone-based Policy Firewalu? K čemu slouží OpenWRT?

   Stručně charakterizujte typy filtrování: paketový filtr, ACL, SPI, aplikační proxy.

   Co je to IDS a IPS? Jaké metody používají pro klasifikaci provozu? Co je to anomaly-based detection a baseline? Jaký je rozdíl mezi IDS a IPS? Co je to HIDS/HIPS, NIDS/NIPS? Uveďte alespoň jeden HIDS/HIPS a alespoň dva NIDS/NIPS. Co je to DPI?
7. Popište princip a funkcionalitu dohledového systému (obecně). Vyberte si jeden z dohledových systémů (např. Nagios, Zabbix, OpenNMS, Zenoss, Cacti) a charakterizujte ho (licence s dostupností, platforma, co dokáže monitorovat, se kterými nástroji spolupracuje, na jakém principu funguje, význačné vlastnosti oproti jiným, apod.).
8. Co je to SIEM? Co do něj můžeme připojit a jaké úlohy by měl plnit? Jmenujte alespoň jeden SIEM.