

Příklady otázek ke zkoušce z předmětu ISA

Akademický rok 2020/2021

Petr Matoušek

30. listopadu 2020

1 Architektura sítě a adresování

1. Popište jednotlivé vrstvy modelu TCP/IP, jejich funkci a protokoly, které na nich komunikují.
2. Definujte zapouzdření a popište, jak probíhá. Uveďte, které síťové prvky, případně software, provádějí zapouzdření dat na konkrétní síťové vrstvě modelu TCP/IP.
3. Definujte adresování. Jak vypadá adresa na jednotlivých vrstvách modelu TCP/IP? Kdo ji přiděluje? Uveďte příklady adres pro jednotlivé vrstvy TCP/IP.
4. Definujte směrování. Ukažte, jak funguje směrování na jednotlivých vrstvách modelu TCP/IP?
5. Popište, jak probíhá směrování u služby (i) DNS, (ii) elektronické pošty, (iii) IP telefonie.
6. K čemu slouží mapování IP adres na MAC adresy a jak probíhá.
7. Popište formát adresy IPv4 a třídy adres. Co je to maska a broadcastová adresa, jak se vypočítají a k čemu slouží?
8. Popište způsob přidělování IPv4 adres. Jak je možné zjistit, komu daná IP adresa patří?
9. Popište formát adresy IPv6 a typy IPv6 adres. Jak probíhá přidělování adres IPv6?
10. Co obsahuje tabulka ARP na počítači a jak ji lze využít? Jak probíhá vyhledávání cesty pro odesílaný paket? Jak lze zkontrolovat, kudy paket půjde?
11. Popište, jak probíhá překlad IPv6 adresy na MAC adresu. Jakým způsobem lze získat tabulku přeložených adres na počítači?
12. Ukažte, jak lze k dané IP adrese dopočítat masku, určit adresu sítě a broadcastovou adresu.
13. Jak lze vypsat seznam služeb, které aktuálně běží na počítači? Které důležité informace výpis obsahuje?
14. Jak lze ověřit, že daný uzel je aktivní a že na něm běží daná síťová služba? Ukažte, jak lze dané informace získat a pomocí jakých nástrojů.

2 Pokročilé programování sítí TCP/IP

1. Definujte protokol a ukažte, jak je možné ho popsat. Uveďte příklad popisu protokolu.
2. Popište komunikaci klient – server. Popište, co je funkcí klienta a serveru. Pro základní síťové služby (např. e-mail, DNS, VoIP, apod.) uveďte příklady klienta a serveru.
3. Popište způsob přenosu dat mezi dvěma aplikacemi na jednotlivých vrstvách modelu TCP/IP při komunikaci pomocí (i) unicastu, (ii) multicastu a (iii) broadcastu. Ukažte, jak se vytváří PDU na jednotlivých vrstvách a inicializují hodnoty adresáta a odesílatele.
4. Co se stane, pokud bude paket při přenosu zahozen? Vysvětlete rozdílné chování u unicastu, multicastu a broadcastu. Čím se liší detekce chyb u IPv4 a IPv6?
5. Ukažte, jaké funkce knihovny BSD socket použijete pro vytvoření TCP klienta a TCP serveru.
6. Popište, jak lze implementovat konkurentní TCP server pomocí funkce `fork()`.
7. Ukažte, jaké funkce knihovny BSD socket použijete pro vytvoření UDP klienta a UDP serveru.
8. Vysvětlete, jaká jsou omezení při implementaci konkurentního UDP serveru. Popište možný způsob řešení.
9. Zapište implementaci broadcastu pomocí BSD schránek na straně vysílající a přijímající stanice.
10. Ukažte, jak lze implementovat multicast pomocí BSD schránek. Uveďte funkce, které použije vysílající a přijímající stanice.
11. Vysvětlete, co jsou spojované schránky UDP a proč se používají. Čím se liší od klasických schránek UDP?

3 Multicast. Zpracování dat na linkové vrstvě.

1. Definujte multicastové vysílání. Jaké adresy používá multicast na L2 a L3 pro IPv4 a IPv6?
2. Vysvětlete princip mapování multicastových adres L3 na adresy L2. Jak vzniká překrývání adres a jaký má vliv na komunikaci?
3. Na čem závisí dosah (viditelnost) multicastového přenosu?
4. Popište, jak probíhá komunikace pomocí multicastu: připojení stanice k multicastovému přenosu, ukončení příjmu, apod.
5. Uveďte příklad síťových služeb, které používají. Co by se stalo, kdyby multicast na LAN nefungoval?
6. Popište vlastnosti multicastového přenosu dat. Čím se liší od unicastu či broadcastu?
7. Popište způsob implementace aplikace pro čtení a vysílání multicastových dat pomocí BSD sockets.
8. Vysvětlete, jaké síťové aplikace využívají přímý přístup k paketům L2 a proč. Jaké znáte prostředky pro implementaci přístupu k datům na L2?
9. Popište způsob použití knihovny Libpcap pro čtení a zpracování paketů. Uveďte konkrétní funkce knihovny libpcap, které se používají.
10. Vysvětlete, co je filtr BPF, jak funguje a k čemu se používá. Ukažte příklad filtrování síťového provozu pomocí BPF.
11. Ukažte, jak lze využít knihovnu Scapy pro čtení a vysílání dat na L2. Které funkce lze využít pro odesílání a přijímání data na L2?
12. Uveďte, v čem se liší použití knihovny BSD socket a libpcap při implementaci počítačové komunikace.

4 Zabezpečení počítačové komunikace

1. Vyjmenujte a popište bezpečnostní rizika při provozování počítačové komunikace. Uveďte příklady útoků a jejich důsledků.
2. Vyjmenujte základní požadavky na bezpečnost počítačové komunikace. Ukažte, jak je lze vyřešit za pomoci konkrétních technologií.
3. Popište princip symetrického a asymetrického šifrování. Diskutujte problém výměny klíčů. Uveďte příklad algoritmů pro symetrické a asymetrické šifrování.
4. Vysvětlete, co je soukromý a co veřejný klíč a jak se používají pro šifrování, zajištění integrity dat a ověření odesílatele zprávy.
5. Vysvětlete, co kryptografický hash, jaký typ kryptografie používá, jak vzniká a k čemu slouží. Uveďte algoritmy pro generování kryptografického heše.
6. Čím se liší hešovací funkce a kryptografická hešovací funkce? Jak probíhá zabezpečení a distribuce klíčů?
7. Vysvětlete, co je elektronický podpis a kde se využívá. Popište proces vytvoření a kontroly elektronického podpisu. Uveďte algoritmy, které se pro tyto operace používají.
8. Definujte certifikát a uveďte, co obsahuje. Kde se využívají digitální certifikáty a jak probíhá ověření platnosti certifikátu?
9. Vysvětlete princip algoritmu Diffie-Hellman a uveďte, k čemu se používá.
10. Popište zabezpečení počítačové komunikace pomocí TLS. Vysvětlete, jak dochází k ustanovení spojení a které informace si strany vyměňují. Jaké jsou nevýhody při použití technologie TLS?
11. Vysvětlete pojem IPSec. Ukažte, jak je IPSec implementován a na jaké vrstvě modelu TCP/IP pracuje. Popište, jakým způsobem IPSec zajišťuje bezpečnost přenosu.
12. Vysvětlete rozdíly při použití transportního a tunelovacího režimu IPSec.
13. Co je to PGP a jaký typ zabezpečení poskytuje PGP? Uveďte, které klíče a algoritmy využívá. Popište postup zabezpečení a zprávy pomocí PGP a její ověření.
14. Uveďte způsob zabezpečení směrovacích protokolů. Na příkladu protokolu OSPF popište, jaké technologie se použijí a jak dochází k výměně klíčů.
15. Jaký vliv má autentizace a šifrování na soukromí uživatele síťových služeb?

5 Systém DNS

1. Popište jmenný prostor DNS, jeho strukturu, způsob uložení dat a přístup k nim.
2. Popište delegaci správy jednotlivých domén v systému DNS. Jak lze najít správce konkrétní domény?
3. Vysvětlete, co je to doména prvního řádu (TLD), druhého řádu, apod. Kdo je spravuje?
4. Jaké znáte typy DNS serverů a čím se liší?
5. Uveďte, jak probíhá přidělování IP adres. Jak lze zjistit, kdo danou IP adresu vlastní?
6. Co jsou reverzní DNS záznamy a k čemu se používají? Uveďte příklad reverzního záznamu.
7. Definujte rezoluci DNS a popište její princip. Porovnejte chování rekurzivního a iterativního DNS serveru. Vysvětlete, kde začíná rezoluce a jak probíhá.
8. Vysvětlete, co jsou kořenové servery DNS a k čemu slouží. Jak lze najít kořenový server?
9. Popište směrování a adresování dotazů v DNS. Co udělá klient DNS, když chce vyhledat konkrétní záznam v globálním jmenném prostoru DNS?
10. Vysvětlete, co znamená autoritativní odpověď DNS a jak ji lze získat.
11. Popište strukturu ukládání dat v DNS. Uveďte, z kterých částí se skládá záznam DNS. Vymenujte základní typy DNS záznamů, jejich použití. Zapište příklady základních DNS záznamů.
12. Vysvětlete použití záznamů SOA, MX, PTR, CNAME, SRV, NAPTR a NS.
13. Jak lze ověřit věrohodnost informací v DNS?
14. Popište protokol DNS a základní části dotazu a odpovědi. Uveďte příklad přenášených dat.
15. Vysvětlete, co je přenos zón a k čemu se používá. Kdy k němu dochází?
16. Vymenujte a popište základní typy útoků na službu DNS. Jak je možné se proti nim bránit?
17. Vysvětlete, jak pracuje DNSSEC a proti čemu chrání.
18. Vymenujte záznamy, které používá DNSSEC. Uveďte jejich použití.
19. Vysvětlete, co je zónový klíč (ZSK) a klíč pro podpis klíčů (KSK). Uveďte, jak se vytvářejí a kde jsou uloženy.
20. Definujte řetězec důvěry (chain of trust) a vysvětlete, k čemu slouží a jak ho lze vytvořit.
21. Diskutujte problém monitorování dotazů DNS versus soukromí uživatele. Jaká data DNS mohou narušit soukromí uživatele?
22. Popište, jak funguje DNS over HTTPS (DoH) a jak se implementuje. Uveďte výhody a rizika této technologie.
23. Porovnejte DoT (DNS over TLS) a DoH (DNS over HTTPS). Uveďte, proti čemu chrání DoT a jak probíhá rezoluce DNS při použití DoT.

6 Poštovní a adresářové služby

1. Popište architekturu elektronické pošty. Vyjmenujte související služby a protokoly, které jsou nezbytné pro správné fungování elektronické pošty.
2. Popište formát zpráv elektronické pošty. Jak se tvoří obálka a tělo zprávy? Vyjmenujte základní hlavičky SMTP.
3. Popište funkci protokolů SMTP, POP3 a IMAP. Uveďte příklad příkazů těchto protokolů.
4. Porovnejte čtení pošty pomocí POP3 a IMAP. Uveďte výhody a nevýhody obou protokolů.
5. Popište formát elektronické adresy. Ukažte, jak probíhá směrování elektronické pošty. Jak se bude chovat systém elektronické pošty, pokud adresát neexistuje?
6. Uveďte, jaké informace loguje poštovní server a k čemu je lze využít.
7. Vysvětlete, co je to MIME a k čemu slouží. Uveďte příklad použití.
8. Vysvětlete princip a použití kódování Quoted Printable a Base64 u elektronické pošty.
9. Ukažte, jak byste zabezpečili přenos elektronické pošty.
10. Popište princip zabezpečení e-mailové zprávy pomocí PGP. Ukažte, jak může adresát ověřit validitu zprávy. Jaké klíče PGP používá?
11. Vysvětlete, co je adresářová služby a k čemu se využívá.
12. Popište způsob uložení dat u služby LDAP. Jak vypadá adresování a vyhledávání dat v systému LDAP?
13. Definujte adresářové schéma a ukažte, k čemu slouží a co obsahuje. Zapište příklad adresářového schématu.
14. Co je to záznam LDAP a z čeho se skládá? Vyjmenujte základní atributy LDAP. Napište příklad záznamu pro třídu objektů *student FIT*.
15. Popište komunikace mezi klientem a serverem LDAP. Ukažte příklad komunikace při vyhledávání dat v adresáři LDAP.
16. Jaké znáte operace protokolu LDAP pro modifikaci dat v adresáři?
17. Ukažte, jak lze lokalizovat LDAP server pro danou doménu.
18. Jakým způsobem se kódují přenášená data protokolem LDAP?
19. Ukažte, jak lze zabezpečit přístup k datům v systému LDAP.
20. Popište způsoby propojení lokálních adresářů LDAP.
21. Popište využití služby LDAP pro vyhledávání adresátů elektronické pošty.
22. Ukažte, jak lze využít službu LDAP pro řízení přístup k webovému obsahu.
23. Vysvětlete mechanismu přístupu k médiu 802.1x. Jak se zde využívá služba Radius a LDAP?

7 Hlasové služby

1. Popište architekturu klasické telefonní sítě, jednotlivé prvky a jejich funkci.
2. Jak probíhá signalizace u klasické telefonní sítě PSTN?
3. Porovnejte vlastnosti PSTN a IP telefonie.
4. Popište architekturu sítě VoIP, základní stavební prvky a jejich funkci.
5. Jaké parametry musí splňovat IP telefonie z pohledu uživatele?
6. Uveďte, jaké základní síťové služby jsou nezbytné pro správnou funkci IP telefonie.
7. Popište, jak vypadá adresování a směrování u IP telefonie pomocí SIP.
8. Popište jednotlivé kroky při navazování a ustavení spojení VoIP pomocí SIP.
9. Ukažte, jak probíhá lokalizace volaného účastníka u VoIP.
10. Popište protokol SIP a základní metody protokolu. Ukažte, jak probíhá výměna dat pomocí SIP (a) při registraci a (b) při navazování spojení.
11. Vysvětlete, k čemu slouží protokoly RTP a SDP. Uveďte, na jaké vrstvě modelu TCP/IP pracují, jaká data přenášejí a jak souvisí s VoIP.
12. Ukažte, jakým způsobem se domlouvají volající strany u VoIP na parametrech spojení, tj. zdrojových a cílových portech pro přenos SIP a RTP, typu použitého kodeku apod. Uveďte příklad.
13. Popište nároky VoIP na velikost přenosového pásma a kvalitu přenosu. Jak je lze zajistit?
14. Srovnajte klasickou IP telefonii pomocí SIP s komerčními VoIP systémy typu Skype, WhatsApp, apod.
15. Popište, jak probíhá převod hlasu do binární podoby. Vyjmenujte a popište jednotlivé fáze převodu. Na kterých zařízeních k převodu dochází?
16. Definujte kodek a uveďte, jak souvisí typ kodeku s požadavkem na přenosové pásmo. Uveďte příklad nejběžnějších kodeků pro IP telefonii.
17. Ukažte, jak lze vypočítat potřebnou šířku přenosového pásma pro jeden hovor VoIP pro daný kodek, velikost hlasového rámce a režii.
18. Vyjmenujte bezpečnostní rizika VoIP a ukažte, jak je lze eliminovat.

8 Prostředky pro správu sítí

1. Vysvětlete, co je cílem správy sítě a jaké dílčí úkoly musí řešit. Ukažte, jaké prostředky k tomu využívá.
2. Vyjmenujte a popište oblasti správy sítě definované podle standardu FCAPS. Pro každou oblast uveďte, jaké úkoly musí správce zajistit a jaké prostředky k tomu může využít.
3. Ukažte, jakým způsobem získává správa sítě monitorovací data. Uveďte, které konkrétní prostředky lze k monitorování využít. Uveďte příklady získaných dat.
4. Popište funkci protokolu ICMPv4 pro správu sítě. Vyjmenujte základní typy zpráv ICMPv4 a popište jejich použití. Vyjmenujte bezpečnostní rizika ICMP.
5. Vysvětlete, jak se využívá ICMPv6 pro sítě komunikující nad IPv6. Vyjmenujte zprávy ICMPv6, které jsou nezbytné pro běh sítě. Na příkladu ukažte jejich použití.
6. Popište architekturu systému SNMP. Vysvětlete funkci jednotlivých prvků systému a způsob implementace.
7. Definujte objekty SNMP (MIB)? Popište jejich formát, způsob identifikace a uložení. Uveďte příklady takových objektů a jejich hodnot.
8. Vysvětlete, co je databáze MIB. Vyjmenujte základní skupiny objektů MIB-2 a konkrétní objekty, které spravují. Vysvětlete, kde je databáze uložena a jak k ní monitorovací systém SNMP přistupuje.
9. Vyjmenujte základní datové typy objektů, které definuje jazyk SMI. Uveďte příklady objektů, které tyto typy využívají.
10. Vysvětlete princip kódování BER. Kde a proč se dané kódování používá?
11. Popište komunikaci v systému SNMP. Vyjmenujte základní příkazy SNMP a jejich funkci.
12. Popište formát komunikačního protokolu SNMP. Jakým jazykem je popsána struktura SNMP? Popište způsob zabezpečení přenosu SNMP.
13. Diskutujte výhody i omezení praktického nasazení monitorování SNMP.
14. Ukažte, jak lze zajistit viditelnost dat v síti. Uveďte příklady pasivního či aktivního monitorování.
15. Srovnajte použití SNMP a NetFlow pro správu sítě. Čím se liší architektury těchto systémů?
16. Ukažte, které informace o síti je možné získat pomocí SNMP a nelze získat pomocí Netflow.
17. Uveďte příklad monitorovacích dat ze sítě, které je možné získat pomocí Netflow a nelze je získat pomocí SNMP.
18. Srovnajte systémy SNMP a syslog. Ukažte, jaké informace lze získat pomocí syslogu a nelze pomocí SNMP.
19. Jaké znáte konkrétní nástroje pro monitorování SNMP? Uveďte příklady.

9 Logování systému a služeb

1. Vysvětlete, k čemu je důležitá synchronizace času v síti. Ukažte, jaké důsledky mohou mít chyby v nastavení času síťových zařízení.
2. Popište princip synchronizace času pomocí protokolu NTP. Jak probíhá komunikace klienta a serveru? Které typy časových razítek se používají? Zakreslete příklad komunikace NTP klienta a serveru v časovém diagramu.
3. Ukažte, jak probíhá výpočtu zpoždění a posunu času při synchronizaci času pomocí NTP.
4. Jakým způsobem lze zabezpečit službu NTP?
5. Popište architekturu logování dat pomocí syslogu. Ukažte, jaké funkce vykonává syslog klient (console) a syslog server? Uveďte příklad logování.
6. Popište komunikační protokol syslog. Jaké úrovně zpráv znáte? Co může být zdrojem logovacích zpráv? Jaké události se logují na síťových zařízeních?
7. Uveďte příklady událostí, které logují následující síťové služby: poštovní server, webový server, server DHCP, Radius, DNS. Ukažte příklad konkrétního využití logovaných dat.
8. Vysvětlete, jak funguje služba TFTP a k čemu slouží.
9. Ukažte, které informace o síti lze získat pomocí logování a nelze získat monitorováním pomocí SNMP či NetFlow.
10. Jakým způsobem je možné zabezpečit službu syslog?

10 Měření provozu na síti pomocí NetFlow

1. Definujte pojmy tok (IP flow) a záznam toku. Uveďte, které položky záznamu o toku jsou klíčové a které statistické. Uveďte příklad toku i hodnot, které se o ukládají do záznamu. .
2. Popište architekturu systému NetFlow. Vysvětlete funkci základních prvků systému.
3. Popište funkci sondy Netflow. Ukažte, jak probíhá monitorování síťového provozu a vytváření vytváření záznamů o tocích.
4. Vysvětlete pojem vzorkování a ukažte, jak se využívá v systému NetFlow. Na jakých prvcích systému Netflow dochází ke vzorkování? Vysvětlete výhody a nevýhody použití vzorkování při monitorování dat.
5. Vysvětlete pojem agregace u systému NetFlow, k čemu agregace slouží a kdy probíhá. Na příkladu záznamů NetFlow ukažte agregaci záznamů o tocích. Uveďte, jaké jsou výhody a nevýhody agregace.
6. Na jaké vrstvě modelu TCP/IP je definován protokol NetFlow?
7. Jaká data z vrstev modelu TCP/IP mohou být monitorována systémem NetFlow? Pro jednotlivé vrstvy uveďte příklady monitorovaných dat.
8. Popište, jak sonda Netflow identifikuje jednotlivé toky. Vysvětlete funkci aktivního a neaktivního časovače.
9. Popište formát protokolu Netflow. Ukažte, jak jsou záznamy o tocích přenášeny v protokolu NetFlow.
10. Vyjmenujte hlavní rozdíly mezi protokolem NetFlow verze 5 a NetFlow verze 9/IPFIX.
11. Popište činnost kolektoru. Ukažte příklady dotazů kolektoru `nfdump` pro vyhledání nejvíce komunikujících uzlů v síti, nejvíce využívaných služeb. Ukažte, jak lze na kolektoru vyhledat komunikaci konkrétního uzlu v zadaném časovém intervalu.
12. Ukažte příklady použití NetFlow pro monitorování sítě.
13. Vysvětlete, co jsou šablony NetFlow a k čemu se využívají.
14. Uveďte, které informace o síti lze získat pouze pomocí NetFlow a nelze získat pomocí SNMP.
15. Ukažte, čím se liší architektura NetFlow a SNMP.

11 Zajištění kvality služeb

1. Definujte SLA (Service Level Agreement) a uveďte, k čemu slouží. Ukažte, jak je možné SLA v síti implementovat.
2. Vyjmenujte základní metody pro zajištění kvality přenosu v počítačových sítích. Ukažte, jak se tyto metody implementují v počítačové síti.
3. Porovnejte metodu rozložení provozu (traffic shaping) a ořezání provozu (traffic policing). Uveďte jejich výhody a nevýhody. Jak je možné tyto metody implementovat?
4. Vyjmenujte typy front, které se používají pro řízení kvality přenosu v počítačových sítích. Popište, jejich základní vlastnosti a uveďte, jak zpracovávají síťový provoz.
5. Vypočítejte výstupní rychlost a maximální zpoždění u front typu FIFO, cyklických front a váhových front. Předpokládejte, že znáte velikost výstupní linky, počet a váhy linek a velikost (délku) fronty.
6. Popište model tekoucího vědra (leaky bucket). Jak bude omezen provoz, pokud bude velikost vstupní fronty nulová? Ukažte, jak se daný model využívá při řešení kvality služeb v síti.
7. Popište model zásobníku žetonů (token bucket). Vyjmenujte parametry, které slouží pro nastavení modelu a jejich význam. Ukažte, jak lze model implementovat.
8. Vypočítejte maximální rychlost výstupu u zásobníku žetonů při vstupních parametrech CBS, CIR a T.
9. Vysvětlete, jak fungují integrované služby (IntServ). Popište jejich výhody a omezení. Ukažte příklad implementace IntServ.
10. Vysvětlete, jak probíhá rezervace přenosového pásma u integrovaných služeb. Jakým způsobem provádí síťové prvky rezervaci pro daný požadavek? Co se stane, pokud danému požadavku nelze vyhovět?
11. Popište architekturu diferenciovaných služeb (DiffServ). Ukažte, jakým způsobem se implementují a jaké třídy kvality přenosu poskytují.
12. Porovnejte model diferenciovaných a integrovaných služeb. Ukažte, v čem jsou výhody a omezení obou modelů.
13. Popište mechanismus RED a způsob implementace. K čemu RED slouží? Jaká je pravděpodobnost zahození přijatého paketu?
14. Jak se změní chování sítě při použití mechanismu RED, pokud upravíme hodnotu Q_{min} či Q_{max} u vstupní fronty?
15. Vysvětlete problém globální synchronizace TCP a vyhladovění TCP. Jak lze tyto problémy eliminovat?
16. Ukažte, jak pracuje mechanismus WRED. Čím se liší od mechanismu RED a jak ho lze implementovat?
17. Pro dané parametry CIR a CBS vytvořte model zásobníku žetonů. Pokud přijdou pakety o dané velikosti v určitý čas, jak se zpracují? Které budou zahozeny a které projdou na výstup?
18. Ukažte zpracování přicházejícího provozu při použití modelu tekoucího vědra. Jak se zpracují jednotlivé pakety?
19. Mějme rychlost výstupní linky R . S jakou rychlostí budou obsluhovány pakety ve frontě typu FIFO, při použití prioritních, cyklických a váhových front? Čím bude dáno maximální zpoždění paketu při zpracování?