## **Základ - 1**

#### Označte nepravdivé tvrzení týkající se porovnání metody přepojování paketů a přepojování okruhů.

- přepojování okruhů: rychlejší, plynulejší, ale při výpadku uzlu se spojení rozpadne

- přepojování paketů: každý může jít jinou cestou, liší se doba přenosu, ale výpadek uzlu není fatální

#### Který z následujících termínů nepatří mezi přenosové parametry počítačové sítě?

Ty které tam patří jsou:

- **Latence**, neboli zpoždění komunikace, tj. doba od chvíle, kdy jsou určitá data

odeslána do sítě, až do doby, kdy jsou doručena na místo určení.

- **Jitter** je rozptyl zpoždění; tato hodnota vyjadřuje, jak pravidelně jsou data

doručována, tj. jak objem přijatých dat kolísá.

- **Ztrátovost** dat znamená, jak často dochází k tomu, že nějaký paket není doručen;

- **Šířka pásma** (bandwidth), parametr často nazývaný „rychlost“

#### Jaké charakteristiky z hlediska přenosových parametrů mají následující typy aplikací resp. protokolů?

Multimediální appky – Obecně jim vadí jiter, VOIP vadí i latence, **neřeší** moc **ztrátovost dat**

Web, mail, apod. – Vadí jim ztrátovost dat

#### Které z následujících tvrzení týkajících se WAN je pravdivé?

#### Charakterizace WAN (Rozlehlá síť):

#### - vzdálený přístup, komunikace

#### - velké vzdálenosti, větší zpoždění

#### - mnoho vlastníků, distribuované řízení

#### Které z následujících tvrzení týkajících se LAN je pravdivé?

#### Charakterizace LAN (Lokální síť):

#### - sdílení prostředků (databázové servery, tiskárny)

#### - menší vzdálenosti, malé zpoždění

#### - jednotné vlastnictví a řízení

#### Které z následujících tvrzení o RFC je pravdivé?

#### Charakterizace RFC:

#### - Requests for Comments představují v současnosti prostředek standardizace na internetu

#### - autor předloží návrh nového protokolu, příslušná pracovní skupina jej posoudí, a pokud to považuje za užitečné, dokument obdrží číslo a je zveřejněn

#### - text dokumentu se nikdy nemění (kromě překlepů a chyb)

#### - Pokud dojde k podstatnějším změnám, je dokument znovu vydán s novým číslem

#### - Změny čísel RFC lze sledovat v souboru rfc-index.txt

#### - Zdaleka ne všemi dodržované

#### - Jsou veřejně přístupné

## **Vrstvy, NAT, URI – 2**

#### Označte nepravdivé tvrzení ohledně vrstevnaté struktury sítí.

#### Charakterizace vrstevnaté struktutury sítí:

#### - snazší dekompozice a popis

#### - snadná změna technologie

#### - spolupráce vrstev

#### Jaké je správné pořadí vrstev OSI modelu od nejvyšší po nejnižší?

#### - Aplikační, prezentační, relační, transportní, síťová, linková, fyzická

#### Označte pravdivé tvrzení o peer-to-peer (P2P) resp. klient-server aplikačních modelech.

#### Klient-server

#### - klient zná pevnou adresu serveru

#### - klient navazuje komunikaci, zadává požadavky

#### - server obvykle obsluhuje více klientů

#### P2P

#### - partneři neznají pevné adresy „zdroje dat“

#### - nejsou vyhraněné role (každý je zároveň klientem i serverem)

#### Jaký typ adres se používá na linkové vrstvě?

#### - MAC adresy

#### Jaký typ adres se používá na fyzické vrstvě?

#### - Žádné

#### Které z následujících tvrzení o doménových jménech je pravdivé?

#### Charakterizace doménových jmen:

#### - Hierarchie je u těchto adres zprava doleva (vpravo nejvyšší)

#### - poslední jméno je takzvaná doména nejvyšší úrovně (TLD)

#### - nižší spravuje vlastník nejvyšší úroveň spravuje ICANN (.cz - CZ.NIC)

#### Jakou TLD (Top Level Domain) najdeme v následujícím URI? <ftp://sunsite.mff.cuni.cz/Network/RFCs/rfc-index.txt>

#### .cz

#### Která z charakteristik překladu adres (NAT) je správná?

#### Charakterizace NAT (IP masquerading):

#### - první paket směřující od klienta k serveru je zachycen směrovačem na perimetru LAN

#### - Směrovač si uloží socketovou adresu (IP adresu a port) příchozího požadavku a nahradí v paketu patřičná pole vlastní externí IP adresou a nějakým portem, který je na směrovači volný

#### - Server tedy posléze odesílá odpověď na tuto upravenou socketovou adresu

#### - Když odpověď dorazí zpátky na směrovač, ten vyhledá příslušnou původní adresu socketu (podle cílového portu použitého serverem), změní patřičná pole v odpovědi zpět na původní hodnoty (IP adresu a port z požadavku) a doručí odpověď klientovi.

#### Které tvrzení týkající se URI je správné?

#### Charakterizace URI (Uniform Resource Identifier):

#### - textový řetězec s danou strukturou, k přesné specifikaci zdroje informace

#### - Tohle se prostě naučit nazpaměť: schéma://autorita[cesta][?dotaz][#fragment]

#### autorita=[jméno[:heslo]@]adresa[:port]

#### Zvolte nesprávnou definici pojmů segmentace, fragmentace, multiplexing a zapouzdření.

#### Správná definice pojmů:

#### Multiplexing - několik komunikačních kanálů v určité vrstvě používá stejný komunikační kanál v podřízené vrstvě

#### Zapouzdření - data + řídící informace vrstvy n do vrstvy n-1

#### Segmentace - rozdělení aplikačních dat na transportní vrstvě

#### Fragmentace - další dělení dat na síťové vrstvě díky malé velikosti MTU (Maximum transmission unit) linkové vrstvy

#### Jak spolupracují vrstvy vertikálně?

#### - Předávají si navzájem data+řídící informace vyšší vrstvy do nižsí (encapsulation)

#### - každá vrstva se stará o odlišnou část práce

**-** dohromady utváří celý proces

#### Co nepatří mezi funkce protokolu?

#### Nenašel jsem v prezentacích, co patří mezi funkce protokolu, tak je zde alespoň definice protokolu.

#### - je to v konvence nebo standard, podle kterého probíhá elektronická komunikace

#### - definuje pravidla řídící syntaxi, sémantiku a synchronizaci vzájemné komunikace

#### - příklady věcí, které protokol dělá:

#### Detekce spojení

#### Definuje jak formátovat zprávy

#### Co dělat s poškozenými daty

#### Jak ukončit spojení

## **Šifrování – 3**

#### Jaké tvrzení o symetrických a asymetrických šifrovacích algoritmech je pravdivé?

#### Charakterizace Symetrického šifrování:

#### - příjemce i odesilatel stejný klíč – musí být tajně domluven

#### - rychlé + vhodné na velká data

#### Charakterizace Asymetrického šifrování:

#### - pro šifrování a dešifrování se používá pár navzájem neodvoditelných klíčů

#### - pomalé, lze šifrovat jen malá data

#### Jaké vlastnosti musí splňovat hashovací algoritmus pro použití v kryptografii?

#### - malá změna dat způsobí zásadní změnu hodnoty kódu (je téměř jednoznačná)

#### - text z kódu neodvoditelný

#### - nalezení textu se shodným kódem musí být obtížné

#### Na jakém principu funguje šifrování elektronické pošty?

#### Diagram, schematic Description automatically generated

#### -Text zašifrujeme náhodným symetrickým klíčem

#### - Symetrický klíč zašifrujeme veřejným klíčem příjemce (asymetrický klíč)

#### - Pošleme tedy symetricky zašifrovaný text + asymetricky zašifrovaný symetrický klíč

#### - Přijemce si symetrický klíč rozšifruje svým tajným klíčem (asymetrický klíč)

#### - Tento symetrický klíč použije k rozšifrování původního textu

#### Na jakém principu funguje elektronický podpis?

#### Diagram Description automatically generated with medium confidence

#### - Z textu uděláme hash

#### - Hash zašifrujeme svým tajným klíčem (asymetrický klíč)

#### - Posíláme pak text + zašifrovaný hash textu

#### ­- Příjemce si pomocí stejné hashovací funkce vytvoří z textu hash

#### - Pak pomocí našeho veřejného klíče (asymetrického) dešifruje náš hash

#### - Oba hashe porovná (pokud jsou ok, tak typek, co to poslal má přístup k tajnému klíči toho, za koho se vydává)

#### Které tvrzení charakterizuje Diffie-Hellmanův algoritmus?

#### - Způsob výměny informací mezi dvěma partnery posílanými nezabezpečeným kanálem tak, aby oba získali sdílenou tajnou informaci (např. symetrický šifrovací klíč)

#### Které tvrzení o klíčích a certifikátech je pravdivé?

#### - Certifikát je klíč doplněný o identifikaci vlastníka a podepsaný vydavatelem, např. certifikační autoritou (CA)

#### - Autenticitu ověřuje třetí strana – veřejná certifikační autorita nebo pavučina důvěry

#### - Pokud důvěřujeme vydavateli, můžeme věřit klíči vlastníka

#### - Struktura certifikátu podle X.509:

#### Certifikát

#### Algoritmus pro elektronický podpis

#### Elektronický podpis

## **SSL/TLS – 3**

#### Jaké tvrzení o SSL resp. TLS je pravdivé?

#### Charakterizace SSL/TSL:

#### - Mezivrstva mezi transportní a aplikační vrstvou umožňující autentikaci a šifrování

#### Princip:

#### 1. Klient pošle požadavek na SSL spojení + parametry.

#### 2. Server pošle odpověď + parametry + certifikát serveru.

#### 3. Klient ověří server a vygeneruje základ šifrovacího klíče, zašifruje ho veřejným klíčem serveru a pošle mu ho.

#### 4. Server rozšifruje základ šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.

#### 5. Klient a server si navzájem potvrdí, že odteď bude jejich komunikace šifrovaná tímto klíčem.

## **Aplikační vrstva – 3**

#### Co patří mezi úkoly aplikační vrstvy v TCP/IP modelu?

#### - Spojuje funkce OSI vrstev 5, 6 a 7

#### - Protokol na aplikační vrstvě definuje:

#### průběh dialogu na obou stranách

#### formát zpráv (textový/binární, struktura,...)

#### typy zpráv (požadavků a odpovědí)

#### sémantiku zpráv, sémantiku informačních polí

#### interakci s transportní vrstvou (jaký protokol bude použit na transportní vrstvě)

#### Který z následujících protokolů není protokolem aplikační vrstvy TCP/IP?

#### Které jsou:

#### DNS, SMTP, POP3, IMAP, FTP, HTTP, Telnet, SSH, SIP, DHCP

#### Který z následujících protokolů se používá v TCP/IP na aplikační vrstvě?

#### - Viz předchozí otázka

#### Které z následujících tvrzení správně popisuje činnost konkrétního aplikačního protokolu?

#### Hodně záleží, co bude na výběr v testu. Obecně sem nelze napsat nic bez znalosti možností odpovědi.

#### Jakým způsobem se v aplikačních protokolech TCP/IP obvykle řeší binární zápis celých čísel?

#### - V TCP/IP protokolech se používá big-endian systém, neboli např. první bajt IP adresy jde po síti jako první

#### - Ale např. Intel má little endian (1 = 0x01, 0x00, 0x00, 0x00)

#### Jakým způsobem se v aplikačních protokolech TCP/IP řeší zápis textových řádek?

#### - Dvojice speciálních znaků CR LF - proměnlivá na OS

#### - Win CR LF

#### - Mac CR

#### - Linux LF

## **DNS – 3**

#### Které z následujících tvrzení o povaze DNS protokolu je správné?

#### - Klient-sever aplikace pro překlad jmen na adresy a naopak

#### - Binární protokol nad UDP i TCP, port 53

#### - Běžné dotazy (do 512B) se vyřizují pomocí UDP

#### - Větší datové výměny probíhají v TCP

#### - Klient se obrací na servery zadané v konfiguraci a postupně získává informace o dalších, dokud nedostane odpověď

#### - Jednotkou dat je „záznam“ (TTL záznamu je v sekundách)

#### Který aplikační protokol se používá pro zjišťování IP adres odpovídajících jménům strojů?

#### DNS

#### Označte správné tvrzení o nameserverech.

#### Typy serverů:

#### - primární: spravuje záznamy o doméně

#### - sekundární: stahuje a uchovává kopii dat o doméně

#### - caching-only: udržuje jen (ne)vyřešené dotazy po dobu platnosti

#### - Každá doména (zóna) musí mít alespoň jeden, ale raději více autoritativních (primárních nebo sekundárních) nameserverů

#### - Aktualizaci zónové databáze vyvolává sekundární server, je ale možné z primárního serveru signalizovat její potřebu

#### - Všechny autoritativní servery vracejí odpovědi označené příznakem autoritativnosti

#### Diagram, schematic Description automatically generated

#### Které tvrzení správně popisuje obvyklou implementaci služby operačního systému "zjisti IP adresu pro dané doménové jméno"?

#### DNS - rekurzivně se ptám serveru (nameserver v dané doméně), ten nerekurzivně vyšších kořenových serverů nastavených v konfiguraci (pokud to nemá v cache), vždy odpověď na co nejkonkrétnější část „zadání“

#### Které tvrzení o bezpečnostních aspektech protokolu DNS je správné?

#### ­- Problematické, DNSSEC je komplikované a rozšiřuje se pomalu

#### - problémy jako cache poisoning (do sekce Authority a Additional je zadána jiná doména – redirekce)

#### Uživateli nejde zobrazit WWW stránka. Při použití IP adresy v URL se stránka správně zobrazí. Který protokol je zodpovědný za chybu?

#### DNS

## **FTP – 4**

1xx předběžná kladná odpověď

2xx kladná (definitivní) odpověď

3xx neúplná kladná odp. (chci další příkaz/něco potřebuju)

4xx dočasná záporná odp. (je možné ptát se znovu)

5xx trvalá záporná odp. (nepodařilo se a neopakuj)

#### Který aplikační protokol se používá k přenosu souborů?

#### - FTP (otevřený textový protokol, požadavky port 21, data port 20 nebo libovolný)

#### - SSH, popř. SMTP

#### Které tvrzení o povaze FTP protokolu je správné?

#### Obecná charakterizace FTP:

#### - vzdálený přístup k uživatelskému účtu za účelem přenosu souborů

#### - je to textový protokol

#### - klient naváže tzv. řídící spojení na server na portu 21 a po něm posílá řádky s příkazy, zatímco server stejným kanálem posílá řádky s odpověďmi

#### - na každý nový přenos se musí otevřít nové TCP spojení, které se po dokončení přenosu zase zavře

**-** Aktivní datové spojení navazuje server. Na to má vyhrazený port 20 nazývaný ftp-data.

- Pasivní datové spojení navazuje klient. O adresu a port si požádá příkazem PASV

#### Které z následujících tvrzení o bezpečnostních problémech FTP je správné?

#### - Heslo se přenáší otevřeně. Je nešifrovaný. Používá se jen tam, kde nehrozí nic bezpečnostního

#### Pokud FTP klient pošle příkaz na FTP server na standardním portu, jaký z následujících portů může obsahovat odpověď jako zdrojový?

#### - 21 - odpověď na příkaz

#### - 20 - při aktivním přenosu

## **Pošta - 4 a 5**

#### Který aplikační protokol se používá pro elektronickou poštu?

#### - SMTP (textový na portu 25)

#### - POP3 (port 110)

#### - IMAP (port 143, nebo na port 993 s TSL)

#### Které z následujících tvrzení o používání poštovních protokolů je správné?

#### Tady může být cokoliv, ale otázka vypadá, že se ptá na etiku, tak ji sem hodím.

#### - přečíst všechny maily, než odpovíte

#### - zvažovat zásah do konverzace, pokud jste jen Cc

#### - nechat příjemci čas na odpověď (ale ověřit doručení lze)

#### - odpovídat rychle, alespoň jako potvrzení

#### - podpis

#### Které z následujících tvrzení o roli jednotlivých komponent v přenosu elektronické pošty je pravdivé?

#### Obecné informace o rolích v přenosu elektro. pošty:

#### - Odesilatel pošle podle SMTP nejbližšímu mail-forwarderu (MTA)

#### - MTA si mail navzájem posílají, dokud nedorazí do cílové destinace

#### - Odesílající MTA se nazývá mail-forwarder, přijímající mail-relay

#### Které z následujících tvrzení o SMTP protokolu je správné?

#### -zjistí server (za zavináčem)

#### - může poslat přímo nebo předá serveru v LAN (mail forwarder) neboli udělá mail submission

#### - každý uzel = MTA (kde je mail relay - fronta)

#### Který příkaz není příkazem SMTP protokolu podle RFC 821?

#### Příkazy jsou (z prezentace):

#### HELO (EHLO má novější ESMTP!), MAIL FROM, RCPT TO, DATA, QUIT

#### Dále podle RFC 821 jsou ještě:

#### RSET, SEND/SOML/SAML FROM, VRFY, EXPN, HELP, NOOP, TURN

#### Označte hlavičku, která se dle RFC 822 v dopisech nevyskytuje.

#### Vyskytuje se:

#### Date, From, Sender, Reply-To, To, Cc, Bcc, Message-ID, Subject, Received

#### Které tvrzení o rozšířeních protokolu SMTP pro přenos souborů a diakritiky je správné?

#### - Původně 7-bit ASCII, kódování souborů pomocí UUENCODE

#### - dnes rozšíření Multipurpose Internet Mail Extension (MIME) – umožňuje strukturovat dokument

#### - Kódování: Base64, Quoted-Printable

#### Které tvrzení o bezpečnostních aspektech poštovních protokolů je správné?

#### - server by měl maily local uživatelů poslat komukoli

#### - přijímat pouze maily lokálním uživatelům

#### - server může při prvotním vložení mailu do systému požadovat, aby se klient autentikoval pomocí ESMTP příkazu AUTH

#### Které tvrzení o autenticitě původu dopisu je správné?

#### - Dopis je vždy otevřená listovní zásilka

#### - Nikdy není jistý odesilatel, ani shoda údajů v obálce a textu

#### - Neotevírat soubory neznámého původu!

## **HTTP – 5**

#### Jak označujeme protokol, kterým se přenášejí webové stránky?

#### HTTP – Hypertext Transfer Protkol

#### Co označuje zkratka HTML?

Hypertext Markup Language

- popisuje obsah i formu

- konkrétní zobrazení v režii klienta

- píší se v něm webové stránky

#### Pokud www prohlížeč pošle dotaz na www server na standardním portu, jaký z následujících portů může obsahovat odpověď jako zdrojový?

#### - 80, 443

#### Které tvrzení o povaze HTTP protokolu je správné?

#### - Port 80 nebo 443 (pokud s TSL), typicky TCP

#### - Formát zprávy:

#### úvodní řádka (požadavek/odpověď), doplňující hlavičky (povinná je pouze Host, server zde může poslat cookies), (volitelné: tělo dokumentu)

* 1xx informativní odpověď (požadavek přijat, probíhá zpracování)
* 2xx kladná definitivní odpověď
* 3xx přesměrování (očekáván požadavek od klienta)
* 4xx chyba na straně klienta (nesprávný požadavek)
* 5xx chyba na straně serveru (nepodařilo se vyhovět požadavku)

- Požadavky jsou nezávislé, komunikace je bezestavová, stav je přenášen dodatečnými daty cookies

#### Která z následujících metod ("příkazů") existuje v HTTP protokolu?

#### Existují:

#### GET, POST, PUT, HEAD, DELETE, TRACE, OPTIONS, CONNECT, PATCH

#### Jaké tvrzení týkající se cookies je správné?

#### - Stav přenášený jako dodatečná data

#### - Mohou obsahovat například preference (nastavení), nějaký token pro autentifikaci přihlášeného uživatele...

#### Jakým způsobem klient obvykle předává serveru data vyplněná uživatelem do ovládacích prvků dialogu?

#### - POST (přímo do těla requestu, není jednoduše v prohlížečích vidět)

#### - GET (do URL)

#### Které tvrzení o možnostech autora ovlivnit dynamickou povahu stránek je nesprávné?

#### No idea.

#### Vyberte správné tvrzení o dynamických WWW stránkách.

#### - Dynamické stránky je možné nechat vygenerovat serverem (s využitím informací, které uživatel zadal, cookies apod.)

#### - Nebo přímo klientem (nejčastěji Javascript)

## **Telnet a SSH - 5**

#### Které tvrzení popisuje správně problematiku vzdáleného přihlášení pomocí protokolů telnet a SSH?

#### Telnet

#### - první způsob emulace terminálu

#### - klient a server se musejí domlouvat, co kdo zobrazí (není příznak odesílatel/příjemce)

#### - jinak se mohou dostat do nekonečné smyčky DO ECHO/WILL ECHO

#### - bezpečnostně je fakt naprd (otevřená hesla apod.)

#### - používá se už jen v uzavřených LAN sektorech

#### SSH

#### - dělá to stejný, co telnet, ale líp

#### - obecně lze použít na transfer dat (otevřít paralelní kanál a být přihlášen + přenášet data)

#### - využívá šifrování, tunelování

#### - SSHFS (zpřístupnění části file systému serveru, klientovy se jeví, jako lokální file system)

#### Které tvrzení o bezpečnosti přístupu přes SSH je správné?

#### Ověření serveru:

#### - Před začátkem komunikace si klient ověří certifikát, nebo otisk klíče serveru (při dalších přihlášeních už nemusí, stačí jen poprvé)

#### - Obecně to moc dělat nemusíme (záleží, kde všude máme stejný hesla apod.)

#### - Jestliže ale přijde zpráva o změně klíče na serveru neočekávaně, je něco sus (můžeme zavolat správcům, jestli je fakt novej klíč)

#### Ověření klienta:

#### - Jméno + heslo

#### - Nebo vygenerovat tajný klíč na klientovy, veřejný uloží na serveru, pak se prokazuje tajným klíčem

#### - Nikdy přihlašování na více serverů bez hesla (ochrana proti červům)

## **VoIP - 5**

#### Co označuje pojem VoIP (Voice over IP)?

#### - Obecné označení technologií pro přenos hlasu po IP

#### Který aplikační protokol (resp. sada protokolů) se používá pro VoIP?

#### H.323 na ASN (binární, bitové protokoly)

#### - je doslova bitový

#### H.225 + Q.931 + H.245 + RTP + RTPC

#### - je to složitý na všechno (čtení, implementace)

#### SIP

#### - náhrada H.323

#### - textový protokol (podobná struktura, jak HTTP, ale jede jak nad TCP, tak UDP)

#### - řeší pouze hledání partnera a navázání spojení

#### - dohoda o parametrech pomocí SDP (SIP zpráva, která nese SDP data má jako MIME uveden application/sdp)

#### - samotné posílání audia/videa je pomocí RTP/RTCP

#### Co označuje pojem SIP (Session Initiation Protocol)?

#### Viz víše