## **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.