## **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 + RTCP

#### - 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

## **NFS a SMB – 6**

#### Který aplikační protokol se používá pro sdílení systému souborů?

#### NFS (Network File System, má relační RPC a prezentační XDR vrstvy), SMB (Server Message Block)

## **NTP – 6**

#### Jakým způsobem se synchronizují hodiny na počítačích v síti?

#### - Pomocí Network Time Protokolu (port 123 UDP)

#### - atomové hodiny = stratum 0, od nich čas odebírají stratum 1, atd.

#### - při přebírání času od strata N k N+1 proběhne výpočet na upřesnění kvůli latenci (jelikož nějakou dobu trvá samotné poslání a přijetí času)

#### Proč se synchronizují hodiny na počítačích v síti?

#### - Stejné timestampy souborů (při sdílení disků např. NFS a SMB)

#### - Možnost porovnávání událostí na různých počítačích

## **DHCP – 6**

#### Jak funguje protokol DHCP?

#### - Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě

#### - Dynamická alokace adres

#### - Časově omezený pronájem

#### - Kooperace více serverů

## **Transportní vrstva - 6**

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

#### - TCP, UDP

#### Se kterou vrstvou TCP/IP je svázán pojem port?

#### Transportní (OSI4)

#### K čemu se používají porty v OSI 4?

#### Aby OS mohl předávat aplikacím data, o která žádají - nevědělo by se komu data patří. Port je "číslo aplikace".

#### Označte úkol, který není předmětem činnosti žádného protokolu transportní vrstvy.

#### - (TCP/UDP) zodpovídá za end to end přenos dat

#### - zprostředkovává služby sítě aplikačním protokolům

#### - umožňuje provoz více aplikací na uzlu

#### Která charakteristika TCP není správná?

#### Charakteristika TCP:

#### – používá se pro spojované služby

#### – klient naváže spojení

#### - data tečou ve formě proudu (streamu)

#### – spojení (relaci) řídí a zabezpečuje TCP, nikoliv aplikace

#### – TCP je komplikované, má velkou režii

#### – příp. méně pravidelné, ale bezeztrátové doručování

#### Jakou informaci najdeme v záhlaví TCP i UDP?

#### - Destination Port, Source Port, Checksum, Data

#### Jaké postupy používá TCP, aby zajistilo spolehlivost přenosu?

#### - Přijmající strana posílá příznak ACK spolu s nastaveným „Acknowledgement number“ na číslo offsetu posledního packetu, který dostala

#### - (tohle pošle buď s daty pro odesilatele, nebo pokud žádná data poslat zpět nepotřebuje, pošle to po nějakém čase jen tak)

#### - Odesilatel má nějaký „window“ (počet dat), který posílá bez ACK od protistrany, pokud window přesáhne, zastaví se a na ACK čeká, pokud ACK nedochází, posílá data znovu

#### Který parametr datového přenosu určuje, jaký rozsah dat může stanice poslat, aniž musí čekat na potvrzení protistrany?

#### - window, použití viz víše

#### Jakou informaci obvykle volí dynamicky klient, jenž se chystá navázat spojení na server?

#### - Sequence Number, zdrojový port

#### Které tvrzení popisuje správně TCP resp. UDP?

#### TCP

#### - viz víše

#### UDP

#### - pro nespojované služby

#### - neexistuje „spojení“, data jsou nezávislé zprávy

#### - jednoduché – musí řídit aplikace

#### - (pravidelný tok za cenu vyšší ztrátovosti)

#### Pokud TCP pakety dorazí v nesprávném pořadí, co se stane?

#### - packety mají Sequence number = příjemce si pakety srovná (na transportní vrstvě)

#### Pokud UDP pakety nedorazí ve správném pořadí, co se stane?

#### - Příjemce může a nemusí srovnat packety na aplikační vrstvě (programátor může pořadí vložit do „dat“ podle nich aplikace může srovnat, jinak implicitně v UDP protokolu není)

#### Co se odehrává během three-way handshake?

#### Table Description automatically generated

#### Co se stane, když jeden z partnerů pošle TCP paket s FIN příznakem?

#### - Klient odešle datagram s nastaveným příznakem FIN (odteď nesmí jít žádná další data z klienta)

#### - Server odpoví datagramem s nastaveným příznakem ACK

#### - Server odešle datagram s nastaveným příznakem FIN

#### - Klient odpoví s nastaveným příznakem ACK

#### - Tím je spojení ukončeno

#### Table Description automatically generated

#### Co usoudíme z následujícího popisu paketu v programu tcpdump?

packet má pouze SYN - je to z three-way-handshake

zdrojová IP.port > cílová IP.port

seq #, window velikost

PSH znamená poslední segment dat

#### Co usoudíme z (kompletního) výpisu programu netstat -an?

#### - Zobrazí výpis všech TCP a UDP serverů a otevřených TCP spojení (UDP nemá spojení)

#### - porty na kterých naslouchají spuštěné procesy

#### - local address 0.0.0.0 - poslouchá na všech rozhraních

#### - foreign address 0.0.0.0 nebo \* znamená, že se může připojit libovolný klient

## **Síťová vrstva – 6**

#### Označte termín, který není funkcí síťové vrstvy.

#### Viz níže

#### Co nepatří mezi úkoly síťové vrstvy v TCP/IP modelu?

#### Co patří:

#### - adresace - protokol síťové vrstvy definuje tvar a strukturu adres komunikujících partnerů

#### - encapsulation (zapouzdření) - řídící data potřebná pro přenos (zjm. adresy) se musí vložit do PDU

#### - routing (směrování) - vyhledání nejvhodnější cesty k cíli přes mezilehlé sítě

#### - forwarding (přeposílání) - předání dat ze vstupního síťového rozhraní na výstupní

#### - decapsulation - vybalení dat a předání transportní vrstvě

#### Jaká informace se přidává do paketu během zapouzdření na síťové vrstvě?

#### IP adresa zdroje a cíle, typ (verze, délka hlavičky, QoS, délka packetu, identifikace fragmentu, time-to-live)

#### Jaký protokol poskytuje na síťové vrstvě službu spolehlivého přenosu dat?

#### “Žádná odpověď není správná“ na síťové vrstvě (na transportní je to TCP)

#### Jaký protokol poskytuje na síťové vrstvě službu nespolehlivého přenosu dat?

#### IP (UDP to od IP přebírá)

#### Označte nepravdivé tvrzení o přidělování IP adres.

#### Centrální IANA (ICANN), regiony RIR (5x, náš RIPE NCC), dále ISP, v lokální síti: lokální správa (automaticky nebo ručně)

#### Označte nesprávnou variantu, jak počítač může zjistit IP adresu, kterou smí používat.

#### Správně:

#### - DHCP, link-local adresy, administrátorem přidělena manuálně

#### Kolik bitů má IPv6 adresa?

#### 128

#### Který z následujících protokolů nepracuje s IP adresami?

#### - pracuje DHCP, DNS, ICMP

#### - nepracuje UDP

#### Která vrstva OSI pracuje s IP adresami?

#### síťová – 3

#### Jak odesilatel zprávy zjistí, jaká část cílové IP adresy přísluší síti a jaká počítači?

#### Podle masky:

#### - jedničky v ní = část IP adresy určující síť

#### - nuly = část IP adresy pro počítač

#### Příklad: 192.168.100.1/16, tedy maska je 255.255.0.0 → 192.168. je část IP adresy určující síť

#### Jaká IPv4 adresa má v části pro počítač samé jedničky?

#### Network broadcast - „všem v dané síti“, normálně se doručí

#### Které tvrzení o typech IP adres je pravdivé? Slide 121-126

#### Prostě projdi prezentaci, moc obecná otázka.

#### V jakém případě není nutná adresace cílového počítače?

#### Broadcast nebo Multicastová adresa

#### Za předpokladu použití implicitních síťových masek označte nesprávně klasifikovanou IP adresu.

#### Pamatovat, že v bináru platí:

#### If it begins with 0, then it's a Class A network.

#### If it begins with 10, then it's a Class B network.

#### If it begins with 110, then it's a Class C network.

#### If it begins with 1110, then it's a Class D network.

#### If it begins with 1111, then it's a Class E network.

#### Kolik a jak rozsáhlých podsítí je třeba na pokrytí sítě s následujícími požadavky na počty připojených počítačů za použití VLSM (Variable Length Subnet Mask)?

#### To se vymyslí na místě.

#### Která z následujících kombinací představuje minimální síť pokrývající tyto unicastové adresy: 10.1.1.106, 10.1.1.111, 10.1.1.119?

#### Idk

#### Která následujících adres představuje korektní adresu počítače?

#### spočítat subnet mask - nesmí být samé nuly ani samé jedničky, adresa konkrétní nesmí být samé jedničky ani samé nuly

#### Které z následujících nastavení může být v této síti správnou adresou počítače?

#### Záleží na odpovědích

#### Defaultní router pro nějakou síť má adresu 172.31.219.33/27. Které z následujících nastavení může být v této síti správnou adresou počítače?

#### 172.31.219.33 - 172.31.219.62

## **Směrování – 7**

#### Které tvrzení o směrování je pravdivé?

#### - Měla by umět každá stanice v TCP/IP síti

#### - Záznam ve směrovací tabulce obsahuje „sloupce“:

#### cíl, maska, gateway

#### - Typy záznamů:

#### – direct (přímo připojená síť, “gateway” je vlastní adresa)

#### – indirect, default

#### - Vznik záznamu:

#### – implicitní (automaticky po přiřazení adresy rozhraní)

#### – explicitní („ručně“ zadán příkazem)

#### – dynamický (v průběhu práce od partnerů v síti)

#### Vyberte správné tvrzení o principu směrovacího algoritmu.

#### Diagram Description automatically generated

#### Jakou informaci z paketu používá každý směrovač pro určení cesty?

#### - IP adresu cíle

## **ICMP a ping – 7**

#### Jaké funkce plní ICMP (Internet Control Message Protocol)?

#### - ICMP slouží pro posílání řídících informací pro IP

#### - Používá IP datagramy, ale není to transportní protokol

#### Vyberte správné tvrzení o účelu a principu programu ping.

#### - zavoláme program ping, začne periodicky vysílat zprávy ICMP Echo

#### - Pokud zpráva dorazí na cílový stroj, jeho síťový software odpoví zprávou ICMP Echo reply

#### - Pokud odpověď dorazí zpátky, ping vypíše řádek s informací o době, jak dlouho trvalo, než dorazila

#### - Program vysílá zprávy s periodou 1

#### - Po přerušní/ukončení vypíše program statistiku

#### Co můžeme usoudit, pokud zavoláme program ping na adresu 127.0.0.1 s výsledkem: 4 packets transmitted, 0 packets received, 100.0% packet loss?

#### - někdo kdo otázku měl v testu tvrdil, že jediná odpověď co dávala smysl je že na počítači je špatně nainstalovaný IP software

## **TTL – 7**

#### Jaké pole IP záhlaví za normálních okolností mění router?

#### TTL

#### Které pole IP záhlaví brání vzniku nekonečné smyčky při doručování?

#### TTL

#### Vyberte správné tvrzení o účelu nebo použití pole IP záhlaví označovaného jako TTL (Time To Live).

#### Prostředek pro ochranu před zacyklením v případě routovací smyčky (chybná konfigurace routerů), udává počet hopů, kterí smí paket ještě přeskočit, při dosazení 0 se posílá ICMP Time Exceeded

## **Routovací a směrové tabulky a protokoly – 7**

#### Jakým příkazem můžeme vypsat obsah routovací tabulky?

#### netstat –r nebo route print

#### Který záznam může být platným záznamem ve směrovací tabulce routeru B z následujícího obrázku?

#### Viz níže

#### Který záznam může být platným záznamem ve směrovací tabulce routeru A z následujícího obrázku?

Podívejte se na tabulky netstat -r nebo na net

router má většinou 2 IP adresy do dvou sítí, které propojuje dest 127.0.0.0 a gateway 127.0.0.1 je vlastní adresa

#### Označte existující pole (sloupec) routovací tabulky.

#### Network Destination, Netmask, Gateway, Interface, Metric, Flags

#### Které tvrzení o metodách řízení směrovacích tabulek je pravdivé?

#### Statické řízení:

#### Cesty se nastavují při startu podle konfigurace - nepružné při změnách

#### - problémy se subnettingem

#### - nesnadné zálohování spojení

#### + méně citlivé na problémy v síti

#### + dostupné i ve zcela heterogenním prostředí

#### vhodné pro jednodušší, stabilní sítě

#### Dynamické řízení:

#### Routery si navzájem vyměňují informace o síti pomocí routovacího protokolu, stanice se jím mohou řídit také, ale v režimu read-only

#### + jednoduché změny konfigurace

#### + síť se dokáže sama „opravovat“

#### + směrovací tabulky se udržují automaticky

#### - citlivější na problémy příp. Útoky

#### Pokud má počítač špatně nastaven defaultní router, co nebude moci?

#### Nebude moci zprávy (data) vysílat jinam než do svého subnetu (a ani příjmat TCP spojení)

#### Označte pravdivé tvrzení o distance-vector routovacích protokolech.

#### • Základní myšlenka:

#### – uzel má u záznamů ve směrovací tabulce i „vzdálenosti“

#### – svou tabulku periodicky posílá sousedům, ti si upraví svoji tabulku a v dalším taktu ji posílají dál

#### • Výhody:

#### – jednoduché, snadno implementovatelné

#### • Nevýhody:

#### – pomalá reakce na chyby

#### – metrika špatně zohledňuje vlastnosti linek (rychlost, spolehlivost, cenu...)

#### – omezený rozsah sítě

#### – chyba ve výpočtu jednoho routeru ovlivňuje celou síť (možnost vzniku routovacích smyček)

#### Označte pravdivé tvrzení o link-state routovacích protokolech.

#### • Základní myšlenka:

#### – každý router zná „mapu“ celé sítě

#### – routery si navzájem sdělují stav svých linek a podle toho si každý modifikuje svoji mapu sítě

#### • Nevýhody:

#### – výpočet mapy je náročnější na výkon CPU i na paměť

#### – při startu a na nestabilních sítích může výměna dat znamenat významnou zátěž sítě

#### • Výhody:

#### – pružná reakce na změny topologie

#### – každý si počítá sám za sebe, chyba neovlivní ostatní

#### – síť je možné rozdělit na menší podsítě (rychlost výpočtu!)

#### – výměna dat probíhá pouze při změnách

#### Které tvrzení charakterizuje Dijkstrův algoritmus?

#### Djikstra se používá k nalezení nejkratší cesty (v grafu). Maximum průchodů = počet vrcholů. Je potřeba ho vždy celý přepočítat když se přidá nová hrana/vrchol

#### Označte pravdivé tvrzení o autonomních systémech (AS)?

#### - Blok sítí se společnou routovací politikou, zavedeny pro snazší routování na globální úrovni, smyslem je sjednotit směřování na globální úrovni

#### - externí routovací protokoly EGP – dnes používaný Border Gateway Protokol BGP

## **IP filtrování, proxy, ARP - 7 a 8**

#### Která z charakteristik IP filtrování je správná?

#### Text Description automatically generated

#### Která z charakteristik proxy serveru je správná?

#### Text Description automatically generated

#### Které zařízení/prostředek implementuje bezpečnostní politiku lokální sítě vůči internetu?

#### směřovač (základem IP filtrování)

#### Router/Firewall/Proxy server/NAT

#### Které tvrzení o ARP je pravdivé?

#### Table Description automatically generated

#### Počítač na obrázku poslal HTTP request, který dorazil na server. Jaké tvrzení o obsahu ARP tabulek na notebooku, switchi, routeru a serveru je pravdivé?

#### Řídit se tím, jak funguje ARP a nějak se to vymyslí.

#### Označte pravdivé tvrzení týkající se MAC adres (ve fungující síti).

#### MAC (fyzická/HW adresa), mohou být stejné v jedné LAN, pokud jsou odděleny routerem

#### Uživatel přesunul počítač do jiné podsítě v síti bez VLSM (Variable Length Subnet Mask) a Proxy ARP. Které z následujících nastavení bude muset zcela jistě změnit?

#### IP

#### Jak budou vypadat zdrojové a cílové IP a MAC adresy paketu poslaného z notebooku na server na trase mezi routerem A a B?

#### Vzhledem k ARP: Zdrojová: IP notebooku, MAC routeru A, cílové MAC routeru B, IP Serveru

#### Jak budou vypadat zdrojové a cílové IP a MAC adresy paketu poslaného jako odpověď serveru na požadavek z notebooku při průchodu podsítí označenou III?

#### Pokud není žádný router (obrázek?) pak prostě zdrojové přímo adresy serveru a cílové notebooku.

#### Jaké kroky musí udělat klientský počítač, aby správně odeslal paket v případě, že cílový server není ve stejné síti?

Vyslat ARP request aby zjistil MAC adresu routeru – poté packet co chtěl odeslat je vyslán přes router podle jeho směrovací tabulky (předtím počítač nezná adresu routeru proto ARP request)

## **Linková vrstva, topologie – 8**

#### Označte pravdivé tvrzení o vztahu linkové a fyzické vrstvy v OSI a TCP/IP

#### TCP/IP se jimi nezabývá

#### Co označuje termín LLC (Logical Link Control)?

#### Text, letter Description automatically generated

#### Co označuje termín MAC (Media Access Control)?

#### 

#### Jaký krok následuje poté, co www klient zjistí adresu cílového serveru a připraví paket v protokolu IP k odeslání?

#### Pošle do Linkové vrstvy - jednotka je rámec, ta připojí mac adresu zdroje a cíle, řídící info LLC, FCS

#### Jaký hlavní smysl má zápatí (trailer) linkového rámce?

#### Obsahuje FCS (Frame check sequence) = kontrolní součet

#### Které tvrzení o deterministickém a nedeterministickém přístupu k médiu je pravdivé?

#### Deterministický přístup:

#### - Někdo nebo něco deterministicky určuje, kdo smí v dané chvíli vysílat.

#### - Nevýhodou je to, že pokud uzel, který „je na řadě“, zrovna nemá co vysílat, jeho vysílací frekvence zůstane nevyužita, což zvyšuje režii a snižuje kapacitu sítě.

#### Nedeterministický přístup:

#### - nikdo neomezuje uzly ve vysílání, takže se následně musí řešit kolize

#### Které tvrzení o topologii sítě je pravdivé?

#### - uspořádání uzlů, zapojení různých prvků do sítě a zachycení jejich reálné a logické podoby „tvar/struktura sítě“

#### Co je základní funkcí CSMA/CD?

#### - během vysílání uzel současně detekuje případnou kolizi

#### - při kolizi zastaví stanice vysílání, upozorní ostatní

#### - počká určitou náhodnou dobu a pokus opakuje (obvykle se postupně prodlužuje interval čekání)

#### - doba vysílání rámce musí být delší než doba šíření z jednoho konce na druhý