Otázky Úvod do počítačových sítí 2016

Úvod

Mírně upravená verze odpovědí na otázky z roku 2015 Vojtěcha Tázlara, otázky se neměnily.

> Nic není zaručeno, nijak jsem neformátoval, překlepů je asi hodně. (Něco jsem konzultoval, některé otázky nemusí být zcela jasné, u otázek typu "co je/znamená je popsáno vše - nejen "překlad" termínu) (Jedná se o kombinaci původního zpracování co bylo postnuté ve skupině + opisy některých slidů + doplnění z netu, každopádně u všeho něco je)
>
> Využijte na vlastní nebezpečí. V. Tázlar

Hlavními změnami jsou opravy překlepů a přepsání do markdownu. Několik odpovědí bylo přepsáno a opraveno. Také jsem zkontroloval, že tu vážně byly všechny otázky (byly).

Stále není nic zaručeno, překlepů je snad už méně.

Jirka Sejkora

Otázky

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

Přepojování okruhů - vybere se pevná cesta pro celou komunikaci, jako přepojování telefonních ústředen. Rychlejší, plynulejší, výpadek znamená rozpad spojení.

Přepojování packetů - každý packet se může v každém uzlu vydat jinou cestou. Výpadek uzlu není fatální.

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

Co je potřeba aby daný protokol fungoval = multimediální (realtime=latency/jitter), SMTP (ztrátovost dat)

Který z následujících termínů nepatří mezi přenosové parametry počítačové sítě?

Zpoždění=Latence/Delay, pravidelnost=Jitter/Rozptyl zpoždění, ztrátovost dat, šířka pásma=Bandwidth

Které z následujících tvrzení týkajících se WAN je pravdivé?

Rozlehlé sítě, vzdálený přístup, velké vzdálenosti=větší zpoždění, mnoho vlastníků=distribuované řízení

Které z následujících tvrzení týkajících se LAN je pravdivé?

Sdílení prostředků (tiskárny, databázové servery), menší vzdálenost=malé zpoždění, jednotné vlastnictví a řízení

Které tvrzení charakterizuje Diffie-Hellmanův algoritmus?

Způsob výměny informací mezi dvěma partnery po nezabezpečeném kanálu, tak aby oba získali sdílenou

tajnou informaci (př symetrický šifrovací klíč)

Které tvrzení charakterizuje Dijkstrův algoritmus?

Open Shortest Path First je interní link state protokol ve kterém se Djikstra používá k nalezení nejkratší cesty (v grafu). Maximum průchodů = počet vrcholů. Je potřeba ho vždy celý přepočítat když se přidá nová hrana/vrchol

Na jakém principu funguje šifrování elektronické pošty?

Data-náhodný sym. Klíč, ten zašifrován veřejným klíčem – oboje posláno, příjemce tajným klíčem rozšifruje symetrický klíč a použije ho na data

Na jakém principu funguje elektronický podpis?

Odesilatel vytvoří hash – ten zašifruje tajným klíčem, přiloží ke zprávě, příjemce veřejným klíčem rozšifruje hash a porovná s vlastním hashem přijaté zprávy

Jaké tvrzení o symetrických a asymetrických šifrovacích algoritmech je pravdivé?

Symetrický = příjemce i odesilatel stejný klíč – musí být tajně domluven, rychlé vhodné na velká data (Historie: šifrovací mřížky, tabulky), dnes analogické principy převedené do digitální podoby+matematika, DES, Blowfish, AES, RC4

Asymetrický = veřejný šifrovací a soukromý (symetrický) dešifrovací klíč (kdo chce zašifruje mi to a le jen já vím jak to přečíst)

Jaké vlastnosti musí splňovat hashovací algoritmus pro použití v kryptografii?

(Hashovací funkce: Pevně z „kódu“ textu, široké uplatnění, CRC, MD5)

Malá změna textu=velká změna hashe=jednoznačný, jednosměrnost=text z hashe neodvoditelný, nalezení textu se shodným hashem obtížné, př. SHA (formálně převod vstupní posloupnosti bitů a nějakou konrétní posloupnost vždy odpovídající délce dané hashovací funkcí.)

Které tvrzení o klíčích a certifikátech je pravdivé?

Autenticitu ověřuje třetí strana – veřejná certifikační autorita (pavučina důvěry), Certifikát = klíč doplněný o identifikaci vlastníka a podepsaný vydavatelem (Certifikační autoritou CA) => ověřovat věrohodnost CA (Podle X.509 obsahuje: certifikát (verze, sériové číslo, vydavatel, doba platnosti, vlastník věř. Klíče, informace o klíči), algoritmus pro el. podpis, elektronický podpis)

Jaké tvrzení o SSL resp. TLS je pravdivé?

Mezivrstva mezi aplikační a transportní umožňuje AUTENTIKACI A šifrování (využívá i HTTPS port 443) Princip: 1) Klient – požadavek na SSL spojení + parametry 2) Server – odpověď + parametry + certifikát 3) Klient – ověření serveru + vygenerovaný základ klíče, zašifrován věř. klíčem serveru 4) Server – rozšifruje a vytvoří šifrovací klíč (stejně tak učiní klient) 5) Vzájemně si potvrdí, odteď probíhá komunikace s tímto klíčem

Označte nepravdivé tvrzení ohledně vrstevnaté struktury sítí.

Snazší dekompozice a popis, změna technologie – rozdělení práce mezi vrstvy ISO/OSI (shora navržený, megalomanský, nepraktický, dobrý jako teoretický)

Jak spolupracují vrstvy vertikálně?

Předávají si navzájem data+řídící informace vyšší vrstvy do nižší (encapsulation) příjemce v opačném směru postupně rozbalí, každá se stará o odlišnou část, dohromady uskuteční proces

Co nepatří mezi funkce protokolu?

Protokol=konvence/standard, podle kterého probíhá el. Komunikace a přenos dat – definuje pravidla syntaxe, sémantiky a synchronizace vzájemné komunikace (detekce spojení, handshake, vyjednání parametrů spojení, zahájení a ukončení zpráv, formát zpráv, co dělat se špatnými/poškozenými daty, detekce a reakce na ztrátu spojení, ukončení relace/spojení)

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

Multiplexing = sdílení kanálu více službami, Zapouzdření (encapsulation) = data+řídící informace vstvy n+1 do n, Segmentace = rozdělení aplikačních dat na transportní vrstvě, Fragmentace = další dělení dat na síťové vrstvě díky malé velikosti MTU (Maximum transmission unit) linkové vrstvy

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

Klient-server = klient zná pevnou adresu serveru, navazuje komunikaci, zadává požadavky, server obsluhuje více klientů najednou, download/upload (DNS, WWW, SMTP)

Peer-to-peer = partneři neznají pevné adresy zdroje dat, nejsou dané role=každý zároveň klient i server (Napster, Gnutella, BitTorrent)

Které tvrzení týkající se URI je správné?

Uniform Resource Identifier (adresování služeb) – textový řetězec s danou strukturou, k přesné specifikaci zdroje informace (dokument/služba) – jednotný systém odkazů, jeden klient pro více služeb (FTP ve WWW), členění na Locator a Name

URI `schéma://autorita[cesta][?dotaz][#fragment]`

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

Které z následujících tvrzení o doménových jménech je pravdivé?

Zleva od nejkonkrétnější po nejobecnější oddělené tečkami, poslední = TLD, nižší spravuje vlastník nejvyšší úroveň spravuje ICANN (.cz - CZ.NIC)

Jaký krok následuje poté, co www server připraví text stránky, rozdělí ho a naformátuje do TCP segmentů?

TCP Segment = celá jednotka vytvořená na transportní vrstvě => pošle na síťovou vrstvu a ta přidá IP src, IP

dst, typ

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

Pošle do Linkové vrstvy, ta připojí mac adresu zdroje a cíle, typ (FCS?)

Jaký krok následuje poté, co počítač, na kterém běží www server, přečte ethernetový rámec od síťové karty?

Vybalí z ethernetového rámce = přečte mac adresy (linková) – pošle výše (síťová)

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

Spojuje 7,6,5 OSI modelu, pravidla komunikace mezi klientem a serverem, stav dialogu, interpretaci dat/definuje: průběh zpracování na obou stranách, formát zpráv (text/binární, struktura), typy zpráv, sémantika zpráv a informačních polí, varianty průběhy dialogu, interakci s transportní vrstvou

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

(TCP/UDP) zodpovídá za end to end přenos dat, zprostředkovává služby sítě aplikačním protokolům, které mají rozdílné nároky na přenos, umožňuje provoz více aplikací na uzlu volitelně: spolehlivost přenosu dat, segmentuje data pro snazší přenos/zpětně skládá, řídí tok dat

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

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

Vyberte správné tvrzení o účelu a principu programu ping.

Program pro diagnostiku sítě (ověřuje funkčnost spojení, není potřeba spešl program na cílovém uzlu, nezaručuje dostupnost služeb – pouze síťové vrstvy)

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`?

Na žádný ICMP datagram nepřišla odpověď = problém se spojením po cestě nebo na cílové stanici (jedná se o loopback adress, někdo kdo otázku měl v testu tvrdil, že jediná odpověď co dávala smysl je že na počítači je špatně nainstalovaný IP software)

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

DNS

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

Pořadí bytů – big endian (1 = 0x00, 0x00, 0x00, 0x01) ale Intel má little endian (1 = 0x01, 0x00, 0x00, 0x00)

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

Dvojice speciálních znaků, proměnlivá na OS. Win CR LF, Mac CR, Linux LF

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

TCP, UDP (kombinace, SCTP, DCCP, MPTCP)

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

viz další

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

viz další

Které z následujících tvrzení správně popisuje činnost konkrétního aplikačního protokolu?

Jsou: DNS, SMTP (ESMTP), POP3, IMAP, FTP, HTTP, Telnet, SSH, SIP, NFS, SMB

Co označuje zkratka STP?

Shielded Twisted Pair - kroucená dvojlinka s kovovým stíněním nebo Spanning Tree Protocol – protokolu pro hledání koster grafu sítě (acyklické podmnožiny sítě – síť by se jinak zahltila přeposíláním rámců v cyklech)

Který aplikační protokol se používá k přenosu souborů?

FTP (SFTP), SSH

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

H.323 na ASN (Abstract syntax notation), SIP (používá RTP/RTCP Realtime Transport Protocol (control) dohodu pomocí SDP (Description) (zabalena v SIP)

Který aplikační protokol se používá pro elektronickou poštu?

SMTP, POP3, IMAP

Který aplikační protokol se používá pro sdílení systému souborů?

NFS (Network File System), SMB (Server Message Block)

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

DNS

Které z následujících tvrzení o RFC je pravdivé?

Request For Comments je prostředek standardizace internetu, mají různý charakter – standardy, informace, návody. Dokumenty se nemění, pokud je změna, prostě se vydá nové RFC – jeho platnost přepisuje starší), aktuální stav v indexovém souboru, zdaleka ne všemi dodržované, návrh RFC projde schvalovacím procesem IAB → IETF/IRTF → WG. Jsou veřejně přístupné.

Které z následujících tvrzení o povaze DNS protokolu je správné?

Klient-server aplikace, běžné dotazy do 512B UDP, jinak TCP, klient se obrací na servery definované v konfiguraci, postupně získává lepší informace, problematika zabezpečení (DNSSEC – komplikované, malé rozšíření zatím), jednotkou dat je Resource Record

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

DNS - rekurzivně se ptám serveru (nastavený uživatelem), ten nerekurzivně vyšších serverů, vždy odpověď na co nejkonkrétnější část „zadání“ - pak by už stejně neměl co říct

Které tvrzení o bezpečnostních aspektech protokolu DNS je správné?

Problematické, podpisy zabezpečené DNS (DNSSEC) je komplikované a rozšiřuje se pomalu – problémy jako cache poisoning = do sekce Authority a Additional je zadána jiná doména – redirekce (příklad provedení: nahradí IP adresy svými variantami, zkopíruje foldery původní hledané stránky a dá do nich malicious software)

Označte správné tvrzení o nameserverech.

Primární – spravuje záznamy o doméně, sekundární – stahují a uchovávají kopii dat o doméně, Caching-only – udržuje jen (ne)vyřešené dotazy po dobu platnosti, každá doména alespoň jeden, lépe více autoritativních NS (primární/sekundární), pro výměnu dat TCP, formát dotazu a odpovědi je ale DNS RR, aktualizace vyvolává sekundární server (v intervalech?) ale je možné vyvolat v případě potřeby přímo primárním serverem.

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

.cz

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

	FTP	SMTP
1xx	předběžná kladná odpověď	"accept, pošlu další zprávu
2xx	kladná (definitivní) odpověď	OK/Beru
3xx	neúplná kladná odp. (chci další příkaz/něco potřebuju)	Beru a něco chci
4xx	dočasná záporná odp. (je možné ptát se znovu)	Teď není čas (spam protecti
5xx	trvalá záporná odp. (nepodařilo se a neopakuj)	Neberu (graylisting)

Které z následujících tvrzení o používání poštovních protokolů je správné?

Které z následujících tvrzení o SMTP protokolu je správné?

Na základě SMTP(25), přímo nebo přístup přes POP3(110)/IMAP(143), kde POP starší – otevřený přenos hesla, dopisy lze stahovat jen celé, není možná práce se strukturou dokumentu, IMAP – novější, možnost šifrovaného spojení, podpora více stránek (složek), možnost vyžádat jen část dopisu, možnost vyhledávat v dopisech, paralelní příkazy, server uchovává informace (stav) o dopisech. (Šifrování přes příkaz STARTTLS (993)

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

(Mail-Forwarder, Mail Realy?) POP/IMAP – protokoly pro přístup (získávání zpráv) k poštovní schránce, SMTP pro best effort (delivery only!) doručování zpráv

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

Původně 7-bit ASCII, kódování souborů pomocí UUENCODE (z UUCP unix-to-unix-copy) = kódování ok ale chybělo systematické začlenění do dopisu – dnes rozšířené Multipurpose Internet Mail Extension (MIME) – umožňuje strukturovat dokument, pro každou část zadat: typ a formát obsahu, znakovou sadu a kódování, další info k zpracování a používat diakritiku – i v některých hlavičkách. Kódování Base64 pocházející z UUENCODE (jiná tabulka a formát řádek), Quoted-Printable – nonASCII znaky uloženy jako řetězce. MIME dnes používán hodně i mimo poštu.

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

Vyskytuje se: Date, From, Sender, Reply-To, To, Cc, Bcc, Message-ID, Subject, Received

Který příkaz není příkazem SMTP protokolu podle RFC 821?

Jsou (z prezentace (slide 67)): HELO (Pozor EHLO má novější ESMTP!), MAIL FROM, RCPT TO, DATA, QUIT Dle RFC 821 ještě jsou i: RSET, SEND/SOML/SAML FROM, VRFY, EXPN, HELP, NOOP, TURN

Které tvrzení o bezpečnostních aspektech poštovních protokolů je správné?

Které tvrzení o autenticitě původu dopisu je správné?

Dopis je otevřená listovní zásilka (řešení šifrováním obsahu, například pomocí PGP – Pretty Good Privacy). Nikdy není jistý odesilatel, ani shoda údajů v obálce a textu (řešení: Sender policy framework=pokus o zpětné doručení, nebo systémem výzva/odpověď, elektronickým podpisem) → neotevírat dopisy neznámého původu, server může vyžadovat autentikaci odesilatele pomocí ESMTP – příkaz AUTH, nebo klient pomocí ESMTP příkazu STARTTLS žádat o spojení pomocí SSL/TLS (šifrování je jinak obecně problémem uživatele ne serveru)

Jak označujeme protokol, kterým se přenášejí webové stránky?

HTTP – Hypertext Transfer Protkol

Co označuje zkratka HTML?

Hypertext Markup Language – (2014 verze HTML5) popisuje obsah i formu, konkrétní zobrazení v režii klienta (je aplikací staršího SGML – Standard Generalized ML, předchůdce XML – eXtensible ML)

Které tvrzení o povaze HTTP protokolu je správné?

Port 80, typicky TCP

Formát zprávy: úvodní řádka (požadavek/odpověď), doplňující hlavičky (požadavek: jazyk, kódování, stáří stránky, autentikace, odpověď: typ dokumentu, kódování, expirace) (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)

Odpověď na jeden požadavek je obvykle jeden dokument, Po jednom perzistentním spojení může jít postupně více požadavků, klienti si většinou otevírají více spojení. Požadavky jsou nezávislé, komunikace je bezestavová, stav je přenášen dodatečnými daty *cookies*

Jaké tvrzení týkající se cookies je správné?

Stav přenášený jako dodatečná data: server například vygeneruje cookies s identifikací spojení a pošle v hlaviččce klientovi, ten je pak při další komunikaci na daný server přidá do hlaviček požadavku (tak to třeba dělá PHP s jeho sessions). Cookies si může i prohlížeč vymyslet, nebo mít přiřazené například z Javascriptu. 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) a GET (do URL).

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

HTTP 1.0: GET, POST, HEAD

HTTP 1.1: GET, POST, PUT, HEAD, DELETE, TRACE, OPTIONS, CONNECT, PATCH

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

(Otázka z testu) „Ak chce dosáhnout dynamičnost stránky musí použít jazyk Java“ (Javascript) → něco v tomhle stylu

Poznámka: Java není Javascript. Obojí běží v klientovi. Java posílá nějak zkompilovanou binárku, Javascript posílá zdrojový kód a podobné jsou si akorát jménem. Je to špatná odpověď, protože dynamická povaha stránek může být dělaná i ze strany serveru, například pomocí reagování na cookies.

Vyberte správné tvrzení o dynamických WWW stránkách.

Dynamické stránky je možné nechat vygenerovat serverem, s využitím informací, které uživatel zadal, cookies

apod. Například jazyk PHP používá CGI nebo nějaký web server (třeba Apache) k vyprodukování dynamické web stránky. Generovat je samozřejmě může jakýkoliv jazyk, CGI umí využívat například Perl, Python... Nic vám nebrání napsat program, který vrací HTML pro webserver i v C# (viz ASP.NET), C++, C nebo dalších rozumných jazycích.

Nebo přímo klientem (nejčastěji Javascript – zdrojový kód interpretován přímo, méně často Java applety – mezikód interpretován za pomoci lokálních knihoven). Zde také existují další alternativy.

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

Telnet (23) nezabezpečený dnes využívaný v rámci LAN nebo při ladění jiných protokolů – využívá síťový virtuální terminál NVT – protokol přenáší oběma směry příkazy a odpovědi ale neumí je rozlišit, SSH nejenom ke vzdálenému přístupu ale obecně pro secure transfer dat. SSH využívá šifrování pro bezpečný přenos dat.

Které tvrzení o bezpečnosti přístupu přes SSH je správné?

Klient ověřuje server (na základě klíče, certifikátu)

Server ověřuje uživatele (heslo, výzvy a odpovědi (OTP), veřejný klíč klienta...)

Ověřovat klíč serveru - man-in-the-middle útok při změně klíče (SSH klient by měl řvát, že se změnil klíč)

Přihlášení bez hesla se váže na privátní klíč - zjednodušeně: necháte na serveru veřejný klíč (místo hesla), při připojení zašifrujete něco co vám dá server privátním klíčem, server si to vaším veřejným klíčem rozšifruje a zkontroluje, že to sedí. Privátní klíč nikdy nejde přes síť!

Nikdy recipročně bez hesla – ochrana proti červům

Co označuje pojem VoIP (Voice over IP)?

Obecné označení technologií pro přenos hlasu po IP

Co označuje pojem SIP (Session Initiation Protocol)?

Protokol, který se stará o navázání spojení dvou partnerů (vyhledat a spojit) pro komunikaci VoIP. Řeší jen signalizaci (vyhledá partnera a naváže spojení), přenos dat pomocí RTP/RTCP, Dohoda o datových kanálech řešena SDP (Description) – jeho data zabalena v SIP

Jak funguje protokol DHCP?

Používá protokol UDP k přidělení adresy počítači (IP adresa, maska sítě, implicitní brána, adresa DNS serveru) Port 67 (server listening) a 68 (klient) (Pro IPv6: 546 server, 547 klient) - UDP Pronájem adresy je časově omezený, po uplynutí 4/8 musí zažádat o novou, pokud ji dostane, běží lhůta od začátku, pokud ne, dokončí 4/8 a konec. (klient si vybírá z nabídky podle adresy/délky pronájmu..)

```
-> DHCPDISCOVER (Broadcastem)
<- DHCPOFFER
-> DHCPREQUEST  * klient si sám vybírá, který offer přijme
<- DHCPACK
-> 4/8 DHCPREQUEST (buď ACK nebo ticho zpět)
-> 7/8 DHCPREQUEST (opět ACK nebo ticho)
-> 8/8 DHCPDISCOVER
```

Jakým způsobem se synchronizují hodiny na počítačích v síti?

Pomocí Network Time Protokolu (123 UDP)

Proč se synchronizují hodiny na počítačích v síti?

Stejné timestampy souborů, možnost porovnávání událostí na různých počítačích – teoreticky by se dalo i bez NTP ale bylo by zbytečně nepohodlné (přepočítavat časové rozdíly mezi uzly atdp.) (Platnosti certifikátu? Od kdy do kdy platí? - aby pro všechny bylo synchronizované)

Které tvrzení o povaze FTP protokolu je správné?

Port 21 command, 20 na přenos dat, je nešifrovaný, používá se spíše na anonymních serverech, pasivní a aktivní spojení kvůli firewallům, možno vyvolat Third Party Transfer

Které z následujících tvrzení o bezpečnostních problémech FTP je správné?

Heslo se přenáší otevřeně. Používá se jen tam, kde nehrozí nic bezpečnostního (anonymní přístup k serveru). - k volně šiřitelným datům (heslo=email apod.)

Která charakteristika TCP není správná?

Platí: použití pro spojované služby, klient naváže spojení – data tečou ve formě proudu (streamu), spojení (relaci) řídí TCP nikoliv aplikace, má velkou režii, je komplikované, (příp. méně pravidelné ale bezeztrátové)

Jaké postupy používá TCP, aby zajistilo spolehlivost přenosu?

Přijímající strana posílá ACK na data, která dostala ACK (číslo které očekává). (wiki) 100 101 102 103 ... <- ACK 104 (chci 104ku), používá sekvenční číslo k identifikaci všech odeslaných packetů, popořadě. Zasílá kontrolní součet u každého packetu, aby se popř. dalo poznat, že je packet poškozený.

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

„windowing“ = potvrzení nejpozději každého n-tého packetu (místo každého) = klient čeká na odpověď po odeslání n packetů – „všechny v téhle sadě dorazily, můžes poslat další sadu“

Co usoudíme z následujícího popisu paketu v programu tcpdump?

Návod na čtení

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

Zobrazí výpis všech aktivních spojení TCP a UDP a porty na kterých naslouchají spuštěné procesy (-an (n) v příkazu: IP adresy v Foreign adress v číselné podobě – není použit reverzní převod pomocí DNS na jména) Proto, Local Adress, Foreign Adress, State

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

Seq# nebo zdrojový port

Jakou informaci najdeme v záhlaví TCP i UDP?

Destination Port, Source Port, Checksum, Data

Které tvrzení popisuje správně TCP resp. UDP?

TCP – viz výše, UDP – pro nespojované služby, neexistuje „spojení“, data jsou nezávislé zprávy, UDP jednoduché – musí řídit aplikace, (pravidelný tok za cenu vyšší ztrátovosti)

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

Sequence number = příjemce si pakety srovná (na transportní vrstvě)

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

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

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

80

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

Co se odehrává během three-way handshake?

Je to pripajanie clienta na server pomocou TCP protocolu (synchronizace Seq numbers mezi klientem a serverem)

```
 Client ----[SYN = 1, Seq_number = c,     ACK = 0    ]----> Server
Client <---[SYN = 1, Seq_number = s,     ACK = c + 1]----- Server
Client ----[         Seq_number = c + 1, ACK = s + 1]----> Server
```

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

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

2. Server odpoví datagramem s nastaveným příznakem ACK
3. Server odešle datagram s nastaveným příznakem FIN
4. Klient odpoví s nastaveným příznakem ACK
5. Tím je spojení ukončeno

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 termín, který není funkcí síťové vrstvy.

viz níže

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

Funkce: přenos dat předaných transportní vrstvou od zdroje k cíli, pro tuto činnost jsou: Adresace – protokol definující tvar a strukturu komunikačních adres partnerů, Encapsulation – zapouzdření – data (+IP src/dst, typ) zapouzdřena do PDU, Routing – směrování = vyhledání nejvhodnější cesty k cíli přes mezilehlé sítě, Forwardování – přeposílání = předání dat ze vstupního síťového rozhraní na výstupní, decapsulation, NAT (IP masquerading), ARP, RIP, ICMP, Ping, TTL

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

IP adresa zdroje a cíle, typ

Jaký protokol poskytuje na síťové vrstvě službu spolehlivého přenosu dat?

Žádný co sme brali → "Žádná odpověď není správná" na síťové vrstvě (na transportní je to TCP)

Jaký protokol poskytuje na síťové vrstvě službu nespolehlivého přenosu dat?

IP

Označte nepravdivé tvrzení o přidělování IP adres.

Centrální IANA, 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.

DHCP, link local adresy, administrátorem přidělena manuálně

Označte pravdivé tvrzení o autonomních systémech (AS)?

Def: Blok sítí se společnou routovací politikou, zavedeny pro snazší routování na globální úrovni – externí routovací protokoly EGP – dnes používaný Border Gateway Protokol BGP (Identifikátor 16 bitové číslo, dnes

přechod na 32 bitová.)

Kolik bitů má IPv6 adresa?

128

Který z následujících protokolů nepracuje s IP adresami?

? = protokoly na síťové vrstvě nebo i třeba DNS a FTP (Směrovací protokoly, Link State, ARP, IP)

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, 0 = část IP adresy pro počítač (první byte rozhoduje o třídě sítě, dnes spíše classless mód = za IP adresou /počet bitů prefixu určujícího síť)

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 této síti“ nesmí opustit síť

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

Implicitní/Subnetting rozšířením síťové části adresy (pomocí síťové masky), classless mód (různé masky = variable length subnet mask VLSM) (Supernetting), speciální adresy by design/definition

Unicast – zasílání paketů pouze jedinému cíli (uzlu/stanici)

Multicast – Posláno na IP adresu cílové skupiny (poslána ale jen jediná zpráva ta dorazí všem v dané skupině – místo vysílání stejné zprávy všem jednotlivcům)

Loopback - 127.0.0.1/8 - packety, co jsou sem poslány jdou ihned zpět jako příchozí.

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

Implicitně – třídy A,B,C,D,E viz slide 121

Vše záleží na zadání/možnostech odpovědí obecně znovu slidy 121-126

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

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

Která následujících adres představuje korektní adresu počítače?

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

Vše záleží na zadání/možnostech odpovědí obecně znovu slidy 121-126

Které tvrzení o směrování je pravdivé?

Měla by umět každá stanice v TCP/IP síti, maska vyjadřuje uvažovanou část adresy cíle, typy: direct – přímo připojená síť (gateway = vlastní adresa), indirect, default, záznam implicitní – automaticky po přiřazení adresy do rozhraní, explicitní – ručně zadán příkazem, dynamický – v průběhu práce od partnerů v síti

Vyberte správné tvrzení o principu směrovacího algoritmu.

Zvol nejspeciálnější záznam (nejdelší maska) → existuje (ne = není cesta), můj stroj (ano = vrať na vstup), moje síť (ano = pošli příjemci) – ne pošli směrovači

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)

Vyberte správné tvrzení o činnosti routeru.

Router (směrovač) je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI (síťová vrstva). Router spojuje sítě (pozor: switch spojuje počítače v místní síti = rozdíl)

Které tvrzení o metodách řízení směrovacích tabulek je pravdivé?

Statické – cesty se navazují při startu, nepružné při změnách, problémy se subnettingem, nesnadné zálohování spojení, méně citlivé na problémy v síti, dostupné i ve zcela heterogenním prostředí → vhodné pro jednodušší stabilnější sítě Dynamické – Routery si navzájem vyměňují informace o síti pomocí routovacího protokolu – jednoduché změny konfigurace, síť se dokáže sama „opravovat“, směrovací tabulky se udržují automaticky, citlivější na problémy/útoky, na počítači musí běžet program obsluhující protokol (routed, gated, BIRD a pro lokální sítě např. RIP a OSPF)

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

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

Podívejte se na tabulky `netstat -r` nebo na net

Označte pravdivé tvrzení o distance-vector routovacích protokolech.

Uzel má u záznamů ve směrovací tabulce i „vzdálenost“, svou tabulku periodicky posílá sousedům, ti si upraví svou tabulku a v dalším taktu ji posílají dál, jednoduché – snadno implementovatelné, Nevýhody: pomalá reakce na chyby, metrika špatně zohledňuje vlastnosti linek (rychlost, spolehlivost, cenu), chyba ve výpočtu jednoho routeru ovlivní celou síť – vznik routovacích smyček

Označte pravdivé tvrzení o link-state routovacích protokolech.

Každý router zná „mapu“ celé sítě, routery si navzájem sdělují stav svých linek a podle toho si každý modifikuje mapu své sítě. Nevýhody: náročnější na výkon CPU a paměť, při startu na nestabilních sítích může výměna dat znamenat velkou zátěž sítě. Výhody: pružně reaguje na změny topologie, každý počítá sám za sebe, chyba neovlivní ostatní, síť je možné rozdělit na menší podsítě (rychlost výpočtu), výměna dat probíhá pouze při změnách.

Jakou informaci z paketu používá každý směrovač pro určení cesty?

IP adresu cíle

Jaké pole IP záhlaví za normálních okolností mění router?

TTL (normální okolnost? (pro sítě za NAT = změna port/IP/MAC))

Označte existující pole (sloupec) routovací tabulky.

Network Destination, Netmask, Gateway, Interface, Metric

Jakým příkazem můžeme vypsat obsah routovací tabulky?

`netstat -r` (případně spolu nějakým dalším přepínačem, `-rn`, `-nr`). `netstat --route` je ekvivalentní.

Které pole IP záhlaví brání vzniku nekonečné smyčky při doručování?

TTL (Time to live)

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

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)

Jaký účel plní default gateway?

Když počítač nezná cestu k danému IP (v lokální síti), vyšle packet na default gateway (router) – ten propojuje sítě takže packet přes něj bude poslán dál

Co se stane, pokud cíl není nalezen v routovací tabulce?

Packet je poslán skrz default gateway – pokud takový záznam v tabulce je, pokud by nebyl – default gateway odpoví ICMP „No route to host“

Která z charakteristik IP filtrování je správná?

Router na perimetru obsahuje informace o tom, jaké IP adresy propouští.

Přísná konfigurace: ven vybrané, dovnitř nic (dobré pro protokoly s jedním kanálem HTTP/SMTP), problém u protokolů s více kanály (FTP/SIP)

Obvyklá konfigurace: ven cokoliv, dovnitř nic – problém třeba s aktivním FTP přenosem, nepoužitelné u protokolů s více kanály (SIP), problém se službami „uvnitř“ (www server, pošta) – lepší oddělený segment=demilitarizovaná zóna

IP filtrování typicky využívá vyšších vrstev než jen síťové.

Která z charakteristik překladu adres (NAT) je správná?

IP Masquerading, router na perimetru privátní sítě „překládá“ privátní adresy na veřejné (nebo jiné privátní ve vnořených sítích), router přepíše IP source na svou vlastní a port na některý ze svých volných – když přijde odpověď zpět v tabulce zjistí podle portu na který přišla, na jaký port a IP v síti má data poslat (viz slide 36)

Která z charakteristik proxy serveru je správná?

Je software na routeru (transp.) nebo i separátní server (může být v netransp.), který stíní klienta přímo od serveru - funguje jako prostředník. Správce sítě může kontrolovat činnost klientů popř. omezit objem provozu na přípojné lince… * Transparentní – SW na routeru, zachytí a uloží požadavek, svým jménem naváže spojení dál (stejně opačně) – není třeba konfigurovat * Netransparentní – je třeba nakonfigurovat aby se požadavky neposílaly přímo, ale na proxy-server v lokální síti (nemusí být router), je nutná podpora protokolu

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

Router/Firewall/Proxy server

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

(Obrázek)

Které tvrzení o ARP je pravdivé?

Konverze MAC a IP adres, neznámá adresa se zjišťuje broadcastovou výzvou, výsledky se ukládají do ARP cache (odpovídající si přidává informace o tazateli), nejde ověřit pravost/správnost odpovědi, neopouští lokální síť, můžu dostat i nevyžádaně (gratious), `arp -a`

Jaké funkce plní ICMP (Internet Control Message Protocol)?

Posílání řídících informací pro IP, používá IP datagramy (ale není transportním protokolem), Time Exceeded (vypršel TTL), Redirect, Echo/Echo Reply (testování dosažitelnosti – `ping`), Parameter problem (chyba v záhlaví datagramu)… vyhledávání routerů, žádost o snížení rychlosti toku datagramů atdp..

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)?

Podvrstva linkové vrstvy umožňující různým protokolům síťové vrstvy přístup ke stejnému médiu (Multiplexing)

Co označuje termín MAC (Media Access Control)?

Podvrstva linkové vrstvy, má na starosti adresaci uzlů a kontrolu přístupu k médiu – kdo, kdy jak může data odesílat a jak je přijímat

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

Deterministicky - riadi sa pravidlami ktore neobsahuju prvok nahody, pravidla su nastavene tak, aby v konecnom case viedli k cielu, aby sa kazdy uzol, ktory usiluje o medium aj k nemu dostal Nedeterministicky - riadi sa pravidlami ktore obsahuju aj niaky prvok nahody, nie je na 100 percent garantovane, ze sa uzlu podari ziskat pristup k mediu, lahsia implemetacia

Které tvrzení o topologii sítě je pravdivé?

(Slide 153)

Topologie sítí = zapojení různých prvků do sítě a zachycení jejich reálné a logické podoby „tvar/struktura sítě“ → Point-to-point/Multipoint (Sběrnice, hvězda, Kruh)

Které z tvrzení o Ethernetu je správné?

Momentálně vůdčí technologie pro lokální sítě, schopná pružně reagovat na progresivní vývoj HW, přizpůsobí se širokému spektru přenosových médií, na Multipoint spojích řízení přístupu pomocí CSMA/CD (na detekci vysílá „jam signál“, exponenciální čekání po 16 pokusech končí chybou), Adresy – 3 byty prefix (výrobce/multicast), 3 byty adresa, dřívě vypálená v kartě dnes nastavitelná

Formáty: Ethernet II, IEEE 802.3 (pozn. není to protokol!)

Které tvrzení o WiFi je správné?

(Poznámka: není to protokol!)

Bezdrátová síť (WLAN), topologie je hvězda, mnoho variant – souhrně IEEE 802.11x (x=a/b/g/n/y)

SSID (Service set ID): řetězec 32 znaků pro rozlišení sítí, Struktura: ad-hoc peer-to-peer = dva klienti navzájem rovní, infrastruktura acces pointů = několik AP které vysílají své SSID, WiFi zařízení dnes všude, problém bezpečnost, (kolize řeší pomocí CSMA/CA)

Co je základní funkcí CSMA/CD? Např. Ethernet

Detekce kolizí – 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

Jak lze charakterizovat repeater, hub, bridge a switch?

Repeater (opakovač) (ve struk. kabeláži hub, rozbočovač) – spojuje segmenty na fyzické vrstvě, řeší větší

dosah (překonává útlum kabelu), neřeší: propustnost (problém kolizí naopak zhoršuje)

Bridge (most) (ve struk. kabeláži switch, přepínač) – spojuje segmenty na linkové vrstvě, řeší: větší propustnost (rozděluje kolizní doménu)

S jakými adresami pracuje hub, přepínač resp. směrovač?

Hub – žádné, Switch - MAC

Jak lze charakterizovat Spanning Tree Protocol resp. Spanning Tree Algorithm?

Protokol pomocí kterého se switche domluví, který z nich nemá forwardovat a bude jen sledovat provoz = najdou minimální kostru grafu a tím zamezí cyklům, STP má nezbytné timeouty – start portů je pomalý, STA lze na portu potlačit „faststart“

Jaké tvrzení o VLAN je pravdivé?

Virtual Lan – prostředek jak po jedné fyzické síti provozovat více nezávislých lokálních sítí, sítě označovány 12bitovým identifikátorem (VLANID), Ethernetový rámec je prodloužen o 32 bitový tag (tagovat může switch, pro koncovou stanici transparentně)

Co označuje termín CRC?

Cyclic Redundancy Check (Cyklický kontrolní součet) – hashovací funkce používaná pro kontrolu konzistence dat, posloupnost bitů považovaná za koeficienty polynomu (ve dvojkové soustavě), ten je vydělen charakteristickým polynomem – zbytek po dělení převeden zpět na bity a použit jako hash = jednoduchá implementace, velká síla

Jaký hlavní smysl má zápatí (trailer) linkového rámce?

Obsahuje FCS (Frame check sequence) = kontrolní součet např pomocí CRC

Kolikrát proběhne výpočet CRC (pro Frame Check Sequence) během přenosu zprávy mezi koncovými zařízeními na obrázku?

Tolikrát kolik je zařízení na dráze přenosu (zdrojový PC, každý router, koncový PC – na switchi ne)

Do hubu jsou zapojeny stanice A, B, C a D. Stanice A je právě uprostřed vysílání rámce stanici D, když stanice B potřebuje vysílat data stanici C. Co musí stanice B udělat?

Počkat než AD dovysílají – jinak kolize

Do switche jsou zapojeny stanice A, B, C a D. Stanice A je právě uprostřed vysílání rámce stanici D, když stanice B potřebuje vysílat data stanici C. Co musí stanice B udělat?

Odeslat svá data (na nic nečeká)

Které tvrzení o médiích používaných v počítačových sítích je správné?

Metalické (kabel) – elektrické pulzy, Optické – světelné pulzy, Bezdrátové – modulace vln

Kolik vodičů obsahuje kabel označovaný jako nestíněná kroucená dvoulinka (UTP)?

8

Jaké tvrzení o kabelech pro propojení dvou uzlů ethernetové sítě je pravdivé?

Dnes standardně UTP – nestíněná kroucená dvoulinka = 4 páry Cu vodičů navzájem zakroucené, pozor na přímý/křížený kabel – dnes obvykle autodetekce, alternativě kabel s kovovým stíněním STP

Jaký je rozdíl mezi jednovidovým (SM) a mnohovidovým (MM) optickým kabelem?

Optická vlákna – jednovídová (singlemode) svítí se laserem, větší dosah, šířka pásma, cena Mnohovídová (multimode) – svítí se led, horčí než SM kromě ceny

Jaký typ adres se používá na linkové vrstvě?

MAC

Jaký typ adres se používá na fyzické vrstvě?

Žádné

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

Prý v odpovědích hlouposti, správná odpověď „MAC“ - prostě vědět co je MAC (fyzická/HW adresa)

V jakém případě není nutná adresace cílového počítače?

Broadcast/Multicastová adresa

Se kterou vrstvou OSI je svázán pojem Ethernet?

Linková = 2.

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.