Souhrn a otázky do sítí

A to se Forste vyplatí

Autor: Milan Veselý

Obsah

Užitečné odkazy

https://www.ksi.mff.cuni.cz/teaching/nswi141-web/pages/
https://github.com/petrroll/mff-stuff/blob/master/site/site_2016.md

Úvodní prezentace – požadavky přenosu, dělení sítí, RFC

Komunikace obecně

Druhy, atributy, přenos zpráv a další věci, který nikoho nezajímají

Požadavek na odolnost elektronické komunikace

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

Přepojování okruhů – pevná cesta pro komunikaci

Rychlejší, plynulejší, ale spojení se při výpadku rozpadne

Přepojování paketů – každý paket jde svoji cestou

Výpadek není fatální, různá doba přenosu paketů

Další požadavky

Bezpečnost dat a bezpečnost infrastruktury

Metody: ověřování uživatelů, kontrola práv, inspekce dat, kryptografie, …

Rozšiřitelnost

LAN: 3 části: core, který je připojený na IS providera, distribution, a access

WAN: Tier 1-3, od těch připojených na páteř až po ISP a domácnosti

Přenosové parametry

Který z následujících termínů nepatří mezi přenosové parametry počítačové sítě? – …

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

Zpoždění (latence, delay)

Pravidelnost (jitter, rozptyl zpoždění)

Ztrátovost dat

Šířka pásma (bandwidth, „rychlost“)

Různé potřeby služeb:

Real time multimédia (videohovor) potřebují dobrou latenci a jitter, …

Obecně multimédia potřebují malý jitter

Data přenosy (WWW, SMTP) potřebují úplná data (nízká ztrátovost dat)

Proto se používá QoS tag

Dělení sítí

Které z následujících tvrzení týkajících se WAN/LAN je pravdivé? – …

Dělíme na LAN, WAN, MAN (ale neexistuje přesná definice)

LAN – sdílení souborů s blízkými zařízeními, většinou limitované budovou, …

Jednotné vlastnictví a řízení, sdílení prostředků (zařízení)

WAN – vzdálený přístup, komunikace, více vlastníků, větší latence, …

A taky na public a private podle toho, jestli je většinou vlastní uživatel

Private může být i virtuální – VPN (spojení dvou private dálkově - tunelem)

Historie internetu

… lol, historie

RFC – Request for Comments

Které z následujících tvrzení o RFC je pravdivé? – …

Způsob jak standardizovat internet (dříve pouze zajímavé návrhy)

Řada dokumentů popisující internetové protokoly (standardy, návody, …)

Pouze doporučení – ne všichni je tedy dodržují

Volně šiřitelné a veřejně přístupné

Místo změn se vydávají nové dokumenty („Obsoleted“, „Updated“)

Schvalovací proces Internet Advisory Board → IETF, IRTF → working groups

Struktura sítě – architektura, model (vrstvy)

Síťový model

Udává počet, strukturu a dělení práce vrstev

Proč dělit do vrstev? Snazší popis, dekompozice a změna technologie.

Příkladem je OSI model

Síťová architektura

Nadřazený pojem modelu

Kromě něho potřebuje i další technologie a protokoly

Zástupcem je TCP/IP

OSI model

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

Označte nepravdivé tvrzení ohledně vrstevnaté struktury sítí. – … Pravda je, že je to snazší na dekompozici a popis, díky tomu, že rozděluje práci více vrstvám. Příklad je nepraktický OSI…

Nepraktický a megalomanský, ale vhodný pro výuku (ale IRL TCP/IP architektura)

7	Aplikační	Předání dat aplikacím a přijímání požadavků uživatele
6	Prezentační	Oprava a konverze dat pro různé systémy (endianita, …)
5	Relační	Řízení dialogu (inicializace, konec, …)
4	Transportní	Stará se o přenos datových bloků (celkovost dat, …)
3	Síťová	Přenos dat mezi dvěma uzly sítě (hledání cesty, …)
2	Linková	Koordinace přenos dat mezi dvěma propojenými uzly
1	Fyzická	Fyzický přenos bitů mezi uzly

Vrstvy OSI modelu

OSI standardy (X.400, X.500, …)

Implementace OSI byla na základě komplikovaných standardů (pošta, …)

TCP/IP architektura

<table>
<tr><td>7</td><td rowspan="3">Aplikační</td><td rowspan="3">FTTP,
HTTP,
SMTP</td><td rowspan="3">DNS,
SIP</td><td rowspan="3">NFS,
XDR,
RPC</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td></tr>
<tr><td>4</td><td>Transportní</td><td colspan="2">TCP</td><td>UDP</td></tr>
<tr><td>3</td><td>Síťová</td><td colspan="3">IP</td></tr>
<tr><td>2</td><td rowspan="2">Síťové
rozhraní</td><td colspan="3" rowspan="2">Ethernet, FDDI, ATM, WiFi, …</td></tr>
<tr><td>1</td></tr>
</table>

Další otázky

Co nepatří mezi funkce protokolu? – Protokol jsou pravidla (standard) pro přenos dat v el. Komunikaci. Definuje pravidla syntaxe, sémantiky, synchronizace vzájemné komunikace (Handshake, detekce spojení, zahájení a ukončení spojení, detekce poškozených dat, …)

Jak spolupracují vrstvy vertikálně? – Vrstvy si navzájem předávají data a řídící informace (zapouzdření – encapsulation) Odesílatel jde od vyšší od nižší a příjemce obráceně

Spojované služby

Connection-oriented (spojované)

Protokolem používaným pro spojované služby je **TCP**

Protokol se o všechno postará, takže aplikace může být jednoduchá

Segmentace dat, rozesílání paketů, kontrola přijetí, …

Je tedy zaručeno spolehlivé (reliable service) dodání dat

Connectionless (nespojované)

Opačný přístup má protokol **UDP**

Aplikace se musí starat o všechno, protokol je tedy velmi prostý

Aplikační vrstva může lépe řídit provoz

Aplikační modely

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

Klent-server

Klient navazuje komunikaci a zadává požadavky

Jeden server má obvykle více klientů

Download x upload

Peer to peer

Každý je zároveň klient a server

Partneři neznají pevnou adresu zdroje dat

Bittorent, Gnutella …

Adresování počítačů

Která následujících adres představuje korektní adresu počítače? – …

Linková vrstva (HW) fyzická MAC adresa (např. ethernet: 8:0:20:ae:6:1f)

Označte pravdivé tvrzení týkající se MAC adres (ve fungující síti). – … (prý tam jsou nonsense, takže pohoda)

Jaký typ adres se používá na linkové vrstvě? – MAC

Jaký typ adres se používá na fyzické vrstvě? –chyták, na fyzické vrstvě se nepoužívají žádné adresy

Dříve byla (vypálená) dána výrobcem, dnes se dá ale změnit

Nerespektuje topologii a nedá se používat pro směrování

nemá pevně daný prefix a sufix

Síťová vrstva (SW) IP adresa (např.: 194.50.16.71, ::1)

Která vrstva OSI pracuje s IP adresami? – 3. vrstva (síťová)

Podle topologie, jednoznačně určuje síť a v ní počítač (prefix, sufix)

Transportní vrstva porty (druhá část socketu po IP adrese)

Aplikační vrstva (uživatel) doménová adresa URI/URL (lze z ní určit IP a port)

Doménový systém

Které z následujících tvrzení o doménových jménech je pravdivé? – … zleva doprava od nejméně významného (dělí je tečky)

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

Domény nejvyšší úrovně (TLD)

Správce ICANN

Např. arpa, com, edu, org, cz, …

TLD .cz

Správce CZ.NIC

SLD a nižší domény (např. cuni.cz)

Správce vlastník

IP adresy

Označte nepravdivé tvrzení o přidělování IP adres. – …

Každý uzel v síti musí mít IP adresu

Dvě verze IPv4 (4 bytes) a IPv6 (16B)

Veřejné adresy (přidělené ISP…) x Privátní adresy (nepřístupně z internetu)

Privátní router překládá přes Network Address Trnaslation (NAT)

Adresa počítače (přidělená administrátorem LAN)

Statická – každý uzel má předdefinovanou x Dynamická – dostane na žádost

Volná – kdokoliv se může připojit x Omezená – host se musí autorizovat

Přidělování administrátorem podle těchto pravidel platí i pro privátní adresy, výjimkou je ale link-local, kde si počítač vybere adresu sám, potom ale může komunikovat jen přímo s dalším link-local

Port

Se kterou vrstvou TCP/IP je svázán pojem port? - Transportní

K čemu se používají porty v OSI 4? – na základě adresy bychom neznali konkrétní službu ke které se připojit (číslo aplikace)

16-bitové celé číslo na identifikaci konkrétní služby

Destination port – musí ho znát klient (většinou je to nějaká well-know service)

Source port – přidělí ho odesílatel z nějakých nepoužívaných čísel

Well-know services

FTP (21), SSH (22), SMTP (25), DNS (53), HTTP (80/443) , SIP

Socket

Jeden konec komunikace, který je identifikovaný IP adresou a portem

TCP/IP připojení je jednoznačně identifikováno pěticí:

zdrojová IP, zdrojový port, cílová IP, cílový port, typ transportního protokolu

Dva kanály mezi dvěma počítači se liší alespoň v zdrojovém portu

Stejná čísla portů můžou být použity pokud je jiný transportní protokol

Princip překladu adres – NAT

Která z charakteristik překladu adres (NAT) je správná? – …

Počítače s privátní adresy jinak nemohou komunikovat s internetem

Princip je takový, že router upraví obsah paketu

Router uloží příchozí socket a nahradí adresu svojí adresou + náhodně vybere port

Až dostane odpověď, tak ji nastaví na původní adresu a dá to klientovi

Adresování služeb

URI

Které tvrzení týkající se URI je správné? – …

Jednoduchý systém odkazů (adresovací metoda)

HTML linky musí umět adresovat různé služby v jednom klientovi

Historicky platilo URL=umístění, URI=název, nyní jsou zaměnitelná

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

Schéma je používaný protokol

Autorita = [jméno[:heslo]@]adresa[:port]

Cesta – podobná cestě ve file systému

Dotaz – např. data z HTML formuláře

Fragment je identifikace lokace na stránce

Datový tok v TCP/IP

Klient zadá URL a aplikační vrstva předá data, adresu a port transportní vrstvě

Transportní vrstva přidá IP a spolu s daty to předá síťové vrstvě

Síťová vrstva – zjistí next-hop (buď ve stejné síti a nebo venku – pak se najde router, který ty data umí poslat do cílové sítě) a pošle data s next-hopem do linkové vrstvy

Linková vrstva – spojí dva next-hopy a pak to předá síťové a buď další hop nebo výš

Multiplexing, zapouzdření

Jaká informace se přidává do paketu během zapouzdření na síťové vrstvě? – zdrojovou a cílovou IP adresou a „transport layer portocol number (typ) a tím vytvoří packet

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

Multiplexing znamená, že více kanálů používá stejný kanál na nižší vrstvě

(spojení více kanálů do jednoho fyzického spojení)

Každý kanál musí dodržovat pravidla – takzvaný protokol, více protokolů může být použito zároveň v jednu chvíli na jedné vrstvě

Protokolu na vrstvě *n* definuje PDU (Protocol data unit) formát *(jednotka dat)*

Software dokončí práci na vrstvě *n* a pošle to dál do *n-1* s commandem

Na to dostane odpověď o úspěchu/neúspěchu

Říká se té výměně interface a formát toho je IDU

Vrstva *n-1* změní command na header a data na body

Hlavička musí například obsahovat identifikaci vrstvy

Celkově se této metodě říká zapouzdření (encapsulation) data vrstvy *n* do dat *n-1*

Příjemce musí provést decapsulation a demultiplexing (kontrola těla a nahoru)

Typy PDU (Průběh přenosu)

Aplikační odešle buď zprávu (nespojované) nebo proud dat (spojované) a pošle to se socketem vhodnému protokolu na transportní vrstvě

Pokud je použito TCP, tak transportní data rozbije na menší bloky a připojí hlavičku s cílovým portem, zdrojovým portem, offsetem rozdělení dat a další

UDP přidá akorát čísla portů a pošle to síťové

Síťová vrstva přidá hlavičku se zdrojovou a cílovou adresou a „transport layer portocol number“ a tím vytvoří packet. Pak to zjistí, jestli to může předat rovnou a nebo to poslat do next-hopu

(Data) linková vrstva vezme paket a připojí mu zdrojovou a cílovou adresu a protože je to poslední softwarová vrstva, tak to PDU (nazývané frame) přidá koncovku nazývanou FCS, kterou vypočítá, aby se dala ověřit správnost dat

Fyzická to prostě přesune a pak to passne linkové

Linková přepočítá FCS a MAC adresu aby zjistila, jestli je to pro ni a podle network code to dá dekapsulovaný síťové

Síťová zkontroluje IP a pošle to do vhodné transportní

Transportní se opět liší podle UDP a TCP…

Bezpečnost – kryptografie, SSL

Autentikace (autentizace, autentifikace) - proces ověření identity

Autorizace – vymezení oprávnění pro daný subjekt

Lokální autentikace: znalost hesla, sw klíč nebo hw token, biometricky

Vzdálená autentikace: u hesel si musíme dávat pozor na odposlech

jednorázová hesla nebo kryptografie (šifrování kanálu)

navíc dost protokolů nemá jak ověřovat a musí být rozšířeny

framework SASL (Simple auth…)

hodí se taky možnost používat autentikační server a protol

centralizace ověřování

One-time password – nereplikovatelná plain textová autentikace uživatele

Dříve byl vytištěný seznam

Pak challenge response (server pošle náhodný kód a klient spočítá odpověď)

Nyní se používá malý hw token, který je přesně časově synchronizovaný se servrem

Kryptografie

Šifrování dat

Jaké tvrzení o symetrických a asymetrických šifrovacích algoritmech je pravdivé? – …

Symetrické

Oba partneři musí znát metodu (subsituce, transpozice, mřížka, …)

Dnes na základě matematiky

Jsou velmi rychlé a hodí se na velká data, pořád ale oba musí mít klíč

Asymetrické

Způsob jak bezpečně předat data přes nezabezpečený kanál

Použít dva klíče – jeden pro šifrování a jeden pro dešifrování

Jednocestná funkce (hledání činitelů velkého součinu a nebo diskrétní logaritmus)

Je to ale na dlouho a navíc musíme věřit veřejnému klíči

Heshování – vytvoření krátkého kódu z textu

Uplatnění v kontrole shody, hledání v tabulce, …

Kód není jednoznačný, takže musíme přimout riziko nebo to dělat částečně

Jaké vlastnosti musí splňovat hashovací algoritmus pro použití v kryptografii? – …

Musí platit, že malá změna původních dat způsobí zásadní změnu

Tedy je kód takzvaně téměř jednoznačný

Funkce je jednocestná a tedy najít text, který má stejný kód je obtížné stejně jako najít jiný text se stejným kódem

Šifrování dat

Na jakém principu funguje šifrování elektronické pošty? – …

Pro efektivní šifrování používáme kombinaci sym. a asym.

Symetricky zašifrujeme data (text), zašifrujeme symetrický klíč veřejným klíčem příjemce. Příjemce klíč svým soukromým klíčem dešifruje a …

Další výhoda je, že šifruji data pouze jednou pro více příjemců

Elektronický podpis

Na jakém principu funguje elektronický podpis? – …

Kombinace asymetrie a hashe

Odesílatel spočítá hash (zašifrovaného či nezašifrovaného) textu a zašifruje ho private klíčem. Potom ho spolu s textem a parametry hashe pošle přijemci

Příjemce rozšifruje veřejným klíčem přijatý hash a potom spočítá hash textu a to pak porovná. Z toho zjistí, jestli odesílatel uměl pracovat s private klíčem a jestli zpráva byla změněna

Diffie-Hellman algoritmus

Které tvrzení charakterizuje Diffie-Hellmanův algoritmus? – …

Metoda, která umožňuje dvěma partnerům dohodnout se na společném tajemství přes nezašifrovaný kanál pomocí prvočísel

Je založen na jednocestných funkcích a strany si posílají pouze výsledku diskrétních logaritmů

Postup

Alice vygeneruje tajné a a veřejná prvočísla p a q
Spočítá si $A = p^a \bmod q$ a pošle p, q a a Bobovi
Bob si zvolí tajné číslo b, spočítá $B = p^b \bmod q$ a pošle B Alici
Alice si spočítá $s = B^a \bmod q$ a Bob si spočítá $s = A^b \bmod q$

Princip: $A^b = (p^a)^b = p^{ab} = (p^b)^a = B^a$

Klíč

Které tvrzení o klíčích a certifikátech je pravdivé? – …

Jak zjistit u asymetrického šifrování autenticitu klíče?

Ke klíči připojíme identifikační značku a necháme ho někým potvrdit

Buď někým komu již důvěřuji – web of trust = Klíč je publikován a ověřen uživateli (následně se o něj rozroste síť důvěry)

Veřejně uznávaná certifikační autorita, to ale není zcela stoprocentní

Certifikát

Je klíč doplněný o identifikaci vlastníka a podepsaný autoritou

Struktura certifikátu podle X.509:

Certifikát: verze, sériové číslo, vydavatel, doba platnosti, vlastník, …

Elektronický podpis a algoritmus pro elektronický podpis

SSL, TLS

Jaké tvrzení o SSL resp. TLS je pravdivé? – …

Jak zabezpečit TCP/IP?

Mezivrstva mezi transportní a aplikační, která umožňuje autentikaci a šifrování

Původně se jmenovala Secure Socket Layer a protkoly s ní používají na konci „s“

SSL bylo od verze 3.0 přejmenován na TLS (starší verze jako 1.0 jsou nedopručeny)

Aplikační vrstva TCP/IP

(Co nepatří mezi a) Co patří mezi úkoly aplikační vrstvy v TCP/IP modelu? – pravidla komunikace, stav dialogu, interpretace dat…

Jakým způsobem se v aplikačních protokolech TCP/IP řeší zápis textových řádek? – Kódování a konec řádky závisí na OS (CR + LF)

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

Pokrývá náplň horních tří OSI vrstev a tedy určuje:

Pravidla průběh dialogu (kdo iniciuje, co může klient požadovat, …)

Formát zpráv (obecně platí, že jsou buď textové nebo binární)

Typ zpráv (seznam požadavků a dopovědí na ně)

Sémantika dat (musí existovat jediná interpretace)

Jaký transportní protokol bude použit a jak

(např. UDP – maximální velikost, TCP – sdružení a rozdělní zpráv)

Protokoly aplikační vrstvy

Který z následujících protokolů se používá v TCP/IP na aplikační vrstvě? – DNS, FTP, SMTP, POP 3, IMAP, HTTP, SSH, VOIP (H.323, SIP), NTP, BOOTP, Telenet, SMB, NFS

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

Které z následujících tvrzení správně popisuje činnost konkrétního aplikačního protokolu? – …

DNS

Které z následujících tvrzení o povaze DNS protokolu je správné? - …

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

Které tvrzení správně popisuje obvyklou implementaci služby OS "zjisti IP adresu pro dané doménové jméno"? - …

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

Klient-server aplikace pro překlad jmen na adresy a naopak

Binární protokol nad UDP i TCP (port 53)

Běžné dotazy do 512B (dnes EDNS, takže i větší) pomocí UDP, pokud je odpověď větší, tak mu server, řekne, že je to truncated

Každá zpráva obsahuje hlavičku a určitý počet záznamů Resource Record

Každý obsahuje jméno, dobu platnosti (TTL), typ záznamu a data

Klient se postupně posílá dotazy na adresy svých uložených nameserverů. Pokud nedostává odpověď tak alespoň a získává informace o dalších (a zvětšuje timeout…)

DNS typy záznamů

SOA (úvodní záznam o každé doméně), NS (nameservery domény), A (IPv4 adresa), AAAA (IPv6 adresa), PTR (reverzní jméno) – IP je pozpátku a jméno, CNAME (aliasy), MX (záznam o tom kdo pro danou doménu přijímá poštu)

DNS Servery

Označte správné tvrzení o nameserverech. – …

Primární (master) – spravuje záznamy o doméně

Sekundární – záloha, která si periodicky stahuje data z primárního

Caching only – udržuje dotaz po dobu platnosti

První dva jsou autoritativní (jejich data jsou ověřená)

Obnovu databáze iniciuje sekundární, ale doporučí i primární

Může ale nastat chvíli prodleva

Každá domenéna by měla mít alespoň jeden či více autoritativních

Pro výměnu dat TCP, formát dotazu a odpovědi je DNS RR

Vyřizování DNS dotazu

Zadám adresu, ta se pošle na name server

I když name server neví nic, tak to musí vyřešit (rekurzivní)

Obrátí se tedy na své kořenové name servery

To už rekurzivní není a první ns si odpovědi cachuje

Postupně si nacachuje všechny mezilehlé servery až najde odpověď

Je to postižený tím, že ve jméně může být tečka a neodděluje domény

DNS dotaz a odpověď

Dotaz má záhlaví s 2B ID a příznaky (FLAGS) *(např. požadavek na rekurzi)*

Další sekce je QUERY s RR obsahujícím dotazované jméno a typ

Odpověď obsahuje v záhlaví opět ID a FLAGS *(autoritativnost odpovědi, …)*

V QUERY zopakovaný dotaz, další sekce je ANSWER s RR odpovědmi

AUTHORITY s listem nameserverů, které můžou pomoct

ADDITIONAL s dodatečnými informacemi (adresy nameserverů)

Bezpečnost

Které tvrzení o bezpečnostních aspektech protokolu DNS je správné? - …

Jak se útočník dostane k dotazu?

Může napadnout lokální síť a nebo se pokusit odhadnout znění dotazu, to se ale nemá šanci povést. Jsou tedy potřeba jiné způsoby:

Cache poisoning – přiměje klienta se zeptat na svůj vlastní legální server, v sekci AUTHORITY mu řekne, že se stará i o .cz

Řešení je postupovat pouze od kořenových serverů

Komplexní řešení: podepsané DNS (rozšíření DNSSEC)

Klíč je uložen u nadřazené domény

Diagnostika

Program nslookup s podpříkazy set type, server, name, IPadr, ls, exit

Na UNIXech podobný program se jménem dig (resp. dril)

FTP

Které tvrzení o povaze FTP protokolu je správné? – …

Které z následujících tvrzení o bezpečnostních problémech FTP je správné? – …

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 (možná může být i zvolený klientem)

Který aplikační protokol se používá k přenosu souborů? – FTP, SSH

Dodnes se používá (i když je celkem starý)

Původně pro přístup k vlastnímu účtu s otevřeným přenosem hesla

Dnes anonymní uživatel a emailová adresa uživatele místo hesla

Webové prohlížeče zobrazují odkaz na FTP stejným způsobem jako odkaz na HTTP

Textový protokol, kde klient naváže řídící spojení na portu 21 a pak posílá příkazy

Kódy odpovědí

1xx (předběžně kladná), 2xx (kladná), 3xx (neúplná kladná),
4xx (dočasně záporná), 5xx (záporná) *to dost protokolů převzalo*

Aktivní/Pasivní datové spojení

FTP používá dodatečné datové kanály na přenos souborů

Aktivní datové spojení znamená, že server navazuje TCP spojení

Adresu a port uživatele má, takže stačí dát svůj port na 20 (ftp-data)

Může ale také použít generický port

To je ale nepraktické a proto většina zahajuje aktivní spojení přes příkaz PORT (nebo EPRT), kterým serveru dá vědět adresu nebo port

Pasivní datové spojení logicky znamená, že TCP navazuje klient

V tom případě bude potřebovat od serveru adresu a port

O ně si požádá příkazem PASV (EPSV) a server odpoví socketem

Dnes je situace složitější kvůli privátním adresám (router by musel u pasivního modifikovat i obsah zpráv a adresy v nich)

Aktivní je lepší, ale omezení může být seznam portů u routeru

FTP Aplikace

Webové prohlížeče, Správce souborů, řádkový příkaz ftp

ftp má příkazy – open, user, close, quit, bye, cd, pwd, … , get, put, …

pozor na textové/binární soubory mezi různými OS

SMTP

Které z následujících tvrzení o SMTP protokolu je správné? – …

Které z následujících tvrzení o používání poštovních protokolů je správné? – …

Který aplikační protokol se používá pro elektronickou poštu? – SMTP (POP3, IMAP)

Které z následujících tvrzení o roli jednotlivých komponent v přenosu elektronické pošty je pravdivé? – (Mail forwaredr, mail transfer agent, mail exchanger) nebo POP/IMAP a SMTP

Textový protokol na TCP pro přenos elektronické pošty (port 25)

Tvar adresy schránka@server

To má nevýhody, že je to příliš závislé na změny názvu serveru a taky to útočníkovi říká příliš mnoho informací – lepší je tedy alias@doména/služba

Původně krátké (< 64kB) zprávy, postupně ale i pro přenos souborů

Příjem a odesílání pošty

Podobně jako u FTP princip posílání zpráv a odpovědí

Uživatel vydá povel k odeslání – většinou ho jen předá mail-forwarderu (tzv. mail-submission), ale může ho doručovat i přímo

Každý uzel, který pak přijímá a dále doručuje se nazývá Mail Transfer Agent

Jednotlivé MTA si dopis předávají pomocí SMTP (uloží do fronty, …)

Pokud je cílový mailbox na serveru dostupném z internetu, tak se poslední MTA pokusí doručit na ten server.

Pokud doručení není možné, tak se to zůstane v posledním MTA

Tomu správce sítě může zabránit nastavením MX záznamu

Ten obsahuje mail exchanger, který přijímá poštu

Příjemce se pak dozví cestu dopisu z hlavičky

Velké soubory bad, protože MTA si zprávy musí ukládat a pak opět posílat

Přístup k poště z pohledu uživatele

Přístup pomocí programu Mail User Agent (MUA)

a) Přímé připojení přes web nebo terminál na MTA s mailboxem
b) Pomocí poštovního protokolu POP nebo IMAP (čtení)
   Stejně se odesílá přes SMTP a ne nutně na stejný server

Ukázka SMTP

Který příkaz není příkazem SMTP protokolu podle RFC 821? – Jsou HELO, DATA, QUIT, MAIL FROM, RCPT TO, …

Nový dopis začíná příkazem MAIL FROM <adresa odesílatele>

Potom jeden nebo více příkazů RCP TO <adresa jednoho příjemce> a každého příjemce server akceptuje zvlášť (250 – ANO x 450 a 550 – NE)

Po 250 přebírá odpovědnost za doručení a nebo informování o neúspěchu

Pak příkaz DATA a na to je odpověď 354 a pak klient může psát text dopisu

Dopis je ukončený tečkou – proto pozor na CR LF tečka uvnitř textu

Poznámky: odesílatel si může dovnitř dopisu napsat libovolné odesílatele a příjemce tomu pak věří

DSN (delivery status Notification) a tedy informaci o doručení má povinnost generovat ten MTA, který odpověděl 250

U toho se nevyplňuje MAIL FROM a potom to má na některých uzlech snazší průchod – to zneužívají spamovací automaty

A to vede k tomu, že správci to zakazují (a s tím i DSN)

Části dopisu

Dopis se skládá ze dvou částí oddělených prázdným řádkem

Záhlaví: Obsahuje hlavičky s relativně pevným formátem a ASCII znaky

Text dopisu

Původně i zde pouze ASCII, postupně ale ESMTP má i 8bit kódování

přes MIME lze definovat strukturu a sémanitku dopisu (přílohy, …)

Hlavičky

Označte hlavičku, která se dle RFC 822 v dopisech nevyskytuje. –
Date, sender, reply-to, to, Cc, Bcc, Message-ID, Subject, Recieved

Date (vzniku), From (adresy i více autorů), Sender (osoba, která posílá), Reply-to (komu odpovědět), To (seznam adresátů), Cc (adresáti s kopií), Bcc (skrytí adresáti kopie), Message-ID (pro vlákna), Subject (předmět), Received (technická hlavička, kterou doplňuje každý uzel – název, čas, …)

Soubory a diakritika

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

Původně 7-bit ASCII a kódování pomocí UUENCODE (z unix-to-unix copy)

Vezme 3 byty a ty rozdělí do 4 bytů, které převede na znaky (33% overhead)

Podle pevné tabulky (v tabulce bylo 26 písmen, 10 číslic, 28 ostatní)

Soubor se obložil begin a end a je tedy potřeba analyzovat celý dopis

MIME (Multipurpose Internet Mail Extension)

RFC 2045-49 umožňuje strukturování

Mail má opět hlavičku a tělo

V hlavičce je typ dokumentu (typ + podtyp – např. audio/mp3), sada znaků, způsob kódování, původní název souboru a způsob zpracování

Podstatný je ovšem multipart a tedy, že tělo je dále strukturované

Aplikace vygeneruje náhodný řetězec, který je použit jako oddělovač

Každá z těchto částí je opět MIME dokument

Základní metody kódování

Base64 – UUENCODE s modernější tabulkou (52 znaků, 10 číslic, 2…)

Quoted-Printable – hlavně pro ASCII text tak, že non-ASCII → =HH

Etika (RFC 1855) … lol – jakože odpovídat rychle, jako Cc zvážit zásah, podpis…

Bezpečnost

Které tvrzení o bezpečnostních aspektech poštovních protokolů je správné? – …

Které tvrzení o autenticitě původu dopisu je správné? – …

Otevřená zásilka – pokud nutno, tak použít šifrování (PGP)

Není jistý odesílatel

Částečné řešení: Sender Policy Framework, pokus o zpětné doručení

Řešení: systém výzva/odpověď, elektronický podpis

Server by měl rozlišovat maily od jeho uživatelů a maily jiným uživatelům

Může být totiž zneužit pro rozesílání hromadných mailů a dostat blok

Pokud dovolí posílat komukoliv je tzv. open-relay

Problém, když se uživatel snaží připojit na svůj server z venku

Existuje rozšíření, které ho zvládne ověřit (ESMTP příkaz AUTH)

ESMTP má také příkaz STARTTLS pro šifrování dopisů pomocí TLS

Spam

Grey-listing – spamboti neopakují pokus doručení, takže jdou na blacklist

Sender policy Framework – kontroluje odkud… je to zrušeno

DKIM – server domény podepisuje text a některé hlavičky

Antispam – odhadování pravděpodobnosti

POP 3

Protokol pro přístup k poštovní schránce

Otevřené posílání hesla – existuje rozšiřující příkaz APOP

Stahuje celou zprávu – i když existuje příkaz TOP

Dnes je nahrazován IMAPem a podpora kvůli backwards compatibility

Plain text je obsoleted

Dříve push pak pull

Ukázka

USER, PAST, LIST, RETR, DELE

Jiné odpovědi než u FTP

IMAP

Od začátku důraz na vzdálený přístup (hledání a stažení pouze určitých informací)

Používá se v kombinaci s TLS (STARTTLS) (pak je port 993 místo 143)

Zabudovaná možnost šifrovat, podpora více schránek (složek), …

Příkazy jsou označovány identifikátory a proto je lze poslat paralelně

Princip distribuované databáze

Databáze informací na obrovském množství serverů

Přišel s tím Gopher – podobné jak dnešní internet

Hypertext

Vylepšení oproti Gopheru:

Nelineární prohlížení umožňující plynule přecházet

Obsahovat i netextové informace (hypermediální text)

Implementace až jako World Wide Web

World Wide Web

Globální informace distribuované po obrovském množství serverů

Základní jednotkou je stránka (v HTML dokumentu)

Popisuje obsah i formu, ale konkrétní zobrazení je na klientovi

Dokumentu buď existují staticky nebo dynamicky

Přenos stránky se odehrává pomocí HTTP (HTTPS)

HTTP (Hypertext transfer protocol)

Které tvrzení o povaze HTTP protokolu je správné? – …

Jak označujeme protokol, kterým se přenášejí webové stránky? – HTTP

Pokud www prohlížeč pošle dotaz na www server na standardním portu, jaký z následujících portů může obsahovat odpověď jako zdrojový? – 80 (HTTP)

Dnes verze 1.1 RFC 7230 a port 80

GET index.html… → server odpoví kódem a MIME (např. HTML)

Formát požadavku:

Úvodní řádka – metoda např. GET pro poslání stránky, …

Doplňující hlavičky – povinná pouze Host ale jsou i jazyk, …

Tělo dokumentu – nepovinné (používá se třeba pro upload…)

Formát odpovědi:

1xx – zpracovává se, 2xx – kladná, 3xx – nějaký další požadavek na klienta, 4xxx – chyba na straně klienta, 5xx – chyba na straně serveru

Hlavičky formálností (čas změny, expirace, protokol, …)

Tělo obsahuje stránku a nebo text chybové zprávy

Metody

Která z následujících metod ("příkazů") existuje v HTTP protokolu? – GET, POST, HEAD, PUT, DELETE, CONNECT

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

GET	prázdné tělo žádosti a v odpovědi je stránka a je bezpečná (nemění obsah serveru) a indempotentní (opakování má vždy stejný efekt)
HEAD	zjednodušená GET, kdy se vrací jen hlavička (B a I)

POST	pošle na server informace např. pro dynamickou stránku a nebo změnu dat serveru
PUT	přepíše dokumentu na serveru nahraným - indempotentní
DELETE	smazání dokumentu - indempotentní
CONNECT	otevře spojení klidně v úplně jiném protokolu

HTTP v.1

Jaké tvrzení týkající se cookies je správné? – …

Odpovědi na jeden požadavek obvykle jeden dokument

Pokud jsou na stránce 3 obrázky, tak celkem 4 požadavky

Verze 1.1 zavedla perzistentní spojení a tedy se nezavírá TCP

Komunikace je bezestavová (server neví které požadavky patří k sobě)

Např nějaké nastavení by se musel předávat opakovaně

To se řeší cookies (server vygeneruje set-cookie a pošle klientovi)

Prohlížeč cookies posílá při každém dalším požadavku na ten server

Cookies např nemohou obsahovat viry, ale pozor na sekundární nebezpečí

Např reklama nebo pokud se cookies dostanou někomu dalšímu

HTTP v.2

Větší propustnost, změna textového charakteru na binární

Tím je hůře čitelný, ale to nebylo už HTTPS

Má vlastní koncept více streamů nad jedním TCP

Server posílá i data o kterých si myslí, že je klient bude potřebovat

Dají se komprimovat hlavičky

HTML (Hypertext Markup Language)

Co označuje zkratka HTML? – jazyk pro obsah a formu dokumentu

Text je doplněn strukturou (odstavce), formátováním (tučně) a sémantikou (adresa)

Aplikace SGML a předchůdce XML

Více detailů je v druhé části přednášky + CSS

Telenet

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

Přihlašování na vzdálené stroje (terminál)

Někdo musí vykreslit stisknutí klávesy, buď automaticky a nebo po odpovědi, …

DO ECHO, DON'T ECHO, WILL ECHO, WON'T ECHO

problém, že nemají příznak zda povel nebo odpověď a může nastat fuck up

Bezpečností problémy jako otevřený přenos hesel, …

Dá se použít i pro navázání spojení na server v jiném protokolu – jak server reaguje

SSH (Secure shell)

Bezpečné vzdálené přihlašování (resp. přenos souborů)

Klient ověřuje server a je šifrovaná komunikace

Druhá verze nám umožňuje:

- Otevírání paralelních kanálů (např. terminál + soubory najednou)
- Tunelování – nechat projet SSH jinou komunikaci
- SSHFS – zpřístupnit část svého souborového systému… jeví se jako lokální

Přihlašování např. putty a přenos souboru např. WinSCP (UNIX ssh a scp)

Bezpečnost

Které tvrzení o bezpečnosti přístupu přes SSH je správné? – …

- Klient ověří server (na základě klíče) nebo se drží podle certifikátu (autority)
- Pokud se přihlašujeme poprvé je riziko, že je zrovna pod útokem malé
  - Teoreticky můžeme ověřování přeskočit
- To ale neplatí pro neočekávanou změnu klíče
- Následuje ověření uživatele
  - Může být jméno a heslo (komunikace je již šifrována)
  - Používání klíčů (na server se uloží veřejný a klient se pak prokáže)
    - Je to pohodlné, ale risky – hodí se dvouúrovňově
  - Internetoví červi fungují tak, že se vyzkouší připojit na všechny počítače, které se můžou připojit na napadnutý a pokud je nastaveno přihlašování bez hesla recipročně, tak se červ dostane dál

VOIP (Voice over IP)

Co označuje pojem VoIP (Voice over IP)? – Obecné označení technologie pro přenos hlasu po IP
Který aplikační protokol (resp. sada protokolů) se používá pro VoIP? – H.323, SIP

Obecné označení technologie pro přenos hlasu pomocí TCP/IP

Lze realizovat pomocí H.323, SIP a nebo proprietárně (třeba Skype)

Hodně problémů (digitalizace hlasu, nalezení partnera, propojení s telefonní sítí, …)

H.323

- Kompletní řešení komunikace (více samostatných protokolů)
  - H.225/RAS (hledání parntera), Q.931m H.245, …
- Šetřivé - binární až na úroveň bitů – velice špatně čitelné
- Dnes nahrazovány úvod (SIP), video/audio (RTP) a řízení (RTCP)

Abstract Syntax Notation

- Základ H.323 protokolů a způsob jak definovat datovou strukturu
- Problém s bitovou implementací – extrémně složité

SIP

Co označuje pojem SIP (Session Initiation Protocol)? – Protokol pro navazování audio/video spojení

Náhrada složitého H.323

Trochu podobně HTTP, ale dá se provozovat jak nad TCP, tak nad UDP

Pro přenos dat se používá RTP + RTCP – SIP hledá cíl a cestu + navazování

V návrhu zavádí proxy – článek, co usnadňuje komunikaci přes hranice sítí

Hlavičky, které zaznamenávají cestu (Via a Record Route) a ID hovoru, …

Dohoda o vlastnostech zařízení řeší Session Description Protocol (SDP)

Příklad SIP session

Příkaz INVITE s URL, proxy řeší hledání cíle

Musí se řešit upravování obsahu SDP odpovídající NAT

Proxy pošle 100 Trying, cílové zařízení pošle 100 trying

Pak cíl pošle 180 ringing, to pro změnu dojde až k volajícímu

Pokud zvedne, tak se pošle 200, proxy opět upraví data a pak ACK

Od této chvíle RTP/RTCP kanály a konec příkaz BYE a odpověď 200

Sdílení souborového systému

Který aplikační protokol se používá pro sdílení systému souborů? – NFS a SMB

Přístup se vzdáleným diskem jakoby byl lokální

NFS (Network file systém)

Velmi používaný na UNIXech

Na připojený disk se odkazuje jako server:cesta a pro uživatele transparentní

Autentikace Kerberos

Na UDP, ale je možné i TCP

SMB (Server Message Block)

Naopak Microsoft, ale existuje možnost ty dva propojit

\\server\cesta a autentikaci provádí systém sám pomocí username a pass

NTP (Network time protocol)

Jakým způsobem se synchronizují hodiny na počítačích v síti? – Network time protocol

Proč se synchronizují hodiny na počítačích v síti? – podstatná z uživatelského hlediska (aktualita souborů a porovnávání)

Synchornizace času mezi uzly sítě

Síť by bez toho asi i fungovala, ale pro uživatele je to lepší

Zdroje mají svoji klasifikace (stratum 0 – atomové hodiny)

Stratum *n* se řídí podle *n-1*

Musí se počítat s latencí od NTP serveru a proto výpočet používá časové známky v odpovědi, které určují pravděpodobný interval a následně Marzullův algoritmus.

BOOTP (Bootstrap protocol)

Původně pro automatickou konfiguraci bezdiskových stanic

Nelze na nich uložit IP, takže je server identifikoval podle MAC a přidělil jim ji

Stanice neví kam to poslat, takže to pošle všude – limited broadcast IP

Routery je nepropouštějí mimo síť

Komplikace při sít s podsítěmi oddělenými routery

BOOTP forwarding nebo BOOTP server v každé síti

DHCP

Jak funguje protokol DHCP? – …

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

Náhrada BOOTP – postupným vylepšováním a přidáváním konfigurace

Stejný formát zpráv

Statická a dynamická alokace adres (kvůli přepisování MAC pevné ztratilo význam)

Navíc router nezná všechny klienty a síť může nabízet méně adres…

Časově omezený pronájem

Možnost zapojení více serverů

Zpětná kompatibilita s BOOTP

Průběh

Klient pošle broadcastově DHCPDISCOVER

Servery posílají DHCPOFFER a klient je chvíli sbírá

Vyberu tu nejlepší (naposledy používaná nebo delší pronájem)

Následně odešle DHCPREQUEST

DHCPACK, jestli je stále volná a začíná běžet pronájem

V polovině doby DHCPREQUEST zvolenému serveru – možná prodloužení

Pokud ne, tak v 7/8 DHCPREQUEST broadcastem a jinak potom od začátku

Prezentační, relační a transportní vrstva OSI

Prezentační (OSI 6)

Popisuje kódování (datová pole, struktury)

Například ASN.1

TCP/IP dal kódování přímo do aplikační

Praktické problémy: CR LF, odlišné pořadí zápisu bytů (TCP/IP používá CR+LF a BE)

Relační (OSI 5)

Nástroj, který řídí komunikaci obou stran

Opět tedy do aplikačního v TCP

Příklad, kdy dialog neodpovídá jednomu spojení (SMTP a SIP)

Transportní (OSI 4)

Zodpovídá za end-to-end přenos dat

Splňuje různé požadavky na přenos různým aplikačním protkolům

Umožňuje multiplexing (více aplikací na jednom uzlu) pro klienta i server

Může také zajišťovat spolehlivost přenos, segmentovat data, řídit tok dat, …

Transportní vrstva v TCP/IP

Které tvrzení popisuje správně TCP resp. UDP? – …

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

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

TCP (Transmission Control Protocol)

Pro spojované služby – po navázání spojení data tečou ve formě proudu

Spojení řídí a zabezpečuje TCP, je ale komplikované a má velkou režii

UDP (User Datagram Protocol)

Používá se pro nespojované služby a data jsou nezávislé zprávy

Spojení musí řídit aplikace, za to je ale UDP jednoduché

Další modifikace a kombinace: SCTP, DCCP, MPTCP

UDP

Jakou informaci najdeme v záhlaví TCP i UDP? – zdrojový a cílový port, a řídící informace (délka a checksum)

Pokud UDP pakety dorazí v nesprávném pořadí, co se stane? – Příjemce je může a nemusí srovnat v aplikační vrstvě

Struktura – v UDP hlavičce se přenáší pouze informace o mlutiplexingu

A to jsou zdrojový a cílový port, a řídící informace (délka a kontrolní součet)

TCP

Která charakteristika TCP není správná? – …

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

Struktura TCP paketu

Pokud TCP pakety nedorazí ve správném pořadí, co se stane? – Sequence number -> příjemce je může srovnat…

TCP musí identifikovat segmenty (relativní offset od počátku streamu)

Pro opačný směr analogické pole ACK number

Flags, Urgent pointer pro out-of-band přenos (např. konec komunikace), …

TCP okno

Jaké postupy používá TCP, aby zajistilo spolehlivost přenosu? – TCP doručuje potvrzení dat…

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

Příjemce potvrdí doručení bloku dat tak, že pošle paket s příznakem ACK a hodnotou Acknowledgment number nastavenou na offset konce dat

Většinou se potvrzení k něčemu připojuje, když ale není k čemu, tak to po určitě době posílá samostatně

Zavádí se také pojem okno – množství dat, které se posílá bez čekání na ACK

Navrhovaná velikost je v poli Window v hlavičce

Zahájení a ukončení spojení

Co se odehrává během three-way handshake? – Přijemce dá vědět počáteční offset…

Co se stane, když jeden z partnerů pošle TCP paket s FIN příznakem? – Ukončí se spojení… skoro

Jakou informaci obvykle volí dynamicky klient, jenž se chystá navázat spojení na server? – (sequence number) spíše zdrojový port, ten se volí i UDP

- Spojení je stav, kdy se klient a server dohodli na komunikaci
- Offset komunikace začíná z důvodu bezpečnosti na náhodném čísle
  - Předání tohoto offsetu odesílatelem se nazývá three-way-handshake
    - Na začátku spojení pomocí tří paketů s prázdnými daty
    - První má příznak SYN a seq number nastavené klientem *(n)*
    - Server pošle paket s příznaky ACK a SYN a ack number *n+1* a seq number se svojí iniciální hodnotou *s*
    - Klient to dokončí tím, že pošle ACK s hodnotou *s+1*
- Pokud chce jedna stran spojení ukončit pošle pošle paket s příznakem FIN
  - Tím dává vědět, že už nepošle žádná dat
  - Druhá strana obvykle pošle zpátky taky FIN
    - Teoreticky se ale může stát, že strana bude posílat další data
    - Potom to klient musí ACKovat aby se to nerozpadlo
      - Tzv jednostraně uzavřené spojení (nedoporučované)

TCP příznaky

- SYN – slouží k synchronizaci čísel segmentů (sequence number)
- ACK – potvrzuje doručení všech paketů (ostře) před Ack-number
- PSH – informuje příjemce, že má celý blok
- FIN – odesílatel už nebude nic posílat
- RST – odesílatel odmítá přijmout spojení (tvrdší FIN)
- URG – urgentní out-of-band data s Urgent pointer

TCP dump na prohlédnutí TCP komunikace (tcpdump, Wireshark, WinPcap)

Co usoudíme z následujícího popisu paketu v programu tcpdump? – …

V materiálech je sice ukázka, ale je to celkem zbytečný

- Tcdump btw ukazuje hodnoty relativně
- Takže three-way-handshake je (SYN : *c*, _), (SYN, ACK : *s*, *c+1*), (ACK: _ , 1)

Výpis existujících socketů

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

- netstat -an vypíše seznam všech TCP i UDP serverů
  - u TCP serverů vypisuje i stav spojení
    - LISTENING (poslouchající server) a ESTABLISHED…
- 0.0.0.0 v druhém sloupci znamená, že server poslouchá na všech rozhraních
- 0.0.0.0 nebo * v třetím znamená, že se může připojit libovolný klient

Síťová vrstva

Označte termín, který není funkcí síťové vrstvy. – … funkcemi jsou adresace, Fzapouzdření, směrování, přeposílání a dekapsulace
Co nepatří mezi úkoly síťové vrstvy v TCP/IP modelu? – …
Jaký protokol poskytuje na síťové vrstvě službu spolehlivého přenosu dat? – žádné
Jaký protokol poskytuje na síťové vrstvě službu nespolehlivého přenosu dat? – IP

Hlavní funkce je přenos dat předaných transportní vrstvou do cíle

Základ pro to je adresace, zapouzdření, směrování, přeposílání a dekapsulace

IP

Které tvrzení o typech IP adres je pravdivé? – … Implicitní, subnetting, supernetting, VLSM, speciální adresy? …
Jak odesilatel zprávy zjistí, jaká část cílové IP adresy přísluší síti a jaká počítači? – podle třídy nebo podle masky
Označte nepravdivé tvrzení o přidělování IP adres. - …

Nespojovaná služba, best effort (nespolehlivá) , nezávislá na médiu

Dvě verze (4B a 16B) a adresa obou se dělí na adresu sítě a adresu uzlu

IP musí mít každý uzel, který chce komunikovat

ICANN má 5 regionálních registrátorů a ty dávají bloky ISPs

Ty pak dávají IP administrátorům sítě (v případě veřejných)

IPv4

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

Struktura hlavičky

Verze a délka hlavičky, QoS, fragmentace, Time-to-live, port, 2x IP, …

Fragmentace nastane, když paket má po zapouzdření větší než maximální povolenou délku pro linkovou vrstvu (MTU)

V takovém případě síťová vrstva fragmentuje

TCP se tomu vyhýbá vlastním dělením (to je segmentace)

Hledá se Path MTU a pak příznak Do not fragment

Adresy podle tří druhů velikosti sítí

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

A (7b a 3B), B (14b a 2B), C (18b a 1B - 2M sítí o 254 počítačích)

254 místo 256 protože vyhrazený význam adres

Nakonec přibyla i D pro multicastové adresy

Speciální adresy

V jakém případě není nutná adresace cílového počítače? – broadcast a multicast
Jaká IPv4 adresa má v části pro počítač samé jedničky? – síťový broadcast (všechny počítače v dané síti)

this host (0.0.0.0/8) – pouze jako zdrojová (když ještě nevíme IP)

loopback (127.0.0.1/8) – tento počítač

IP adresa s nulovou částí počítače je adresa sítě

Poslední IP adresa v bloku adres (jedničky na adrese počítače) je síťový broadcast (všechny počítače v dané síti)

Omezený broadcast (255.255.255.255), který neopustí síť

Privátní adresy – jedna síť class A, 16 class B a 256 class C (…NAT)

Link local adresy – volně k dispozici (nelze komunikovat mimo síť)

Subnetting

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. 001x xxxx

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

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 adresu

Dělení na třídy je málo jemné a proto v lokálních sítích posun vpravo

K tomu je potřeba ještě síťová maska (1 na místě adresy sítě)

Pak to můžem jednoduše priANDovat a zjisti, jestli je v naší

Často ale classless formát, kde se za lomítko napíše počet bitů

Rozčlení síť na menší celky, ale sníží počet adres

Nedoporučuje se podsíť se samými 0 a 1

VLSM (Variable Length Subnet Mask) pokud chceme měnit velikost

Opačný směr (posun vlevo) je supernetting

Naštěstí se ale dnes používají privátní adresy a těch je dost

Krize internetu

Přidělování nemělo přísná pravidla

Přeplňovaly se tabulky centrálních směrovačů

To by se dalo řešit tím, že by dvě sousední sítě měli sousední hodnotu

Classless InternetDomain Routing

To bychom ale museli hromadu sítí přečíslovat

Taky bylo jasné, že sítě dojdou…

IPv6

Kolik bitů má IPv6 adresa? – 128 bitů (16 bytů)

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

Zápis s dvou dvojtečkou a CIDR zápisem masky a tunelování IPv4…

Druhy

Unicastová adresa (speciální Loopback, Link-Scope, Unique-Local)

Link-Scope je novější název pro link-local

Unique-Local je obdoba privátních

Mutlicastová – adresa skupiny uzlů

Anycastová – unicast pro více uzlů

Dodatečné otázky

Jaký krok následuje poté, co www klient zjistí adresu cílového serveru a připraví paket v protokolu IP k odeslání? – předá linkové vrstvě a ta připojí MAC, typ, FCS

Který z následujících protokolů nepracuje s IP adresami? – linkové a fyzické určitě ne… naopak DNS, FTP, ARP, IP, link state

Směrování

Který záznam může být platným záznamem ve směrovací tabulce routeru A z následujícího obrázku? (resp routeru B) – …
Jakou informaci z paketu používá každý směrovač pro určení cesty? – Cílovou IP adresu
Které tvrzení o směrování je pravdivé? – …

Přirovnání ke křižovatkám…

Hledání dalšího směrovače pro cestu (next-hop router) – používá se směrovací tabulka

- V ní jsou adresa cílové sítě s maskou (rozsahem) a routery
- Pro cestu se vybere nejmenší okolí cíle

Příklad směrovací tabulky

Pokud má počítač špatně nastaven defaultní router, co nebude moci? – bude moct vysílat zprávy jen do své sítě

Budou v ní tři přímé záznamy (automaticky po konfiguraci síťového rozhraní)

- Vlastní adresa – loopback (není přes next-hop, ale přímo na nás)
- Hlavní síť naší LAN – opět nejde přes router, ale na vlastní adresu
- Třetí je point-to-point k ISP. To je BTW jediný stroj (router ISP)

Nepřímé záznamy

- Podsítě v naší LAN – router s tou adresou, která je v naší síti
- Default – Směřuje všechno na router ISP

Principy směrování

Označte existující pole (sloupec) routovací tabulky. – Cíl, maska a gateway (+interface a metrika)

Měla by to umět každá TCP/IP stanice

Záznam má cíl, masku a gateway (buď router nebo adresa vlastní síťového rozhraní)

- Podle gateway jsou záznamy přímé a nepřímé

Z hlediska vzniku dělení na implicitní (automaticky), explicitní (ručně) a dynamický

Dříve ještě host route (maska /32 a užší maksa net nebo subnet route)

Směrovací algoritmus

Vyberte správné tvrzení o principu směrovacího algoritmu. – …
Co se stane, pokud cíl není nalezen v routovací tabulce? – Buď default nebo nelze doručit
Jaký účel plní default gateway? – Pošle se to na ni, když nevím kam jinam

Vyhledám všechny záznamy ve směrovací tabulce, které se shodují s cílem

- Žádný záznam – nelze doručit (skoro vždycky ale obsahuje aspoň default)
- Jinak z nich vybere ten s nejširší maskou (ten nejspeciálnější)
  - Pokud je to náš počítač, tak se to zařadí na vstup
  - Pokud je to přímý záznam, tak se to předá linkové
  - Jinak se paket předá po linkové vrstvě do next hop routeru

Konfigurace sítě

Příkazy na UNIX: ipconfig (nastavení IP), route (záznamy v tabulce), dhclient (DHCP)

U Windows je to v nastavení

ICMP

Jaké funkce plní ICMP (Internet Control Message Protocol)? – … posílá řídící info (echo, unreachable, time exceeded, …)

Posílání řídících informací pro IP

Používá IP datagramy, ale není transportní

Např Echo, Echo reply – dosažitelnost (ping), Destination Unreachable, Time Exceeded, Source Quench (snížení rychlosti), Router Solicitation, Redirect, …

Ping

Vyberte správné tvrzení o účelu a principu programu ping. – … diagonóza sítě

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 – problém s IP softwarem. Po cestě se totiž ztratit nemůže

Zprávy ICMP Echo a ICMP Echo reply používá program ping

Základní prostředek na diagnostiku

Periodicky vysílá Echo a to pokud dorazí, tak server odpoví Echo reply

Na uzlu nemusí běžet žádný program

Zprávy posílá každou sekundu a pak z toho udělá statistiku round-trip time

Neznamená to, že se na server můžeme připojit a nemusí to platit ani opačně

Time To Live

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

Které pole IP záhlaví brání vzniku nekonečné smyčky při doručování? – TTL

Jaké pole IP záhlaví za normálních okolností mění router? –zmenšit TTL (a teoreticky překlad adres NAT)

V IP záhlaví – ochrana před zacyklením při špatné konfiguraci

Udává počet hopů a při 0 se pošle ICMP Time Exceeded

Diagnostika

Jakým příkazem můžeme vypsat obsah routovací tabulky? - netstat –r nebo route print

Diagnostika výpisem routovací tabulky příkazem netstat –r (? route print)

Příznaky H (host), G (gateway – nepřímý), D (dynamický)

Dá se přidat -n k zabránění překladu na jména

Další krok ping, ten ale moc nepomůže

Nevím, jestli paket nedorazil, server nefunguje nebo nedorazil zpátky

(Tabulky jsou totiž jednosměrné)

Traceroute

Využijeme TTL a budeme postupně zvyšovat o jedna

Statické řízení směrovacích tabulek

Které tvrzení o metodách řízení směrovacích tabulek je pravdivé? – …

Cesty se nastaví při startu podle konfigurace

Je to nepružné, má to problémy se subnettingem, … ale méně citlivé na problémy

Vhodnější pro malé stabilní sítě

Redirekce (ICMP Redirect)

Způsob jak statickým řízením pokrýt složitější síť

Když router zjistí, že paket posílá zpět do stejné sítě, tak pošle ICMP Redirect

Ten si to do routovací tabulky přidá správnou cestu

Ten nový záznam bude pod písmenem D (dynamický)

Bezpečnostní riziko je šíření špatného ICMP Redirectu

Dynamické řízení směrovacích tabulek

Routery si navzájem vyměňují informace o síti pomoci routovacího protokolu

Jednoduchá konfigurace, automatická sebeoprava, ale citlivější na problémy (útoky)

Na routeru musí běžet software (například BIRD)

Distance vector protokoly

Označte pravdivé tvrzení o distance-vector routovacích protokolech. – …

Uzel má u záznamu ve směrovací tabulce vzdálenost

Svoji tabulku periodicky posílá sousedům a podle toho se to upravuje

Ačkoliv je to jednoduché, tak se snadno šíří chyby a není přesná metrika

RIP (Routing information protocol)

Metrikou je počet routerů

Rozsah je omezen na 15 hopů (16 je nekonečno)

Používá Bellman-Fordův algoritmus

Nemusíme opakovat výpočet na rozdíl od Dijkstrova

Metriku se tedy hodí zatížit podle rychlosti linek

Musíme zvětšit počet hopů

Proč je ale nekonečno tak malé? – možné race conditions

Když vypadne síť a hned na to dostane router zprávu, že…

Síť se pak dokud se to nenasčítá na nekonečno tváří jako živá

Vylepšení RUP – Triggred updates (výpadek se pošle hned)

– Split horizon (nevrací informace autorovi)

– Poison reverse (autorovi dá otrávená data)

Link state protokoly

Označte pravdivé tvrzení o link-state routovacích protokolech. – …

Posílají se pouze informace o stavech linek a router si drží mapu celé sítě

Výpočet je proto náročnější za to chyba se nešíří, pružnější…

Open shortest path first

Které tvrzení charakterizuje Dijkstrův algoritmus?

Používá Dijkstrův algoritmus

I ten by na větší sítě nestačil a proto se dá dělit na podsítě

Rozdělena na dva stupně: páteř a další oblasti

Cesta má tedy nejvýše tři části (na páteř, po páteři, z páteře)

Metrika path cost (definuje administrátor)

Může být například propustnost, latence, vzdálenost, cena, …

Autonomní systémy

Označte pravdivé tvrzení o autonomních systémech (AS)? – …

Jak se mění směrování pro celý internet? Jednotlivé bloky jsou AS

Musí mít stejnou routovací politiku

Typicky je mají velké společnosti a ISPs

My jsme teď ukazovali interní routovací protokoly, tady ale používají externí (EGP)

Nejznámější je Border Gateway Protocol (BGP)

Musí umět zahrnout další faktory hodnocení cest a zabránit smyčkám (path-vector)

IP filtrování

Která z charakteristik IP filtrování je správná? – …

Zavádějící název, protože se filtruje na transportní vrstvě (které porty…)

Router, kterým je připojena lokální síť určuje bezpečnostní politiku

Přísná konfigurace (ven vybrané, dovnitř nic) – problém u FTP, SIP, …

Obvyklá (ven cokoliv, dovnitř nic) – problém u aktivních FTP, SIP

Pozn. směr je podle navazování

Při hostování webu musíme otevřít díru (pak se část zavádí zvláštní DMZ segment)

Proxy server

Která z charakteristik proxy serveru je správná? – …

Server, který kontroluje provoz určitého protokolu

Bezpečnostní, technické a výkonnostní důvody

Transparentní – krajní router sítě zachytí požadavek, zkontroluje ho a pustí dovnitř

Netransparentní – klient sám musí posílat nějakému jinému proxy serveru

ARP (Address Resolution Protocol)

Které tvrzení o ARP je pravdivé? – …

Označte pravdivé tvrzení o vztahu linkové a fyzické vrstvy v OSI a TCP/IP. – TCP/IP se tím nezabývá, ale jinak ARP…

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

Spojový článek mezi síťovou a linkovou vrstvou

Umožňuje zjišťovat linkové na základě síťových (My budeme mluvit o IP a Ethernet)

Aby zjistil MAC adresu next hopu pošle ARP dotaz na broadcastovou MAC (FF:FF…)

Tazatel si unicast odpověď uloží do ARP cache – obsah se dá vypsat přes arp -a

Komunikace nejdále po rozsahu linkové sítě – stejné MAC v síti jen pokud mezi nimi router

Chybí ale zabezpečení – nevyžádané ARP (částečně se řeší pevným nastavením ARP cache)

Proxy ARP

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?

Když router zjistí, že se z A do B nelze dostat, tak na ARP dotaz vrátí svoji adresu

Je to v případě, že zatajíme, že síť je rozdělená na více podsítí

V ARP cache je pak víc IP se stejnou MAC (to jinak může být známka napadení)

Linková vrstva

Jaký hlavní smysl má zápatí (trailer) linkového rámce? - Obsahuje FCS (Frame check sequence) – kontrolní součet např. pomocí CRC

Co označuje termín LLC (Logical Link Control)? – horní vrstva linkové, která se stará o ukládání a identifikaci před multiplexingem

Co označuje termín MAC (Media Access Control)? – dolní vrstva, která se stará o adresaci a řízení přístupu ve fyzickém segmentu sítě

Dělí se na dvě podvrstvy – Logical Link Control a Media Access Control

LLC – přístup různých protokolů k jednomu médiu a tedy multiplexing

MAC – řídí adresaci uzlů a přístup k médiu (je závislá přímo na technologii na které běží)

Datová jednotka linkového přenosu je rámec (frame), který obsahuje:

Synchronizační pole – start condition pro cílovou stanici

Hlavičku – přinejmenším MAC adresy obou stran a řídící LLC informace

Data (payload) nadřazeného protkolu

Patičku – závěrečná část, obsahuje Frame Check Sequence pro kontrolu správnosti

Síťové topologie

Které tvrzení o topologii sítě je pravdivé? – …

Uspořádání uzllů ve dvou spodních OSI

Mutlipoint

Sběrnice (sériové zapojení na stejné médium)

Snadné přidání počítače, přerušení znamená rozpad sítě

Hvězda (centrální prvek) neboli strukturovaná kabeláž

Dnes nejčastější, stanice se připojují UTP, je stále sběrnicová

Zařízení jsou nejčastěji připojená na switch (zastrčením do portu)

Kruh (např Token-ring a FDDI)

Point to point

Např. RS-232

Možnost prodloužit mezizařízením (modem – na telefonní spojení)

Dá se propojit i bezdrátově

Řízení přístup k médiu

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

Deterministický způsob – něco řídí, kdo právě vysílá (síť je tak často nevyužívaná)

V token-ringu se šíří zvláštní paket (token) a když chce zařízení vysílat, tak token nahradí svými daty a příjemce si data vezme a pak opět pošle token

nebo například zvláštní uzel, který posílá signál ostatním zařízením

Nedeterministický způsob – nikdo neomezuje uzly a jen se řeší kolize

Point to point rozlišujeme podle toho, zda může přijímat a zároveň vysílat

Half-duplex – neumí → kolize

Full-duplex – umí

Řešení kolizí

Co je základní funkcí CSMA/CD? – při vysílání detekovat kolize, upozornit na ně a pak vyčkat náhodnou dobu

CSMA = Carier sense with multiple access

CSMA – Uzel kontroluje nosnou (přenosové médium) a pokud není volná, tak čeká

Můžou ale dojít k vícenásobnému přístup a to se řeší rozšířením

CMSA/CD – Během vysílání detekuje kolizi a při ní zastaví a informuje

Po kolizi počká náhodnou dobu, kterou navíc zvyšuje

Doba vysílání rámce musí > doba šíření po segmentu (kolizní okénko)

Uzel by mohl odvysílat celý rámec a nedozvědět se o kolizi

Limituje max. délku segmentu a min. velikost rámce

CSMA/CA (např. WiFi) – když je nosná volná, tak vysílá celý rámec a čeká se na ACK

Ethernet

Které z tvrzení o Ethernetu je správné? – …

Se kterou vrstvou OSI je svázán pojem Ethernet? – 2. vrstva (linková)

Dva běžné formáty (IEEE 802 a Ethernet II)

Používá CSMA/CD

6B ethernetové adresy (první tři prefix výrobce, další tři vlastní číslo)

Pokud jsou adresy stejné je potřeba jednu z nich změnit nebo je oddělit routrem

Pak je v prezentaci useless tabulka pokroku

Struktura ethernetového rámce

Oba časté typy mají destination a source potom ale rozdíl

Ve v2 je typ, data a FCS a v IEEE je délka, hlavička, data a FCS

VLAN (Virtuální sítě)

Jaké tvrzení o VLAN je pravdivé? – …

Po jedné fyzické síti provoz více nezávislých LAN

Do rámce se vsune VLAN tag s číslem virtuální sítě (VLANID)

Dá se udělat i transparentně, tak že switch bude pro jednu konkrétní síť tag odebírat

U centrálního routeru se konfiguruje jako trunk a switch pak nedělá nic

Switche musí být schopny pracovat s většími rámci než povolené maximum

CRC (Cyclic Redundancy Check)

Co označuje termín CRC? – Hashovací funkce pro kontrolu dat

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

- *Počítají ho PC a routery (switche ne)*

Většina kontrolních mechanizmů používá pro kontrolu dat právě CRC

Je to založené na dělení polynomů

Převedeme posloupnost bitů na polynom s binárními koeficienty

Ten vydělíme charakteristickým polynomem a výsledek na posloupnost…

Jednoduchá HW implementace

n-bitový CRC detekuje 100% chyby s lichým počtem bitů kratší než *n*

dost pravděpodobně i delší chyby

WiFi (neboli WLAN - Wireless LAN)

Které tvrzení o WiFi je správné? – …

Skupina protokolů IEEE 802, které se používají pro bezdrát v pásmech 2,4 a 5 GHz

Používá CSMA/CA a hvězdicovou topologii

Je možné ji strukturovat i ad-hoc peer-to-peer, ale obvykle access pointy ve středu

Sítě se rozlišují SSID

Pozor na bezpečnost

Fyzická vrstva

Které tvrzení o médiích používaných v počítačových sítích je správné? – …

Jaký krok následuje poté, co počítač, na kterém běží www server, přečte ethernetový rámec od síťové karty? – decapsulation linkovou vrstvou (přečte MAC) a případně předá síťové vrstvě

Má na starost přenos dat po konkrétním médiu (mohou být optické, metalické, bezdrátové)

Převod digitální informace na analog

Druhy přenosu

Analog x digital

Ve skutečnosti je vše kolem analogové (proud)

Digitální označuje rozhodnutí do jakého intervalu proud spadá

Převod do analogu přes modem a do digitalu před codec

Baseband x broadband

Baseband používá prostě hodnoty signálu (a kóduje je)

Je pak potřeba hodinový signál

Ethernet používá kódování Manchester, kdy se v tiknutí mění signál

Broadband používá přenosy v širokém pásmu a ty moduluje (amplituda, …)

Např AM nebo FM rádio

Nestíněná kroucená dvoulinka (UTP)

Kolik vodičů obsahuje kabel označovaný jako nestíněná kroucená dvoulinka (UTP)? – 4 páry (8 vodičů)

Jaké tvrzení o kabelech pro propojení dvou uzlů ethernetové sítě je pravdivé? – UTP, pozor na křížený/přímý kabel

4 měděné vodiče zakroucené kolem sebe (to snižuje vyzařování a příjem záření)

V prostředí se silným rušením se ještě odstiňuje (STP)

100Mb Ethernet vuyžívá jen dva páry – mezi počítače je to možno pak rozdělit

Osazování RJ 45 na UTP výstupní na jedné straně musí být z druhé strany vstupní

Dnes MDI/MDIX autodetekce

Optické vlákna

Jaký je rozdíl mezi jednovidovým (SM) a mnohovidovým (MM) optickým kabelem? – svítí se laserem vs LED

Šíří se jako viditelné světlo přes křemíkové vlákno

Jednovidová (singlemode) má užší jádro a používají laser

Výrazně omezen lom paprsků a proto lepší dosah a přenosová kapacita

Mnohovidová (multimode)

Používají se LED diody a parsky se zde více lámou (takže menší dosah)

Segmentace sítě

Jak lze charakterizovat repeater, hub, bridge a switch? – …

S jakými adresami pracuje hub, přepínač resp. směrovač? – hub žádné, switch – MAC, router MAC a IP

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

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 data

Repeater (ve strukturované kabeláži hub) spojuje segmenty na fyzické vrstvě

Ačkoliv zvětšuje dosah, zhoršuje kolizi (prodlužuje dobu šíření rámce)

Bridge (ve strukturované switch) naopak poskytuje lepší propustnost

Musíme se posunout na linkovou vrstvu

Rozumí tedy MAC adresám a posílá rámce jen tam, kde je to nutné

Kromě propustnosti zlepšuje i bezpečnost

Ještě se hodí full duplexově připojit centrální router a centrální server

Learning bridge (BUS, BUM)

Přepínače si za každým portem udržují tabulku MAC adres

Ze začátku je prázdná a postupně ji zjistí podle odpovědí

Spanning Tree Algoritmus

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

Co označuje zkratka STP? – … buď tohle nebo (Shielded Twisted Pair - kroucená dvojlinka s kovovým stíněním)

Pokud máme dva switche, tak metoda learning bridge selže

Musíme tedy najít kostru grafu sítě

Switche se musí dohodnout, kdo potlačí forwardování (blocking)

Používá se na to protokol STP – to ale chvíli při strtu sítě tvá

To vyřeší faststart, kdy se protokol vypne

Celkově nezařazené otázky

Jaké kroky musí udělat klientský počítač, aby správně odeslal paket v případě, že cílový server není ve stejné síti? – Vyslat ARP aby zjistil MAC adresu routeru a pak přes směrovací tabulku

Vyberte správné tvrzení o činnosti routeru. – přeposílá datagramy k jejich cíli mezi sítěmi (spoj probíhá na síťové vrstvě)

Které zařízení/prostředek implementuje bezpečnostní politiku lokální sítě vůči internetu? – router/firewall/proxy server

Jak budou vypadat zdrojové a cílové IP a MAC adresy paketu poslaného z notebooku na server na trase mezi routerem A, B? – zdrojové: IP notebooku, MAC routeru A, cílové: IP serveru, MAC routeru B

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

Vyberte správné tvrzení o dynamických WWW stránkách. – server side x clinet side

Server side lze udělet téměř v čemokilv (přes CGI) *Klient nejčastěji v Javascriptu a méně často Javu*

Které tvrzení o možnostech autora ovlivnit dynamickou povahu stránek je nesprávné? – prý v testu bylo „musí použít Javu“