TEXT S OTÁZKAMI

Sada protokolů TCP/IP je standardem pro síťovou komunikaci a tvoří základ internetu. Je organizována do čtyř konceptuálních vrstev. Na rozdíl od sedmivrstvého referenčního modelu OSI, který slouží jako komplexní teoretický rámec, TCP/IP je praktičtější implementace. Proces, při kterém data procházejí vrstvami směrem dolů, se nazývá enkapsulace: k datům se na jednotlivých vrstvách přidávají režijní informace (obvykle hlavička, na linkové vrstvě i patička) a tím vzniká datová jednotka (PDU) dané vrstvy.

1. Aplikační vrstva (Application Layer): Definuje protokoly pro koncové aplikace (HTTP, SMTP). V kontextu OSI modelu tato vrstva abstrahuje funkce relační a prezentační vrstvy.
2. Transportní vrstva (Transport Layer): Zajišťuje logickou komunikaci mezi procesy na koncových zařízeních.
    - TCP (Transmission Control Protocol): spojově orientovaný protokol. Před přenosem dat navazuje spojení (three-way handshake), garantuje doručení, správné pořadí a integritu dat pomocí potvrzování (acknowledgements) a řízení toku (flow control). Datovou jednotkou je segment.
    - UDP (User Datagram Protocol): nespojový protokol bez záruk. Datovou jednotkou je datagram. Hlavní výhodou je minimální režie, což ho činí vhodným pro přenosy citlivé na zpoždění (např. DNS, streaming).
3. Síťová vrstva (Internet Layer):Zodpovídá za globální adresaci a směrování datagramů napříč různými sítěmi. Klíčový protokol IP (Internet Protocol) definuje formát logických IP adres, které slouží k jednoznačné identifikaci zařízení v síti. Jeho úkolem je najít cestu k cílovému zařízení, ale sám o sobě je nespolehlivý – doručení negarantuje. Datová jednotka této vrstvy se nazývá paket (nebo IP datagram).
4. Spojová vrstva (Link Layer): Zajišťuje přenos dat v rámci lokální sítě (např. mezi počítačem a routerem). Pracuje s fyzickými (MAC) adresami. Data z vyšší vrstvy (pakety) jsou zde zapouzdřeny do datové jednotky zvané rámec (frame), která je následně odeslána po fyzickém médiu (Ethernet, Wi-Fi).

Enkapsulace tedy znamená, že aplikační data jsou zabalena do TCP segmentu nebo UDP datagramu, ten je zabalen do IP paketu a ten je nakonec zabalen do ethernetového rámce pro odeslání. Každá vrstva komunikuje pouze se svými sousedními vrstvami.

Otázky:

1.Co se stane s IP paketem, když sestupuje ze Síťové vrstvy na Spojovou vrstvu v procesu enkapsulace?

a) Je rozdělen na několik menších segmentů, aby se vešel do rámce.
b) K paketu je přidána hlavička s fyzickými adresami (MAC) a patička pro kontrolu chyb, čímž se z něj stane datová jednotka zvaná rámec.
c) Je přejmenován na datagram, aby mohl být zpracován protokolem UDP.
d) Rámec ze Spojové vrstvy je vložen dovnitř IP paketu pro zajištění fyzického doručení.

2.Na základě popisu v textu, který z následujících výroků nejpřesněji vystihuje vztah mezi TCP a IP?

a) TCP využívá služeb IP pro směrování dat, přičemž kompenzuje jeho nespolehlivost přidáním vlastních záruk.
b) IP využívá TCP k tomu, aby spolehlivě doručil pakety na správnou IP adresu.
c) TCP a IP jsou dva nezávislé protokoly, které pracují na stejné vrstvě a řeší stejný problém doručování dat.
d) TCP je zodpovědné za globální adresaci a IP za logickou komunikaci mezi procesy.

3.Proč je podle textu pro DNS dotazy vhodnější UDP než TCP?

a) Protože UDP garantuje, že DNS dotaz dorazí vždy ve správném pořadí.
b) Protože DNS dotaz je malý a vyžaduje rychlou odpověď; režie spojená s navazováním TCP spojení (handshake) by byla zbytečným zdržením.
c) Protože UDP používá logické IP adresy, zatímco TCP používá fyzické MAC adresy, což je pro DNS efektivnější.
d) Protože UDP, na rozdíl od TCP, dokáže komunikovat napříč různými sítěmi.

4. Uživatel si prohlíží webovou stránku (HTTP). Která vrstva je zodpovědná za to, aby data doručená jeho prohlížeči byla kompletní a ve stejném pořadí, v jakém byla odeslána ze serveru?

a) Aplikační vrstva, protože protokol HTTP má vlastní mechanismy pro řazení paketů.
b) Síťová vrstva, protože protokol IP zajišťuje doručení ve správném pořadí.
c) Transportní vrstva, konkrétně protokol TCP.
d) Spojová vrstva, protože rámce jsou v lokální síti vždy doručovány sekvenčně.

5.Jaký je zásadní rozdíl ve funkci Síťové vrstvy a Spojové vrstvy podle popisu v textu?

a) Síťová vrstva používá IP adresy pro doručení dat kamkoliv na světě, zatímco Spojová vrstva používá MAC adresy pro doručení pouze v rámci lokální sítě.
b) Síťová vrstva je zodpovědná za spolehlivý přenos, zatímco Spojová vrstva za nespolehlivý.
c) Síťová vrstva zapouzdřuje rámce do paketů, zatímco Spojová vrstva zapouzdřuje segmenty do rámců.
d) Síťová vrstva pracuje pouze s protokolem TCP, zatímco Spojová vrstva pracuje s Ethernetem i Wi-Fi.

LOGICKÉ

Představ si, že máš následující seznam čísel, kde chceš zjistit, která jsou prvočísla, pomocí algoritmu ***Eratosthenovo síto***. Tento algoritmus funguje tak, že začínáme s číslem 2, označíme všechny jeho násobky jako neprvočísla, a tato neprvočísla z daného seznamu odstraníme. Poté pokračujeme na další číslo, které není označeno jako neprvočíslo, a opakujeme tento postup, dokud neprojdeme celý seznam. Po každé iteraci odstraníme všechna neprvočísla.

Tvůj seznam čísel je:
[34,283,32,20,38,27,56,11,13,19,45,50]

6.Jak bude vypadat seznam po třetí iteraci algoritmu Eratosthenova síta?

a) [283,11,13,19]
b) [283,11,13,19,45]
c) [283,11,13,19,45,50]
d) [283,11,13,19,56]

Jako správce serveru sleduješ jeho provoz pomocí logu. Tento log obsahuje různé stavy serveru, včetně informací o přetížení, chybách(ERROR) a varováních(WARNING). Tvé úkolem je zjistit, jak dlouho byl server pod vysokým zatížením (vysoké využití CPU nebo paměti).

```
2025-10-25 07:30:00 INFO Server started successfully
2025-10-25 07:35:00 INFO User login successful
2025-10-25 07:45:00 WARNING CPU usage exceeded 90%
2025-10-25 07:50:00 INFO CPU usage back to normal
2025-10-25 07:55:10 WARNING Memory usage high, over 80%
2025-10-25 08:00:00 INFO Memory usage back to normal
2025-10-25 08:05:30 WARNING CPU usage exceeded 95%
2025-10-25 08:10:00 INFO CPU usage back to normal
2025-10-25 08:15:00 INFO Server running smoothly
2025-10-25 08:20:00 WARNING CPU usage exceeded 90%
2025-10-25 08:25:00 INFO CPU usage back to normal
2025-10-25 08:30:00 WARNING Memory usage high, over 80%
2025-10-25 08:35:00 INFO Memory usage back to normal
2025-10-25 08:40:00 INFO Server running smoothly
```

7.Zjisti, jak dlouho byl server pod vysokým zatížením (buď vysoké využití procesoru nebo paměti)?

a) 20 minut a 30 sekund
b) 24 minut a 20 sekund
c) 15 minut a 45 sekund
d) 18 minut a 10 sekund

Jako lingvista pracující pro tajnou službu ses dostal/a ke zprávě zašifrované metodou, která na první pohled vypadá jako jednoduché nahrazení písmen. Háček je v tom, že substituční abeceda není pevně daná – je dynamicky vytvořena na základě tajného klíčového slova. Bez znalosti klíče je standardní frekvenční analýza téměř k ničemu.

Tvým úkolem je zašifrovat zprávu pomocí této metody.

Jak to funguje:

1. Vytvoření šifrovací abecedy: Šifrovací abeceda se vytvoří tak, že na její začátek se umístí unikátní písmena z klíčového slova a za ně se připojí zbytek písmen z původní abecedy (používáme abecedu americkou) v jejich normálním pořadí.

- Krok A: Příprava klíče Vezmi klíčové slovo a odstraň z něj všechna písmena, která se opakují. Příklad s klíčem TRANSMITTER -> unikátní písmena jsou TRANSMIE.
- Krok B: Sestavení nové abecedy Na začátek napiš unikátní písmena z klíče. Za ně doplň zbývající písmena abecedy (od A do Z) v jejich standardním pořadí, přičemž vynecháš ta, která už jsou v klíči použita.

  Příklad s klíčem TRANSMIE:

  - Začátek: T R A N S M I E
  - Zbytek abecedy: B, C, D, F, G, H, J, K, L, O, P, Q, U, V, W, X, Y, Z
  - Výsledná šifrovací abeceda: T R A N S M I E B C D F G H J K L O P Q U V W X Y Z

2. Šifrování: Šifrování probíhá jako jednoduchá substituce. Každé písmeno otevřeného textu se nahradí písmenem, které stojí na stejné pozici v nově vytvořené šifrovací abecedě.

- Původní abeceda: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- Šifrovací abeceda: T R A N S M I E B C D F G H J K L O P Q U V W X Y Z

  Příklad šifrování slova CAT:

  - C (3. písmeno) -> A (3. písmeno v šifrovací abecedě)
  - A (1. písmeno) -> T (1. písmeno v šifrovací abecedě)
  - T (20. písmeno) -> Q (20. písmeno v šifrovací abecedě)
  - Výsledek: **ATQ**

8.Zašifruj slovo "*INVASION*" pomocí klíčového slova "*CRYPTOGRAPHY*".

a) FSHXLFSM
b) FSHXMFSL
c) FSHXLFSL
d) HIUCNHJI

DevOps inženýr nasazuje sadu tří závislých mikroslužeb: Autentizační službu (A), Službu pro objednávky (B) a Notifikační službu (C). Nasazovací nástroj může v jednom kroku buď NASADIT jednu službu, nebo RESTARTOVAT jednu službu. Služby mají striktní pravidla pro spouštění:

- Služba B (objednávky) nemůže běžet, pokud neběží služba A (autentizace), jinak by zpracovávala neautorizované požadavky. Pokud je A restartována, B se musí okamžitě restartovat také.
- Služba C (notifikace) pro své spuštění vyžaduje, aby služba B (objednávky) byla alespoň jednou úspěšně nasazena a spuštěna (nemusí běžet v momentě spuštění C, ale musí mít záznam o předchozím běhu).

9.Inženýr začíná s prázdným prostředím (žádná služba neběží). Jaký je minimální počet kroků k tomu, aby všechny tři služby běžely stabilně?

a) 3 kroky
b) 4 kroky
c) 5 kroky
d) 6 kroky

Graf zobrazuje procentuální rozložení dat v cloudovém úložišti projektu "Chimera", který má celkovou velikost 50 TB.

- Uživatelská data: 60 %
- Systémové logy: 25 %
- Zálohy: 10 %
- Dočasná mezipaměť (Cache): 5 %

Tým se rozhodl provést optimalizaci nákladů. Plán je zkomprimovat jednu desetinu systémových logů. Kompresní poměr je 5:1, což znamená, že data po kompresi zaberou pouze jednu pětinu původní velikosti.

10.Jaká bude celková velikost úložiště projektu "Chimera" po této optimalizaci?

a) 48 TB
b) 45 TB
c) 46,67 TB
d) 49 TB

POROZUMĚNÍ TEXTU

RAID je technologie, která umožňuje spojit několik fyzických pevných disků do jednoho logického celku za účelem zvýšení výkonu nebo odolnosti proti selhání. Například v režimu RAID 1 (zrcadlení) se všechna data zapisují identicky na dva disky současně. Pokud jeden disk selže, systém bez přerušení pokračuje v práci s daty z druhého disku. Naopak RAID 0 (prokládání) rozděluje data a zapisuje jejich části střídavě na všechny disky v poli. Tím se dramaticky zvyšuje rychlost čtení i zápisu, protože disky pracují paralelně. Cenou za tento výkon je však nulová redundance – při selhání jediného disku v poli RAID 0 dochází ke ztrátě všech dat na logickém disku

11.Jaký je hlavní rozdíl v důsledcích selhání jednoho disku mezi poli RAID 0 a RAID 1, jak je popsáno v textu?

a) U RAID 1 dojde ke ztrátě poloviny dat, zatímco u RAID 0 se neztratí nic.
b) U RAID 0 dojde ke ztrátě všech dat v poli, zatímco RAID 1 může pokračovat v provozu bez ztráty dat.
c) Selhání disku v RAID 0 pouze zpomalí systém, kdežto v RAID 1 ho zcela zastaví.
d) V obou případech (RAID 0 i RAID 1) je nutné okamžitě vyměnit oba disky, aby se předešlo ztrátě dat.

Firewall je síťové bezpečnostní zařízení, které monitoruje a řídí příchozí a odchozí síťový provoz na základě předem definovaných bezpečnostních pravidel. Funguje jako bariéra mezi důvěryhodnou vnitřní sítí (např. vaše domácí síť) a nedůvěryhodnou vnější sítí (např. internet). Firewall může být implementován hardwarově jako samostatné zařízení, nebo softwarově jako program běžící na počítači. Zatímco tradiční firewall analyzuje pouze hlavičky datových paketů (IP adresy, porty, protokoly) a nevidí do jejich obsahu, moderní tzv. Next-Generation Firewall (NGFW) provádí hloubkovou inspekci. Dokáže tak analyzovat i samotný obsah přenášených dat (payload) a odhalit například malware nebo pokusy o průnik, které by běžným firewallem prošly bez povšimnutí.

12.Které z následujících tvrzení je v souladu s funkcí firewallu, jak je popsána v textu?

a) Všechny typy firewallů dokáží identifikovat a odstranit viry v souborech stahovaných z internetu.
b)Tradiční firewall filtruje provoz pouze na základě adres a portů, zatímco moderní NGFW kontroluje i samotný obsah dat.
c) Hardwarový firewall je méně bezpečný než softwarový, protože běží na samostatném zařízení.
d) Firewall primárně slouží ke zrychlení internetového připojení tím, že blokuje nepotřebný provoz.

HTTP cookies jsou malé textové soubory, které webový server ukládá do prohlížeče návštěvníka. Slouží k uchování stavových informací, protože samotný protokol HTTP je bezstavový. Typickým využitím je udržení uživatele přihlášeného – server po přihlášení pošle cookie s unikátním identifikátorem relace a prohlížeč ho pak přikládá ke každému dalšímu požadavku, čímž server ví, o kterého uživatele se jedná. Cookies také umožňují

personalizaci obsahu nebo sledování uživatele napříč stránkami pro reklamní účely, což je důvodem obav o soukromí a zavedení regulací jako GDPR.

13.Jaký problém protokolu HTTP řeší cookies podle uvedeného textu?

a) Jeho neschopnost přenášet obrázky a videa, kterou cookies doplňují.
b) Jeho pomalost, kterou cookies zrychlují díky ukládání dat na straně uživatele.
c) Jeho nedostatečné zabezpečení, které cookies plně nahrazují šifrováním.
d) Jeho neschopnost pamatovat si předchozí interakce, kterou cookies řeší uchováním informací o relaci.

Ačkoliv se termíny „virus“ a „červ“ často zaměňují, jedná se o dva odlišné typy škodlivého softwaru (malware), které mají odlišný způsob šíření a způsobují různé druhy problémů.

- **Počítačový virus** je škodlivý program, který se šíří tím, že vloží svůj kód do existujícího, legitimního programu nebo souboru (takzvaný hostitel). Virus se neaktivuje, dokud není spuštěn v hostitelském programu, a potřebuje lidskou interakci k dalšímu šíření. Příkladem je **ILOVEYOU virus**, který se šířil prostřednictvím e-mailových příloh a vyžadoval, aby uživatel otevřel infikovanou přílohu.

- **Počítačový červ** je nezávislý škodlivý program, který ke svému šíření nepotřebuje hostitele. Červ se aktivně replikují a šíří po síti, vyhledává zranitelné systémy, které může infikovat, a to bez jakékoliv interakce uživatele. Příkladem je **WannaCry**, červ, který v roce 2017 zneužil zranitelnost v systému Windows a šířil se napříč organizacemi a počítačovými sítěmi bez jakéhokoli zásahu uživatele.

14.Jaký je podle textu rozhodující rozdíl ve způsobu šíření mezi virem a červem?

a) Virus se šíří pouze přes e-mail, zatímco červ se šíří pouze po lokální síti.
b) Červ ke svému šíření aktivně využívá síť a nepotřebuje lidský zásah, na rozdíl od viru, který je závislý na spuštění hostitelského souboru.
c) Virus je samostatný program, kdežto červ se musí vždy připojit k jinému souboru
d) Červi jsou vždy neškodní a pouze zpomalují síť, zatímco viry vždy mažou data

Při zálohování dat existuje několik strategií. Úplná (full) záloha zkopíruje všechna vybraná data. Je nejjednodušší na obnovu, ale časově a prostorově nejnáročnější. Inkrementální (přírůstková) záloha ukládá pouze změny, které nastaly od poslední jakékoliv zálohy (ať už úplné, nebo inkrementální). Je velmi rychlá a malá, ale obnova vyžaduje poslední úplnou zálohu a všechny následující inkrementální zálohy v řadě. Diferenciální (rozdílová) záloha ukládá změny, které nastaly od poslední úplné zálohy. Je větší a pomalejší než inkrementální, ale k obnově stačí pouze poslední úplná záloha a poslední diferenciální záloha.

Představte si následující scénář: V neděli proběhne úplná záloha. Od pondělí do soboty probíhá každý den jedna záloha.

15.Které soubory by stačily k obnově systému do stavu v sobotu večer, pokud by se používala diferenciální metoda zálohování?

a) Pouze záloha ze soboty
b) Záloha z neděle a všechny zálohy od pondělí do soboty
c) Pouze záloha z neděle a záloha ze soboty.
d) Pouze záloha z pátku a záloha ze soboty