OSI 5, 6, 7 - soketové programování, převod formátů dat, šifrování, komprese, autentizace

OSI 5 - Relační vrstva

Relační vrstva zajišťuje vytvoření, správu a ukončení relací mezi komunikujicími aplikacemi.

Hlavní funkce:

- Navazování, udržování a ukončování relací
- Synchronizace dat mezi aplikacemi
- Dialog management (half-duplex, full-duplex komunikace)
- Obnovení relace po chybě pomocí kontrolních bodů
- Řízení interakce (kdo může vysílat a kdy)

OSI 6 - Prezentační vrstva

Prezentační vrstva zajišťuje správnou interpretaci dat mezi komunikujícími systémy

Hlavní funkce:

- Konverze mezi různými formáty dat
- Šifrování a dešifrování dat
- Komprese a dekomprese dat
- Kódování znaků (ASCII, EBCDIC, Unicode)

OSI 7 - Aplikační vrstva

Aplikační vrstva je nejvyšší vrstva OSI modelu, poskytuje přímé rozhraní pro uživatelské aplikace

Hlavní funkce:

- Identifikace komunikačních partnerů a ověření dostupnosti
- Určení dostupnosti zdrojů a přístupových práv
- Synchronizace kooperujících aplikací
- Zajištění autentizace a soukromí
- Výběr mechanismů pro obnovu chyb

Socketové programování
Soketové programování je způsob, jak vytvářet aplikace, které komunikují přes síť. Socket je koncový bod komunikace - něco jako zásuvka v síti, přes kterou můžeme posílat a přijímat data. Umožňuje nám komunikaci mezi PC v síti - chatovací aplikace, webové servery, online hry

Funkčnost
1. **Server** vytvoří socket, naváže ho na konkrétní port a čeká na připojení
2. **Klient** vytvoří socket a aktivně se připojí k serveru
3. Po připojení **obě strany posílají a přijímají data** přes socket
4. Nakonec obě strany spojení uzavřou

Typy socketů
TCP sockety - spolehlivé, spojované spojení, garantuje doručení
UDP sockety - rychlejší, nespolehlivé, bez garance doručení nebo pořadí

Multiplexing
Slouží pro obsluhování více klientů současně.

Převod formátů dat
Proces transformace dat z jednoho formátu nebo reprezentace do jiného, se zachováním jejich struktury a dat. Skoro každý systém používá odlišný formát k různým věcem a proto používáme převody.

Hlavní formáty dat
XML - univerzální značkovací jazyk, ukládání a přenos dat, poměrně upovídaný - hodně značek - zvětšuje veliksot
JSON - jednodušší a lehčí alternativa k xml, dříve pro js a teď prakticky všude používaný, používá se k API
CSV - jednoduchý formát pro tabulková data
Binární formáty - efektivnější než textové formáty

Serializace a deserializace
Serializace - převod objektu nebo datových struktur v paměti do formátu, který lze uložit
Deserializace - opačný proces - rozbalení serializace a získaní dat

Způsoby převodu
Přímý převod - z jednoho formátu přímo do druhého
Kanonický přístup - převod přes meziformát (např. všechny formáty se nejprve převedou do XML a pak do cílového formátu)
Mapování schémat - definice pravidel pro převod mezi odpovídajícími elementy různých formátů

Šifrování
Proces převodu běžného textu na šifrovaný formát podle matematických algoritmů a klíčů. Pouze příslušným klíčem lze získat zpět. Šifrování nám zajišťuje bezpečnost - online bankovnictví atd….

Typy šifrování
Symetrické šifrování
- Stejný klíč pro šifrování a dešifrování
- rychlé, efektivní pro velká data
- méně bezpečné
- AES, DES, Blowfish, ChaCha20

Asymetrické šifrování
- Dva různé klíče pro šifrování a dešifrování
- bezpečnost, digitální podpisy
- pomalejší
- RSA, ECC…

Hybridní
- Kombinace obou
- Asymetrické pro výměnu symetrického klíče, symetrické pro data
- spojuje bezpečnost a rychlost

Hashovací funkce
Jednosměrná matematická funkce, která převádí data na výstup pevné délky. Z hashe nelze odpovdit vstupní data, menší změny mají vliv na celkovou délku. SHA, SHA-256, SHA-3

Komprese
proces zmenšování velikost dat odstraněním nadbytečných informací. Jejím cílem je snížit nároky na ukládání a přenos dat, ale zanechání původní informace, pro větší kompresi se toho obětuje víc.

Principy
Kódovací redundance: Neefektivní použití kódů pro symboly (např. použití 8 bitů pro každý znak, i když by stačilo méně)
Mezisymbolová redundance: Opakující se vzory nebo předvídatelné sekvence symbolů
Psychovizuální/psychoakustická redundance: Informace, které lidské smysly nedokáží dobře rozlišit (využívá se u ztrátové komprese)

Typy komprese
1. Beztrátová - přesná rekonstrukce původních dat bez ztráty, txt, programy, databáze,
2. Ztrátová - část nenávratně ztracena, fotografie, video, zvuk

Algoritmy
Beztrátové - Huffmanovo kódování, RLE….
Ztrátové - JPEG, MP3…..

Měření komprese
Kompresní poměr - proměr veliksot původních dat k velikosti komprimovaných
Úspora místa - procentuální úspora místa dosažena kompresí

Autentizace
Proces ověření identity uživatele, zařízení nebo systémů před poskytnutím přístupu ke zdrojům.

Použití
- Zajištění, že do sítě vstupují pouze oprávnění uživatelé a zařízení
- Ochrana citlivých dat a systémů před neoprávněným přístupem
- Vytvoření základu pro dohledatelnost aktivit v síti (audit)
- Splnění bezpečnostních standardů a regulací

Autentizační protokoly
Kerberos - založení na tiketech
Radius - používáný pro Wifi, VPN…
IEEE 802.1X - řízení přístupu k síti na úrovni portů

Hesla, certifikáty, 2FA…..