1. a) Carui nivel apartine TCP, precizati functiile si caracteristicile acestuia.

b) diferenta intre serviciile cu confirmare si cele orientate pe conexiune

c) cum se face conexiunea la TCP

d) controlul fluxului la TCP

e) verificarea segmentelor la TCP

REZOLVARE

1.a)TCP apartine nivelului transport,nivel ce are ca functie transportarea datelor de la masina sursa la masina destinatie intr-o maniera sigura si eficace d.p.d.v al costurilor.

De asemenea,ofera interfata uniforma cu utilizatorii.

TCP (Transmission Control Protocol) este cel mai folosit protocol de transport.

Adigura livrarea sigura a datelor pe o retea nesigura.

Este orientat pe conexiune.Stabileste o conexiune permanent intre client si server.

Realizeaza controlul congestiei,adaptand viteza de transmisie.

Are un overhea mare,in comparative cu UDP-ul.

Este full-duplex,are confirmare.

Protocolul utilizat de TCP este protocolul cu fereastra glisanta.

In TCP conexiunile se stabilesc folosindu-se “Three Way Handshake”.

b)**Diferenta dintre serviciile cu confirmare si cele orientate pe conexiuneAICI subiectul e ciudat,nu e bine scris dar am inteles de la cineva ca s-a dat diferenta intre datagrame si CV**

Serviciile cu confirmare sunt cele cu datagrame,iar cele orientate pe conexiune ,cu circuite virtuale.

Stabilirea circuitului virtual nu e necesara la datagrame,pe cand la circuitele virtuale este obligatorie.

Adresare este diferita:la datagrame,fiecare pachet contine adresa complete pentru sursa si destinatie si la circuitele virtuale,fiecare pachet contine un numar mic de circuite virtuale.

La datagrame,ruterele nu pastreaza informatii despre conexiuni,pe cand fiecare circuit virtual necesita spatiu pentru tabela ruterului per conexiune.

La datagrame,fiecare pachet e dirijat independent,pe cand la CV,calea e stabilita la initierea CV si toate pachetele o urmeaza.

Daca ruterul se strica,la datagrame nu are niciun effect decat pachete pierdute in timpul defectari.La CV,toate circuitele care trec prin ruterul defect sunt terminate.

c)Conexiunea TCP se face prin “Three Way Handshake”.

Serverul asculta ,clientul incearca se se conecteze si trimite primul pachet(SYN).

Serverul primeste SYN-ul si raspunde cu SYN-ACK.ACK-ul ajunge la client,clientul trimite ACK(confirmarea de primire) si conexiunea e realizata.

d)Fluxul de date e transmis pe o cinexiune TCP limitat de minimul dintre dimensiunea ferestrei receptorului si capacitatea retelei.

Algoritmul de control al congestiei:

-Foloseste un prag(threshold)

-La un time-out,pragul e setat la jumatate din fereastra de congestive

-Se aplica procedeul de crestere a ferestrei de congestive pana atinge pragul.

-Peste prag se aplica o crestere liniara.

SAU(aici nu sunt sigura ca am gasit mai multe,prima e din cursuri,a doua din carte)

Fiecare maşină care suportă TCP dispune de o entitate de transport TCP, fie ca proces utilizator,

fie ca parte a nucleului care gestionează fluxurile TCP şi interfeţele către nivelul IP. O entitate TCP

acceptă fluxuri de date utilizator de la procesele locale, le împarte în fragmente care nu depăşesc

64K octeţi (de regulă în fragmente de aproximativ 1500 de octeţi) şi expediază fiecare fragment ca o

datagramă IP separată. Atunci când datagramele IP conţinând informaţie TCP sosesc la o maşină,

ele sunt furnizate entităţii TCP, care reconstruieşte fluxul original de octeţi.

e) Există două limite care restricţionează dimensiunea unui segment. în primul rând,

fiecare segment, inclusiv antetul TCP, trebuie să încapă în cei 65.535 de octeţi de informaţie

utilă IP. în al doilea rând, fiecare reţea are o unitate maximă de transfer sau MTU (Maximum

Transfer Unit), deci fiecare segment trebuie să încapă în acest MTU. în realitate, MTU este în

general de câteva mii de octeţi, definind astfel o limită superioară a dimensiunii unui segment.

Dacă un segment parcurge o secvenţă de reţele fără a fi fragmentat şi ajunge apoi la o reţea ai

cărui MTU este mai mică decât dimensiunea segmentului, ruterul de la frontiera acelei reţele

fragmentează segmentul în două sau mai multe segmente mai mici.

2. a) detectia si corectarea erorilor

b) la ce folosesc sumele de control si confirmarile.

c) sa calculezi crc pt cuvantul pe 16 biti "PC" si polinoml x^4+x+1 (sau cam asa ceva )

a) ) Corectarea erorilor este mai complexă decât detectarea lor.

Detectia erorilor utilizează sindromul, o combinatie liniară a simbolurilor

cuvântului de cod,pe cand corectarea erorilor necesită aflarea zerourilor unor polinoame cu coeficienti

functii rationale de componentele sindromului

b) **Suma de control(Checksum)** este folosita pentru detectarea eorilor de transmisie.

Un pachet este trimis de la transmitator avand o anumita suma de control.Daca la receptie,suma de control a pachetului este alta decat cea initiala inseamna ca pachetul a fost modificat,daca suma este aceeasi inseamna ca datele din pachet sunt corecte.

**Confirmarile** reprezinta o solutie pentru a preveni inundarea receptorului de catre transmitator.

Presupunem ca avem un canal fara erori,canal pe care se trimit pachete cce contin anumite date.

Transmitatorul trimite pachet dupa pachet,nesttind daca receptorul ii poate face fata .

Viteza cu care se trimit pachetele trebuie sa fie mai mica sau cel putin egala cu viteza cu care se primesc.

Astfel,folosim confirmarile.Transmitatorul trimite un pachet,receptorul il primeste si trimite un cadru de confirmare.Transmitatorul primeste cadrul de confirmare si doar atunci poate trimite urmatorul pachet.

c)

3.1.a) Organizare DNS

b)RR la DNS

c)Daca pe un calc pot fi doua nume dns din nivelul superior, daca da de ce , daca nu de ce nu

a) Sistemul de nume DNS are o organizare ierarhică, sub formă de arbore. Acesta are o rădăcină unică  (root) care are subdomenii.  Fiecare nod al arborelui reprezintă un nume de domeniu sau subdomeniu.

b)Una dintre componentele DNS este reprezentata de Înregistrări de resurse (RR - resource records)- Baza de date DNS conţine înregistrări de resurse. Aceste înregistrări provin din mapările între nume şi obiecte din reţea.

c)Pot fi dar nu stiu de ce

3.2 explicare chei secrete, chei publice, si ceva cu incredere la certificate, daca A primeste de la B un certificat semnat de X, dar A nu-l recunoaste pe X, cum face sa fie sigura ca e bun sau cv de genu

REZOLVARE

Protocoalele de criptare se împart în două clase generale: cu chei secrete (de exemplu,

DES, IDEA) şi cu chei publice (de exemplu RSA). Folosirea acestor protocoale este uşoară; partea dificilă este reprezentată de gestiunea cheilor.

**Criptografia asimetrică** este un tip de criptografie care utilizeaza o pereche de chei: o cheie publică și o cheie privată.

Cele două mari ramuri ale criptografiei asimetrice sunt:

1.Criptarea cu cheie publică – un mesaj criptat cu o cheie publică nu poate fi decodificat decat folosind cheia privată corespunzătoare. Metoda este folosită pentru a asigura confidențialitatea.

2.Semnături digitale – un mesaj semnat cu cheia privata a emițătorului poate fi verificat de catre oricine, prin acces la cheia publica corespunzatoare, astfel asigurandu-se autenticitatea mesajului.

Autoritate de încredere care eliberează certificatul și certifică faptul că cheia publică inclusă aparţine persoanei cu numele ataşat.

Un certificat trebuie revocat când:

–Cheia primară (secretă) este compromisă.

–Cheia primară este pierdută.

–O persoană pleacă din companie.

Revocarea trebuie cunoscută de toţi utilizatorii