A:(coospace-szes)

2. feladat1.1Írd le az Internet fontosabb építőelemeit, ezek rövid leírását!(10 pont)

Az internet a “hálózatok hálózata”, ami milliárdnyi összekötött eszközből álló, kommunikációs kapcsolatokkal összekötött és csomagkapcsolók által írányított végberendezésből és ISP-kből áll. Az internet működését protokollok határozzák meg, amelyek vezérlő hatással vannak az üzenetek küldésére és fogadására, ezek határozzák meg az üzenetek sorrendjét és a rajtuk végrehajtandó akciókat. Főbb internetszabványok : RFC, IETF. (Request For Comments, Internet Engineering Task Force)

3. feladat1.13Mi a különbség a vírus és a féreg között? (10 pont)

A vírus önsokszorosító fertőzés melyet adott állományok lefuttatásával aktiválunk (pl email csatolmány). Működésük és terjedésük csak bizonyos közegben lehetséges. Ha ez nem áll rendelkezésre akkor nem működőképes. Nem feltétlenül okoznak kárt, sokszor csak kisebb bosszantó tevékenységeket művelnek.

Két ciklusuk van: elöször megpróbálnak minél jobban elterjedni, majd egy esemény bekövetkezésekor kifejtik a hatásukat : lehet adatok törlése, felülírása, megsemmisítése, menüpontok eltüntetése stb..

3 nagy fajtát különböztetünk meg : Állomány vagy programvírus ; Bootvírus ; Makróvírus.

A féreg is önsokszorosító , amely passzívan tud állományokat küldeni és futtatni.

A vírusokkal ellentétben nem szükséges hordozóközeg a terjedésükhöz. Önmagukban a számítógépes hálózatokat felhasználva terjednek. Gyors terjedésük miatt manapság ezek a legveszélyesebbek. Sokféle kárt tud okozni de már a terjedésével is sávszélességet foglal.

4. feladat3.1.7 Lehet-e UDP felett is megbízható átvitel? Ha igen, hogyan?(20 pont)

Lehet, de ezt az alkalmazás rétegben kell biztosítani alkalmazás specifikus hibakezeléssel.

4.1.10 Ismertesd az IPv4 címzés motivációját, felépítését! (30 pont)

Az IP cím állomások és forgalomirányítók 32 bites azonosítója (IPv4 esetén). Az IP cím nagyértékű bitjei az alhálózatot azonosítják. Az állomás részt az alacsonyabb értékű bitek jelölik. Az azonos alhálózattal bíró IP című interfészek elérik egymást forgalomirányító nélkül is.   
4 oktettünk (8 bit) van. Alapvetően 5 osztályt különböztetünk meg : A (8 hálózat - 24 host), B (16 hálózat - 16 host) , C (24-8), D (multicast címek), E (speciális jövőbeli felhasználásra).  
CIDR : a cím tetszőleges hosszúságú alhálózati része, a cím formátum a.b.c.d/x, ahol x # bitek száma a cím alhálózati részében.

B:

2.1.1,Hol futnak a hálózati alkalmazások? Szemléltesd az alkalmazás és a hálózat viszonyát egy ábrával.

A hálózati alkalmazás protokollok megvalósítási koncepciói az Alkalmazásrétegben kerülnek megvalósításra.   
  
A hálózati alkalmazások különböző végrendszereken futnak és a hálózaton keresztül kommunikálnak, így nem szükséges szoftvert írni a hálózat gerincébe elhelyezkedő eszközökre, tehát a gerincben lévő eszközök nem futtatnak felhasználói alkalmazásokat. Ilyen alkalmazások pl.: e-mail, web, távoli bejelentkezés, hang IP felett (skype) , tárolt videók lejátszása stb..

2.2.6,Vesd össze a kliens szerver és P2P architektúra (fájl megosztás esetén).

Tegyük fel hogy van egy F méretű fájlunk amit N db csomópontra szerenénk elosztani. A kérdés, hogy mennyi időre van szükség. Vegyük figyelembe, hogy a csomópontok feltöltési, letöltési kapacitása véges erőforrás.  
Kliens-szerver architektúra esetén N db fájl másolatot szorosan kell küldeni, aminek következménye hogy ha egy másolat küldési ideje F/us , akkor N db másolat küldési ideje : NF/us (ahol us a szerver feltöltési kapacitása, F pedig a fájl mérete).  
Ekkor minden kliensnek le kell tölteni a másolatot. Ha dmin = minimális kliens letöltési sebesség, akkor min. kliens letöltési ideje = F/dmin.   
Így tehát megkapjuk hogy a szükséges idő Dc-s >=max{NF/us, F/dmin}. Láthatóan ez N-nel lineárisan nő.  
P2P esetén a szervernek elég legalább egy másolatot átvinnie, így ehhez szükséges idő F/us. Kliens oldalon viszont minden kliensnek kell egy másolat. A min. kliens letöltési ideje F/dmin. N darab kliens esetén a klienseknek összesen NF bitet kell letölteniük. Ehhez szükséges idő DP2P >=max{F/us, F/dmin, NF/(us+ Σui)}. Látható hogy bár N lineárisan nő, de Σui csökkenteni fogja az értéket.   
Végeredményként megállapítható hogy P2P esetén a fájl megosztás gyorsabb módszer.

2.2.2,Miért elosztott a DNS?

Ha a DNS központosított szolgáltatás lenne, több lehetséges probléma is felmerülne. Példáult a meghibásodások egy pontba koncentrálódnának, ez által akár az egész szolgáltatás is leállhatna. E mellett a forgalom volumene is jelentős problémát okozna, hisz eszközök százmilliói által generált kéréssorozatot kellene kielégítenie.  
Egyetlen DNS szerver nem lehetne elég közel minden eszközhöz , ez által távoli helyekről indított kéréseket csak hatalmas késleltetéssel tudna kiszolgálni a szerver.  
A DNS elosztottsága megkönnyíti a karbantartást is, mivel ha minden rekordot egy adatbázisban tartanánk akkor azt állandóan frissíteni kellene az új host-ok listájával.  
Összességében kijelenthető hogy nem skálázható a gondolat. Ezért lett a DNS elosztott.

4.1.12Ismertesd a hierarchikus címzés motivációját a CIDR elvét.

A hálózat az ISP-től kapja meg az IP alhálózati részét. A hierarchikus címzés segítségével a forgalomirányító információ hatékonyan kezelhető. A hierachia lényege hogy vannak hálózatok és ezen belül hostok. Így célszerű a címet két részre bontani, hálózati rész és ezen belül host azonosító.  
CIDR (Classess Inter-Domain Routing) : a cím tetszőleges hosszúságú alhálózati része, a cím formátum a.b.c.d/x, ahol x # bitek száma a cím alhálózati részében.

C:

1.10 vonalkapcsolt előnyei a csomagkapcsoltan szemben 10,

A vonalkapcsolt rendszerek előnye rendszerint a számított kis késleltetésben rejlik, illetve abban hogy a logikai csatornák teljes egészében elkülönülnek egymástól. Nagy előnye még e mellett hogy ez a legolcsóbb kapcsolódási technológia.

Itt nem léphet fel torlódás. Csomagkapcsolt technológia esetén az információ korlátozott maximális méretű lehet.

1.2 hálózat határ eszközök fogalmai közege 10 pontos feladatok

Mivel az internet sok, különböző méretű hálózatok összességéből áll, a különböző hálózatok között határok vannak. A szerverek gyakran adatközpontokban vannak. A host lehet kliens és szerver.

A kommunikáció közegét illetően két fajtájú lehet: vezetékes , és vezeték mentes.

A rendszereket a határ forgalomirányítókhoz kell kapcsolni. Esetünkben ez lehet mobil hozzáférés, intézményi hozzáférés vagy lakossági hozzáférés. A hozzáférési hálózat sávszélessége eltérő lehet.

DSL (digitális előfizetői vonal) esetén a dedikált vonalon hang/adat a DSLAM központi iroda berendezéséig a meglévő telefonvonalat használja. Az adat az internetre , a hang a telefonhálózatba megy.

Otthoni hálózat esetén beszélhetünk vezetékmentes eszközökről, vezetékmentes hozzáférési pontról, vezetékes Ethernetről, forgalomirányító, tűzfal, NAT, kábel vagy DSL modemről amely a fejállomás vagy központi iroda felé/felől megy.

A fizikai vonal az adó és vevő között található. Írányított közeg esetén a jelek adott irányba jobban terjednek: réz, optikai kábel, koaxális.

TP(csavart érpár) két szigetelt csavart ér, ami a Category 5 esetén 100Mbps, 1 Gbps Ethernet, Category 6 esetén 10 Gbps.

2.2.1 dns példával 20,

A DNS (tartomány elnevezés rendszer) egy elosztott elnevezési rendszer, ami sok névkiszolgálló hierarchiájaként épül fel. Célja, hogy az emberek számára kézenfekvőbb hostnevekek és a routerek számára kézenfekvőbb IP címek közötti konverziót megvalósítsa. Ennek megvalósításához a gépek név kiszolgálókkal beszélnek, hogy feloldják a neveket (cím/név átalakítás). Ez az internet egyik alapvető protokollja, ami Alkalmazásrétegbeli protokollként van megvalósítva.   
A DNS legfőbb szolgáltatásai közé tartozik a gépnév IP megfeleltetés, a host aliasin , a levelező szerver aliasin illetve a terhelés elosztása.

4.1.13 Nat 30

A NAT (Network Address Translation) hálózati címfordítást végez. A helyi hálózat kívülről nézve csak egy IP címen látszik. Az ISP-től nem kell egész címtartomány csak egy IP cím. A belső címzést tetszőlegesen változtathatja. ISP-t válthat úgy, hogy belülről nem kell újracímeznie. A belső eszközök explicit módon nem címezhetőek meg közvetlenül a hálózatról, ami segíti a biztonságot.  
Megvalósítása a NAT forgalomirányítóval lehetséges. A kimenő datagram kicseréli a (forrás IP cím, port #)-ot minden egyes kimenő datagramban a (NAT IP címre és egy új portra#).  
Megjegyzi (a NAT címfordító táblában) minden (forrás IP, port#) hozzárendelést a (NAT IP, új port) párokhoz.  
A bejövő datagramokat kicseréli a (NAT IP, új port#) minden bejövő datagram cél mezőiben megfelelő NAT táblában tárolt (forrás IP, port#) párossa.  
Létezik dinamikus és statikus NAT is.

D:

4.1.10ipv4 cimzes

Az IP cím állomások és forgalomirányítók 32 bites azonosítója (IPv4 esetén). Az IP cím nagyértékű bitjei az alhálózatot azonosítják. Az állomás részt az alacsonyabb értékű bitek jelölik. Az azonos alhálózattal bíró IP című interfészek elérik egymást forgalomirányító nélkül is.   
4 oktettünk (8 bit) van. Alapvetően 5 osztályt különböztetünk meg : A (8 hálózat - 24 host), B (16 hálózat - 16 host) , C (24-8), D (multicast címek), E (speciális jövőbeli felhasználásra).  
CIDR : a cím tetszőleges hosszúságú alhálózati része, a cím formátum a.b.c.d/x, ahol x # bitek száma a cím alhálózati részében.

1.6 internet 5 rétege es szolgaltatasaik

* alkalmazási réteg: hálózati alkalmazások támogatás, FTP, SMTP, HTTP
* szállítási réteg: processz-processz adatátvitel TCP, UDP
* hálózati réteg: az adatcsomagok irányításáért felelős IP, forgalom irányító protokollok
* vonal: adatátvitel a szomszédos hálózati elemekhez Ethernet, WiFi, PPP
* fizikai réteg: bitek a “vezetéken”

3.1.2multiplexalas demultiplexalas

A multiplexálás a küldőnél több szoftver csatorna adatát kezeli, és hozzáadja a szállítási réteg fejlécét (ezt használják a demultiplexálásra). Minden egyes, hoszton futó folyamatlan lehet egy vagy több socketje. A szállítási réteg nem közvetlenül a folyamathoz juttatja el a szegmenst, hanem a szegment fejlécében lévő portszám szükséges az azonosításhoz, és a fogadó hoszt innen tudja kiolvasni.  
A demultiplexálás a fogadónál a fejléc információit használja a megkapott szegmensek kézbesítésére.  
A gép IP datagramokkat kap, amelyek rendelkeznek egy forrás és egy cél IP címmel.  
Minden datagram egy szállitás rétegbeli szegment visz, és minden szegmensnek van egy forrás és egy cél portszáma.   
A gép ezeket az IP címeket és port számokat használja, hogy a szegment az adott szoftvercsatornába irányítsa.   
Két fajta demultiplexálásról beszélhetünk: -Kapcsolatmentes (UDP esetén)  
 -Kapcsolatorientált (TCP esetén)

2.2.4 dns feloldas egy peldaval

Tegyül fel, hogy a cis.poly.edu névre hallgató host szeretné megszerezni a gaia.cs.umass.edu IP címét a kommunikáció érdekében. Legyen a Műegyetem lokális DNS szervere a dns.poly.edu és a gaia.cs.umass.edu autoratív DNS szervere.  
Ekkor a folyamat iterált lekérdezéssel az alábbi:  
 1. A cis.poly.edu host küld egy DNS kérést az ő lokális DNS szerverének, a   
 dns.poly.edu-nak. A kérés tartalmazza a gaia.cs.umass.edu host nevet,  
 ugyanis az ehhez tartozó IP címet szeretnénk megtudni.  
 2. A lokális DNS szerver továbbítja a kérést egy gyökérponti DNS szerver felé. A gyökérponti DNS szerver az edu végződés alapján megkeresi az összes ehhez tartozó TLD szerver címét , és visszaküld egy IP cím listát a lokális DNS szervernek.  
 3. A lokális DNS szerverünk egy újabb DNS kérést küld, de ezt már a listában szereplő TLD szerverek valamelyikének intézi.  
 4. A TLD szerver fogadja a kérést, viszont ő már az umass.edu végződés alapján keres egyezést az adatbázisban.  
 5. A TLD szerver a válaszban visszaküldi a lokális DNS szerver számára a megfelelő autoratív DNS szerver IP címét (a dns.umass.edu-jét).  
 6. Végül a lokális DNS szerver harmadjára is elküldi a DNS kérést, de már közvetlenül a dns.umass.edu-nak.  
 7. A dns.umass.edu autoratív DNS szerver válaszol a gaia.cs.umass.edu IP címével.  
 8. A lokális DNS szerver a fogadott IP címet továbbítja a kérést indító host felé, a cis.poly.edu-nak.  
Lehetőség van rekurzív lekérdezésre is, ez esetben a névfeloldás terhét a felkeresett szerverre tesszük.

E:

1.6 Sorold fel az Internet protokoll verem 5 rétegét. Melyek az alapvető szolgáltatásaik?

**( Volt már a D csoportban )**

2.2.5 Milyen DNS biztonsági problémákat ismerünk?

Ma már számos sebezhetőséget fedeztek fel és használtak ki rosszindulatú felhasználók.  
Egyik ilyen a DNS-gyórsítótár mérgezés, melynek során a gyorsítótárazó névkiszolgálókba juttatnak nem hiteles válaszokat, (hosszú TTL értékkel), így a mérgezett címeket lekérdező alkalmazások a kívánt cél helyett a támadó által kontrollált hálózati címekre csatlakoznak.  
A DNS felerősítéses támadás a DDoS-al járó támadások gyakran használt formája, amely a nyílvánosan rendelkezésre álló DNS szervereket használja, hogy az áldozat rendszerét a megsokszorozott DNS forgalommal túlterhelje.  
Alkalom adtán a gyökér szerverek ellen is próbálnak DDoS támadásokat intézni, de ez általában sikertelen szokott lenni, hisz ezeket könnyebb kikerülni a logikális DNS szerverek gyorsítótárazásai és a forgalom szűrés miatt.  
A TLD szerverek bombázása ezzel szemben más sokkal veszélyesebb lehet.

6.2.3 Ismertesd az ARP protokollt.

Címfeloldási protokoll. A kérdés hogy hogyan tudjuk meg az interfész MAC címét ha ismerjük az IP címét? Az ARP (Address Resolution Protocol) tábla a LAN-on lévő minden IP csomópontnak van egy ilyen táblázata. Feladata az IP/MAC cím hozzárendelések az egyes LAN csomópontokhoz. TTL(time to live) az egyes bejegyzések élettartalma (tipikusan 20sec).  
Az ARP feladata hogy cél IP címet megkeresse a helyi tárban és hozzárendelje a MAC címet. Ha nem találja akkor üzenetszórásos kérést küld a hálózatba IP cím alapján a MAC címet kérve, amire csak a gép fog válaszolni ami az adott IP-vel rendelkezik.

8.1.3 Ismertesd a nyilvános kulcsú kriptográfia RSA verziójának alapjait.

(Rivest–Shamir–Adleman)  
Az üzenet egy bitmina. Ezt a bitmintát egy egész szám egyedi módon jellemzi. Ezek alapján az üzenet titkosítása egyenértékű a szám titkosításával.  
Az RSA napjainkban a leggyakoribb titkosítási eljárás. Az eljárás elméleti alapjait a moduláris számelmélet és a prímszámelmélet egyes tételei jelentik.  
Válasszunk két nagy prímet p-t és q-t.  
Számoljuk ki N=pq-t  
N lesz a modulusa mind a nyílvános, mint a titkos kulcsnak.  
Válasszunk egy olyan egész számot, e-t, melyre teljesül hogy 1 <e <. Az e-t nyilvánosságra hozzuk mivel ez a nyílvános kulcs kitevője. A nyílvános kulcs az N modulusból és nyílvános e kitevőből áll.

F:

1.7 Írd le azt a három alapelvet amelyen a mai Internet alapul (Kleinrock, Cerf és Kahn)

1961: Kleinrock a várakozási sor elméletét bemutatja a csomagkapcsolás hatákonyságát. A csomagkapcsolt architektúra lehetővé teszi a hálózati kommunikációs eszközök és csatornák időben megoszott használatát több egység között.

1974: Cerf és Kahn megalkotják a hálózatok összekapcsolásának / együttműködésének architektúráját. Fontosabb elveik a minimalizmus, autonómia, azaz a hálózatok összekötéséhez nem kell azok belső struktúráját megváltoztatni.

A legjobb szándék szerinti szolgáltatásmodell, az állapontmentes forgalomirányítok és a decentralizált vezérlés.

2.2.2 Miért elosztott a DNS?

Ha a DNS központosított szolgáltatás lenne, több lehetséges probléma is felmerülne. Példáult a meghibásodások egy pontba koncentrálódnának, ez által akár az egész szolgáltatás is leállhatna. E mellett a forgalom volumene is jelentős problémát okozna, hisz eszközök százmilliói által generált kéréssorozatot kellene kielégítenie.  
Egyetlen DNS szerver nem lehetne elég közel minden eszközhöz , ez által távoli helyekről indított kéréseket csak hatalmas késleltetéssel tudna kiszolgálni a szerver.  
A DNS elosztottsága megkönnyíti a karbantartást is, mivel ha minden rekordot egy adatbázisban tartanánk akkor azt állandóan frissíteni kellene az új host-ok listájával.  
Összességében kijelenthető hogy nem skálázható a gondolat. Ezért lett a DNS elosztott.

2.1.5 Vesd össze röviden az TCP és az UDP szolgáltatásait.

**TCP:** Megbízható átvitelt biztosít a küldő és fogadó processzusok között.   
 Folyam szabályozás miatt a küldő nem árasztja el a vevőt.  
 Torlódás vezérlést alkalmaz, ami visszafogja a küldőt amikor a hálózat túl terhelt.  
 a TCP az általa összekapcsolt alkalmazásoktól "függetlenített" adatírási és adatküldési ütemezéssel/időzítéssel/sebességgel rendelkezik, és a minimális áteresztőképesség sem biztosított.  
 Kapcsolat orientált, tehát szükséges egy kapcsolat kialakítása a küldő és   
 fogadó között (SYN/ACK).  
**UDP:** Az átvitel megbízhatatlan a küldő és fogadó processzusok között.  
 Az UDP esetében nem biztosított a megbízhatóság, a folyam szabályozás,  
 a torlódás vezérlés, az időzítés, az áteresztőképesség garanciája, a  
 biztonság, de még a kapcsolat kiépítése sem.   
 Viszont lehetővé teszi hogy kapcsolat építése és bontás nélkül is üzeneteket  
 lehessen küldeni.

8.1.5 Ismertesd a man-in-the-middle támadást és ennek kezelését adó digitális tanúsítvány koncepciót.

Tegyük fel hogy A és B személyek kommunikálni szeretnének, de C személy rosszindulatú szándékkal ezt megpróbálja megakadályozni, jobban mondva lehallgatni.  
Ekkor C A-ként jelentkezik be B szemszögéből, és B-nek A szemszögéből.  
Az üzenetváltás közepén C áll aki így minden kommunikációt képes elfogni.  
Ezt elég nehéz észrevenni, hisz a felek mindent megkapnak amit a másik küld.  
A digitális tanúsítvány egy olyan koncepció mely lehetőséget ad hogy a hagyományos aláírást tudjuk helyettesíteni az informatika világában.  
Ez ellenőrízhető és nem hamisítható.