

IDK3070 "Kommunikatsioonivõrgud..."

(sügis 1999)

Eksam on kirjalik. Kasutada võib kasutada kõiki kirjalikke materjale ja Interneti vahendeid, välja arvatud elektronpost ja jututoad.

Allpool on loetletud teemad, millest on loengutel räägitud – põhiosa küsimusi eksamil ongi nende teemade kohta ja neile tuleb anda pikemad vastused.

Enamuse teemade järel on peenikeses kirjas loetletud teemad, mida loengutel on ehk ainult mainitud. Eksamiküsimused selliste teemade kohta on formuleeritud nii, et neile tuleb anda lühike vastus, kusjuures see vastus on suhteliselt hõlpsasti leitav Internetist.

Iga küsimuse K jaoks saab olema määratud max vastuse eest antav punktide arv P_K – seega võib vastuse eest saada 0.. P_K punkti. Eksamihinde määrab kogutud punktide summa.

Referaat ja HTML-lehekülg on võrdsustatud eksamiküsimustega - nende eest saadud punktid lähevad hinnet määravasse summasse.

1. Jaamad ja sidekanalid. Võrgu topoloogia. Kommunikatsiooni erinevad aspektid: marsruutimine, seanss, võrk kui jaotatav ressurss (pöördumine). Kommunikatsiooniteenuste liigitus: ühendusega ja ühendust loomata: datagrammid ja virtuaalne kanal. Kokkuleppe saavutamine võrgus. Valimised võrgus.

2. Võrgu protokollide mõiste. Protokollide mitmekihiline arhitektuur. ISO OSI etaloon(raam-)mudel. N-kiht, N-objekt, N-teenus, N-protokoll. (N/N-1)-liides. Info (paketi) liikumine kihist kihti. Service Access Point.

3. Füüsiline kiht. Bit- ja bait-orienteeritud protokollid. Repiiterid. Protokollide ATM ülesehitus.

- ✓ Ethernet'i kaabeldused 10Base2 ("peenike"), 10Base5 ("paks"), 10BaseT ("keerupaar")
- ✓ Cyclic Redundancy Check (CRC) arvutamine ja veakindlus
- ✓ ISDN – Integrated Services Digital Network

4. Kanali kiht. MAC alamkiht. Ligipääsumeetodid: CSMA/CD, markeriga siin, markeriga ring. LLC alamkihi stsenaariumid. Link Support Layer. Sillad.

- ✓ IEEE 802.4 Token-passing Serial Bus: kuidas liitub uus jaam loogilisse ringi?
- ✓ IEEE 802.5 Token-passing Ring: protokollide ülesehitus

5. Võrgu kiht ja selle alamkihid. Protokollid IP ja ICMP. ID struktuur. IP-tunneldamine.

- ✓ protokollide X.25 ja *Frame Relay* ülesehitus; nende võrdlus
- ✓ SLIP – Serial Line Internet Protocol (RFC 1055, 1144)
- ✓ PPP - Point-to-Point Protocol (RFC 1331)
- ✓ NAT – Network Address Translation (RFC 1631)
- ✓ IP Security (RFC 1826, 1827)
- ✓ ARP – Address Resolution protocol
- ✓ DHCP – Dynamic Host Configuration Protocol

6. Marsruutimise strateegiad. Dünaamiliste strateegiate Link State, Traditional Distance Vector ja Advanced Distance Vector võrdlus.

- ✓ OSPF – Open Shortest Path First (RFC 1247)
- ✓ RIP – Routing Information Protocol (RFC 1058)
- ✓ BGP – Border Gateway Protocol (RFC 1267)

7. Lülitavad sillad (switches). Virtuaalsed kohtvõrgud VLAN.

- ✓ VPN – Virtual Private Network
- ✓ Süsteem Privador: <http://www.cyber.ee/>

8. Transpordi kiht. Protokoll TCP. Pakettide fragmenteerimine ja defragmenteerimine. Pistikud (sockets).

- ✓ TCP ooteajad (taimerid) (RFC 761)
- ✓ UDP – User Datagram Protocol (RFC 768)
- ✓ TLS – Transport Layer Security (RFC 2246)

9. Tulemüürid, nende võimalik ülesehitus ja asend võrgus.

- ✓ Süsteem Barrikaad: <http://www.cyber.ee/>

10. Pakettide filtreerimise põhimõtted. Filtreerimisreeglite koostamise alused.

11. Hajussüsteemide turvalisus. Krüpteerimine avaliku ja salajase võtme meetodiga.

- ✓ krüptoalgoritmid DES ja RSA
- ✓ AES – Advanced Encryption Standard
- ✓ <http://home.cyber.ee/helger/crypto/>

12. Tuvastamine (autentimine) avaliku ja salajase võtme meetodiga. Digitaalne allkiri (signatuur). Sertifitseerimine.

- ✓ SSL – Secure Socket Layer
- ✓ Süsteem Kerberos: <http://www.kerberos.com/>
- ✓ Süsteem SSA: <http://www.cyber.ee/>
- ✓ Cuculus – Time Stamping System: <http://www.cyber.ee/infosecurity/projects/cuculus.html>

13. Seanssi kiht. Esituse kiht. Rakenduse kiht. Interneti protokollivirn.
Protokollid FTP, Telnet, SMTP ja MIME, DNS, HTTP. Cache, proxy.

- ✓ CCITT X.409 Presentation Transfer Syntax
- ✓ FTP – File Transfer Protocol (RFC 959) käsud.
- ✓ EDI – Electronic Data Interchange. EDIFACT.

14. Klient-server süsteemid. Ligipääs failidele hajussüsteemis:
transaktsioonid, tupiku vältimine.

- ✓ kolmekihilised klient/server-rakendused (näiteks: A & A, 1998, nr.2)
- ✓ tehinguhaldurid (transactions managers), näiteks A & A, 1998, nr.4.

15. Võrdne-võrdsega (*peer-to-peer*) süsteemid. Võrguvahendid süsteemis
Windows'95.

- ✓ JINI Technology (näit. A & A, 1999, nr.2)
 - ✓ WAP – Wireless Application Protocol (näit. Arvutimaailm, 1999, nr.9)
-