



Försättsblad tentamen/ Examination cover

Anonymkod / Anonymous code

0 0 0 1 - 0 8

Skriv anonymkod på varje ark / Write anonymous code on all sheets

0717296596

D T 2 0 1 7

Datorkommunikation och nät

0 5 0 0

Teori för datorkommunikation

2 0 1 5

- 1 0

- 2 6

Tentamensdatum / Exam date

Ifylles av tentamensvakt / To be filled by the invigilator

Antal inlämnade ark:

110

Signatur:

Don

Resultat / Results

Ifylles av lärare / To be filled in by teacher

1	2	3	4	5	6	7	8	9	10
5,5	4	5,5	1,5	5	1	3	Duggor 3,5		
11	12	13	14	15	16	17	18	19	20
								25,5	

S:a poäng	Betyg
29	3

Uppgift nr:
Question no:

1a

Poäng:
Score:

5,5

Lärarens anteckning:
Teacher's notes:

1a) 3p

b) 2,5p

IP-adress: 130.140.213.25

Subnetwork: 255.255.192.0

Klass B eftersom $128 < \underline{130} < 191$

XXXX.XXXX

IP:

Klass B \Rightarrow Network id: 130.140

Host id: 213.25

Subnet mask:

Network id: 255.255

Host id: 192.0

$$\frac{\text{Subnet mask host id}}{\text{IP host id}} = \frac{192.0_{10}}{213.25_{10}} =$$

$$= \frac{11000000.00000000}{11010101.00011001} =$$

• Subnetwork id: $11_2 = \underline{3}_{10}$

• Internal host id: $10101.11001_2 = \underline{21.25}_{10}$

Uppgift nr:
Question no:

1b

Poäng:
Score:Lärarens anteckning:
Teacher's notes:

N : anger antal routor i nätet + sändande dator

d_{proc} : Anger processen - tiden

d_{trans} : Anger transmission-tiden $\frac{L}{R}$, där L är antal
biter ett paket har och R är hastighet i bps.

d_{prop} : Anger distansen och hastighet av paketet

$$\frac{d}{c} = \frac{\text{distanst i m}}{\text{hastighet}} \leftarrow \begin{array}{l} 3 \cdot 10^8 \text{ m/s i etern} \\ 2 \cdot 10^8 \text{ m/s i fiber} \end{array}$$

Uttrycket dend-end kan approximeras om
distanse mellan noderna är väldigt långt
som i fallet av en satellit i rymden.

Lika tid i sändande dator och routor,
Samt d'que ne & C.

Uppgift nr:
Question no:

2a

Poäng:
Score:

4

Lärarens anteckning:
Teacher's notes:

?

2a) 2p

?

R

✓

?

2b) 2p

a.

- SMTP är ett skjutande protokoll
- Push/pull menas epost som blir skickad ^(push) och hämtad ^(pull) från epost-servern.
- HTTP används ofta för överföring av epostmeddelanden.
- IMAP kan användas för att skicka och ta emot meddelanden och användas främst i epost-klienter såsom Outlook.
- Dataformatet består av 7-bitsers ASCII.
Tillägget SMA ✓ används för att skicka andra format.
MIME
- Dataformatet iika tillägget överförs i audio-video-codec san använder FTP.
Genom det finns möjlighet att kunna överföra bilder osv. Beskrivning efterfrågas.

Uppgift nr:
Question no:

2b

Poäng:
Score:

—

Lärarens anteckning:
Teacher's notes:

- FTP skickas kontrollinformationen "out-of-band" R
- "in-band" menas att information skickas över på samma band?, som tex HTTP. \leftrightarrow
- "Out-of-band" skickar istället över information på olika band. \leftrightarrow ?
- Portarna 20 och 21 används av FTP. R x 2
- Port 21: Transfer data ✓ } ?
- Port 20: Transfer received data...
- FTP är tilståndorienterad och håller därför reda på information. R

Transportshiklet: logisk kom. mellan processer.

- a. (Transportshiklet kan ge en förbindelse-orienterad tjänst eller en förbindelselös tjänst. Med eller utan kitteringar.
- TCP ger en förbindelseorienterad tjänst vilket ger kitteringar.

b.

0101	0101	0101	0101	(1)
+ 1010	1010	1010	1010	(2)
1111	1111	1111	1111	(1+2)
1000	0000	0000	0000	(3)
(1) 0111	1111	1111	1111	wrap-around
			1	
1000	0000	0000	0000	(1+2+3)
+ 0111	1111	1111	1111	(4)
1111	1111	1111	1111	(1+2+3+4)

Checksumma = 1-komp (1+2+3+4) =

= 0000 0000 0000 0000

- c.
- Idle repeat request: Sändningsfönster
1
- Selective repeat : k/2
- Go-back-N : k-1

- d. $\alpha < 1$ Rekommenderas. ($\alpha = 0,125$)

- Man använder $estimated_{RTT}$ för att approximera värdet med olika störmåtar i åtanke.
- Man bestämmer RTT för att kunna beräkna hur lång tid det tar för ett paket att komma fram till mottagaren plus tiden för ett paket att komma tillbaka.

Uppgift nr:
Question no:

3

Poäng:
Score:

5,5

Lärarens anteckning:
Teacher's notes:

3a) 0,5p

b) 3p

c) 0,5p

d) 1,5p

R

Med k=16:

=8

=15

$R \times 2$

Vad för det?
Ja, $estimated_{RTT}$ används för att beräkna timeout-värde.
(R)

Uppgift nr:
Question no:

4

Poäng:
Score:

1,5

Lärarens anteckning:
Teacher's notes:

4a) 0,5 p

b) 1 p

- a. Routers huvuddelar består av brandvägg, switch, hubb och buffer. ← Både in och ut.

$$B = \frac{RTT}{C} \sqrt{=} = \frac{200 \cdot 10^{-3}}{1 \cdot 10^9} = 200 \text{ Mbps} \checkmark$$

- b. init $F = \{1\}$ [1] T-kostnad: 0

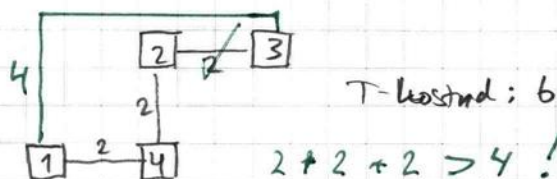
Billigaste väg ut först:

$$F = \{1, 4\} \quad [1] \xrightarrow{2} [4] \quad \text{T-kostnad: 2}$$

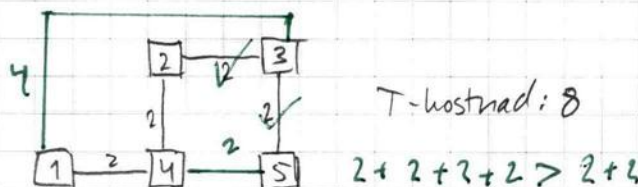
Sedan gå till lägsta nod på billigaste sätt:

$$F = \{1, 4, 2\} \quad [1] \xrightarrow{2} [4] \xrightarrow{2} [2] \quad \text{T-kostnad: 4}$$

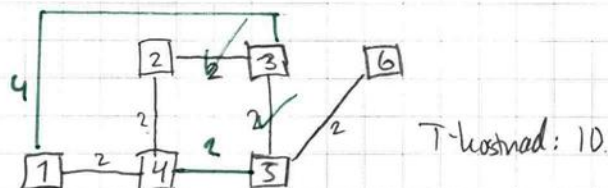
$$F = \{1, 4, 2, 3\}$$



$$F = \{1, 4, 2, 3, 5\}$$



$$F = \{1, 4, 2, 3, 5, 6\}$$



Alla noder uppfyllda: STOP!

Varför inte till "3" eller "5" före "2"?

Fel väg!

Fel väg!
Missförstått
av algoritman!

Lika kostnader
från "1" till
"2", "3",
och "5".
Regel bör
skrivas ut.
Ej poäng-
avdrag.

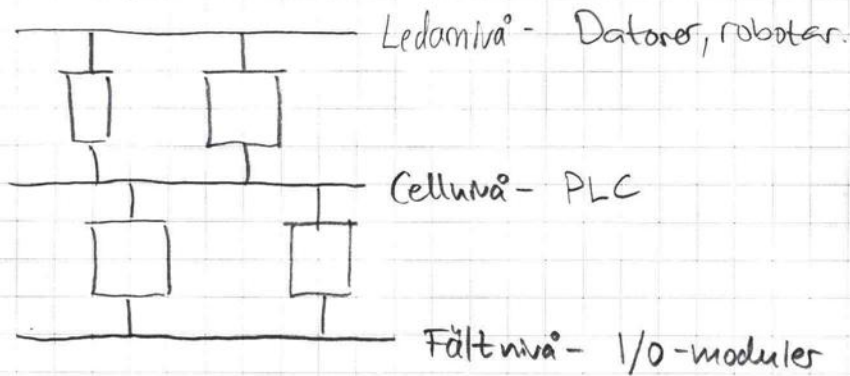
a.

Omsändning
nummern

	k	Intervall	
1	1	1	0-1
2	2	2	0-3
...	9	4	
10	10 (backoff)	...	0-1023
16	10	...	0-1023

Det används för att paket ska kollidera
med varandra en gång till efter en kollision
genom lägga tid väntetid på ett paket
innan den släpps ut igen. Max tio sekunder,
och då sker det back-off för att förhindra
att tiden växer.

b.



I den högsta nivån kan tex övervakningsystem
användas för att se till att systemet fungerar
utan problem.

Uppgift nr:
Question no:

5

Poäng:
Score:

5

Lärarens anteckning:
Teacher's notes:

5a) 1,5p

R x 3

b) 3,5p

R x 3
R x 3

R

Uppgift nr:
Question no:

6

Poäng:
Score:

1

Lärarens anteckning:
Teacher's notes:

6 a) 1p

b) 0

c) -

?

Fråga!
Piggybacking
för FEC.

a.

Best-effort innebär att paket skickas
så snabbt som möjligt men det garanteras

inte att det inte blir paket-loss. R2

(Den väntar dessutom inte på kutteringar)

b.

Piggybacking innebär att kutteringar skickas

samtidigt som ett önskemål om ett

nytt paket skickas. Vid omskickning av

ett föregående paket, fortsätter paket-

strömmen utan att bli störd av störningar.

c.

-

Uppgift nr:
Question no:

7.

Poäng:
Score:

3

Lärarens anteckning:
Teacher's notes:

7 a) 2p

b) 1p

c) 0

a. • Kryptering av meddelande med.
En privat nyckel skickas från avsändaren
som sedan måste dekrypteras med en
publik nyckel hos mottagaren.

Genom att använda digitala signaturer,
kan man säkerställa att "nyckeln"
är från korrekt sändare och att
nyckeln endast kan dekrypteras med
rätt dekrypteringsmetod hos mottagaren. + integritet!

$H(m)$ innebär att ett meddelande har
fått innehållet gömt genom hash-funktionen
som omvandlar text till chiffer.

Meddelande-chiffret krypteras senare hos
sändaren och skickas till mottagaren
som dekrypterar nyckeln och kollar ifall
det hashade meddelandet verkligen ska
till denna mottagare så meddelandet inte
syns ifall denne är obehörig.

Det är bättre att använda $K_S(H(m))$ istället
för bara $K_S(m)$. Lysas man dekryptera
 $K_S(m)$ genom nacking osv syns meddelandet
för alla; men om hashing-metod används syns
inte meddelandet även om dekryptering har
skett då bara en specifik mottagare kan
ta emot hash-meddelandet.

Uppgift nr:
Question no:

7.

Poäng:
Score:

—

Lärarens anteckning:
Teacher's notes:

b. WEP (Wireless Encryption Password)

Används i WLAN-nätverk (wireless) och ger möjlighet för användaren att skydda
sina nätverk och trafiken i den genom
kryptering och lösenord. R×2

c. IPsec använder protokollen, TCP och
HTTPS.✓
✓