Norwegian University of Science and Technology
Department of Telematics

Contact during exam [Faglig kontakt under eksamen]:
Bjarne E. Helvik (92667)

EXAM IN COURSE [EKSAMEN I EMNE]
TTM4120 Dependable Systems [Pålitelige systemer]

Wednesday [Onsdag] 2008-05-21
09:00 – 13:00

The English version starts on page 2.

Den norske bokmålsutgaven starter på side 5.

Hjelpemidler:
D - No printed or handwritten material is allowed. Predefined simple calculator [Ingen trykte eller håndskrevne hjelpemidler tillatt. Forhåndsbestemt enkel kalkulator]

Sensur 2008-06-12

English version[1]

This exam deals with some dependability issues related to the two layer network shown in Figure 1. In some of the questions, we regard a single network element or a single layer, and simplifying assumptions may be taken. The network has nodes in four sites, indexed 1 to 4. The nodes of the two layers, routers and SDH add-drop multiplexers, are co-located and the interconnection between the router and the multiplexer at the same site is fault free. It is also assumed that all nodes (routers and multiplexers) are fault free. The IP-layer network is fully meshed with bidirectional links between all nodes. The "IP-links" are carried by an unidirectional SDH ring.

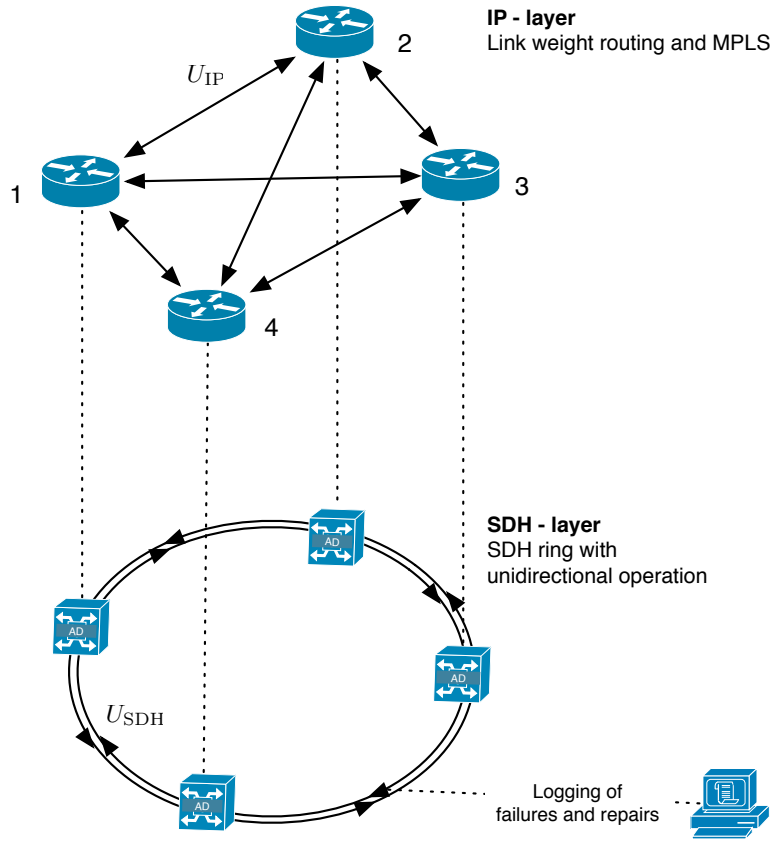


Figure 1: Sketch of the two layer network studied.

We monitor one of the SDH links in the network for more than $6\,000$ hours. The alternating up and down instants in the first $6\,000$ hours are logged, and the successive durations are listed in Table 1. At 6000 hours, the link is working. After a repair, the link is regarded as new.

a) What is the interval availability observed for the link during the first $6\,000$ hours of operation? Make a plot of the empirical reliability function. (The scaled paper on Page 8 may be used.)

[1] In case of divergence between the English and the Norwegian version, the English version prevails.

Table 1: Observed up and down times in hours of a link.

Up times	32	2158	16	9	2307	271	32	33	627	115
Down times	7.6	10.2	9.1	7.6	5.8	8.2	9.5	12.7	17.5	8.4

b) What is the observed mean down time? From the observations in Table 1, what do you consider to be the more likely down time distribution i) a negative exponential distribution or ii) a gamma distribution? Motivate the answer.

Observing the link for a longer period, the reliability function of the link is found to be best modelled by $R_L(\tau) = \exp(-(\lambda\tau)^\alpha)$. Link failures occur independently of the time between preceding failures.

c) What is the the name of the distribution? What is the failure rate? If $\alpha = 1/2$, what is the failure rate when $\tau \to \infty$? Given that $\int_0^\infty R_L(\tau)\, d\tau = \lambda^{-1}\Gamma(\alpha^{-1} + 1)$, what is the failure intensity of the link when $t \to \infty$, where t denotes the time since the system was put into operation?

In the next question, assume that the unavailability of a link in the IP-layer is U_{IP} and that links fail and are repaired independently of each other.

d) Draw the necessary reliability block diagrams and find the availability of communication (connectivity) between nodes 4 and 2 when i) at most one link (one leg) may be used to establish a connection, ii) when at most two links (two legs) may be used and iii) when there is no limitation on the number of links used. It is not necessary to simplify the expressions for the availability.

Three options are considered for ensuring the availability of communication between nodes 4 and 2: i) 1+1 protection, ii) 1:1 protection and iii) restoration.

e) Explain shortly how the three options may be realised at the IP-layer. Use the assumptions above of independent links failures and repairs, and disregard the time needed to establish and/or put an alternate route/path into operation. Determine the availability of communication (connectivity) between nodes 4 and 2 when recovery options i), ii) and iii) are used. Simplification of the expressions for the availabilities is not required.

Regard the case where there is no limitation on the number of links used. All IP layer links have capacity $C_{ij} = 2$. The offered traffic between nodes i and j is $\mathsf{A}_{ij} = 1$ and the traffic is symmetrical, i.e. $\mathsf{A}_{ij} = \mathsf{A}_{ji}$.

f) The network is regarded as intact only when all offered traffic is carried, i.e. all nodes can communicate with any other without loss or reduction of the offered traffic. Will the IP-layer network be intact with one, two and three link failures? Motivate the answer. Hint, use that the network is symmetrical. Use the assumptions above of independent links failures and repairs, and disregard the time needed to establish and/or put an alternate route/path into operation.

All the traffic between two nodes will follow the same route (non bifurcation). Determine the availability of the IP layer network.

Regard both network layers in Figure 1. The failures of the IP-layer links can no longer be regarded as independent. All the traffic between two nodes will follow the same route (non bifurcation). An IP-link may fail for two reasons:

- the router interface or other equipment specific for a single link fails. These failures occur and are repaired independently of each other and of failures at the SDH-layer. The link unavailability due to these failures is U^*_{IP}. The time to these failures is n.e.d. and the failure intensity for a link is λ_{IP}.
- the SDH-layer does not support the link. The time to these failures is n.e.d., and the intensity as seen by an IP-link is λ_{SDH}.

Assume that the links on the SDH-layer fail and are repaired independently of each other and of failures at the IP-layer. Failures affect both directions. The unavailability of a SDH-layer link is U_{SDH}.

g) With the assumptions above, determine the availability of the two layer network when the network is regarded as intact only when all offered traffic are carried. Hint, identify the failure modes that takes the network down.

Regard a router r using a link $[r, d]$ for forwarding packets toward a destination d. When the link fails, either due to the failure of equipment specific for the link at the IP-layer, e.g. an interface card, or due to a failure at the SDH-layer, the router will for some time not be able to forward packets on an established route to the destination. Denote this time T_d. If the failure is on the SDH-layer, the connection (IP-link) will be recovered in a negative exponentially distributed (n.e.d.) time T_{SDH} with expectation μ^{-1}_{SDH}. In this case, the router takes no action. If the failure is due to equipment specific for the link at the IP-layer, the router will detect it in an n.e.d. time with expectation μ^{-1}_{det}. The router then waits a time with expected duration $5\mu^{-1}_{\text{SDH}}$, not to interfere with a potential ongoing SDH-layer recovery. For the sake of simplicity this time is also assumed to be n.e.d. The router will then mark the link as down and trigger a rerouting process in the network. After a n.e.d. time T_r with expectation μ_r^{-1}, a new route to the destination is established.

The repair time of a failure at the SDH-layer and a failure at the IP-layer are both n.e.d. with expectations θ_{SDH} and θ_{IP} respectively. After a repair at the SDH-layer, it is reconfigured to fault free operation in the time T_{SDH} as after a failure. After a repair at the IP layer, the routing in r is changed with no impairment of the traffic flow.

h) Assume at most one failure at a time. Draw a state diagram that may be used to find the unavailability of a route from r to d due to the recovery delays. For each state indicate whether the system is working or not and specify the operational mode of the system (e.g. No link failures, fault free operation).

Norsk bokmål utgave[2]

Denne eksamen omhandler pålitelighetsproblemstillinger knyttet til nettet med to lag vist i Figur 1 på side 2. I noen av spørsmålene betraktes kun ett nettelement eller ett lag, og forenklende antakelser kan bli tatt. Nettet har noder plassert fire steder. Disse er indeksert 1 til 4. Nodene på de to lagene, rutere og SDH "add-drop" multipleksere er plassert på samme sted, og forbindelsen mellom dem er feilfri. Det er også antatt at alle noder (rutere og multipleksere) er feilfrie. Nettet på IP-laget er fullstendig maskenett med bidireksjonale lenker mellom alle noder. "IP-lenkene" er ført av en unidireksjonell SDH ring.

Vi overvåker en av SDH lenkene i nett i mer enn $6\,000$ timer. De alternerende tidspunktene hvor lenken går opp og ned i løpet av de første $6\,000$ timene er logget og de ulike varighetene av påfølgende oppe- og nedetider er vist i Tabell 2. Ved 6000 timer er lenken oppe (arbeidende). Etter hver reparasjon kan lenken pålitelighetsmessig betraktes som ny.

Tabell 2: Observerte oppe og nede tider for en lenke målt i timer.

Oppe tider	32	2158	16	9	2307	271	32	33	627	115
Nede tider	7.6	10.2	9.1	7.6	5.8	8.2	9.5	12.7	17.5	8.4

a) Hva er den observerte intervalltilgjengeligheten for lenken de første $6\,000$ driftstimene? Lag et plott av den empiriske funksjonssannsynligheten (reliability function). ("mm-papiret" på side 8 kan brukes om ønskelig.)

b) Hva er den observerte midlere nedetid? Fra observasjonene i Tabell 2, hva anser du for å være den mest trolige underliggende nedetidsfordelingen i) en negativ eksponensial fordeling eller ii) en gamma fordeling? Begrunn svaret.

Ved å observere lenken over et lengre tidsrom finner en at dens funksjonssannsynlighet best kan modelleres ved $R_L(\tau) = \exp(-(\lambda\tau)^\alpha)$. Lenkefeil inntreffer uavhengig av tidene mellom tidligere feil.

c) Hva kalles (navnet) denne fordelingen? Hva er feilraten? Hvis $\alpha = 1/2$, hva er feilraten når $\tau \to \infty$? Gitt at $\int_0^\infty R_L(\tau)\,d\tau = \lambda^{-1}\Gamma(\alpha^{-1}+1)$, hva er feilintensiteten til lenken når $t \to \infty$ hvor t angir tiden siden systemet var satt i drift?

I neste spørsmål, anta at utilgjengeligheten til en lenke på IP-laget er U_{IP} og at lenkene feiler og blir reparert uavhengig av hverandre.

d) Tegn de nødvendige pålitelighetsblokkskjema og bestem tilgjengeligheten av kommunikasjon (forbindelse) mellom node 4 og node 2 når i) maksimalt en lenke (ett hopp) kan benyttes til å

[2] I tilfelle uoverensstemmelse mellom den engelske og norske utgaven, er det den engelske som er gjeldende. Engelske betegnelser anvendes hvor ingen norsk oversettelse ble funnet.

etablere forbindelsen, ii) maksimalt to lenker (to hopp) kan benyttes til å etablere forbindelsen, og iii) når det ikke er noen begrensning på hvor mange lenker som kan benyttes. Det er ikke nødvendig å forenkle uttrykkene for tilgjengeligheten.

Tre muligheter vurderes for å sikre tilgjengeligheten til kommunikasjon mellom nodene 4 og 2: i) 1+1 beskyttelse (protection), ii) 1:1 beskyttelse (protection) og iii) gjenoppretting (restoration).

e) Forklar kort hvordan de tre mulighetene kan realiseres på IP-laget. Bruk antakelsene over om uavhengige lenkefeil og -reparasjoner, og se bort i fra tiden som er nødvendig tid for å etablere en annen rute/vei og/eller sette denne i drift. Bestem tilgjengeligheten til kommunikasjon (forbindelse) mellom nodene 4 og 2 når "recovery" mulighetene i), ii) og iii) benyttes. Det kreves ikke at uttrykkene for tilgjengelighetene forenkles.

Betrakt tilfellet hvor det ikke er noen begrensning på antall lenker som kan benyttes til "recovery". Alle IP-lag-lenkene har kapasitet $C_{ij} = 2$. Den tilbudte trafikken mellom nodene i og j er $\mathsf{A}_{ij} = 1$, $\forall i \neq j$ og trafikken er symmetrisk, dvs.. $\mathsf{A}_{ij} = \mathsf{A}_{ji}$.

f) Nettet regnes om intakt kun når all tilbudt trafikk blir ført, d.v.s. alle noder kan kommunisere med alle andre uten å redusere tilbudt trafikk eller få tap. Vil IP-lag-nettet være intakt med en, to og tre lenkefeil? Begrunn svaret. Hint, bruk at nettet er symmetrisk. Bruk antakelsene over om uavhengige lenkefeil og -reparasjoner, og se bort i fra tiden som er nødvendig for å etablere en annen rute/vei og/eller sette denne i drift. All trafikken mellom to noder vil følge den samme ruten (non bifurcation). Bestem tilgjengeligheten til nettet på IP-laget.

Betrakt begge nettlagene i Figur 1 på side 2. Feilene til lenkene på IP-laget kan ikke lenger betraktes som uavhengige. All trafikk mellom to noder vil følge den samme ruten (non bifurcation). En IP-lenke kan feile av to grunner:

- ruter "interfacet"eller annet utstyr som er spesifikt for en enkelt lenke failer. Disse feilene antas å inntreffe og bli reparert uavhengig av hverandre og feil på SDH laget. Lenkeutilgjengeligheten på grunn av disse feilene er U^*_{IP}. Tiden til disse feilene er n.e.d. og feilintensiteten for en lenke er λ_{IP}.
- SDH-laget fører ikke lenken. Tiden til disse feilene er n.e.d. og intensiteten sett fra en IP-lenke er λ_{SDH}.

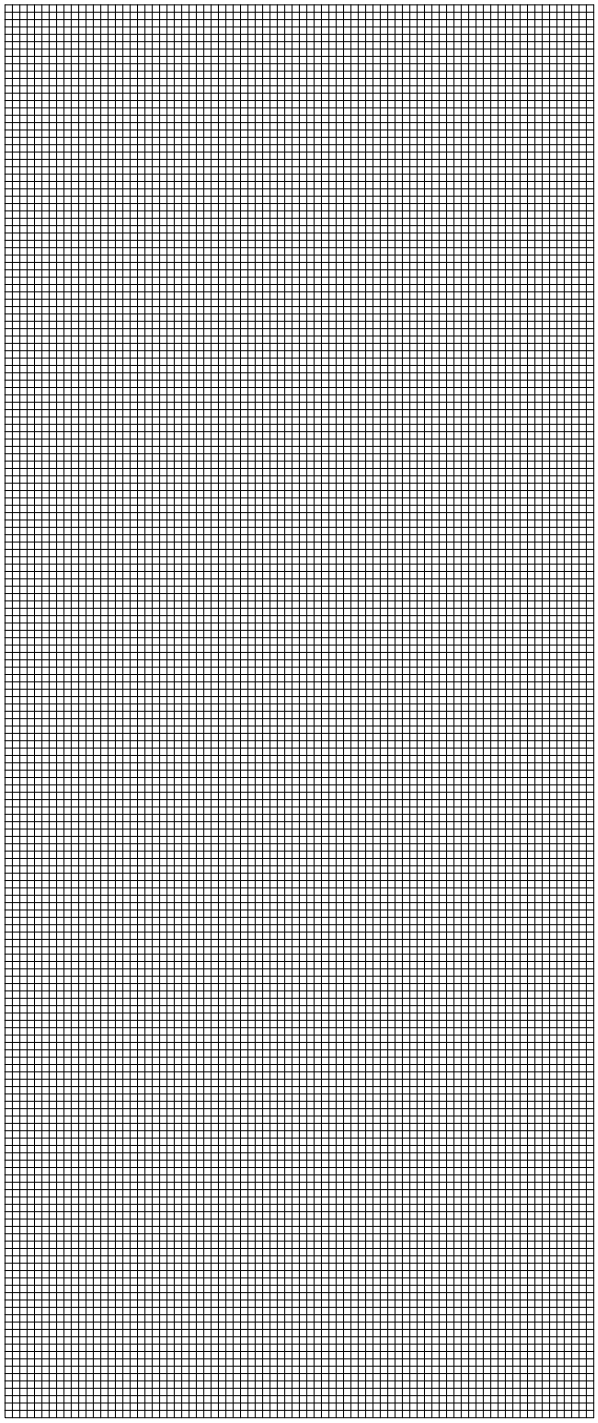
Anta at lenkene på SDH-laget feiler og blir reparert uavhengig av hverandre, og av feil på IP-laget. Feil påvirker (tar ned) begge retningene. Tilgjengeligheten til en SDH-lenke er U_{SDH}.

g) Med antakelsene ovenfor, bestem tilgjengeligheten til tolagsnettet når det anses for å være intakt (oppe) kun når all tilbudt trafikk blir ført. Hint, identifiser hvilke feilmodi som tar ned nettet.

Betrakt en ruter r som bruker lenken $[r, d]$ til å sende pakker til destinasjon d. Når lenken feiler, enten på grunn av utstyrsfeil på IP-laget spesifikk for lenken, eller på grunn av en feil på SDH-laget, så vil ruteren i noen tid ikke være i stand til å sende pakker langs en etablert rute til destinasjonen. Kall denne tiden T_d. Hvis feilen er på SDH-laget, så vil forbindelsen (IP-lenken) bli gjenopprettet i løpet av en negativ eksponensial fordelt (n.e.d.) tid T_{SDH} med forventning μ_{SDH}^{-1}. I dette tilfellet vil det ikke skje noen feilhåndtering i ruteren. Hvis feilen skyldes utstyrsfeil på IP-laget, vil ruteren detektere dette i løpet av en n.e.d. tid med forventning μ_{det}^{-1}. Ruteren venter så en tid med forventning $5\mu_{\text{SDH}}^{-1}$, for ikke å interferere med en eventuell pågående "recovery" på SDH-laget. For enkelhets skyld antas også denne tiden å være n.e.d. Ruteren vil så markere lenken som nede og starte en rerutingsprosess i nettet. Etter en n.e.d. tid T_r, med forventning μ_r, blir en ny rute til destinasjonen etablert.

Reparasjonstiden av feil på IP-laget og på SDH-laget er begge n.e.d. med forventninger på hhv. θ_{SDH} og θ_{IP}. Etter en reparasjon på SDH-laget rekonfigureres det til normal drift i løpet av T_{SDH} som ved feil. Etter en reparasjon på IP-laget, vil rutingen i r endres uten at det har noen skadevirkninger for trafikk-flyten.

h) Anta at maksimalt en feil inntreffer ad gangen. Tegn et tilstandsdiagram som kan benyttes for å finne utilgjengeligheten av en rute fra r til d på grunn av feilhåndteringsforsinkelser (recovery delay). For hver tilstand, angi om systemet arbeider (er oppe) eller ikke, og angi det operasjonelle modus til systemet. (F.eks. Ingen lenkefeil, normal drift.)



Student nr.: .....

Eksamen i fagnr./emnekode: TTM4120

Studieprogram: .....

Dato: 2008-05-21

Antall ark:.....