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 10.

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.

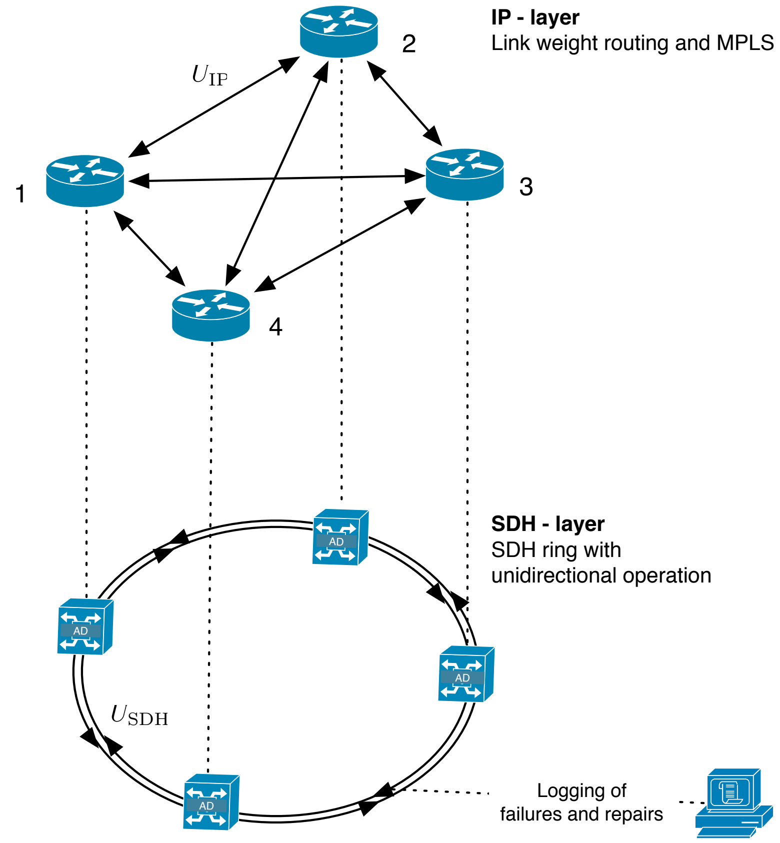


Figure 1: Sketch of the two layer network studied.

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 13 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

The data

TableForm[{fint, dtimes}]

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

The interval availability

Aint = 1 − (dtimes.Table[1, {Length[dtimes]}]/6000) =0.9839

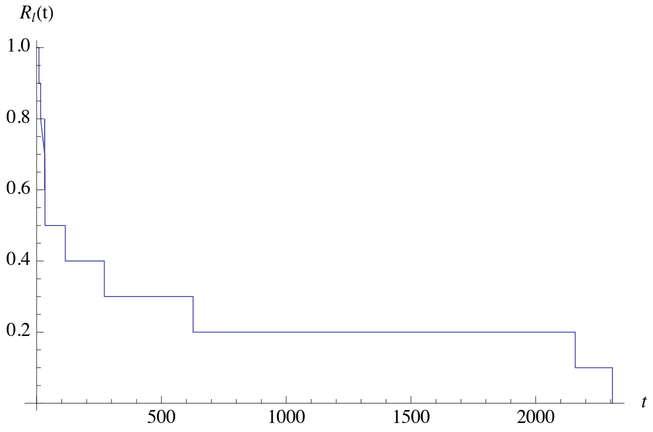
The reliability function plot

Sort the up times in ascending order **T_F = Sort[fint];**

Create a list of couples {t,R(t)} **R_e = Table [{T_F[[i]], 1 − i /Length [T_F]} , {i, Length [T_F]}] ;**

Add the value for t=0 to the list, R(0)=1.**R_e = Prepend [R_e, {0, 1}] ;**

Generate the plot, **p1 = StepPlot [R_e] ; Show [p1, AxesLabel → {t, "R_l(t)"}]**

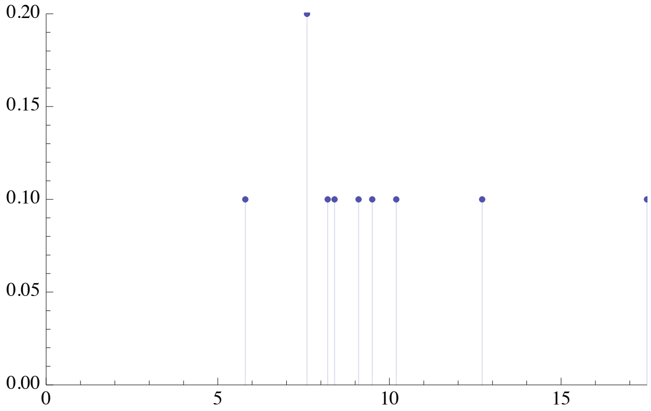


b) What is the observed mean down time? From the observations in Table 1, what do you consider to be the more likely down time distribution i) a negative exponential distribution or ii) a gamma distribution? Motivate the answer.

The mean down time observed

dtimes.Table[1, {Length[dtimes]}]/Length[dtimes] = 9.66 or **Mean[dtimes]** = 9.66

Distribution



There are very few up interval durations close to zero where we would have found most the durations in case i). The data is clustered below the mean, with a small tail. This is characteristic for a gamma distribution with a shape parameter larger than $3 \sim 5$.[2]

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?

Weibull distribution.

The failure rate is $\lambda_w(\tau) = \alpha\lambda(\lambda t)^{\alpha-1}$. [This may either be remembered, see eq. (1.9) in the lecture notes, or derived, see section 1.3.1 in the lecture notes.] $\lim_{\tau\to\infty} \lambda_w(\tau)||_{\alpha<1} = 0$.

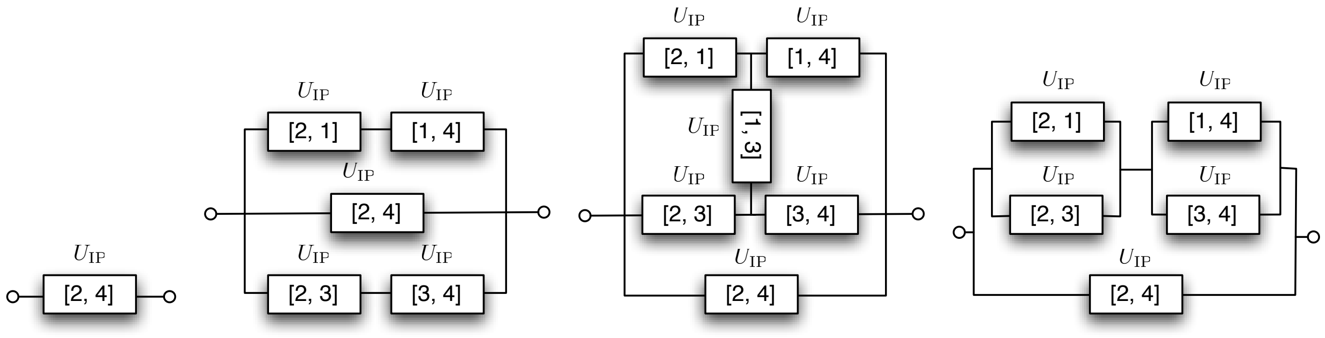
The limiting failure intensity is the inverse of the expected time between failures, see eq. (1.19) in the lecture notes. Hence, $\lim_{t\to\infty} z_w(t) = \lambda\Gamma(\alpha^{-1}+1)^{-1}$ or $1/(\lambda^{-1}\Gamma(\alpha^{-1}+1)+\text{MDT})$ if the down times are accounted for. (Both answers are OK since the question does not give hints that the MDT should be considered.)

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.

[2] In this case, the parameter used for generation is 10.

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.

Block diagrams for the three cases are shown in the figure below. Case iii) yields a bridge structure. Conditioning on whether element [1, 3] do not work or work, reduces it to two series parallel structures, iii.1) and iii.2) respectively.



i) ii), iii.1) iii) iii.2)

$\mathbf{Link} = \{1 - U_{\mathrm{IP}}, 1\}\,;$

$A_{ii} = (\mathbf{SysC1} = \mathbf{Link} \coprod (\mathbf{Link} \sqcap \mathbf{Link}) \coprod (\mathbf{Link} \sqcap \mathbf{Link}))//\mathbf{First} = 1 - (1 - (1 - U_{\mathrm{IP}})^2)^2 U_{\mathrm{IP}}$

$A_{ii}//\mathbf{Simplify} = 1 - 4U_{\mathrm{IP}}^3 + 4U_{\mathrm{IP}}^4 - U_{\mathrm{IP}}^5$

$(\mathbf{SysC2} = \mathbf{Link} \coprod ((\mathbf{Link} \coprod \mathbf{Link}) \sqcap (\mathbf{Link} \coprod \mathbf{Link})))//\mathbf{First} = 1 - U_{\mathrm{IP}} (1 - (1 - U_{\mathrm{IP}}^2)^2)$

$A_c = \mathbf{BridgeStruct[Link, SysC2, SysC1]//First}$

$= (1 - U_{\mathrm{IP}}) (1 - (1 - (1 - U_{\mathrm{IP}})^2)^2 U_{\mathrm{IP}}) + (1 - (1 - U_{\mathrm{IP}})^2)^2 U_{\mathrm{IP}} (1 - U_{\mathrm{IP}} (1 - (1 - U_{\mathrm{IP}}^2)^2))$

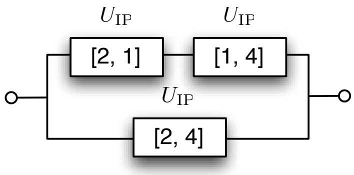
$A_{iii}//\mathbf{Simplify} = 1 - U_{\mathrm{IP}} + 4U_{\mathrm{IP}}^4 - 4U_{\mathrm{IP}}^5 - 7U_{\mathrm{IP}}^6 + 8U_{\mathrm{IP}}^7 + 2U_{\mathrm{IP}}^8 - 4U_{\mathrm{IP}}^9 + U_{\mathrm{IP}}^{10}$

The reductions, as carried out by the Simplify command is not required.

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.

*ad i) and ii):*1+1 and 1:1 protection may be realised by using two LSPs (MPLS label switched paths) between the two nodes. The difference is that in 1+1 protection the packets will continuously be sent on both paths, while in the 1:1 case, they will be sent on only one path. Switching of paths will require some signalling and incur a small delay. Disregarding this delay (see text) the dependability model becomes the same. Using the direct paths as one of the two, the model and availability becomes:



$A_{\text{Prot}} = 1 - (1 - (1 - U_{\text{IP}})^{2})\, U_{\text{IP}} = U_{\text{IP}}^{3} - 2U_{\text{IP}}^{2} + 1$

*ad iii):*In the restoration case, a working route between the nodes are found by the link weigh routing protocol applied (is-is or ospf). This will always find the shortest route, if any, corresponding to case iii) in question d).

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 the following failure modes:

- When there are no link failures, ϕ_0, all the traffic are carried, $I(\mathsf{A}_{ij}, \phi_0) = 1,\ \forall i, j.$
- With one link failure,$\phi_x,\ x = 1, \ldots, 6$, all the traffic is still carried, $I(\mathsf{A}_{ij}, \phi_x) = 1,\ x = 1, \ldots, 6,\ \forall i, j$. (This is easily seen since the network is symmetrical.)
- With two or more link failures,$\phi_x,\ x \geq 7$, traffic will be lost, $\exists i, j,\ I(\mathsf{A}_{ij}, \phi_x) = 0,\ x \geq 7$ and the network will be down (not intact). This is seen by regarding two failed links in the two cases, using that the network is symmetrical:
  - Failed links are connected to the same node. In this case it is trivially seen that the remaining link is overloaded.
  - Failed links are not connected to the same node, i.e. each node is still connected to two working links. However, studying the feasible route sets, no rout-set is found which does

not require the use of one link for three streams, e.g. links 1,3 and 2,4 are failed

s<->d \ link	1,2	1,4	2,3	3,4
1<->2	x			
1<->3		x		x
1<->4		x		
2<->3			x	
2<->4			x	x
3<->4				x

- A network with more than two link failures can not carry more traffic.

Hence,

$$A_{\text{traffic}} = \sum_{\forall x} \Pr(\phi_x) \prod_{\forall i,j} I(\mathsf{A}_{ij}, \phi_x) = \sum_{x=0}^{6} \Pr(\phi_x) = (1-U_{\text{IP}})^6 + 6U_{\text{IP}}(1-U_{\text{IP}})^5 = -\left(U_{\text{IP}} - 1\right)^5 \left(4U_{\text{IP}} + 1\right)$$

The last simplification is not required.

The question may also be solved by using binomials.

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.

Any single link failure on the SDH-layer will not have any effect on the IP-layer. Any double link (or more) failures will cause several link failures on the IP-layer (the network will be partitioned) and a traffic loss. It is possible, but tedious and unnecessary in this simple symmetrical case, to determine in detail the effect of each SDH-layer failure on the IP-layer. Hence, we simplify and introduce the failure modes ψ_x of the SDH-layer, i.e.

- When there are no link failures, ψ_0, all the traffic are carried, $I(\mathsf{A}_{ij}, \psi_0) = 1$, $\forall i, j$.
- With one link failure,ψ_x, $x = 1, \ldots, 4$, all the traffic is still carried, $I(\mathsf{A}_{ij}, \psi_x) = 1$, $x = 1, \ldots, 1$, $\forall i, j$.
- With two or more link failures,ψ_x, $x \geq 5$, traffic will be lost, $\exists i, j$, $I(\mathsf{A}_{ij}, \psi_x) = 0$, $x \geq 5$ and the network will be down.

Hence, we have for this layer

$$A_{\text{SDH}} = \sum_{\forall x} \Pr(\psi_x) \prod_{\forall i,j} I(\mathsf{A}_{ij}, \psi_x) = \sum_{x=0}^{4} \Pr(\phi_x) = (1 - U_{\text{SDH}})^4 + 4U_{\text{SDH}}(1 - U_{\text{SDH}})^3$$

It is seen that if we interpret the solution in question f) to be the availability with respect to failures occurring in equipment on the IP-layer we obtain a series system of the layers. The two layer network is available if both layers are available, that is$A_{\text{two-layer}} = A_{\text{traffic}}|_{U_{\text{IP}} \rightarrow U^*_{\text{IP}}} \cdot A_{\text{SDH}}$.

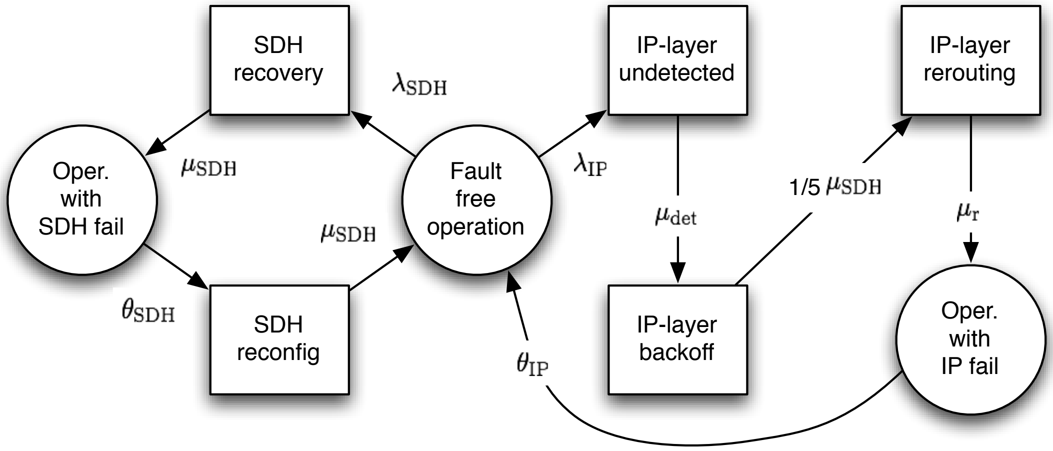
An alternative formalism, based on the discussion above, is to regard the two layer system as a series of a 5-out-of-6 system and a 3-out-of-4 system.

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_{SDH}^{-1}. 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_{det}^{-1}. The router then waits a time with expected duration $5\mu_{\text{SDH}}^{-1}$, 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).

See figure below.



(At the exam, a number of students regarded the case where we may have a simultaneous IP and SDH link failures, i.e. the at most one failure at a time assumptions is only partially used. This is of course correct, but yields a more complex diagram. Some students had also modelled the repair as starting immediately after the failure, i.e. the repair may be completed before the recovery. This is not what happens in a real system, but since it is not stated in the text, this solution is also accepted. Anyhow, due to the differences in time constants, the deviation in numerical results between these to models are negligible.