NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4120 Dependable systems

Academic contact during examination: Bjarne E. Helvik

Phone: 92667

Examination date: 2013-05-24

Examination time (from-to): 09:00 - 13:00

Permitted examination support material: (D) No printed or hand-written support material is allowed. A specific basic calculator is allowed.

Other information: Sensur 2013-06-14

Language: English

Number of pages: 9

Number of pages enclosed: 1

Checked by:

Date Signature

We regard a cellular access network as illustrated in Figure 2. It is constituted by 4 identical base stations which are covering an area as shown in the figure. The base stations are connected to a controller with individual cables. These are laid in ditches that are shared between cables in some stretches, as illustrated. The lengths, $\ell_1, \dots, \ell_4$, of cables and ditches are as indicated in Figure 2.

The following information is available for the various elements of the access network:

Base station The base station are subject to three types of failures. $1)$ Non-permanent failures due to transient, logical failures, etc. These failures may be rectified by a restart of the base station. The intensity of these failures in a base station is λ_t. $2)$ Permanent failure of the base station electronics, which occurs with intensity λ_p. $3)$ Failure (damage) of the base station infrastructure, i.e. antennas, tower, cabling, housing, power supply, etc. The accumulated intensity of this type of failures is λ_i. All failures occur independently.

When a base station failure is detected, a restart will always be attempted. A restart takes the time T_t. If the restart does not succeed, a repairman visits the site. If it is a permanent failure of the electronics, he will repair the failure and the base station returns to operation. If it is an infrastructure failure, he will write a damage report. The repairman's visit to the site takes the time T_p whether he manages to repair the electronics by himself or if he has to write a report. However, infrastructure failures will need to be repaired by a special crew and this operation will take time T_i. See Figure 1 for an illustration. All $T_x$es are independent of each other and negative exponentially distributed parameter μ_x, where $x \in \{t, p, i\}$.

Cable Cables, as illustrated in the figure, provide bi-directional links between their termination points. A cable has a constant failure intensity per length unit of α_c. (Hence, the failure intensity of the cable between the lower right base station and the controller is $\alpha_c \ell_4$.) All failures occur independently. All cable failures affect both directions. The mean repair time of a cable failure is d_c.

Ditch A ditch failure implies that all cables in the ditch fail. (A common cause of a ditch failure is a digger accidentally cutting the cables.) Ditch failures have a constant failure intensity per length unit of α_g. All failures occur independently. The mean repair time of a ditch failure is d_g. When a ditch failure is repaired, all cables affected by the failure is repaired at the same time.

Controller The availability of the controller is A_s and its mean down time is d_s. It may be assumed that the failure process is Poisson. The connection between the controller and the core network does not fail.

A user that is covered by more base stations, like **B** in Figure 2, may connect to any of these stations. If a connection through a base station fails, reestablishing a connection through another base station takes in this context a negligible time.

For the sake of simplicity, we do not regard service failures due to failures of the radio link between user and base station.

a) Let say user **A** in Figure 2 is connected to the core network. What is the failure intensity, λ_A, experienced by user A? If the connection to this user lasts for a time θ_s, what is the expression for probability that it will be completed without being interrupted? Let say the probability density function for the duration of connections is $f_\theta(t)$, give an expression for the probability that a connection will be interrupted.

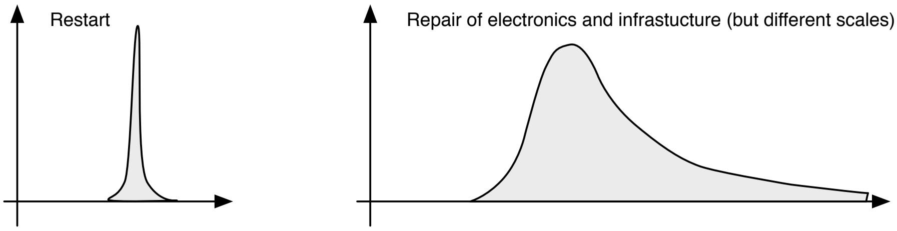
$$\begin{aligned}\lambda_A &= \lambda_t + \lambda_p + \lambda_i + (\alpha_c + \alpha_g)(\ell_1 + \ell_2) + (1 - A_s)/(A_s d_s) \\ R_A(\theta_s) &= \exp(-\lambda_A \theta_s) \\ P_A\{\text{Connection failure}\} &= \int_{\theta=0}^{\infty} R_A(\theta) \cdot f_\theta(\theta) d\theta\end{aligned}$$

b) The negative exponential distribution of T_x, $x \in \{t, p, i\}$ is an approximation for mathematical tractability. More precisely why is this approximation made? Discuss briefly (approximately a half hand written page) how well it will fit real distributions for the duration of these activities and make simple sketches of how the density distributions (pdf) typically will look like. No scales are required.

The approximation is introduced to give the system Markov properties, i.e. the all information about the past history of the system (included the time in the current state) is contained in the current state of the system, i.e. the memoryless property.

The restart time is a (near) deterministic activity and will have a corresponding distribution, i.e., it has a poor fit to the n.e.d.

The electronics and infrastructure repair times will include significant administrative and logistic delays in addition to the active repair time. Hence, there will by no immediate repairs. These three activities has high variability and may have heavy tails and the times T_x, $x \in \{p, i\}$ will look more like the density distributions below.



Regard a single base station.

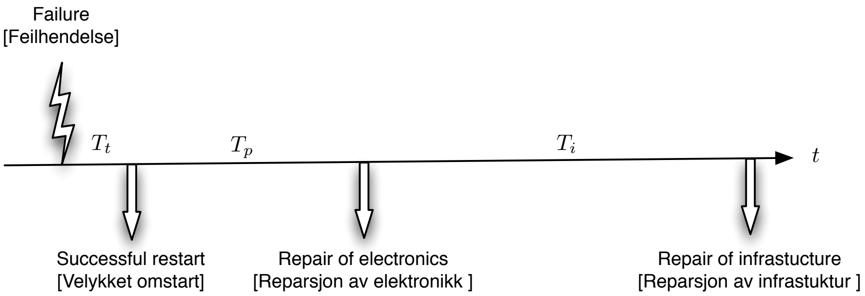


Figure 1: Illustration of base station failure rectification procedure.

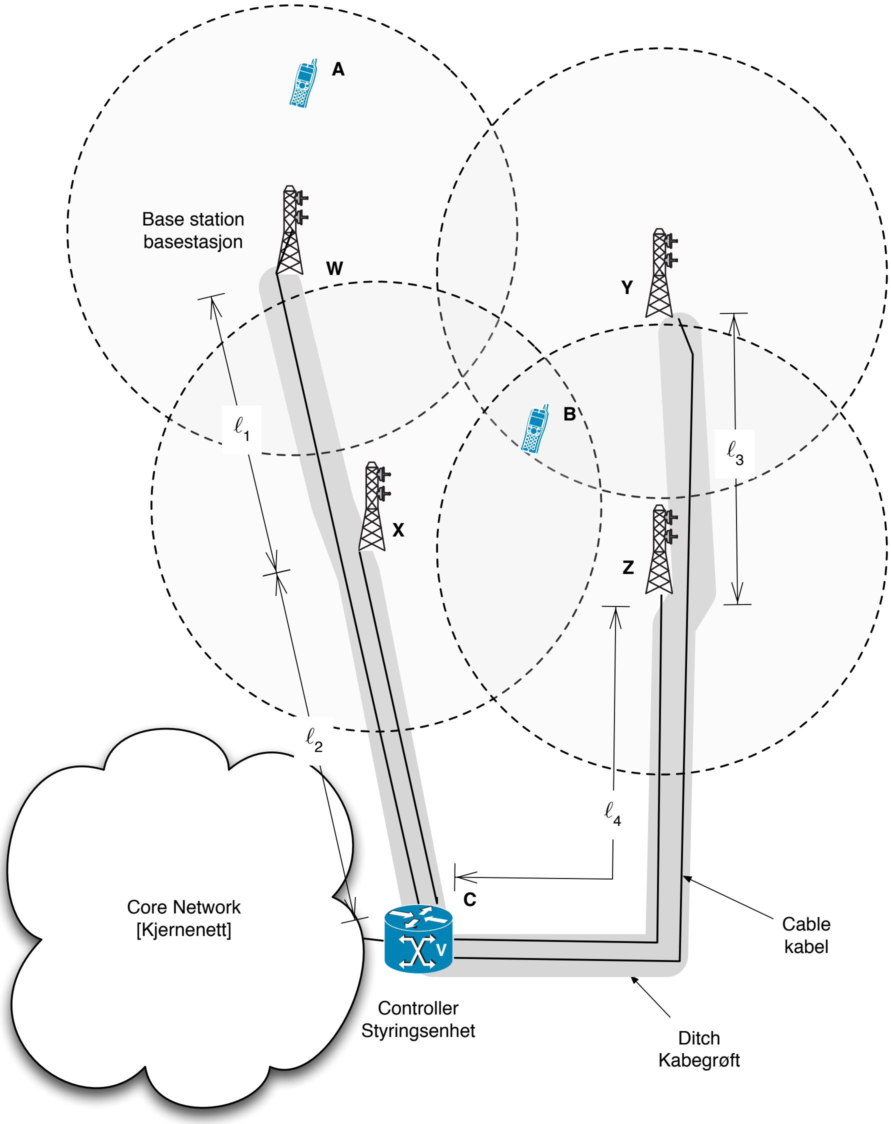
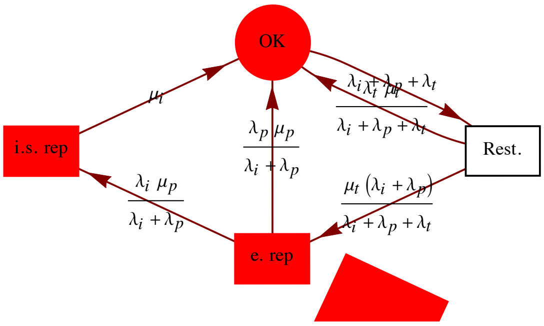


Figure 2: Cellular access network

c) We would like to find the asymptotic availability A_{bs} of the base station. Establish a Markov model for the base station using the information about the failing and fault handling described above. Based on this model, establish a set of equations that may be used to determine A_{bs}.

Note that the ouput intensity of the first restoration states must be made proportional to the relative failure intensities, which corresponds to the failure type occurrence probabilities.


OK
μ_i
i.s. rep
$\frac{\lambda_p \mu_p}{\lambda_i + \lambda_p}$
$\lambda_i + \lambda_p + \lambda_t$
$\frac{\lambda_t \mu_t}{\lambda_i + \lambda_p + \lambda_t}$
Rest.
$\frac{\lambda_i \mu_p}{\lambda_i + \lambda_p}$
$\frac{\mu_t (\lambda_i + \lambda_p)}{\lambda_i + \lambda_p + \lambda_t}$
e. rep

Numbering the state clockwise from top, 1,2,3,4 yields the following transition matrix

$$\Lambda = \begin{pmatrix} -\lambda_i - \lambda_p - \lambda_t & \frac{\lambda_t \mu_t}{\lambda_i+\lambda_p+\lambda_t} & \frac{\lambda_p \mu_p}{\lambda_i+\lambda_p} & \mu_i \\ \lambda_i + \lambda_p + \lambda_t & -\mu_t & 0 & 0 \\ 0 & \frac{(\lambda_i+\lambda_p)\mu_t}{\lambda_i+\lambda_p+\lambda_t} & -\mu_p & 0 \\ 0 & 0 & \frac{\lambda_i \mu_p}{\lambda_i+\lambda_p} & -\mu_i \end{pmatrix}$$

Introducing the normalization constant

$$\Lambda_n = \begin{pmatrix} -\lambda_i - \lambda_p - \lambda_t & \frac{\lambda_t \mu_t}{\lambda_i+\lambda_p+\lambda_t} & \frac{\lambda_p \mu_p}{\lambda_i+\lambda_p} & \mu_i \\ \lambda_i + \lambda_p + \lambda_t & -\mu_t & 0 & 0 \\ 0 & \frac{(\lambda_i+\lambda_p)\mu_t}{\lambda_i+\lambda_p+\lambda_t} & -\mu_p & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

and defines the state probability vector with A_{bs} inclusive defined $p = \{A_{\mathrm{bs}}, p_2, p_3, p_4\}^T$.

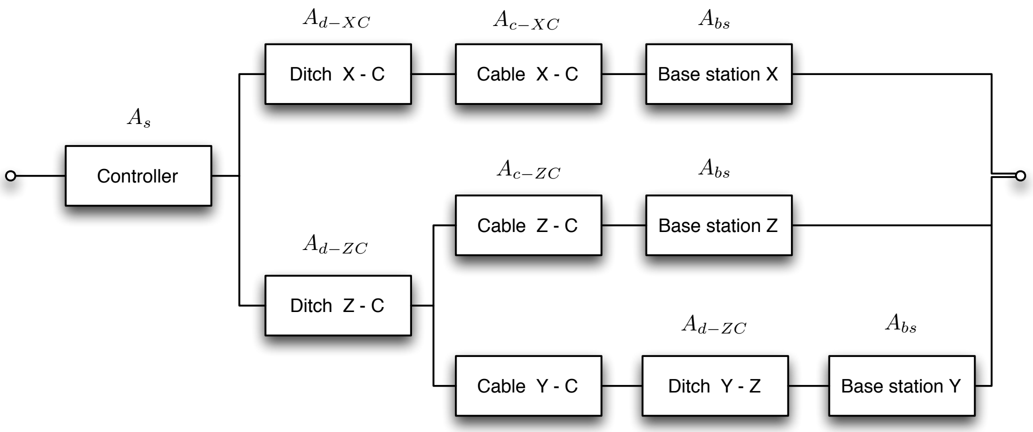
A_{bs} is then obtained by solution of $\Lambda_n p = \{0, 0, 0, 1\}^T$.

d) Establish a reliability block diagram and find an expression, or a set of expressions, for the availability of the service for user **B,** A_B**,** in Figure 2. The variables of the expression should be the parameters defined in the beginning of the text and A_{bs} in question **c)**. It is not required that you reduce or simplify the expression. Which additional assumption(s) must be made if the reliability block diagram shall be a well-founded model of the service?

Using the notation from Figure 2 and prefixing the streches with c for cable and d for ditch, yields the following element availabilities acding to the familiar relation $\frac{1/MDTT}{1/MDT+\text{<failure intensity>}}$.

$A_{\text{c-YC}} = \frac{1}{d_c\left(\frac{1}{d_c}+(l_3+l_4)\alpha_c\right)} = \frac{1}{(l_3+l_4)\alpha_c d_c+1}$, $A_{\text{c-ZC}} = \frac{1}{l_4\alpha_c d_c+1}$, $A_{\text{c-XC}} = \frac{1}{l_2\alpha_c d_c+1}$, $A_{\text{d-ZC}} = \frac{1}{l_4\alpha_g d_g+1}$, $A_{\text{c-XC}} = \frac{1}{l_2\alpha_g d_g+1}$ and $A_{\text{d-YZ}} = \frac{1}{l_3\alpha_g d_g+1}$.

The block diagram deduced fromFigure 2



$A_{c-YC} = \left((l_3+l_4)\,\alpha_c d_c + 1\right)^{-1}$

From the block diagram we obtain

$A_X = A_{bs}A_{\text{c-XC}}A_{\text{d-XC}}$, $A_Z = A_{bs}A_{\text{c-ZC}}$, $A_Y = A_{bs}A_{\text{c-YC}}A_{\text{d-YX}}$,

$A_R = A_{\text{d-XC}}(1-(1-A_Y)(1-A_Z))$ and

$A_B = A_s(1-(1-A_X)(1-A_R))$.

We must assume that multiple ditch and cable failures are repaired independently of each other.

It is assumed that "cable failures", i.e. failure of one or both cables in a ditch is the dominant cause of service failure in the access network. Hence, for the remaining questions, we assume that all failures are either failure(s) of a single cable or that all cables in a ditch fail simultaneously. Base stations and the controller are regarded as fault free.

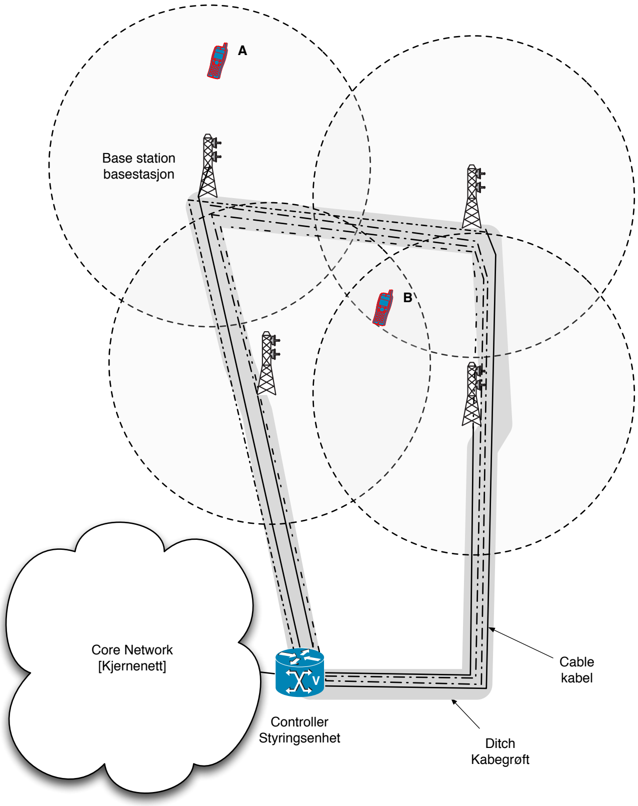
Below, more survivable designs for the communications between base stations and the controller will be sought and investigated. In answering the following questions, new ditches and cabling may be introduced. However, the introduction of new ditches and new cables should be sought to be kept as small as possible due to cost reasons. (By small is meant that the new lengths introduced should be short.) New ditches are far more costly than cables. Furthermore, new functionality may be introduced in the current cable termination points (base stations and controller) to perform switching, add-drop, routing, etc. This functionality may be regarded as fault free. However, no new media for communication, like radio between base stations and the controller, may be introduced.

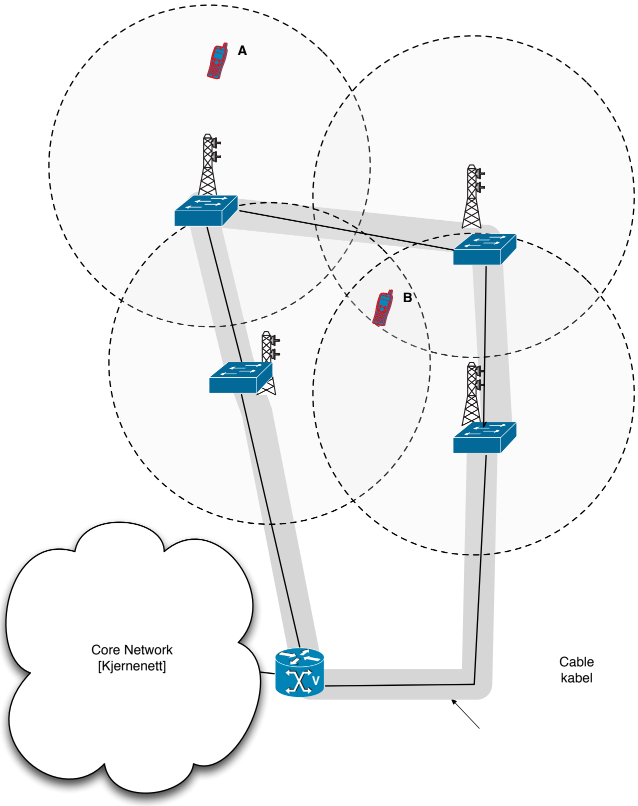
e) Propose two new designs that makes the access network fault tolerant with respect to any single cable failure under the simplifications and assumptions above. You may use the attached sheets to make sketches. Explain briefly how the fault handling/reconfiguration works in your designs. What strengths and weaknesses do your two designs have?

By introducing a ditch between W ogd Y we may have two disjoint paths from all base stations to the controller, which enables a redundancy scheme with independent failing in the alternative paths.

This may be used to establish a survivable systems by different means. For instance:

- Simple protection protection switching via other branch, working in 1+1 or 1:1 modes. As illustrated in the figure below. Variants of these using multiplexing schemes is of course also an option.
- A ring network with add drop multiplexing (keep in mind that the links are bidiretional). See the figure below. The ring may be operated in various modes. Cf. the textbook.
- The physical ring given by the ditches may alo be used otherwise, e.g. by replacing the add-drop muxes in the figurer by routers and perform restoration at the IP layer (OSPF, IS-IS).





Brief pro & contra discussion

	Strength	**Weakness**
Simple protection via other branch,	Option to run 1:1 or 1+1 configuration. Fast and simple protection switching	A lot of additional cabling/fibres/multiplexing
ring., protection switched with add drop multiplexing	Simple off the shelf techn. Option to run 1:1 or 1+1 configuration. Fast and simple protection switching	Since all traffic must be carried on one fibre in a failure state, there may be a capacity/performance problem. (Unlikely in this example)
ring introduce routers and restoration	Simple off the shelf techn.	Slower recover than protection schemes. Like above, there may be a capacity/performance problem.

Dealing with the question **f)**, we assume that all failures are ditch failures, i.e., the only failures that occur are those that cause all cables in a ditch to fail (in both directions). Let Φ_0 denote the operational mode where there are no failures in the access network and Φ_{ij} denote the operational mode where the is a ditch failure between i and j and that this is the only failure in the network. The indexes i and j refer to the base stations $\mathsf{w}, \mathsf{x}, \mathsf{y}, \mathsf{z}$ and the controller c in Figure 2, i.e., $i, j \in \{\mathsf{w}, \mathsf{x}, \mathsf{y}, \mathsf{z}, \mathsf{c}\}$ and $i \neq j$. Assume that $P(\Phi_0)$ and $P(\Phi_{ij})$ are known for all the cable stretches in Figure 2 as well those you have introduced in your answer to **e)**.

f) Based on the design in question **e)**[1] you consider as the best, derive an upper and lower bound for the availability of the service in the access network. (Note that this should be done only for one network, and it is not necessary to motivate why this is considered as the best.) The service is available when all base stations can be used. Note that the steps in the derivation should be motivated. You may assume that there will be sufficient capacity in all working operational modes.

As stated above, $P(\Phi_{\mathsf{wx}})$ may also be considered as known. Both designs above will provide a working service in spite of any single (ditch) failure, i.e., in all failure modes the has a known probability. Being pessimistic, we may assume that the service fails in all other modes. Hence, a lower bound on the availability is formed by

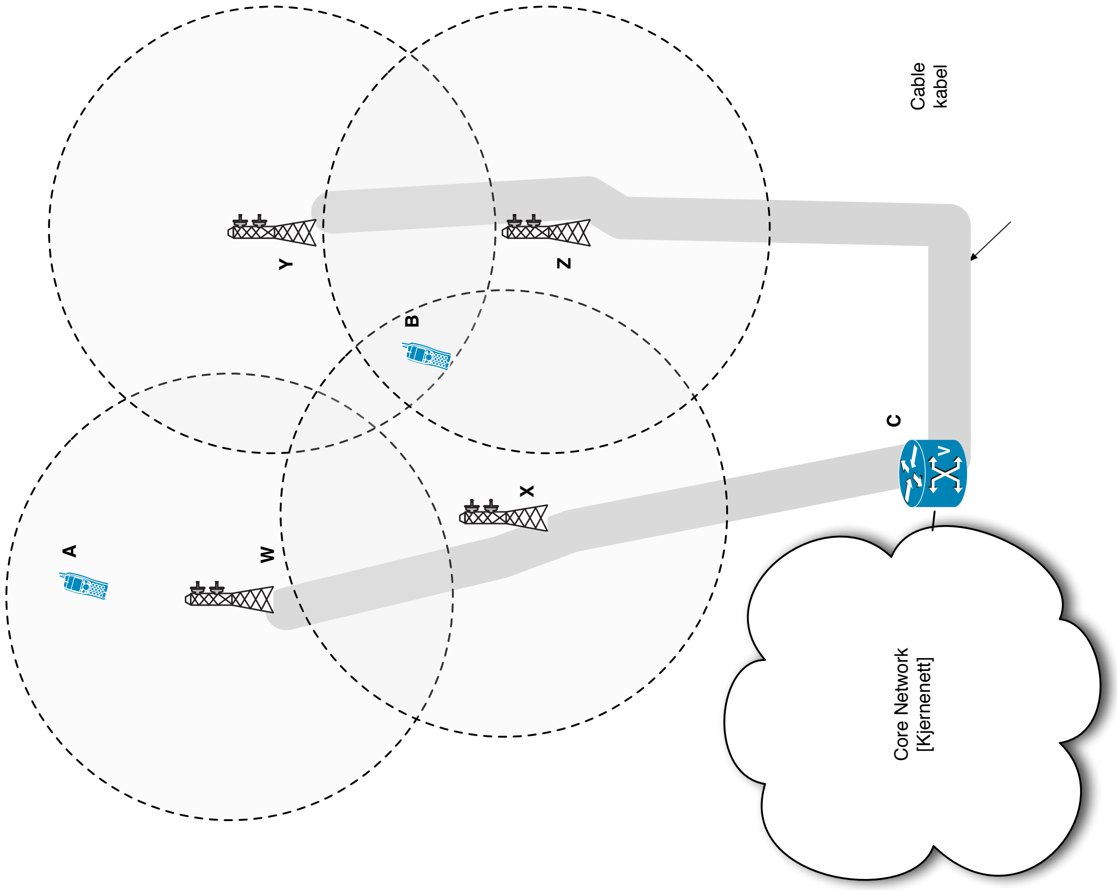
$$A_S \geq A_l = P(\Phi_0) + P(\Phi_{\mathsf{wx}}) + P(\Phi_{\mathsf{xc}}) + P(\Phi_{\mathsf{cz}}) + P(\Phi_{\mathsf{zy}}) + P(\Phi_{y\mathsf{w}})$$

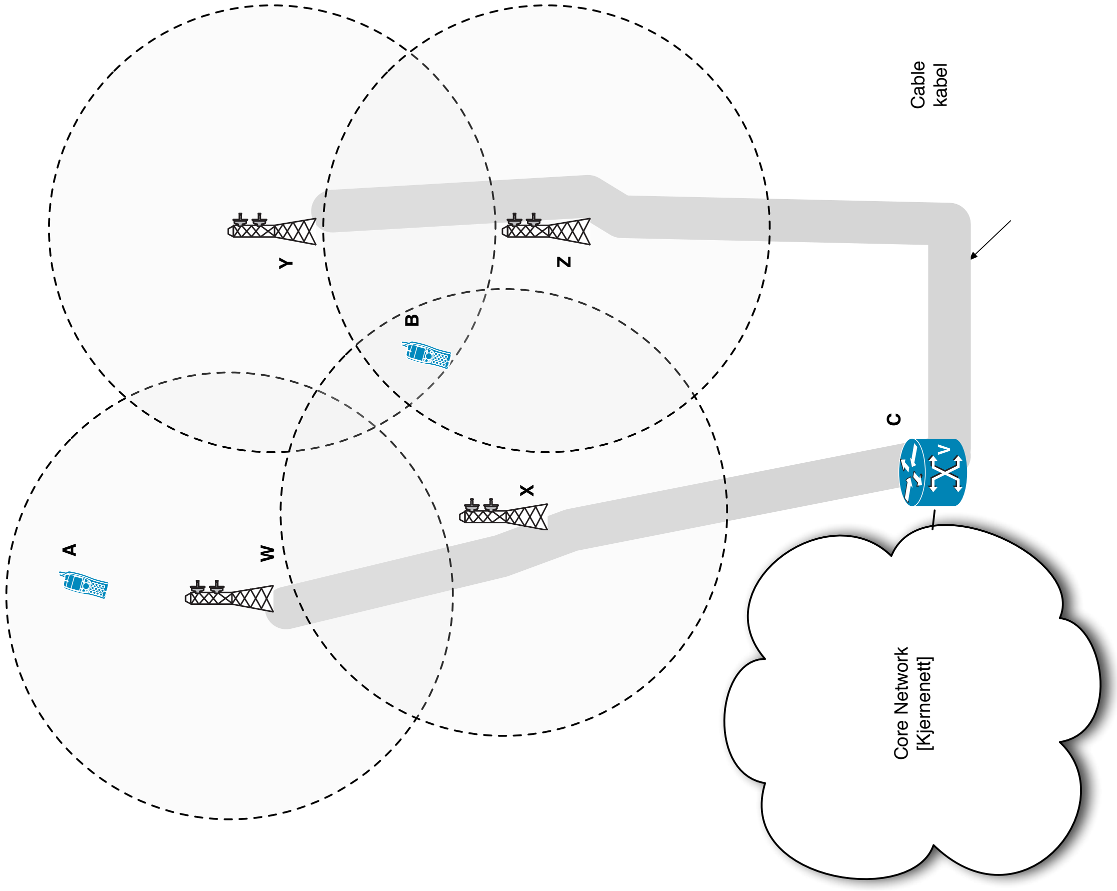
On the other hand, we my be optimistic and assume that all the modes we do not know the probability of, are working, i.e., implying that all states are working, yields an upper bound

$$A_S \leq A_u = 1$$

The gap between the bound are $A_u - A_l = 1 - P(\Phi_0) + P(\Phi_{\mathsf{wx}}) + P(\Phi_{\mathsf{xc}}) + P(\Phi_{\mathsf{cz}}) + P(\Phi_{\mathsf{zy}}) + P(\Phi_{y\mathsf{w}})$.

[1] If you have not dealt with this question, use the design in Figure 2.


Cable
kabel
Y
Z
B
C
X
W
A
Core Network
[Kjernenett]


Cable
kabel
Y
Z
B
C
X
W
A
Core Network
[Kjernenett]