Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMENSOPPGAVE I TTM4130 – EXAM IN TTM4130
TTM4130 - Tjenesteintelligens og mobilitet
TTM4130 – Service intelligence and mobility
SOLUTION, with some diffeences in page numbering)

Faglig kontakt under eksamen:	Lill Kristiansen
Tlf.:	97 72 72 27
Eksamensdato / Date:	5 juni 2012 / June 5th 2012
Eksamenstid /Time:	09:00-13:00 / 9:00 am – 1:00 pm
Vekttall / Credits :	7,5 SP
Examination aids:	**D:** No written and handwritten examination support materials.
	A specified, simple calculator is permitted.
Tillatte hjelpemidler/	**D:** Ingen trykte eller håndskrevne hjelpemidler tillatt
	Bestemt, enkel kalkulator tillatt
Språkform / language:	**English** English is the master text (authoritative)
	(Norwegian text is for information only)
	Answer can be in English, nynorsk or bokmål
Number of pages in English:	5 (pages 2-6)
Antall sider bokmål:	5 (sidene 7-11)
Antall sider nynorsk:	0
Appendix (in English):	2 pages (pages 12-13)
Sheets for answers:	4 sheets to be handed in (pages 14-17)
Sensurdato/Results:	**26. juni 2012**

You should **start by reading through all the material** and then decide which sequence you want to use when answering the exercises.

Write down your own assumptions if the text is unclear, or if information is missing.

At the very back you will find some sheets with diagrams which you are asked to use in some of the tasks.

Exercise 1. (10 %) About SIP and IMS

a) List the 3 types of CSCF that are defined in IMS. List also a database entity.

P-CSCF, I-CSCF and S-CSCF (proxy, interrogating and serving) **HSS (DB)**

b) Fill in the sheet on page 15 (follow the instructions).

Exercise 2. (13%) On GPRS

The following is an illustration of GPRS as of 1999.

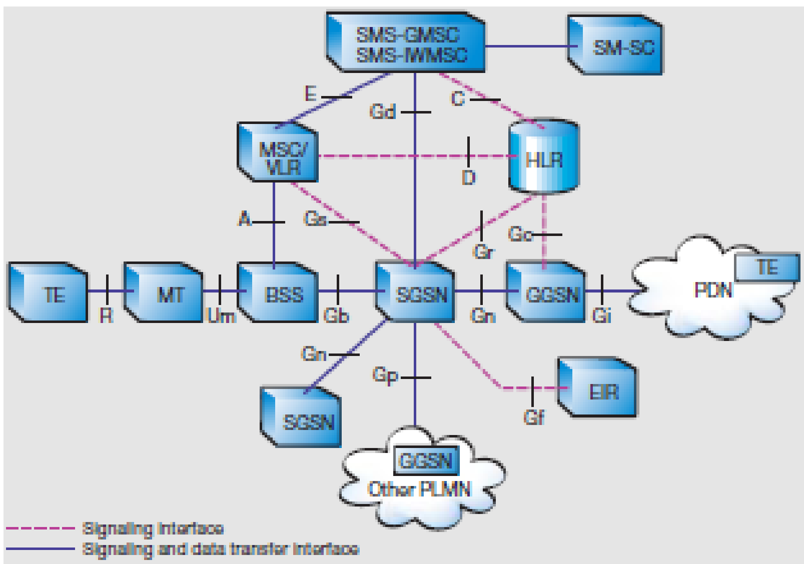


Figure 1 GPRS reference figure from 1999.

a)

a1) Explain what the acronym PDN means.

Packet data network

a2) Give an example of a PDN.

The internet or a company's corporate network (NOTE how small the Internet looks compared to the GPRS-network!)

a3) X.25 is one technology that can be used in a PDN. List at least one other technology that is typically used in PDN.

IP (TCP/IP or similar will also be honoured)

b) As seen in Figure 1 SGSN is connected to BSS (Base Station Subsystem).
b1) Identify one other entity in that belongs to the same level in the network hierarchy as the SGSN.

MSC

b2) Explain briefly the role of SGSN.

SGSN does briefly the same for PDP contexts as MSC does for call setup, by being the anchor point in the PLMN
Some more details (not needed): SGSN is the anchor point in the PLMN for PDP-contexts, it is important is establishing PDP contexts towards an APN, by resolving APN via internal DNS server. SGSN established an IP-tunnel to right GGSN. (In case of mobility a new SGSN and a new MSC will be allocated (via intergrated mobility management)

c) Make an illustration or explain by text where in Figure 1the SS7-based signalling is used, and where IP-based signalling/messages is used.

In almost all of the figure ss7 will be used: Interfaces between SGSN, GGSN, MSC and HLR all use ss7 (Gb, Gs, D,Gr,, Go, (as well as the signalling part of Gn) IP is not used for signalling in GPRS, but IP is used for messages between terminal and the PDN (via an IP tunnel from SGSN to GGSN)
(the use of signalling over the radio is outside of this course)

d) **List** at least two parameters needed in order to establish a PDP context. Explain the role of APN (Access Point Name) during this process.

Short answer: QoS, APN and GGSN
Role of APN: APN is identifying the PDN, APN is resolved in SGSN and the the GGSN is obtained

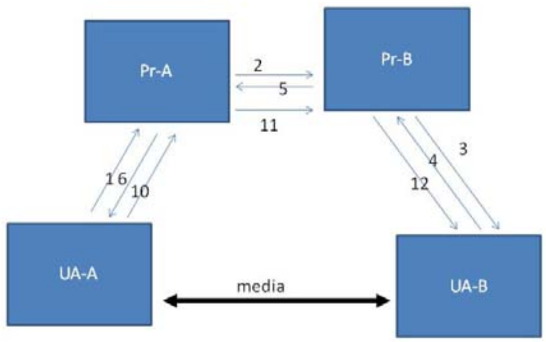
Exercise 3 (54%) About SIP and SDP as in IETF (almost as in the lab)

Your tasks in this exercise are to work with some data which could have been real data captured via Wireshark in the lab. The setup, the preconditions and the test cases are described in appendix page 11, and the results as seen in Wireshark are shown on page 12. This setup and software follows the IETF standard, and is not directly related to IMS and IMS entities.

This part of the exam counts for 54 points (54% of the total points), and the points on each letter a), b) etc. varies between 3 and 6 points

a) Part a) is about proxies running in so-called proxy-mode (as statefull proxies utilizing Record-Route, as you did in most of the lab). Look at the results from test run 1 given in Table 3 and Table 4 in Appendix page 12 and combine it with your knowledge of SIP as defined in RFC3261.
Use the drawing sheet on page 13 for your answer and follow the instructions given.

b) Draw a collaboration diagram (as a so-called SIP trapezoid) showing the complete call setup. Illustrate the media flow(/s) and where the signalling is going. Number the signalling messages.



Numbers refer to answer to 1a. 100 not shown 180 shown (4-6)
(200 OK 7-9 (from UA-B via... to UA-A) not shown due to **lazyness**

(Note: My intention was that statefull proxy/proxy mode is used here (as in a), but an answer using ACK directly will also be fully honoured)

c) Illustrate what happens when after 2 min. of conversation the calling party decides to ”hang up” (i.e. Alice is pressing the red button on her user interface). Show SIP signalling, do not show media packets or media flows. Use the same MSC as in a) or a separate figure.

See answer to a) bottom part

d) List all messages from your answer to a) which are containing the *SDP offer*, and list separately all messages which are containing the *SDP answer*. You may answer by marking with “o” and “a” on one or several messages on the previous answer to a) (page 13) or write the answer in plain text.

SDP offer: messages 1) 2) and 3) (all INVITE messages)
SDP answer: Messages 7), 8) and 9) (all 200 OK messages) (or see answer to a)

e) Table 1 shows some important parts of an SDP offer and the corresponding answer side by side:

Table 1 SDP offer and SDP answer side by side

Offer	**Answer**
o=alice 2890844526 2890844526 ++	o=bob 2890844730 2890844730 ++
m=audio 49170 RTP/AVP 0	m=audio 49100 RTP/AVP 0
a=rtpmap:0 PCMU/8000	a=rtpmap:0 PCMU/8000
m=video 51372 RTP/AVP 31	m=video 0 RTP/AVP 31
a=rtpmap:31 H261/90000	(an empty a-line)

Assume these values are form test run 1 and combine this with your answer from a) (page 13) in order to answer the following questions:
e1) Towards which IP address and port number will UA-A send audio?

A will send towards the port number sent in the answer from B and use the IP-address of this answer (as no other IP-address is given for the media in the a-line)
i.e. to **(…) .247 port 49100**

e2) Will UA-A receive video from UA-B? In case of “yes”: On which IP address and port number will UA-A receive video? In case of “no”: Why not?

Answer to the English version of the text:
No

Because: m=video 0 means that UA-B rejects the whole video stream, which in 2-way by default (in case video was oneway e.g. having attribute sendonly the answer may turn out different)

Answer to the Norwegian version of the text (mixing send/receive) is the same: **No, UA-B rejects whole media stream video (both ways) (by using port number 0 in the m-line for video)**, thus UA-A will neither receive nor send video in this case

f) Explain the role of Via.

Via ensures that response messages may follow the same path back as the corresponding METHOD was following on the way forward. Acts as a stack (pop-of on the way back)

g) Explain the role of Record-Route in routing of signalling messages.

Record-Route will make it possible for later SIP methods (requests) within the same dialogue to follow the same path. It works as follows: In the response messages as Via is popped off, R-route is added. (R-R is received in 180/200 and used to route later ACK)

Additional info (not needed): In 1f) (direct mode/ stateless proxy) R-route is not used, and ACK is sent directly (using contact field)

(in parantesis/ not needed in an answer) : Even if R-Route is used and ACK goes via the proxies, the proxies may still be stateless, if the only thing they do is to forward messages. When proxy is involved it may do charging, and it may be statefull (in order to handle AS etc) , (e.g. tear down the call at own initiative (or when prepaid account is empty)

h) It is a fact that if the INVITE message is lost before reaching UA-B it will be resent by UA-A.

h1) Explain how UA-A can determine the need to resend INVITE.

After sending INVITE (or any METHOD except ACK) UA-A is waiting for a final response (200, 4xx or similar) and starting a timer. If this timer @UA-A fires (before

a final response is received), UA-A will resend INVITE.

Note (not needed in an answer): UA-A may not know whether INVITE is lost, or if the response is lost, byt in both cases resending METHOD will work well.

h2) Explain the mechanism in the protocol to differentiate between a resending of a previous INVITE from a new INVITE (which may be sent towards the same callee). You may give the name of a particular header as part of your answer.

A resent message (like INVITE) will have **same CSeq value as the previous message of the same type** (INVITE) (and same call-ID and tags etc.). This is different when a new (re-) INVITE is sent during an ongoing call in order to change media types, then CSeq is increased).

i) Now we are running the same test again. In this 2nd test run we have configured both proxies in so-called “direct mode” (as stateless proxies not utilizing Record-Route).

Answer by using the sheet on page 14 and follow the instructions.

as the answer to a), but ACK goes directly towards UA-B (at least we observe that is it sendt from UA-A, but it may be lost in the network…)

j) Assume that packet loss causes the ACK message not to reach UA-B.

j1) What will UA-B do in this case?

UA-B will notice that ACK is not arriving (after sending final response a timer is started for this). **If after certain time (details not needed) no ACK is received by UA-B the timer on UA-B will fire, and prev. message (200, 4xx) is resent**

j2) What will UA-A do in this case?

Short answer: UA-A will do nothing signalingwise
Slightly longer answer: UA-A has sent an ACK (which has no response), thus as seen from UA-A everything is fine. UA-A will start sending audio (before of after ACK is sent) . **If a resent 200 OK arrives (via proxies) towards UA-A, it will ACK again. (**Media may continue regardless of this resending) as the offer-answer negotiation is finished).

k) In a 3rd test run both proxies are in “proxy mode” (as statefull proxies) and the (partial) wireshark observations are given in Table 5 and Table 4 on page 12.

k1) Explain why you cannot be sure that Pr-B is *receiving* 200 after 180, even though the Wireshark results show that 200 is *sent* after 180 from UA-B.

As signalling goes over UDP both packet loss and packet swop may take place, in particular Pr-B may receive 200 and then 180 later.

k2) Explain what will happen signalling-wise if packet loss causes the ACK message to be sent from Pr-A but not reaching Pr-B.

If ACK does not reach Pr-B, it will not reach UA-B neither. Thus **UA-B will notice that ACK is missing (as explained in j), and UA-B will resend 200 OK**

l) Assume that UA-B has implemented the following policy: It will not *send* media before it has received the ACK message. We may use the term this "late media sending" for this.

Explain what is the earliest possible time (relative to the timeline for UA-B) that UA-B must be prepared to *receive* media packets according to RFC3264 (the offer-answer model). You may mark this time with a * on the MSC (page 13) or explain otherwise.

Note: the information about early media is given in order to confuse you (in real working life unnecessary correct info will often be given).

Answer: UA-B does not know the policy implemented by UA-A, hence it must follow RFC3264. **RFC3264 states that the answerer (here UA-B) must be prepared to receive media as soon it has sent its answer with its own port number (i.e. at the time when sending 200 OK)**

m) Assume that UA-A has implemented the following policy: It will send RTP media packets as soon as possible (before it is sending the ACK message). We may call this "early media sending".

Give at least two reasons why UA-B must be prepared to receive P1 (first rtp packet) and P2 (ACK) in either order.

answer alt. 1: Even if UA-A is sending rtp first and the ACK, possible packet swopping may cause the order to be the same or the opposite when arriving at UA-B.

answer alt. 2: UA-B does not know the policy implemented by UA-A, (as UA-B will typically talk to many different UA's). Hence it must be prepared to talk to some UA-A sending ACK first and then first media Packet (as well as this UA-A sending in other sequence, in addition comes packet swopping).

(any of these answers will be fully honoured)

Exercise 4. (23%) Application server in IMS and IN-node in GSM+Camel

This part of the exam counts for 23 points (23% of the total points), and the points on each letter a), b), c) etc. varies between 3 and 6 points.

We start this task by illustrating the use of application servers (AS) in IMS, and the somewhat similar concept of an IN-node in Camel.

(figure deleted)
Figure 2 IMS Call setup as a simplified collaboration diagram (from IMS book, slightly edited). **In this case both originating side and terminating side are involving AS for special services. The HSS is in this case related to the terminating side.**

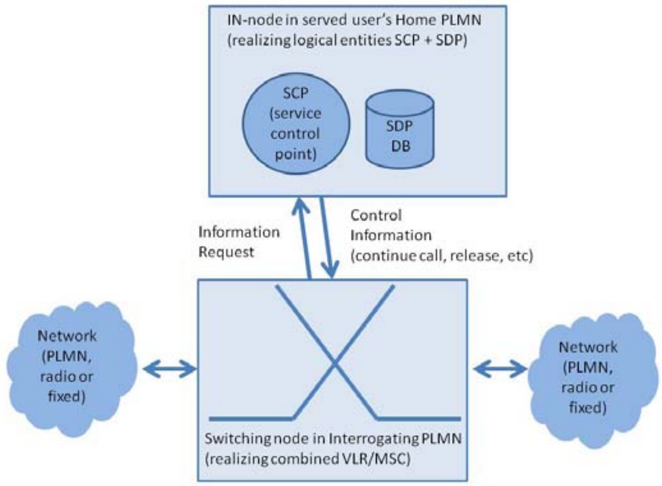


Figure 3 A simplified view of Camel during a call setup attempt (signalling). The MSC is placed in a so-called Interrogating PLMN (IPLMN). The MSC may or may not be a serving MSC of the particular user (depending on the case).

a) Fill in the sheet on page X

b) Identify one interface in Figure 2 which is not using SIP, and explain what protocol this interface is using. You may refer to this interface by referring to the corresponding number in Figure 2.

c) Explain the meaning of CSI within the context of Camel.

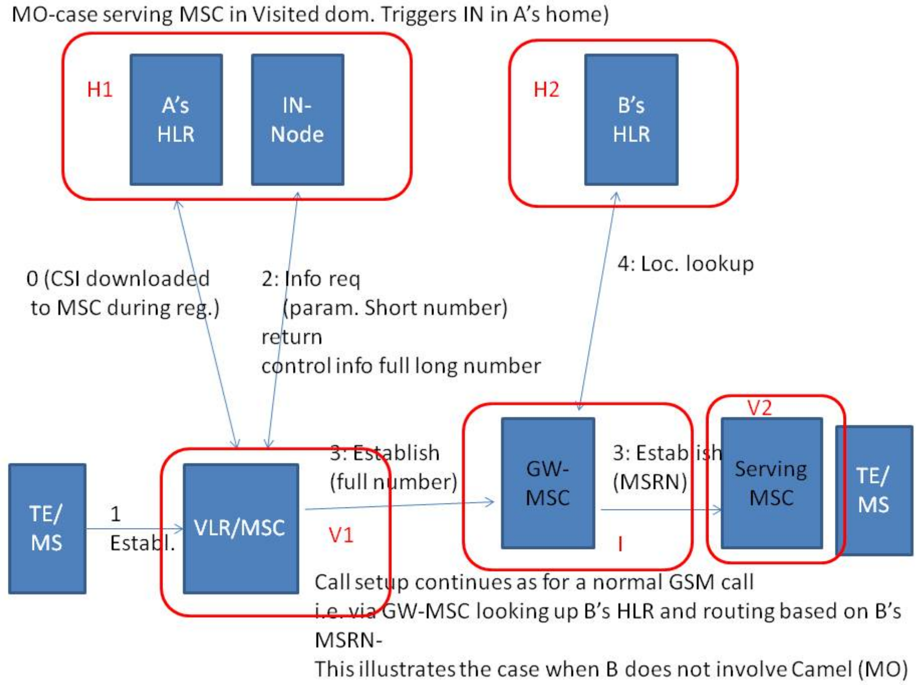
Customer Subscription Data

d) An IN-node in Camel acts as a kind of Application Server (AS) for GSM subscribers. This may support *originating* services like company-wide-short-number-service. In IMS the triggering of the AS on originating side happens in the home domain (see Figure 2). But the role of the home and the visited networks are *different* in GSM+Camel.

Assume user A is roaming and is originating a call which need interaction with the IN-node via Camel (e.g. because A subscribes to company-wide-short-number-service). In Camel this is called the MO-case (MO=Mobile Originated).

Draw a sequence diagram / collaboration diagram to illustrate the message sequence when this call is initiated. You are asked to draw a diagram at approximately the same level as in Figure 2. **Explain** how the *visited* network plays a role. **Hint:** It is a good idea to include a description of the role of the HLR on the originating side.

Answer d):



(ignore some wholes in the numbers…)

NB: the red domain boarders are not required in a full answer, but shown for illustration (same goes for e)

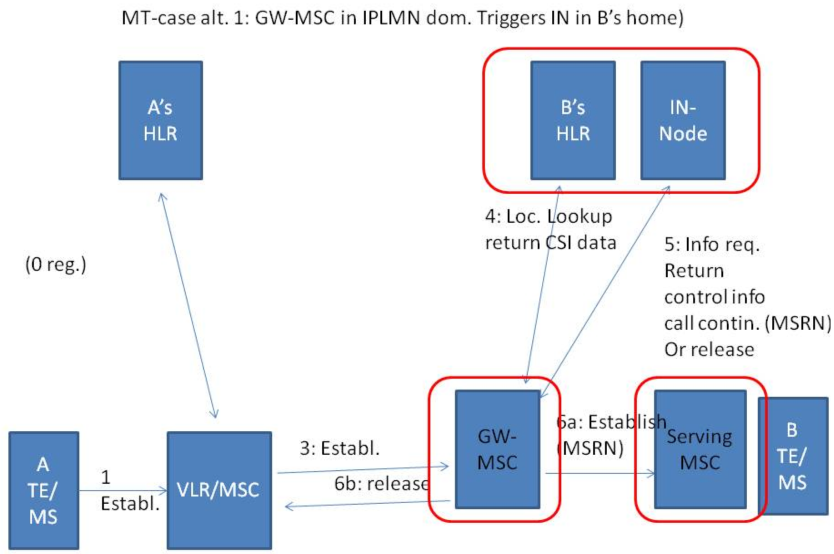
e) An IN-node in Camel acts as a kind of Application Server (AS) for GSM subscribers. Camel allows for IN-nodes in the home network to support *terminating* services like personal-assistant (a kind of Do-not-disturb service), which is directing some calls to Voicemail, and some calls through to the user, based on some non-standardized rules and personal data defined in the IN-node. In IMS the triggering of the AS on the terminating side happens in the *home* domain (see Figure 2). But the roles of the various network domains are *different* in GSM+Camel.

Assume user B is roaming and is receiving a terminating call which need interaction with the IN-node via Camel (e.g. because B has activated his personal-assistant service). In Camel this is called the MT-case (MT=Mobile Terminated).

Draw a sequence diagram /collaboration diagram to illustrate the message sequence when this call is routed towards user B. You are asked to draw a diagram at approximately the same level of detail as in Figure 2. **Explain** how the *interrogating* network (IPLMN) plays a role. **Hint:** It is a good idea to include a description of the role of the HLR on the terminating side.

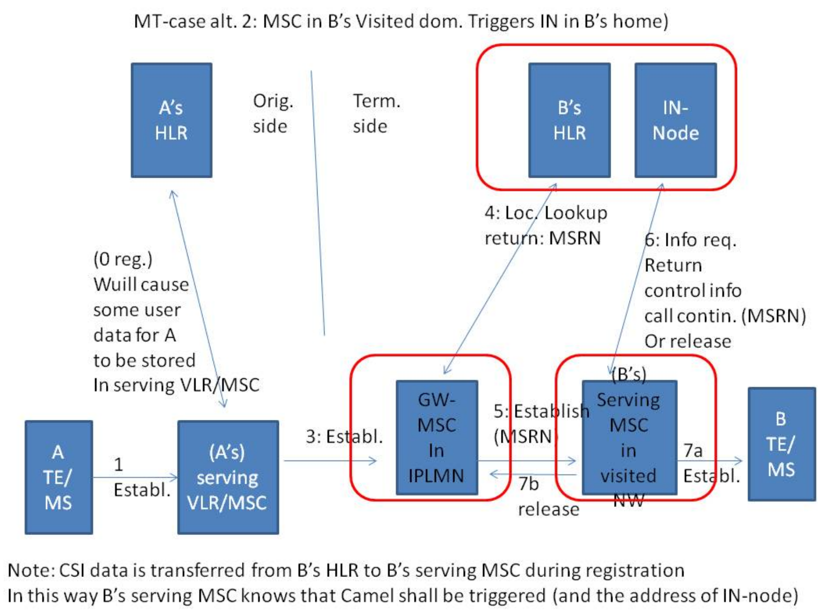
There are two options for this to happen in Camel for the MT-case, chose *one* of the options in your answer.

Answer e) (ignore some wholes in the numbers… I am too lazy to redraw this figures):



In this alternative (alt.1) the role of the HLR is to send down CSI data to GW-MSC in IPLMN during the HLR lookup. These CSI data will include address of the IN node, and make it possible for GW-MSC to route the relevant call to IN-node (via Info request). This is the oldest alternative in Camel (ignore some wholes in the numbers…)

Alt. 2 (a newer alternative in Camel) works as illustrated below



The sep. line between orig. side and term. side may be added, but is not needed in a full answer (domain boarders are not needed)

Appendix

1. Information related to exercise 3 (SIP in the lab)

1.1. Set up in the test cases reported

We are using 4 physical machines all running relevant SIP software, with no use of virtual machines. We follow the traditional setup called "SIP trapezoid" having two proxies.

In exercise 3a)- 3c) (test run 1) you shall assume that both proxies are configured to be in so-called "proxy-mode" (or as a statefull proxy, utilizing Record-Route header).

In exercise 3.i) (test run 2) you shall assume that both proxies run in so-called "direct-mode" (or as stateless proxy, not using Record-Route). In both cases the signaling SIP runs over UDP (as in your lab).

We used wireshark only on two of these machines, as detailed in Table 2.

Table 2 Set-up and configuration during the test cases (ignore the start of all IP addresses)

Physical entity	PC-1	PC-2	PC-3	PC-4
IP-address	(..).246	(..).192	(..).193	(..).247 (typo)
Role of the SIP SW	UA	Proxy	Proxy	UA
SIP SW details	Some-1 (supporting also video)	Some-2	Some-3	Some-4
Instances name	UA-A	Pr-A	Pr-B	UA-B
Wireshark	Yes	No	No	Yes

Special info: UA-B was configured not to use auto-reply.

1.2. Preconditions

Alice on UA-A is registered successfully with Pr-A. Bob on UA-B is registered successfully with Pr-B. UA-A has "Bob" registered in the address book.

1.3. Test execution

Alice on UA-A chooses the entry "Bob" in the address book and presses the green button. (This will cause the UA-A to initiate a call towards Bob@....).

After the phone rings at UA-B, a human (Bob) presses the green button to accept the call.

(What happen after this is up to the candidate to describe as he/she follows the tasks described in exercise 3)

1.4. Test results (see next page)

1.5. Test verdict

Test is passed (this means that all SIP signaling is according to specification RFC3261), that all SDP messages are according to offer-answer model, and that audio worked both ways.

Partial test results first test run (task 3 a) and second test run (task 3 i)

The data captured in Wireshark on PC-1 and PC-4 looked as follows:

Table 3 Data from Wireshark (data is captured at PC-1). Filter: SIP and SDP
NB: We are not showing what happened after the message at time T5.

Time	Source	Destin.	Protocol	Info
T1	(..).246	(..).192	SIP/SDP	Request: INVITE sip:Bob@ ... with session descr.
T2	(..).zzz	(..).246	SIP	Status: 100 Giving a try
T3	(..).zzz	(..).246	SIP	Status: 180 Ringing
T4	(..).zzz	(..).246	SIP/SDP	Status: 200 OK with session description
T5	(..).246	(..).xxx	SIP	Request: ACK

NB: The value of the source and destination is withheld for some of the messages. The candidate shall be able to find out the value of zzz and xxx by themselves.
NB2: Notice that the values of IP addresses marked zzz and xxx may differ between the test runs. The values of some of the headers (not shown) may also vary between the test runs.

Table 4 Data from Wireshark (data is captured at PC-4). Filter: SIP and SDP
NB: We are not showing what happened after the message at time t3

Time	Source	Destination	Protocol	Info
t1	(..).193	(..).427	SIP/SDP	Request: INVITE sip:Bob@ … with session description
t2	(..).247	(..).yyy	SIP	Status: 180 Ringing
t 3	(..).247	(..).yyy	SIP/SDP	Status: 200 OK with session description

NB: The value of the destination is withheld for some of the messages. The candidates shall be able to find out the value of yyy by themselves. (yyy may vary between the test runs)

Partial test result 3rd test run (exercise 3 k)

Table 5 Data from Wireshark (data is captured on PC-1). Filter: SIP and SDP

Time	Source	Destination	Protocol	Info
T1	(..).246	(..).192	SIP/SDP	Request: INVITE sip:Bob@ … with session description
T2	(..).uuu	(..).246	SIP	Status: 100 Giving a try
T3	(..).uuu	(..).246	SIP	Status: 200 OK with session description
T4	(..).uuu	(..).246	SIP/SDP	Status: 180 Ringing

NB1: The value of the source or destination is withheld for some of the messages. The candidates shall be able to find out the value of uuu by themselves.

The test data captured on PC-4 is given in Table 4.

Candidate number .... **page ..... of ......**

Study program .... **(fill in your own data here)**

Use this sheet to answer exercise 3a) (proxy mode)

This task is about proxies running in so-called proxy-mode (as statefull proxies utilizing Record-Route, as you did in most of the lab). Look at the results from test run 1 given in Table 3 and Table 4 in Appendix page 12 and combine it with your knowledge of SIP as defined in RFC3261.

Task a1) Complete instance names and IP-addresses on the boxes on top.

Task a2) Draw one MSC showing the whole set of signalling messages being exchanged within the given timeframe between all 4 involved entities. Use the data from the Wireshark observations, and add messages on the entities where no Wireshark observation is given. Mark clearly which messages are not captured by Wireshark, by adding "no" (for "not observed") on all relevant messages.

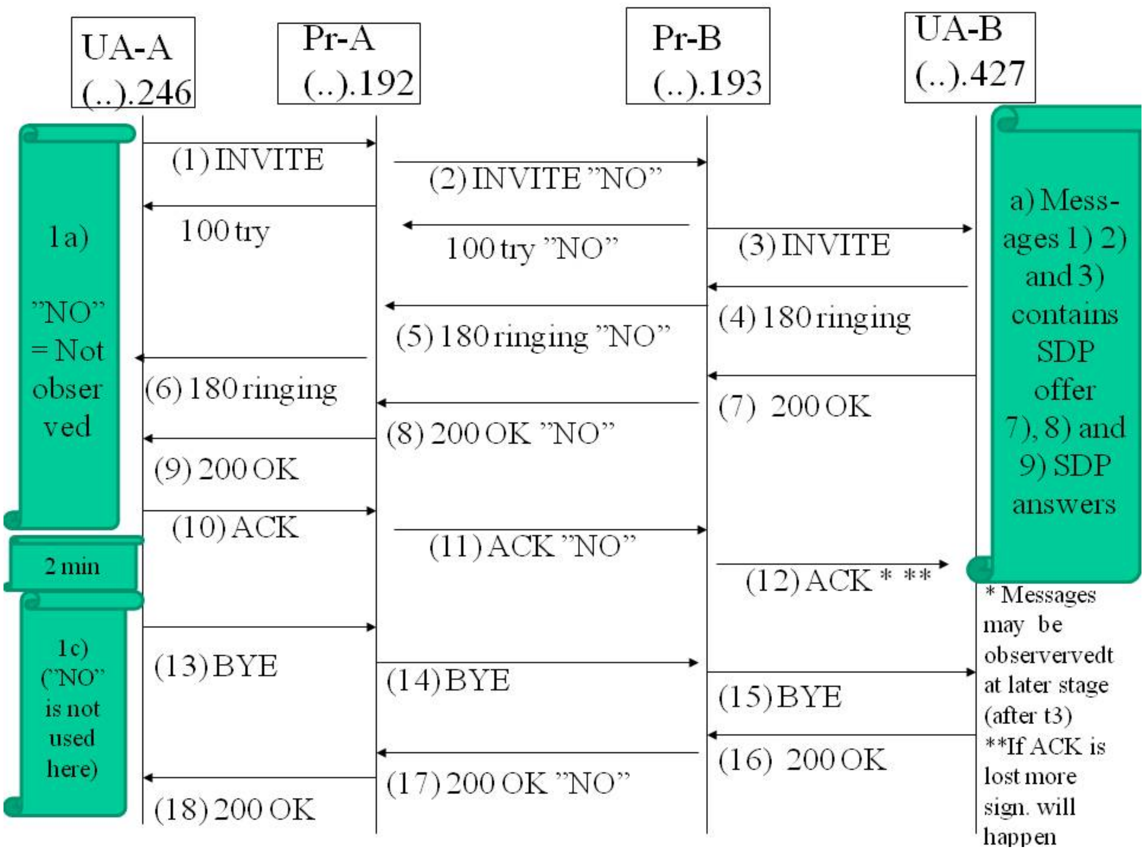


Figure 4 Answer to exercise 3a) here. (Use the same diagram to answer 3c) if you want and have room). Answers to other parts of exercise 3 may also be added here if you find that feasible.

Note: 427 is a typo for 247 (consistency all over). No deduction if these two numbers are mixed or 427 is used all over)

Note 2: Candidate may also stop after (10) ACK (as no observation after t3 on UA-B is shown in the test result table)

Candidate number .... **page ..... of ......**

Study program .... **(fill in your own data here)**

Use this sheet to answer exercise 3i) (direct mode)

Now we are running the same test again. In this 2nd test run we have configured both proxies in so-called "direct mode" (as stateless proxies not utilizing Record-Route). The results are given by Table 3 and Table 4 on page 12.

Task a1) Complete instance names and IP-addresses on the boxes on top.

Task a2) Draw one MSC showing the whole set of signalling messages being exchanged within the given timeframe between all 4 involved entities.

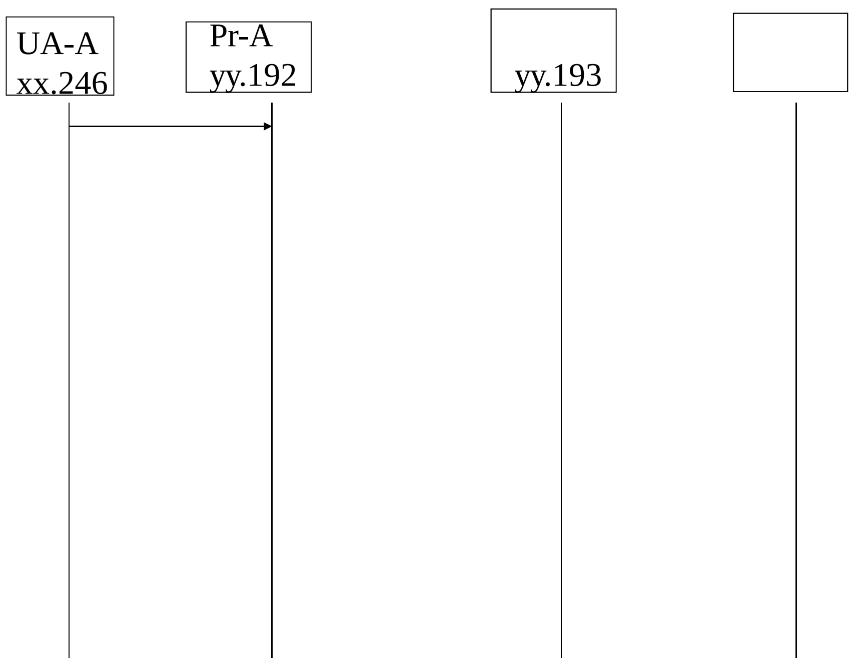


Figure 5 Answer to exercise 3i) here.

As a) but ACK goes directly from UA-A to UA-B

Empty space may be used by the candidate.

Candidate number .... **page ..... of ......**

Study program .... **(fill in your own data here)**

Use this sheet when answering exercise 1 b)

Task b1): Fill in correct names instead of …-CSCF, …-CSCF and …-CSCF.
Task b2): Complete the following call flow (message sequence chart) on the terminating side. Do this by filling in all messages between the first and the last arrow shown, i.e. all messages relating to the terminating side from INVITE to ringing. Show SIP messages, but show also briefly message(/s) to/from HSS.

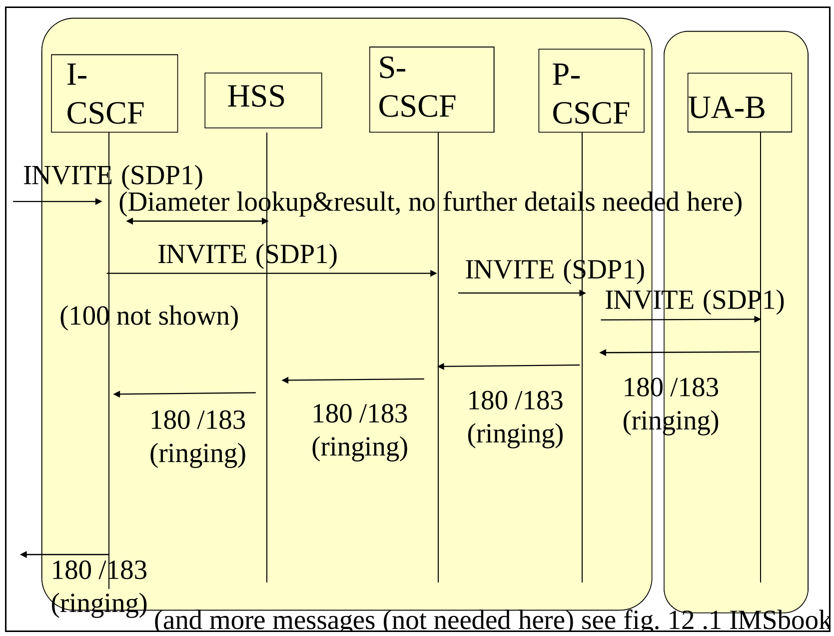
Originating side	***Terminating side (Bob is non-roaming in this case)***
From Alice Via…. Via Alice's home domain	*(empty space, do not write here)*
	
To Alice's home domain For further routing to Alice's UA.	**(empty space do not write here)**

Figure 6 Answer to exercise 1 b) goes in the right hand-side of this figure

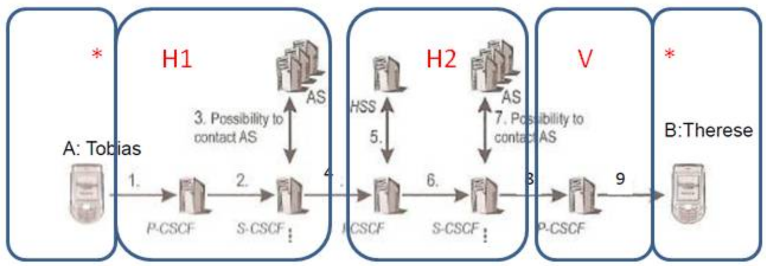
Comment: In IMS first 183 is used with PRACK and then later 180 with the real ringing. The intent was not to show the details with all PRACK, resource reservation and multiple offer/answers. The intent was to show intil first 183 message.
This answer using 183 is identical to the answer of a previous exam. (same fig. with 180/ringing) is also OK. Formally 183 goes with session progress, not with ringing, see the full complicated figure in IMS book fig. XX

Candidate number .... **page ..... of ......**

Study program .... **(fill in your own data here)**

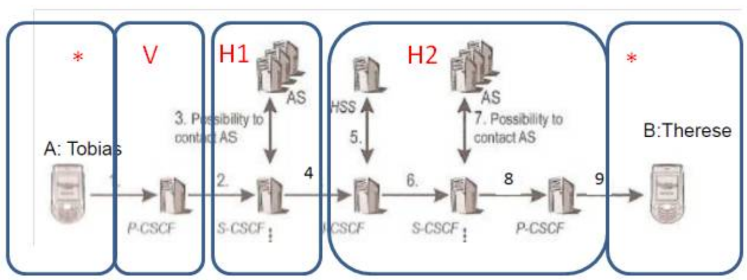
Answering sheet for exercise 4a) on IMS

Add domain boarders to these figures corresponding to the following 2 cases.



H1: Tob's home
H2: Ther.'s home

Answer: Case: Tobias is non-roaming, Theresa is roaming to Austria.*



Answer: Case: Tobias is roaming to Finland, Theresa is non-roaming. *

* It is equally valid to draw the terminal as part of the visited network, see fig. 11.5
According to fig. 3.43 is is more correct to draw terminal in same (sec.) domain as P-CSCF
However, if the user owns his own terminal it is natural to draw it in a separate domain

H1 is Tobias home domain (French-op1) H2 is Therese's home domain (Hung-op-a)

V is the visted doian of Tobias Or Therese Respectively (Finland op-2/ Austria op-d)