Laboratori de telemàtica

Pràctica 4

Anàlisi de les trames LAPD

• Assignació del TEI

Abans de començar a transmetre informació cada un dels terminals ha d'aconseguir un TEI (Terminal Endpoint Identifier). Aquest nombre l'identifica en la xarxa de nodes. Per aconseguir-lo envia les següents trames:

```
(EQ) 4 12:54:23 LAPD: SAPI=63 TEI=127 Type=UI P=0 FCS=Good
  Frame Type          = 0x03 (UI)
  Poll/Final          = 0 (Not Poll)
  Reference Number    = 38739
  Mgmt. Message Type  = 1 (Identity request)
  Action Indicator    = 127
```

D'aquesta trama veiem que el SAPI (Service Access Point Identifier) és 63 (TEI Management). Aquest camp identifica quin tipus d'informació conté el protocol superior. En aquest cas veiem que és TEI Management, amb el que sabem que la trama serà per a assignar un TEI o demanar-ne un. El TEI destinació és 127, tots els 7 bits a 1, que és la direcció boradcast i que, per tant, s'enviarà a tots els nodes de la xarxa. El detall de la resta de camps:

UI que vol dir Unnumbered Information, és una trama d'informació que no està numerada i que, per tant, no s'ha de confirmar (es pot perdre amb facilitat). Aquest tipus de trama es fa servir ja que encara no hi ha connexió establerta.

El camp Reference Number és un nombre aleatori de 16 bits que es fa servir per a identificar la petició i distingir-la d'altres que es puguin estar produint en aquell instant.

Management Message Type indica el tipus de missatge de gestió de TEI. Serà 1 per a demanar un TEI i 2 per a assignar-ne un (com es veu a continuació).

Action Indicator conté la informació del procés. En aquest cas com que és una petició el camp realment no importaria, però posa 127 que és un TEI que no pot tenir cap node (per ser el de broadcast).

Analitzem ara la resposta:

```
(LN) 5 12:54:23 LAPD: SAPI=63 TEI=127 Type=UI P=0 FCS=Good
  Frame Type          = 0x03 (UI)
  Poll/Final          = 0 (Not Poll)
  Reference Number    = 38739
  Mgmt. Message Type  = 2 (Identity assigned)
  Action Indicator    = 68
```

Altra vegada només canvia el Management Message Type que és el que assigna una identitat i ara sí que trobem un valor al camp AI, que conté el TEI assignat al node, en aquest cas el 68.

• Establiment d'una trucada entre els dos terminals

Si ara truquem a un altre node aquest haurà de respondre. En aquest cas particular ens centrem en trucar a un node del nostre lloc de treball el qual tampoc té TEI. Justament després de l'assignació del TEI capturem els següents paquets:

```
(EQ) 6 12:54:23 LAPD: SAPI=0 (Call Control) TEI=68 Type=SABME P=1 FCS=Good
(LN) 7 12:54:23 LAPD: SAPI=0 (Call Control) TEI=68 Type=UA    F=1 FCS=Good

(EQ) 8 12:54:23 LAPD: SAPI=0 TEI=68 Type=Info P=0 Ns=000 Nr=000 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x06; Type = SETUP
    Coding Std                = CCITT
    Info Trans Cap            = 3.1 KHz Audio
    Transfer Mode             = Circuit
    Transfer Rate             = 64 Kbit/s
    Layer Id                  = Layer 1
    Lay 1 Prot                = G.711 A-law
  Information Element         = Calling Party Number (0x6c)
    Number Digits             = 42
  Information Element         = Called Party Number (0x70)
    Number digits             = 41
(LN) 9 12:54:23 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=001 FCS=Good

(LN) 10 12:54:23 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=000 Nr=001 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x06; Type = CALL PROC
  Information Element         = Channel Identification (0x18)
    Interface Id Present      = Implicit
    Interface Type            = Basic
    Channel                   = Exclusive
    D-channel                 = No
    Info Chan Selection       = B1
(EQ) 11 12:54:23 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=001 FCS=Good

(LN) 12 12:54:23 LAPD: SAPI=0 TEI=127(Broadcast) Type=UI    P=0 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2a; Type =    SETUP
```

Observem que hi ha una connexió (comandes SABME i UA) i una trama de SETUP. Aquesta trama conté les dades d'inici de la trucada. Conté la velocitat de transmissió, la codificació de la senyal de veu (llei A o llei μ), la freqüència de mostreig i els nombres de telèfon (receptor i emissor) entre d'altres informacions.

El següent paquet és el CALL PROCEEDING que envia la central al nostre terminal per acceptar la trucada i indicar que esperi. Acte seguit tornem a veure el mateix paquet de SETUP però ara per a la direcció de broadcast. Aquest paquet l'envia la central a tothom ja que aquesta no sap els números de telèfon de cada terminal i d'aquesta manera la persona que tingui el número de telèfon destí contestarà (es donarà per al·ludida).

Com ja hem dit cap dels terminals tenia TEI i en aquest punt el terminal amb el número marcat no en té, per això tornem a veure el procés d'adquisició de TEI per part del terminal que haurà de respondre:

```
(EQ) 13 12:54:23 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI    P=0 FCS=Good
  Reference Number    = 22368
  Mgmt. Message Type  = 1 (Identity request)
  Action Indicator    = 127
(LN) 14 12:54:23 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI    P=0 FCS=Good
  Mgmt. Entity Id     = 15
  Reference Number    = 22368
  Mgmt. Message Type  = 2 (Identity assigned)
```

Ara veiem que el terminal que ha de contestar es connecta i respon a la trucada:

```
(EQ) 15 12:54:23 LAPD: SAPI=0 (Call Control) TEI=69 Type=SABME P=1 FCS=Good
(LN) 16 12:54:23 LAPD: SAPI=0 (Call Control) TEI=69 Type=UA    F=1 FCS=Good
(EQ) 17 12:54:23 LAPD: SAPI=0 TEI=69 Type=Info  P=0 Ns=000 Nr=000 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2a; Type = ALERTing
  Call Reference Length       = 1
  Call Reference Flag         = 1 (TO side that originated call ref)
  Call Reference Value        = 0x2a
```

```
(LN) 18 12:54:23 LAPD: SAPI=0 TEI=69 Type=RR    F=0 Nr=001 FCS=Good
(LN) 19 12:54:23 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=001 Nr=001 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x06; Type = ALERTing
(EQ) 20 12:54:23 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=002 FCS=Good
```

Veiem que el terminal que acaba d'aconseguir un TEI (69) es connecta (SABME i UA) i envia un missatge de ALERTING. El missatge és retransmès per la central fins al terminal que ha efectuat la trucada (68). Durant tot el procés es veuen varis RR per a confirmar paquets rebuts (mirar el Ns i Nr de cada paquet). Es veu clarament com la connexió a nivell 2 s'encarrega de comprovar el CRC (camp FCS) així com confirmar dades rebudes i transportant les dades Q.931 a les seves trames d'informació.

Ara es realitza la connexió (una vegada despengem el telèfon, podem veure el temps entre l'últim RR i el primer CONNECT). El terminal que despenja envia un connect i la central li respon amb un ACK. La central fa el mateix procés amb el terminal que està esperant per la trucada.

```
(EQ) 21 12:54:26 LAPD: SAPI=0 TEI=69 Type=Info  P=0 Ns=001 Nr=000 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2a; Type =  CONNect
(LN) 22 12:54:26 LAPD: SAPI=0 TEI=69 Type=RR    F=0 Nr=002 FCS=Good
(LN) 23 12:54:26 LAPD: SAPI=0 TEI=69 Type=Info  P=0 Ns=000 Nr=002 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2a; Type = CONN ACK
(EQ) 24 12:54:26 LAPD: SAPI=0 TEI=69 Type=RR    F=0 Nr=001 FCS=Good
(LN) 25 12:54:26 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=002 Nr=001 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x06; Type =  CONNect
(EQ) 26 12:54:26 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=003 FCS=Good
(EQ) 27 12:54:26 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=001 Nr=003 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x06; Type = CONN ACK
(LN) 28 12:54:26 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=002 FCS=Good
```

Com es pot veure hi ha un CONNECT en l'instant que l'usuari despenja i un CONN ACK per part de la central. Just després l'altre extrem rep el CONNECT i respon amb el CONN ACK. Tot això amb més trames RR per confirmar les dades.

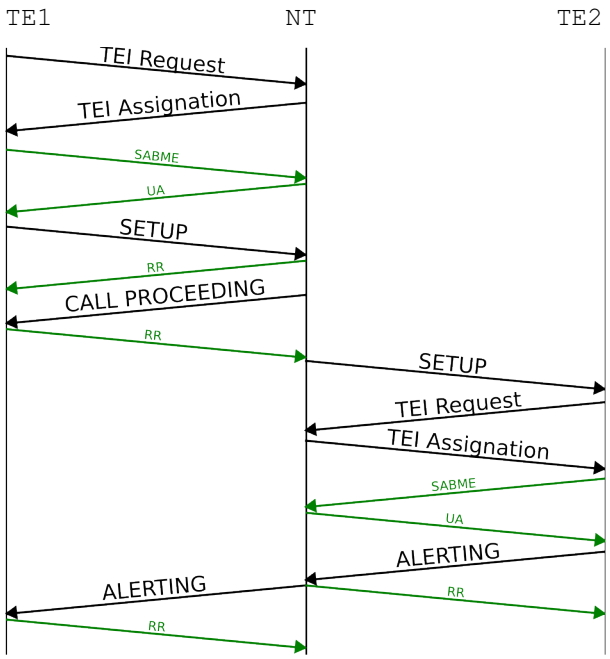
Ara mostrem el bolcat que veiem quan ens desconnectem (pengem el telèfon).

```
(EQ) 29 12:54:27 LAPD: SAPI=0 TEI=69 Type=Info  P=0 Ns=002 Nr=001 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2a; Type = DISConect
    Coding Std                = CCITT
    Cause                     = Normal Clearing
    Cause Decimal Value       = 16
(LN) 30 12:54:27 LAPD: SAPI=0 TEI=69 Type=RR    F=0 Nr=003 FCS=Good
(LN) 31 12:54:27 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=003 Nr=002 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x06; Type = DISConect
    Coding Std                = CCITT
    Cause                     = Normal Clearing
    Cause Decimal Value       = 16
(EQ) 32 12:54:27 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=004 FCS=Good
(EQ) 33 12:54:27 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=002 Nr=004 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x06; Type =  RELease
(LN) 34 12:54:27 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=003 FCS=Good
(LN) 35 12:54:27 LAPD: SAPI=0 TEI=68 Type=Info  P=0 Ns=004 Nr=003 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x06; Type =  REL COM
(EQ) 36 12:54:27 LAPD: SAPI=0 TEI=68 Type=RR    F=0 Nr=005 FCS=Good
(LN) 37 12:54:27 LAPD: SAPI=0 TEI=69 Type=Info  P=0 Ns=001 Nr=003 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2a; Type =  RELease
(EQ) 38 12:54:27 LAPD: SAPI=0 TEI=69 Type=RR    F=0 Nr=002 FCS=Good
(EQ) 39 12:54:27 LAPD: SAPI=0 TEI=69 Type=Info  P=0 Ns=003 Nr=002 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2a; Type =  REL COM
(LN) 40 12:54:27 LAPD: SAPI=0 TEI=69 Type=RR    F=0 Nr=004 FCS=Good
```

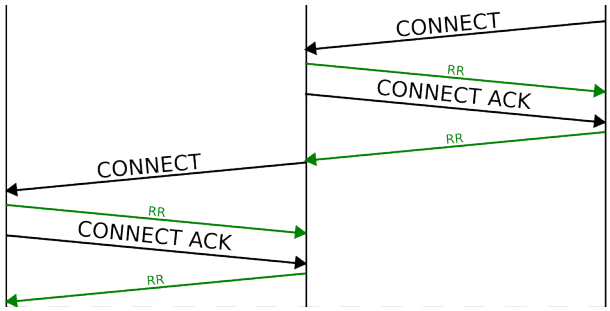
Veiem les trames DISCONNECT que envia un terminal a la central i aquesta novament a l'altre terminal. Després es confirmen amb una RELEASE (del terminal a la

central) i un RELEASE COMPLETE (de la central al terminal) i aquest procés es produeix a l'inrevés a l'altre costat. A les trames de DISCONNECT veiem la causa de la desconnexió. El camp Coding Std indica que el codi és el definit per l'estandard del ITU (International Telecommunication Union), el codi en aquest cas és el 16, que és Normal clearing. Això vol dir que l'usuari ha penjat. N'hi ha d'altres causes com el 18 (ningú respon i s'aborta la connexió) que no hem provat.

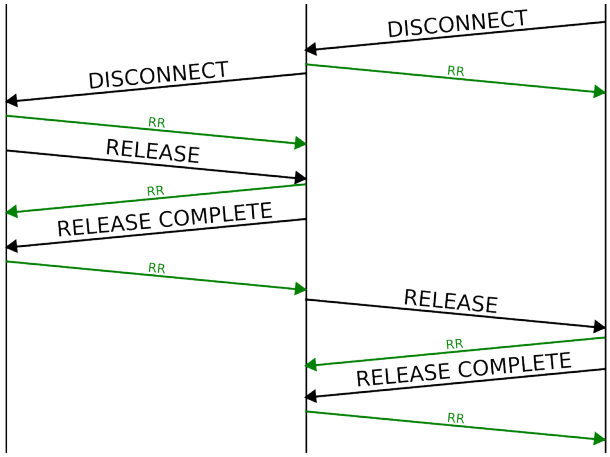
Com a resum complet posem un diagrama temporal.



Fase d'inicialització (marcatge i ring) a l'esquerra.



Fase de connexió (despenjar el telèfon i parlar).



Fase de desconnexió. En aquest cas penja la persona que ha rebut la trucada.
Si hagués penjat l'altra el procés hagués estat el mateix canviant els papers.

• Manteniment de la línia a nivell 2

Ara mirem el manteniment de la línia a nivell 2 un cop hem finalitzat la trucada. Recordem que aquesta va establir dues connexions mitjançant la trama SABME.

```
(LN) 4 12:34:23 LAPD: SAPI=0 TEI=66 Type=RR    P=1 Nr=016 FCS=Good
(EQ) 5 12:34:23 LAPD: SAPI=0 TEI=66 Type=RR    F=1 Nr=018 FCS=Good
(EQ) 6 12:34:23 LAPD: SAPI=0 TEI=67 Type=RR    P=1 Nr=003 FCS=Good
(LN) 7 12:34:23 LAPD: SAPI=0 TEI=67 Type=RR    F=1 Nr=006 FCS=Good
```

Es veu com la central envia RR amb el bit de Poll a 1 per aconseguir una resposta (bit de Fi a 1). Amb això la central sap que el terminal està funcionant.

Vam fer una proba consistent en desconnectar un terminal de forma sobtada (sense enviar la comanda DISC). Veiem com la central intenta detectar la caiguda de la terminal.

```
(LN) 37 12:37:55 LAPD: SAPI=0 TEI=66 Type=RR    P=1 Nr=016 FCS=Good
(LN) 38 12:37:56 LAPD: SAPI=0 TEI=66 Type=RR    P=1 Nr=016 FCS=Good
(LN) 39 12:37:57 LAPD: SAPI=0 TEI=66 Type=RR    P=1 Nr=016 FCS=Good
(LN) 40 12:37:58 LAPD: SAPI=0 TEI=66 Type=SABME P=1 FCS=Good
(LN) 41 12:37:59 LAPD: SAPI=0 TEI=66 Type=SABME P=1 FCS=Good
(LN) 42 12:38:00 LAPD: SAPI=0 TEI=66 Type=SABME P=1 FCS=Good
(LN) 43 12:38:01 LAPD: SAPI=0 TEI=66 Type=SABME P=1 FCS=Good
(LN) 44 12:38:02 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI P=0 FCS=Good
(LN) 45 12:38:03 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI P=0 FCS=Good
(LN) 46 12:38:04 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI P=0 FCS=Good
(LN) 47 12:38:04 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI P=0 FCS=Good
```

El que fa la central és que al tercer RR que no té resposta intenta reconnectar-se fent servir SABME. Després de 4 SAMBE sense resposta la central opta per fer servir el mecanisme de TEI Management per comprovar que realment està enviant trames al terminal que vol. Per aquest motiu envia 4 trames de TEI Management amb el camp de Management Message Type a Identity check. Amb això demana una resposta al terminal que tingui el TEI que està buscant. Com que en aquest cas tampoc respon, a les 4 trames sense resposta simplement tanca la connexió. La propera vegada que el terminal estigui en línia haurà de demanar un nou TEI per a poder comunicar-se.

• Establiment d'una trucada entre un terminal i un node de la central

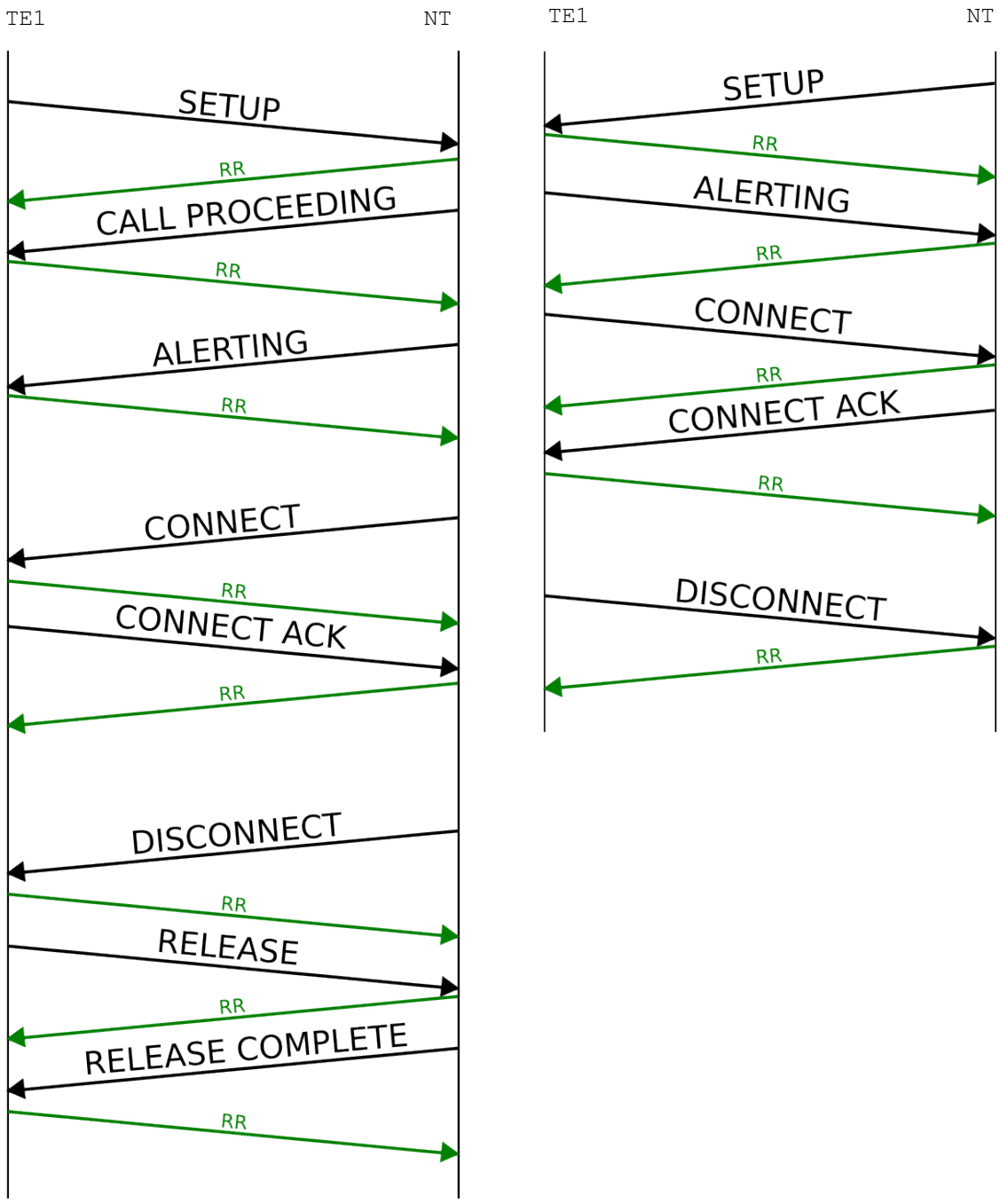
Per a veure més clarament el desenvolupament d'una trucada en fem una a un telèfon que estigui directament connectat a la central. Així no veurem cap tipus de missatges cap al telèfon en qüestió. En aquest cas el nostre terminal no té cap TEI assignat.

```
(LN) 8 13:01:19 LAPD: SAPI=0 TEI=127(Broadcast) Type=UI    P=0 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2c; Type = SETUP
(EQ) 9 13:01:19 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI    P=0 FCS=Good
(LN) 10 13:01:19 LAPD: SAPI=63 TEI=127(Broadcast) Type=UI    P=0 FCS=Good
(EQ) 11 13:01:19 LAPD: SAPI=0 TEI=70 Type=SABME P=1 FCS=Good
(LN) 12 13:01:19 LAPD: SAPI=0 TEI=70 Type=UA    F=1 FCS=Good
(EQ) 13 13:01:19 LAPD: SAPI=0 TEI=70 Type=Info  P=0 Ns=000 Nr=000 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2c; Type = ALERTing
(EQ) 19 13:01:21 LAPD: SAPI=0 TEI=70 Type=Info  P=0 Ns=001 Nr=000 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2c; Type =  CONNect
(LN) 20 13:01:21 LAPD: SAPI=0 TEI=70 Type=RR    F=0 Nr=002 FCS=Good
(LN) 21 13:01:21 LAPD: SAPI=0 TEI=70 Type=Info  P=0 Ns=000 Nr=002 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2c; Type = CONN ACK
(EQ) 22 13:01:21 LAPD: SAPI=0 TEI=70 Type=RR    F=0 Nr=001 FCS=Good
(EQ) 23 13:01:22 LAPD: SAPI=0 TEI=70 Type=Info  P=0 Ns=002 Nr=001 FCS=Good
                Q.931: Protocol = CallCtrl; CR = 0x2c; Type = DISConect
```

```
(LN) 24 13:01:22 LAPD: SAPI=0 TEI=70 Type=RR    F=0 Nr=003 FCS=Good
(LN) 25 13:01:26 LAPD: SAPI=0 TEI=70 Type=Info  P=0 Ns=001 Nr=003 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2c; Type =  RELease
(EQ) 26 13:01:26 LAPD: SAPI=0 TEI=70 Type=RR    F=0 Nr=002 FCS=Good
(EQ) 27 13:01:26 LAPD: SAPI=0 TEI=70 Type=Info  P=0 Ns=003 Nr=002 FCS=Good
                 Q.931: Protocol = CallCtrl; CR = 0x2c; Type =  REL COM
```

Es veu el procés d'adquisició d'un TEI i l'establiment de la connexió de nivell 2. Després es veuen totes i cada una de les etapes de la trucada, però ara no les veiem repetides, ja que no estem capturant les trames que arriben al telèfon de la central.

Novament presentem l'esquema temporal:



En el diagrama de l'esquerra es realitza una trucada de terminal local a node directament connectat a la central, mentre que al diagrama de la dreta veiem la recepció d'una trucada des d'un node directament connectat a la central.

Les diferències (sense tenir en compte les obvietats de que tota la comunicació es realitza de forma inversa) són la trama de CALL PROCEEDING i les trames de RELEASE. La primera no la veiem en cas de ésser trucats ja que aquesta trama té com a objectiu avisar al que truca que la trucada és correcte i que s'està esperant a que l'altra persona despengi el telèfon. És necessària ja que si no seria impossible detectar situacions com per exemple números incorrectes o un telèfon que comunica. La trama de RELEASE no apareix degut a que el telèfon està connectat a la central i aquesta no necessita confirmar l'alliberació del canal.