Action at the CPP:

After reception of the message to check for free channels, the CPP transmits its preferred free channel to the origination CFP. Normally, this will be the channel having the lowest field strength as measured by the CPP. The CPP may need to briefly hop to candidate channels to evaluate their field strengths, interrupting the call. After reception of a link re-establishment message, the CPP checks the given channel (and the list of free channels) for the presence of CHMF and the appropriate IDs in the D-channel for a period of up to $T_{re} + 4 \cdot T_{re2}$.

Three eventualities exist:

i) The CPP detects CHMF in the SYN channel and a matching PID and LID in the D channel. The CPP then responds with MUX2 with SYNCP in the SYN channel and PID and LID in the D channel. The B-channel connection is re-established.

ii) No recognized response is received before the expiry of the receive time. The CPP then attempts to re-establish the connection with the origination CFP and checks the original channel for the presence of CHMF and the appropriate IDs in the D-channel for a period of up to $T_{re}$.

iii) No recognized response is received before the expiry of the receive time. The CPP may then rescan the Common Signalling Channels and initiate the call set-up procedure to the base station with the maximum relative received signal strength. The call is re-routed to the appropriate base station by the CCFP.

Link re-establishment attempts must cease when the 10 s handshake timeout ($T_{hlost}$) expires.

## 4. Data Services

### 4.1 Introduction

This section describes the data services supported by PCI.

Four different data services are supported over the 32 kbit/s B channel:

(1) full-duplex asynchronous data services
(2) transparent data services
(3) X.25 packet data services
(4) Group III (G3) Fax services

The asynchronous data service allows subscribers to access landline computer facilities with asynchronous data rates of 300 to 19200 bit/s (300, 1200, 2400, 4800, 9600, 14400 and 19200 bit/s). It also allows landline subscribers to access portable terminals with the same asynchronous rates. Asynchronous data employs an Automatic-Repeat Request (ARQ) protocol for the retransmission of errored blocks , together with a Forward Error Correction (FEC) scheme. A flow control mechanism is used to control the data rate at the user terminal or the host computer when severe degradation of radio transmission occurs for a long period of time.

The transparent data service provides the user with unrestricted access to the 32 kbit/s B channel, or to subrate channels. Data rates are synchronous and user selectable. The supported rates are: 300, 1200, 2400, 4800, 9600, 14400, 19200 and 32,000 bit/s. The service has the capability of providing FEC for all rates except 32 kbit/s, at the user's request. Reed Solomon (RS) codes are used for FEC similar to the asynchronous data service. However, there is no ARQ protocol and there is no guarantee of data integrity.

The X.25 packet data service supports the use of X.25 terminals over the system. X.25 terminals may be connected to a data terminal and send/receive data over a public or private landline packet data network.

The G3 Fax service allows G3 Fax machines to be connected to a PCI data terminal, and send/receive fax messages over (a) a public or private landline packet data network that supports a FaxPad (see section 4.5 for more discussion), or (b) through a circuit switched connection.

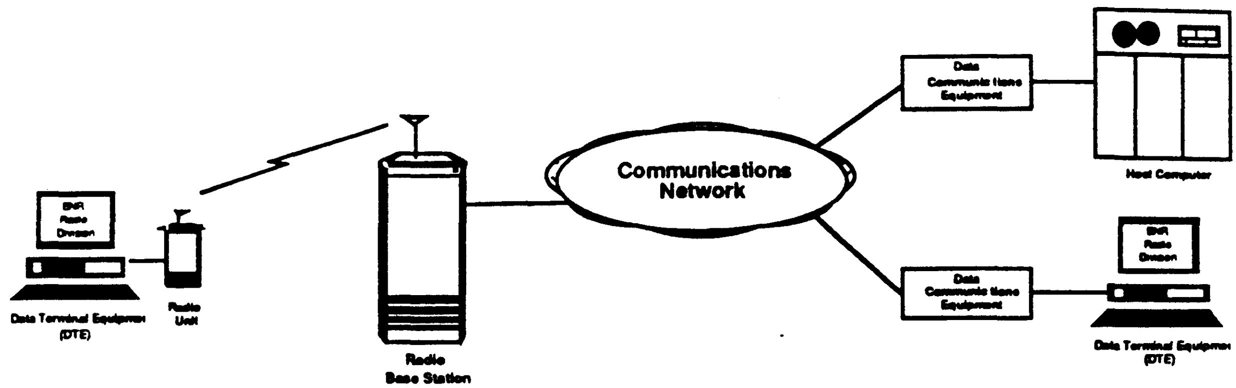
### 4.2 Asynchronous Data Transport

#### 4.2.1 General System Configuration

Fig. 4.1 shows the general system configuration of the asynchronous data service. A subscriber may connect a Personal Computer (PC) or a Data Terminal Equipment (DTE) directly to the portable data terminal through an RS-232 interface. The data terminal runs the asynchronous data firmware that is responsible for the transport of data over the radio link. The corresponding asynchronous data software runs at the Base station and Network Controller. After appropriate conversion, the data is transmitted through the network to a Data Communications Equipment (DCE) device which is connected to a host computer, a workstation, or any other device that appropriately interfaces to it.

In effect two protocols exist: one for the radio link and one for the landline link, with appropriate protocol conversion taking place at the Radio Base station.

Figure 4.1
**General system configuration for asynchronous data service**




4.2.2 System Description

Fig. 4.2 shows the main components of the system that enable the asynchronous data service which are:

- PAD - Packet Assembler/Disassembler
- RDLL - Radio Data Link Layer
- LPL - Land-Line Physical Layer.

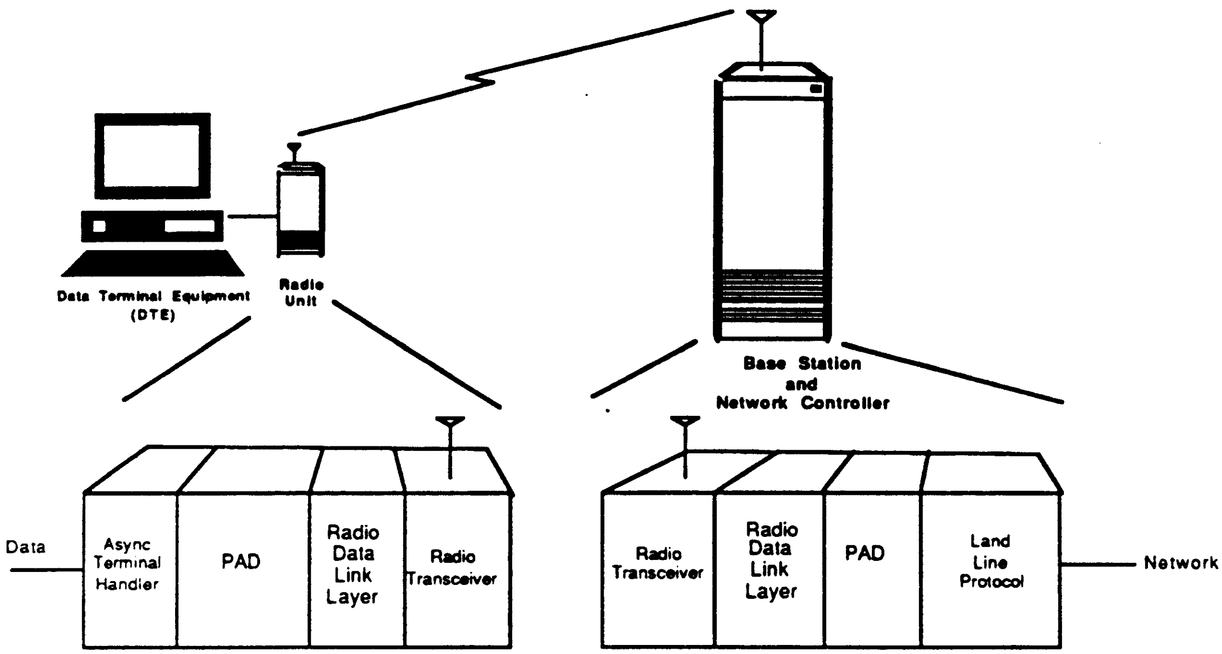
The PAD provides for the asynchronous to synchronous interface between the asynchronous PC or DTE to the synchronous radio data link. The RDLL implements Forward Error Correction (FEC)[2] together with an Automatic Repeat Request (ARQ) protocol[3]. The LPL provides access to a variety of computer facilities. The PAD and RDLL reside in both the PCI data terminal and the Base station and Network Controller, whereas the LPL resides only at the Base station and Network Controller side. The asynchronous terminal handler provides the RS-232 interface to the PC or DTE.

---

[2] S. Lin and D. Costello, "Error Control Coding: Fundamentals and Applications," Prentice-Hall, April 1983.

[3] S. Lin, D.J. Costello, M.J. Miller, "Automatic-Repeat Request Error-Control Schemes", IEEE Communications Magazine, Vol. 22, No. 12, pp. 5-17, December 1984.

**Figure 4.2 System description**




4.2.2.1 Land-Line Physical Layer (LPL)

The LPL provides access to land-line computer facilities. It may be one of the existing asynchronous standards such as voiceband modems or rate adaption protocols. By conforming to widely used standards, there is no need to use specialized network termination equipment for users accessing land-line computer facilities from a portable data terminal.

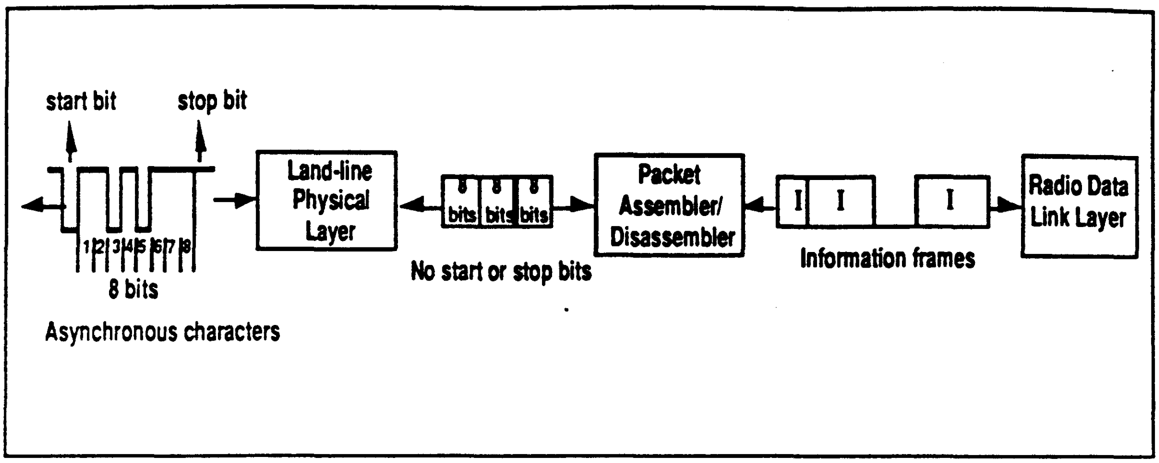
Examples of LPLs may be:

- V.32 modem (9600/4800 bit/s)
- V.22 bis modem (2400/1200 bit/s)
- V.21 modem (300 bit/s)
- Bell 212A modem (1200/300 bit/s)
- Rate adaption protocols (e.g. V.120)
- Others for further study (e.g. MNP for some modems)

4.2.2.2 Packet Assembler/Disassembler (PAD)

The Packet assembler/disassembler lies between the LPL and the RDLL (in the Base Station and Network Controller case). In the forward direction the LPL receives asynchronous characters from the land-line. Asynchronous characters typically consist of a start bit that indicates the start of a character, one or more stop bits that indicate the end of the character, and a certain number of bits in between that define the specific character. The characters may also contain a parity bit . The LPL strips these asynchronous characters from their start, stop and parity bits and provides the PAD with the remaining bits. An example is shown in Fig. 4.3 for the case of 1 start, eight data bits, 1 stop, no parity. The PAD assembles the asynchronous characters into information frames that are passed on to the RDLL for transmission over the synchronous radio link.

**Figure 4.3 Packet Assembler/Disassembler**




In the reverse direction the PAD receives information frames from the RDLL, disassembles them into characters, and passes them to the LPL.
The PAD also provides for an XON-XOFF flow control mechanism in order to prevent buffer overflow when radio transmission degrades for a long period of time. The PAD generated flow control does not interfere with terminal or user generated flow control. The PAD buffers should be made sufficiently long to avoid overflow due to transmission delays and DTE response times.

At the portable data terminal side, the PAD performs the exact same functions, with the exception that it receives/sends asynchronous characters to a terminal handler instead of the LPL.

4.2.2.3 Radio Data Link Layer

The RDLL is responsible for the transport of data over the radio link. It must overcome the transmission impairments presented by the mobile radio channel. The radio data link layer uses a Type I Hybrid Automatic Repeat Request (ARQ) scheme. This scheme combines Forward Error Correction (FEC) with an ARQ protocol.

If an ARQ protocol is used alone then, because of the severity of the radio channel, the throughput would degrade rapidly with increasing bit error rate. The application of FEC coding reduces the probability of an ARQ frame error, and thus limits the number of retransmissions which in effect increases the throughput.

4.2.2.3.1 Forward Error Correction

Reed-Solomon (RS) block codes are used for FEC. RS codes have proved to be very powerful and efficient codes for use in the mobile radio channel environment [4]. Some of the advantages that RS codes offer are:

- sufficient flexibility to support various coding rates with no program redesign. This will be required for the support of different land-line access rates (see section 4.2.2.3.3).
- the coding rate can be optimized for each different land-line access rate.
- the codes can support simultaneous correction and detection. This eliminates the need for using a cyclic redundancy check (CRC) at the ARQ level. Greater detection capability than with a CRC-16 is possible, and more parity symbols can be provided by eliminating the CRC.
- low computational complexity

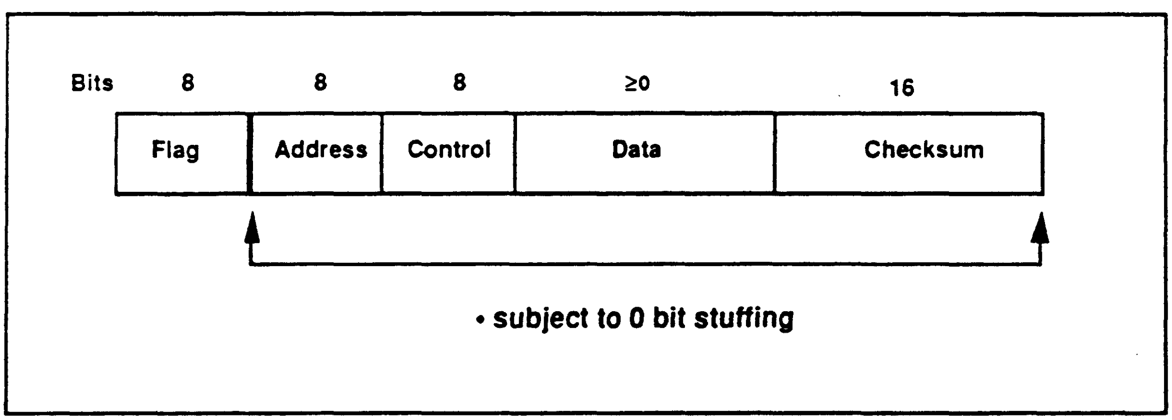
An RS code is described as a (n,k,d) code in this context, where k is the number of data symbols, n-k is the number of parity symbols and d is the number of parity symbols (out of the n-k parity symbols) reserved for error detection.

4.2.2.3.2 Automatic Repeat Request Protocol

The ARQ protocol used is one derived from the High-Level Data Link Control (HDLC) family[5]. The protocol is a modified version of the Link Access Procedure Balanced protocol (LAPB).

LAPB is a bit oriented data link layer protocol which uses zero bit stuffing to preserve the uniqueness of flag bytes, which are used to indicate the start of each LAPB frame. A LAPB frame is shown in Fig. 4.4.

Figure 4.4 LAPB frame




[4] G. Mony, B. Toplis, J. Michaelides, Performance Assessment of Data Transport Alternatives for Digital Cellular Radio , IEEE Vehicular Technology Conference, pp. 336-340 , 1990.

[5] International Standards Organization. "Data communication - High-Level data link control procedures - Consolidation of elements procedures," Ref. No. ISO 4335-1983(E)

The flag byte is at the beginning of each frame, and is used to indicate the start of the frame. The address byte is used to distinguish commands from responses (for point-to-point lines). The control byte is used primarily for sequence numbers and to distinguish the different types of frames. The information field is used for arbitrary information and may be arbitrarily long (length is actually limited by the effectiveness of the Cyclic Redundancy Check (CRC)). The CRC bytes are used for frame error detection.

4.2.2.3.2.1 Modified LAPB

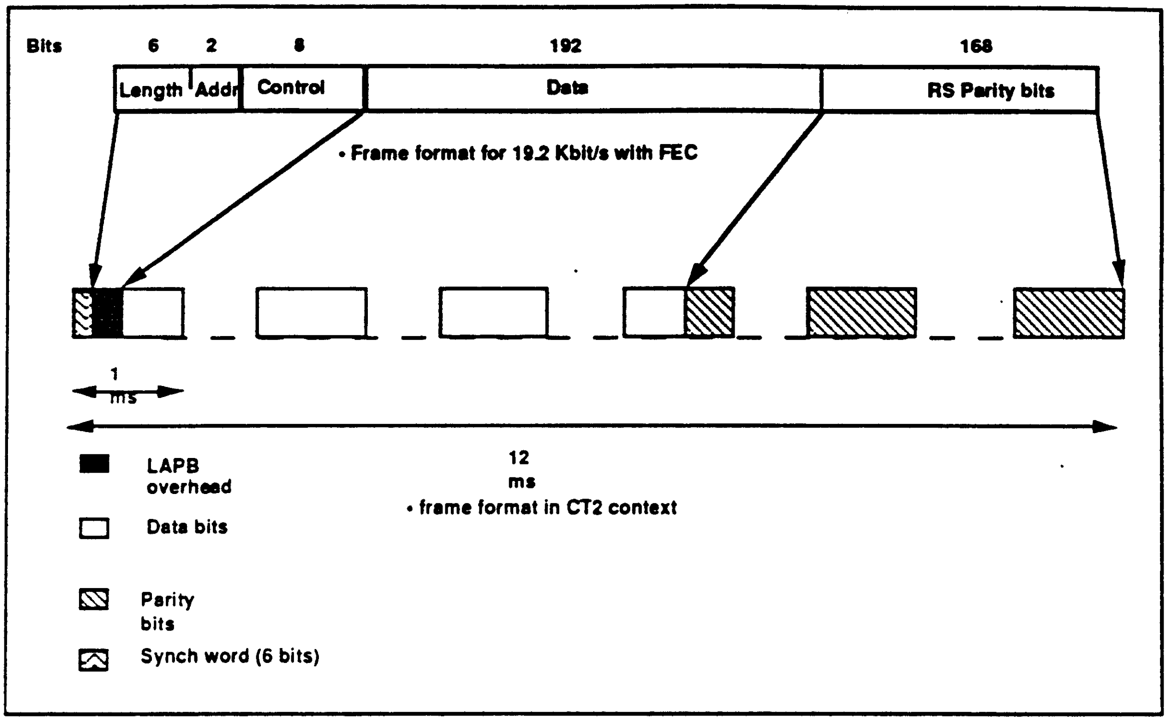
The LAPB frame is to be inserted in a number of transmit bursts. A synchronization word (6 bits) is used at the beginning of the frame to establish which burst is first in the frame. Thus, by sharing PCI framing, the LAPB flag bytes and zero bit stuffing can be eliminated. The ARQ frame length information must be added to the frame header, which can be multiplexed into the address byte of LAPB. The length information is six bits long, which is sufficient to cover the maximum length of data in a LAPB frame. The elimination of the flag bytes and zero bit stuffing results in an increased number of available bits that are used by the FEC code. The data field is a multiple of 8, since it will contain a certain number of eight bit characters. When there is not enough data to fill the maximum data field available, then arbitrary information is used for filling. The CRC bytes are also eliminated, since RS codes already provide for error detection capability. The resulting frame is shown in Fig. 4.5, where I is the number of eight-bit characters to be transmitted.

Figure 4.5 Modified LAPB frame

| Bits | 6 | 2 | 8 | 8*I |
|---|---|---|---|---|
| | Length | Addr | Control | Data |

The modified LAPB frame is aligned with the Multiplex 1 burst structure (CAIS, part 2, Figure 2.2). Multiplex 1 supports 64 B channel bits. Six bursts are used to carry a complete LAPB frame plus the FEC parity bits (see Fig. 4.6).

**Figure 4.6 Frame Format in PCI Context**




In order to provide the maximum desired throughput of 19.2 kbit/s, we need at least 192 bits out of the 384 bits provided by six transmit bursts. The PAD strips the start, stop and parity bits so the asynchronous rate of 19.2 kbit/s translates to a 15.36 kbit/s synchronous rate over the air interface (19.2 * 8/10= 15.36). This corresponds to 184.32 bits for a 12 ms frame. However, since we restrict the LAPB data field to be a multiple of 8 we actually need 192 bits. Adding the bits required by the length+address and control bytes we get:

$$192+8+8 = 208 \text{ bits}$$

If we use an RS code with 6 bits per symbol, then the maximum block length we can use is 63 symbols or 378 bits. The resulting RS code is (378/6,208/6)=(63,35;1) with 1 parity symbol reserved for error detection. Also, the LAPB timeouts have to be customized for the PCI network implementation.

4.2.2.3.3 Multimode FEC

In the case of the lower rates (eg. 9600 bit/s, 4800 bit/s etc.) it is advantageous to use a different more powerful FEC code, that would utilize the extra available capacity. This would provide better error protection and consequently it would improve the throughput. Experimental results of using this method have been demonstrated for 9600 bit/s[6].

Therefore, a multimode FEC technique is used, where the FEC code used is determined by the maximum bit rate provided by the user. Table 4.1 lists the resulting RS codes.

**Table 4.1 Multimode FEC**

| Mode | Rate (bit/s) | RS code (n,k;d) |
|---|---|---|
| 1 | 300 | (63,4;1) |
| 2 | 1200 | (63,6;1) |
| 3 | 2400 | (63,7;1) |
| 4 | 4800 | (63,11;1) |
| 5 | 9600 | (63,19;1) |
| 6 | 14400 | (63,27;1) |
| 7 | 19200 | (63,35;1) |

### 4.3 Transparent Data Service

The transparent data service provides the user with an unrestricted access to the 32 kbit/s B channel, or to subrate channels. Data rates are synchronous and user selectable. The supported rates are: 300, 1200, 2400, 4800, 9600, 14400, 19200 and 32,000 bit/s. The service has the capability of providing FEC for all rates except 32 kbit/s, at the user's request. Reed Solomon (RS) codes are used for FEC similar to the asynchronous data service. However, there is no ARQ protocol, and there is no guarantee of data integrity.

### 4.4 X.25 Packet Data Service

This service allows terminals with X.25[7] capabilities to communicate with private or public landline packet data networks (Fig. 4.7).

In Fig. 4.7, the X.25 layer 2 at the portable data terminal communicates with the X.25 layer 2 of the X.25 terminal. The data is then given to the RDLL for transmission over the radio link. At the Base station and Network controller, the RDLL (a) passes the data to an X.25 layer 2 for transmission over a landline packet data network or (b) distributes the data locally. In the

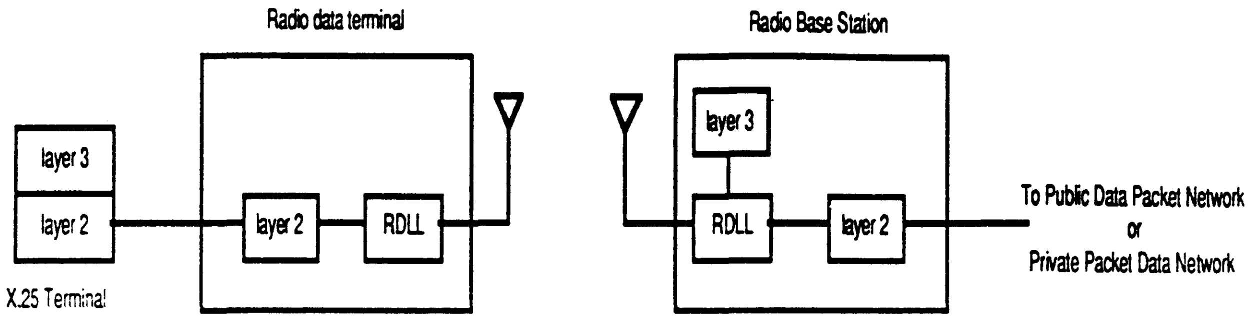
---

[6] G. Mony, J. Michaelides, B. Toplis, Asynchronous Data Transport on Digital Cellular Radio, Worldwide Personal Communications Comforum, June 1990.

[7] The International Telegraph and Telephone Consultive Committee. "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit," Recommendation X.25, Malaga-Torremolinos, 1984

second case, an X.25 layer 3 is implemented at the Base station and Network Controller for communicating with the X.25 terminal's layer 3.

**Figure 4.7 X.25 Packet Data Service**



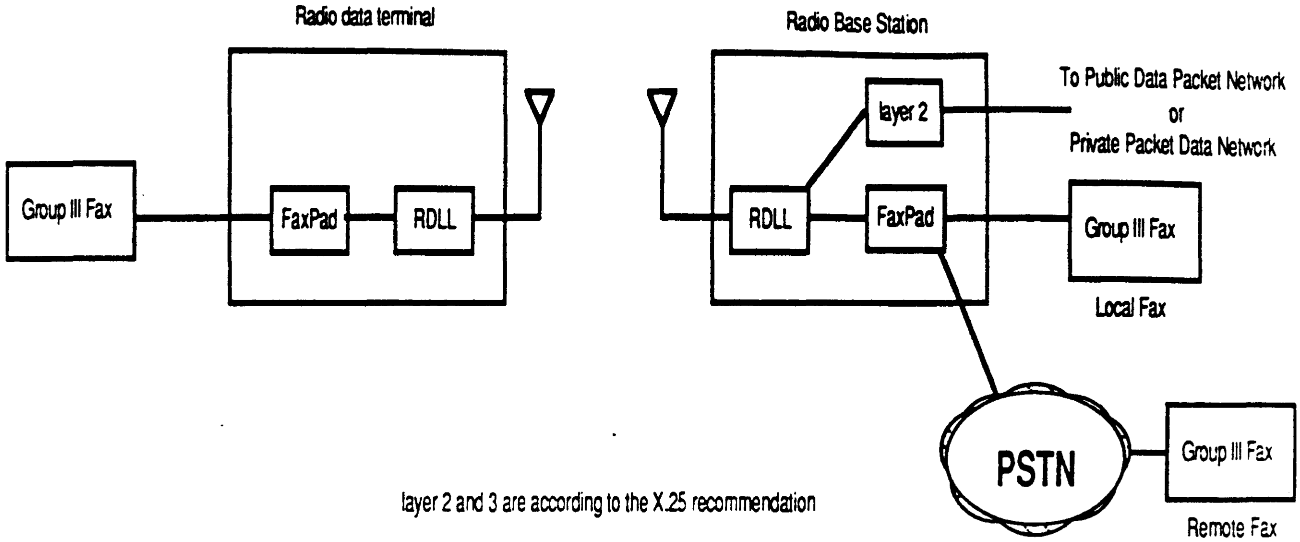

layer 2 and 3 are according to the X.25 recommendation

An asynchronous terminal can also communicate over a landline packet data network by accessing a PAD using the asynchronous data capability of the PCI system, as described in section 4.2.

### 4.5 Group III Fax Service

The PCI system supports the transmission and reception of G3 Fax messages. A G3 Fax machine is connected to the PCI data terminal via an analog or digital interface (Fig. 4.8). A FaxPad is used as an interface between the fax protocol and the radio transport. The FaxPad provides for appropriate mechanisms in order to communicate with a G3 Fax machine and to receive the user data. It also provides for the exchange of control information between FaxPads. It assembles/disassembles the user data and control information into/from packets, using datafields defined in the X.25 recommendation (packet level). The FaxPad uses the RDLL as its layer 2.

**Figure 4.8 G3 Fax Service**




A G3 Fax machine connected to a PCI data terminal may access a G3 Fax machine (a) over a landline packet data network or (b) through a circuit switched connection. In the first case, the FaxPad located at the PCI data terminal communicates with a corresponding Faxpad located within the landline packet data network. This case allows G3 Fax machines connected to PCI data terminals to access G3 Fax machines that use a packet data network to transmit or receive their messages. In the second case, the FaxPad located at the PCI data terminal communicates with the FaxPad located at the Base station and Network controller for a circuit switched connection to a local G3 Fax machine, or to a G3 Fax machine connected to the Public Switched Telephone Network (PSTN).

In case the FaxPad is implemented within the G3 Fax machine, then this Fax machine may use the X.25 packet data service (as described in section 4.4) for the transmission/reception of Fax messages.

Currently, the CCITT is in the process of examining recommendations X.5, X.38 and X.39, which specify a FaxPad that would provide connection of G3 Fax machines through packet data networks. These recommendations could be used for the implementation of the FaxPad shown in Fig. 4.8.

The RDLL is the same as specified for the asynchronous data service.

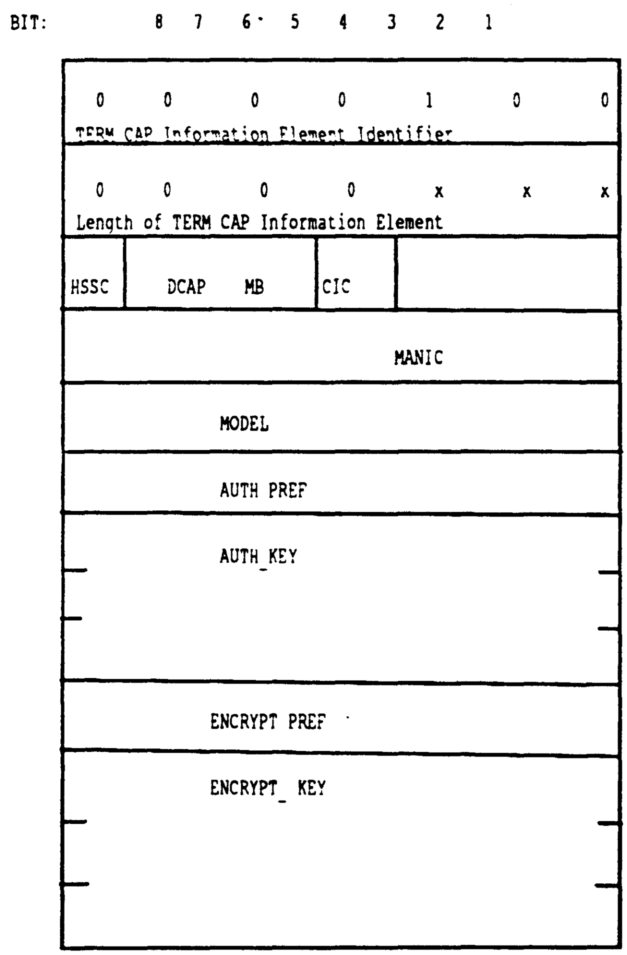
## 5. Security

Cryptographic techniques can provide both privacy and authentication. Annex C of the CT2 CAIS specifies the mechanisms of basic authentication to be used in PCI handsets.

### 5.1 Layer 3 Information Elements

#### 5.1.1 Terminal Capabilities Information Element

Encryption for calls is offered as an option in the PCI system. The option is invoked via the Terminal Capabilities Information Element (TERM_CAP). This information element is described in the CAIS Signalling Layer 3, Section 2.2.10. Additional fields are added to the Terminal Capabilities Information Element to support encryption.




Encrypt_Pref is used by the CPP to indicate to a CFP which of the encryption algorithms offered by the CPP is the CPP's preferred algorithm. If only one algorithm is offered, this must be indicated as the preferred algorithm in this field.

Encrypt_Key is a bit field used to indicate to a CFP which encryption algorithms the CPP is capable of performing. A bit if set to 1 indicates that the CPP is capable of performing the associated algorithm, and if the bit is set to 0 the CPP is not capable of performing the associated algorithm.

5.1.2 Alternative Encryption Request Information Element (ENCRYPT2_REQ).

This alternative encryption request information element is used by a CFP to initiate the alternative call encryption process.

BIT: 8 7 6 5 4 3 2 1

| |
|---|
| 0 x x x x x x x<br>ENCRYPT2 REQ Information Element Identifier |
| Length of ENCRYPT2 REQ Information Element |
| ENCRYPT NO |

ENCRYPT_NO is used to indicate to the CPP which (if any) of the encryption algorithms offered by the CPP is to be used.

## 5.2 Mutual Authentication & Encryption Key Generation

The voice/data channel (B channel) is encrypted using a private key cryptosystem. The private key cryptosystem could be based on the encryption function "F" used for Telepoint authentication. Two private keys are used (one for each direction of transmission). The private keys are derived by extending the telepoint authentication procedure (CAIS, Annex C). A new pair of encryption keys is generated for each session or call.

A handset contains identification information which is transmitted to the CFP during the setup and authentication phases of a call. This information is sufficient to uniquely identify the handset. The handset also stores internally a PIN number which is transmitted to the base station during the setup and authentication phases of a call.

To avoid problems of fraud (arising from the monitoring of the air-interface and the cloning of valid handsets) the PIN is encrypted before transmission over the air-interface.

The process by which the content of the PIN field is interrogated by the base and the handset authenticated is:

-The base transmits to the handset a 32-bit random challenge (RAND1) in the Layer 3 Information Element AUTH_REQ where it is received as RAND1'.

-The handset encrypts the 64-bit PIN using an encryption function "F", and using RAND1' as the key to produce the the 32-bit cyphered-PIN (CPIN1).

-The handset then transmits CPIN1 to the base in Layer 3 Information Element AUTH_RES where it is received as CPIN1'.

-The base determines the expected-PIN (E-PIN1) for the handset using the Identification Information and using the same function "F", with RAND1 as the key, calculates the expected value of CPIN1 (E-PIN1).

-The base compares the received CPIN1 (CPIN1') with the expected value (E-PIN1). If the values match the handset is judged to be valid.

A similar process can be used to authenticate the base to the handset:

-The handset transmits to the base a 32-bit random challenge (RAND2) in the Layer 3 Information Element AUTH_REQ where it is received as RAND2'.

-The base encrypts the 64-bit PIN using an encryption function "F", and using RAND2' as the key to produce the the 32-bit cyphered-PIN (CPIN2).

-The base then transmits CPIN2 to the handset in Layer 3 Information Element AUTH_RES where it is received as CPIN2'.

-The handset encrypts the 64-bit PIN using the same function "F", with RAND2 as the key, calculates the expected value of CPIN2 (E-PIN2).

-The handset compares the received CPIN2 (CPIN2') with the expected value (E-PIN2). If the values match the base is judged to be valid.

The process by which the encryption key (Key_P_to_F) for the CPP to CFP link is obtained is:

-the handset and base each encrypt the 64-bit PIN using the encryption function "F" and using CPIN1 as the key to produce the 32-bit cyphered CPIN1 (C-CPIN1).

Key_P_to_F = C-CPIN1.

The process by which the encryption key (Key_F_to_P) for the CFP to CPP link is obtained is:

-the handset and the base each encrypt the 64-bit PIN using the encryption function "F" and using CPIN2 as the key to produce the 32-bit cyphered CPIN (C-CPIN2).

Key_F_to_P = C-CPIN2.

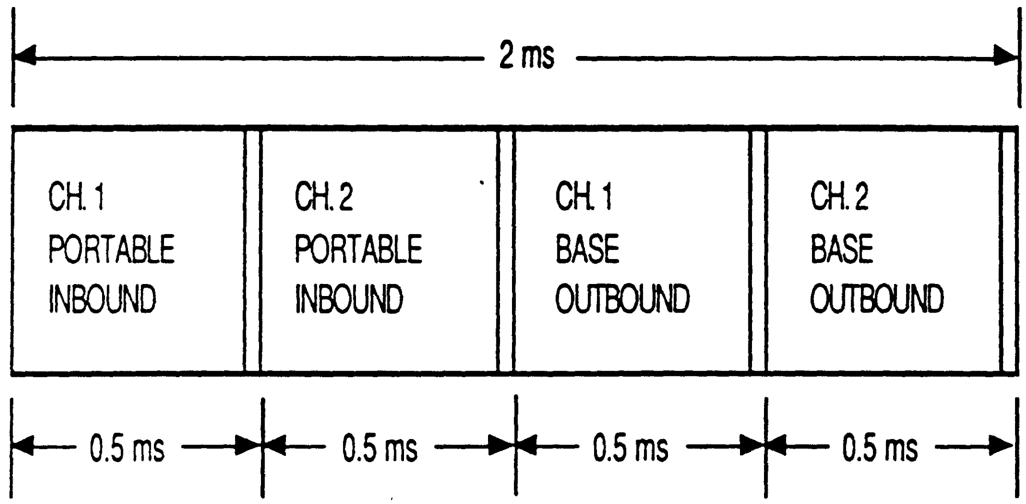
The method can be easily generalized to generate 64-bit keys if required.

The sections above have assumed that the base station, given the identity of the handset (and account), will know the value of the PIN expected from the handset (E-PIN).

## 6. Half-Slot Channels

The provision for half-slot channels will allow PCI to take advantage of future low bit rate speech coders and/or more efficient modulation schemes. A number of different frame structures are possible. One option, presented in Fig. 6.1, would allow the use of 2-channel TDMA on each standard 2 ms frame. Radios using the half-slots would still have to meet the channel spectral mask and power levels; thus, they would cause no more interference than standard full-slot transmitters.

**Figure 6.1: Frame Structure for Half-Slot Channels**



BNR

Annex to

**Northern Telecom's**

Response to
NOI Gen. Docket No. 90-314
RM-7140
RM-7175

# PCI

# A Common Radio Standard for Personal Communications Interface

Issue 1.3
September 1990

BNR

Annex to

**Northern Telecom's**

Response to
NOI Gen. Docket No. 90-314
RM-7140
RM-7175

# PCI

# A
# Common Radio Standard
# for
# Personal Communications Interface

Issue 1.3
September 1990

## Introduction

This document describes the common radio interface specification for a Personal Communication Interface (PCI). This is based upon BNR studies of requirements for low power radio Personal Communications Services (PCS) ranging from single and multiple line residential "cordless" applications, public access applications, and large in-building wireless business communications applications. The interface makes use of moden digital modulation and access techniques to achieve a high traffic capacity and very high spectrum utilization efficiency. Dynamic channel allocation techniques are utilized to facilitate the efficient assignment of resources in high traffic applications. The dynamic channel allocation process is also well suited to shared spectrum assignments.

The specification addresses the interworking between fixed and portable radio units operating in the PCS band, including Public Access Services and Business and Residential Applications. This specification is based on the CT2 Common Air Interface Specification (MPT 1375 CAIS[1]) developed in the United Kingdom, and includes evolutionary enhancements and modifications to meet a broad range of PCS requirements.

The PCI specification consists of two parts:

1. The CT2 Common Air Interface Specification (CAIS) comprising:

| | |
|---|---|
| MPT 1375 | dated May 1989 |
| Amendment 1 to MPT 1375 | dated November 1989 |
| Annexes A, B, C | dated November 1989 |
| Amendment 2 to MPT 1375 | dated February 1990 |
| The specification for UK Function "F" | released December 1989 |

   Copies of MPT1375 and various annexes are available from the U.K. Department of Trade & Industry, or from Mr. Craig Hall, Northern Telecom Inc., (615) 734-4000.

2. An Annex specifying enhancements to the CT2 CAIS.

   CT2 CAIS is an open standard. It deliberately leaves sections of the message space undefined in order to accommodate future expansion of services and facilities. CT2 already provides for the addition of data and security features. The Annex defines a standard implementation of these features.

---

[1] MPT 1375, "Common Air Interface Specification", Department of Trade & Industry, Radiocommunications Division, London SE1 8UA.

**Classes of Equipment**

There shall be two classes of equipment:

i ) Equipment meeting the provisions of the CT2 CAIS, operating in the PCS spectrum allocation.

ii ) Equipment meeting the provisions of both the CT2 CAIS and the annex of enhancements specified in this document. Equipment in this class, both base stations and terminals, shall be capable of interworking with equipment in class (i) above.

The remainder of this document is a draft of the annex which specifies the enhancements to the CT2 CAIS.

**Annex: Enhancements to CT2 CAIS**

Where applicable, reference to the relevant clause(s) of the CT2 CAIS have been provided. Acronyms are as defined in the CAIS.

## 1. Operating frequencies

The channel carrier center frequencies shall be:

$$(f_l - 0.05) + (0.05 \times n) \text{ MHz}$$

where n is the channel index,
and $f_l$ is the lower frequency band edge.

The same carrier frequency shall be used for transmission in both directions between fixed and portable stations.

The lower frequency band edge, $f_l$, is 900 MHz. The lowest channel index, n, is 1. The largest channel index is 1200. This provides for channel center frequency assignments in the range from 900 MHz to 959.95 MHz. Not all channel indices are allowed.

The PCS exclusive bands are defined by channel indices as follows :

| | | |
|---|---|---|
| 930-931 MHz | n = | 603,605,607,609,611,613,615,617,619. |
| 940-941 MHz | n = | 803,805,807,809,811,813,815,817,819. |

Within the index ranges 603-619 and 803-819 (inclusive) only odd numbers may be used.

| | | |
|---|---|---|
| 902-928 MHz | (ISM band) | n=43 to 559 |

Other indices, to specify a channel frequency outside the PCS exclusive bands, may only be used subject to constraints of sharing with other local users of the bands.
Within the index range 882-1040 only even numbers may be used.

Channels 603 and 803 are reserved for use for the common signalling channels. Channels 882, 884, 1038, and 1040 are also designated for common signalling channels where sharing conditions permit. Further signalling channels may be designated if required.

## 2. Common Signalling Channels

This section defines the structure of the common signalling channels (CSCs) and their usage. The purpose of adding CSCs to the CT2 CAIS is to provide the following improvements: call set-up to the base station with the strongest signal, thereby extending capacity and performance; faster call set-up, and decreased scan-time requirement at the portable stations, thereby extending standby battery life and facilitating the delivery of value-added services. Where equipment is intended to make use of the CSCs, the manufacturer shall make a declaration to this effect. Where such a declaration has been made, the equipment shall conform to the requirements of this section. The transmitters and receivers using the CSCs shall meet the RF performance requirements of the CAIS.

### 2.1 Common Signalling Channel Frequencies

Channels 603 and 803 are reserved for use as common signalling channels. Channels 882, 884, 1038, and 1040 are also designated as common signalling channels where sharing conditions permit. Further signalling channels may be designated if required.

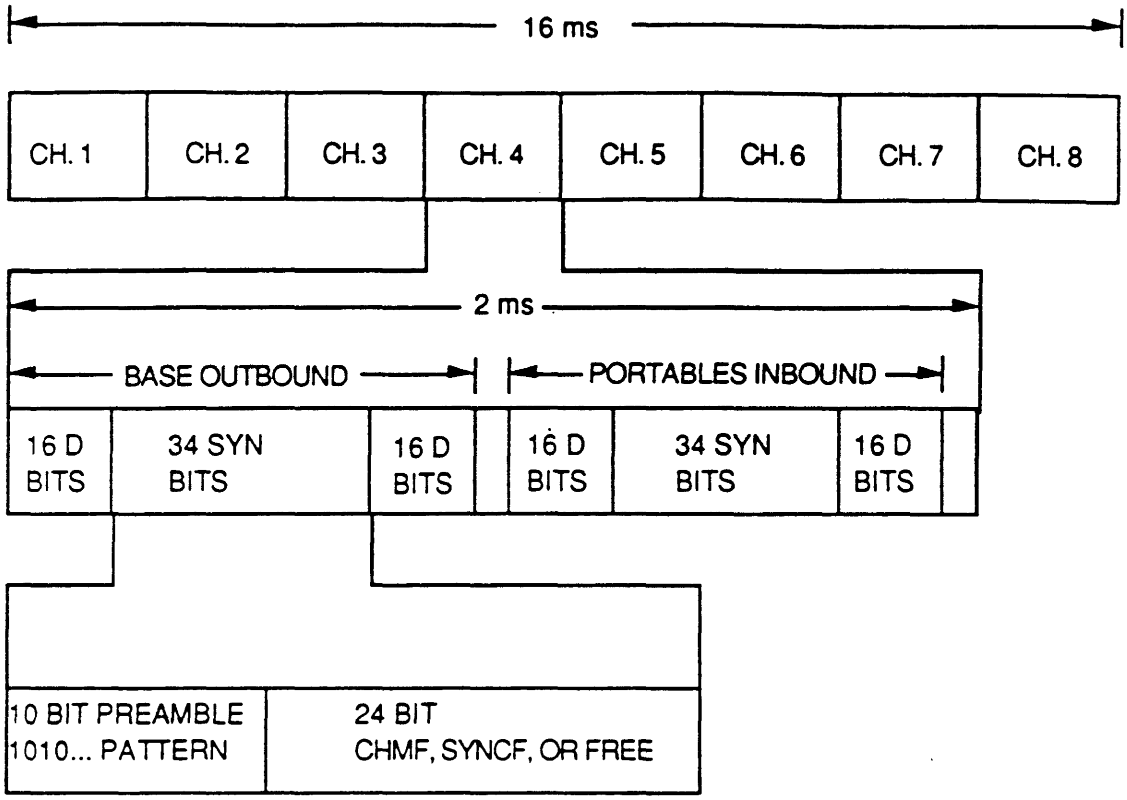
These signalling channels operate at frequencies as follows :

| Channel | Frequency (MHz) |
|---|---|
| 603 | 930.1 |
| 803 | 940.1 |
| 882 | 944.05 |
| 884 | 944.15 |
| 1038 | 951.85 |
| 1040 | 951.95 |

### 2.2 Multiplex Structure of the Common Signalling Channels

Each of the carriers reserved for CSC use supports eight CSCs in TDMA mode. Figure 2.1 shows the frame structure used to multiplex eight CSCs onto a given carrier. This frame structure shall be known as MUX4. The transmission rate and modulation technique shall be those specified in the CAIS, namely, 72 kb/s Gaussian-shaped FSK with peak deviation between 14.4 and 25.2 kHz under all possible data patterns. The RF envelope ramp up and ramp down profiles shall meet the requirements of the CAIS, part 1, figure 1.2. The burst structure of MUX4, shown in Figure 2.2, is identical to that of the MUX2 format of the CAIS (see CAI, part 2, figure 2.3). A burst is 66 bits long. Each inbound (CPP to CFP) burst follows 5.5 bit periods after the end of the outbound burst. The CPP synchronizes its timing to the CFP. Like MUX2, MUX4 contains two sub-multiplexes: the SYN channel and the D-channel. The SYN channel contains words which indicate the status of the channel, and is used to gain bit and burst synchronization. The 2 kb/s D-channel is used for layer 2 and 3 messaging, as well as to indicate the status of the channel.

Figure 2.1 & 2.2 : MUX4 Frame and Burst Structure




## 2.3 Dynamic Allocation of Common Signalling Channels

A base station shall be defined as a cordless fixed part (CFP) containing a number of radio fixed parts (RFPs), which are under common control, and their associated antennae. Only one CSC may be used at a given time by a CFP, no matter how many RFPs it contains. The particular RFP within the CFP that operates on the CSC may change from time to time. Every CFP shall also support calling channel detection and link set-up establishment in regular CT2 CAI mode, on the PCS exclusive channels, as described in the CAIS, part 2.

A CFP shall select a CSC on which to operate by the following algorithm:

i) Upon power-up or reset, the CFP shall scan all CSCs and select a free channel upon which to operate. A "scan" and a "free channel" shall be defined as in the CAIS, part 1, appendix B, section 18.3.4. Briefly, a free channel is one where the received field strength is below 40 dB relative to 1 μV/m, or failing that, the channel with the lowest field strength. Where a number of free channels exist, manufacturers shall use such selection strategies as to ensure random or uniform distribution of the CSCs in use, in accordance with the CAIS, part 1, Appendix B, section 18.3.3.

ii) A CFP may have given up its CSC because the radio supporting it was needed to service a call on a traffic channel. When a radio does become available to re-establish a CSC, the original CSC shall be scanned and if free shall be the one selected for use.

iii) If interference is encountered on the CSC in use, a CFP may drop it and re-establish on a new carrier frequency (of the ones reserved for CSCs) and/or time-slot. However, two re-establishments shall not be initiated within a time period of $T_{cscr}$ ($T_{cscr}$=10 s) of each other.

## 2.4 Multiple Access Protocol on a Given CSC

A CFP may put the CSC into four modes:

broadcast mode - broadcast information for all CPPs,
emergency broadcast mode - vital information for all CPPs,
paging mode - information for a specific CPP, and
conversation mode - a communication link established to a specific CPP.

The SYN and D channels contained in the base outbound burst shall be used to indicate the current mode.

### 2.4.1 Broadcast Mode

Broadcast mode is the normal mode during idle periods. The CFP shall set the SYN channel word to FREE. FREE is a 24 bit pattern with low autocorrelation and low cross correlation with the 24-bit words CHMF and SYNCF, defined in the CAIS, part 2, section 2.1.1. The presence of FREE in the SYN channel means that the inbound burst in the next frame may be used by any CPP. The D-channel contains the CFP identification, BID, as well as any value-added layer 3 messages that the CFP wishes to broadcast to CPPs. Layer 3 messages in broadcast mode shall be continually re-broadcast for a period of at least $T_{rb}$ ($T_{rb}$=15 s) or until there is a change in operating mode. This minimum broadcast time is to ensure that CPPs can go for reasonable periods of time without decoding the D-channel (to save power), yet will not miss any broadcast information.

Normally, a CPP registers with the base station whose CSC is received with the highest field strength. The CPP then periodically monitors that CSC (and may monitor others as well). If the CPP fails to receive broadcasts on the CSC for a period of greater than $T_{mon}$ ($T_{mon}$=5 s), then it shall attempt to register with another base station. If registration fails, the CPP shall revert to regular CT2 CAI mode.

### 2.4.2 Emergency Broadcast Mode

Emergency broadcast mode is used when the CFP has broadcast information for all CPPs in its cell and wants to force reading of the information. The CFP shall set the SYN channel word to CHMF, and the D-channel address code word shall contain a PID, to be known as ALL. ALL is a specific PID which is not used by any handset as a PID. The presence of ALL as the PID also indicates that the inbound burst may be used by any CPP. The D-channel contains any vital information that the CFP wishes to broadcast to CPPs. Layer 3 messages in emergency broadcast mode shall be continually re-broadcast for a period of at least $T_{fcyc2}$ ($T_{fcyc2}$=1.4 s) or until there is a change in operating mode. This ensures that CPPs can "sleep" for reasonable periods of time between checking the CSC, yet will not miss emergency broadcast information.

### 2.4.3 Paging Mode

Paging mode is used for call set-up from the CFP to the CPP. The CFP shall set the outbound SYN channel word to CHMF, and the D-channel address code word shall contain the PID for the CPP in question. No other portable may transmit during the inbound timeslot until the SYN channel word reverts to FREE, or the PID reverts to ALL.

### 2.4.4 Conversation Mode

The CFP puts the CSC in conversation mode after contacting a specific CPP, or in response to a link request from a CPP. The CFP shall set the SYN channel word to SYNCF, and the D-channel address code word shall contain the PID for the CPP in question. No other portable may transmit during the inbound timeslot until the SYN channel word reverts to FREE, or the PID reverts to ALL.

### 2.4.5 Multiple Access Contention Resolution

It may occasionally happen that two CPPs, seeing the CSC is free (i.e. in broadcast or emergency broadcast mode) both attempt simultaneously to begin transmitting on the same inbound timeslot. In this case a collision may occur. A CPP which fails to receive the expected CFP response to its link request shall wait a random number of MUX4 frames before again attempting to transmit on the CSC. The CPP shall ensure that the CSC is in broadcast or emergency broadcast mode before re-attempting transmission.

## 2.5 Layer 2 and 3 Message Formats

The layer 2 and 3 messages shall be formatted as described in the CAIS, parts 2 and 3. The "Link re-establish on a given channel" layer 2 message (CAIS, part 2, section 3.5.6) shall be extended to two octets in order to specify the increased number of channels in the allocation.

Subsequent sections shall refer to address code words (ACWs). These are 64-bit (two MUX4 frame) packets of information. Each ACW is preceded by a synchronization burst that contains the D-channel synch word, SYNCD, as its final 16 bits. Thus, the transmission of an ACW requires three frames, or 48 ms. The synchronization burst format and ACW formats are described in the CAIS, part 2, sections 3.3 and 3.4.

## 2.6 Uses of the Common Signalling Channels

### 2.6.1 Registration of a CPP

The CSCs facilitate roaming and higher performance by providing a means for registration of CPPs with the nearest (strongest) base station. Once a CPP has registered with a base station, incoming calls (CFP to CPP) can be set up quickly, as the CPP need only monitor that base station's CSC for paging messages.

The CPP, having scanned all CSCs, chooses a base station on which to attempt registration. This will normally be the base station whose CSC gave the highest field strength reading. The CPP waits until the CSC is in broadcast or emergency broadcast mode (see section 2.4 above) before beginning transmission.

Registration proceeds according to Figure 2.3. The CPP begins transmitting in MUX4 on the inbound time-slot with its SYN channel word set to CHMP. The D-channel ACW sent is a LINK_REQUEST containing the CPP's PID and the desired base station's BID. If a response is not received from the CFP, the CPP follows the contention resolution procedure of section 2.4.5 above.

The CFP normally responds by setting the SYN channel word to SYNCF to put the CSC in conversation mode. It sends a LINK_GRANT ACW which contains a LID for subsequent handshaking.

The CPP completes the handshake with an ID_OK ACW. It also sets its SYN channel word to SYNCF for the remainder of the registration process. Layer 3 is then initialized, and registration proceeds as it would in CT2.

If registration cannot be completed on a CSC, then the CPP shall revert to CT2 CAI operation within the PCS exclusive allocation.

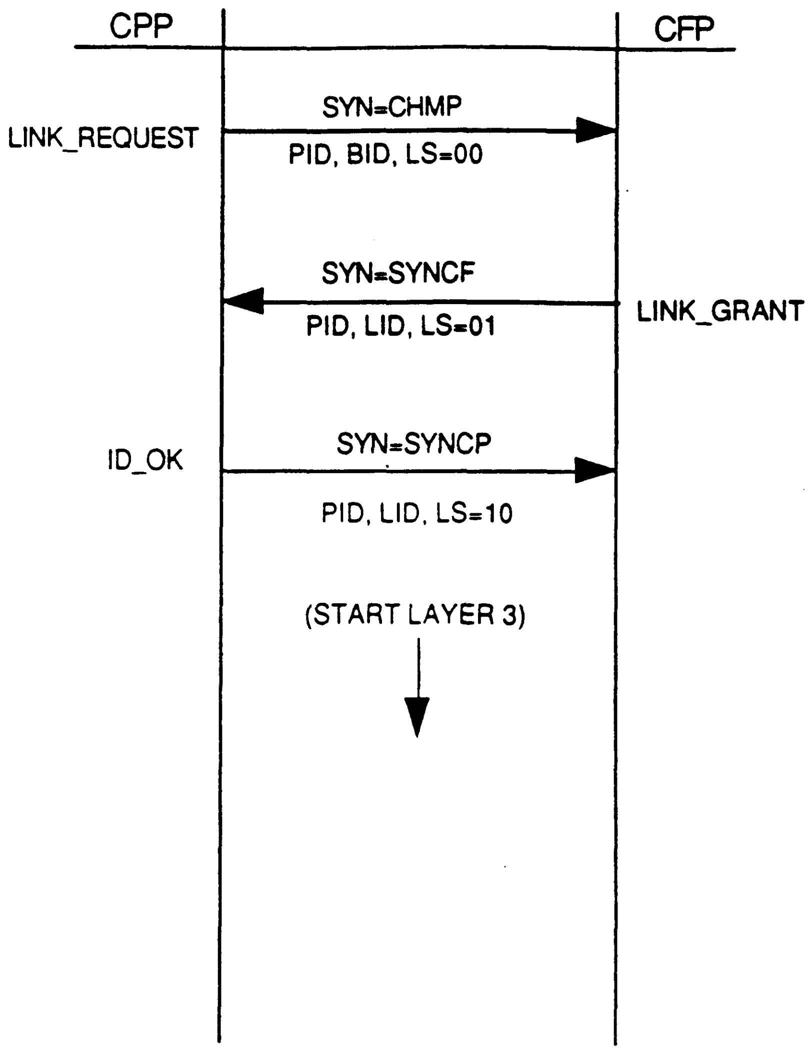



Figure 2.3 CPP Registration

2.6.2 Call Set-Up From CFP to CPP

Refer to Figure 2.4. The CFP puts the CSC in paging mode by setting the SYN channel word to CHMF and by issuing an ID_OK ACW that contains the CPP's PID and the base station's BID. This paging message (which may also be part of a multiple ringing poll) is continually re-broadcast until either the CPP responds or a timeout of $T_{fcyc2}$ ($T_{fcyc2}$=1.4s) expires. If the timeout expires, the CFP shall attempt call set-up on a traffic channel in regular CT2 mode, as described in the CAIS, part 2.

The CPP normally responds by setting its SYN channel word to SYNCP and issuing a LINK_REQUEST ACW.

The base station responds by setting its SYN channel to SYNCF and issuing a LINK_GRANT ACW that assigns a link reference LID for the call. The CSC is now in conversation mode.

The CPP echoes back this LID in an ID_OK ACW.

The CPP and CFP now agree on a traffic channel for call set-up to proceed on. The CFP always has the last word in this process, but the CPP has some choices. The CFP sends a list of candidate free channels to the CPP. The CPP checks one or more during the idle part of the MUX4 frames, and confirms its first choice back to the CPP.

Having agreed upon a traffic channel, the CFP issues a "Link Re-establish on a Given Channel" ACW (see CAIS, part 2, section 3.5.6) and switches to the agreed-upon channel. It then begins transmitting in MUX2 and sends an ID_OK ACW containing the LID for the call. If it fails to receive a reply within a timeout period of Tsu (Tsu=100 ms), it tries another free channel from the list for a further period of Tsu. This procedure may continue for up to a maximum of five free channels.

The CPP checks the agreed-upon channels, starting with the preferred choice. When it sees the ID_OK ACW from the CFP, it issues its own ID_OK ACW to complete the handshake. Layer 3 is then initialized and call set-up proceeds as in regular CT2.

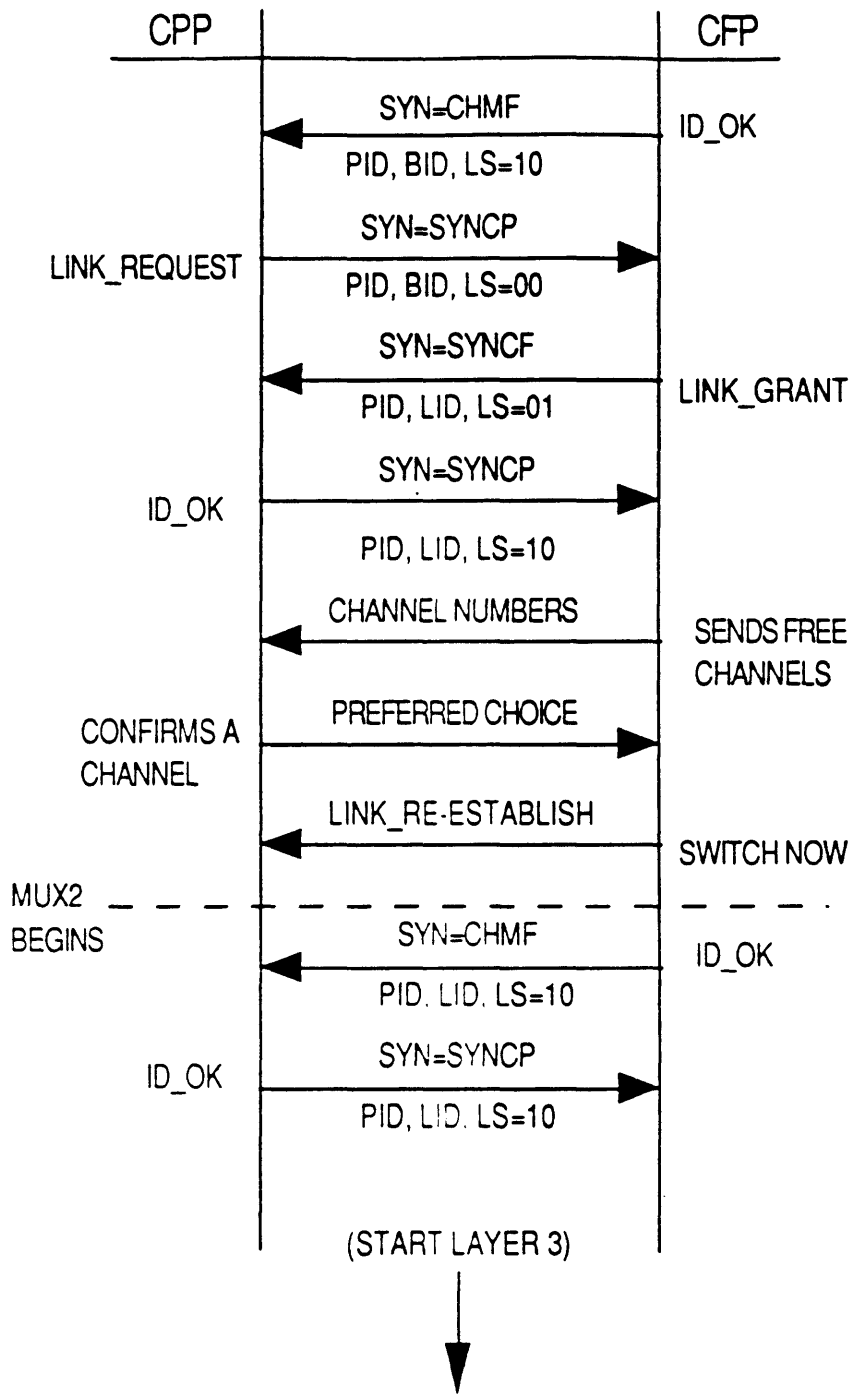



Figure 2.4 Call Set-Up From CFP

2.6.3 Call Set-Up From CPP to CFP

The call set-up procedure from CPP to CFP, shown in Figure 2.5, is identical to the CFP to CPP call set-up procedure, except that the initial CFP ID_OK paging message is absent. If call set-up cannot be completed on the CSC, then the CPP shall attempt to set-up the call on a traffic channel in regular CT2 CAI mode.

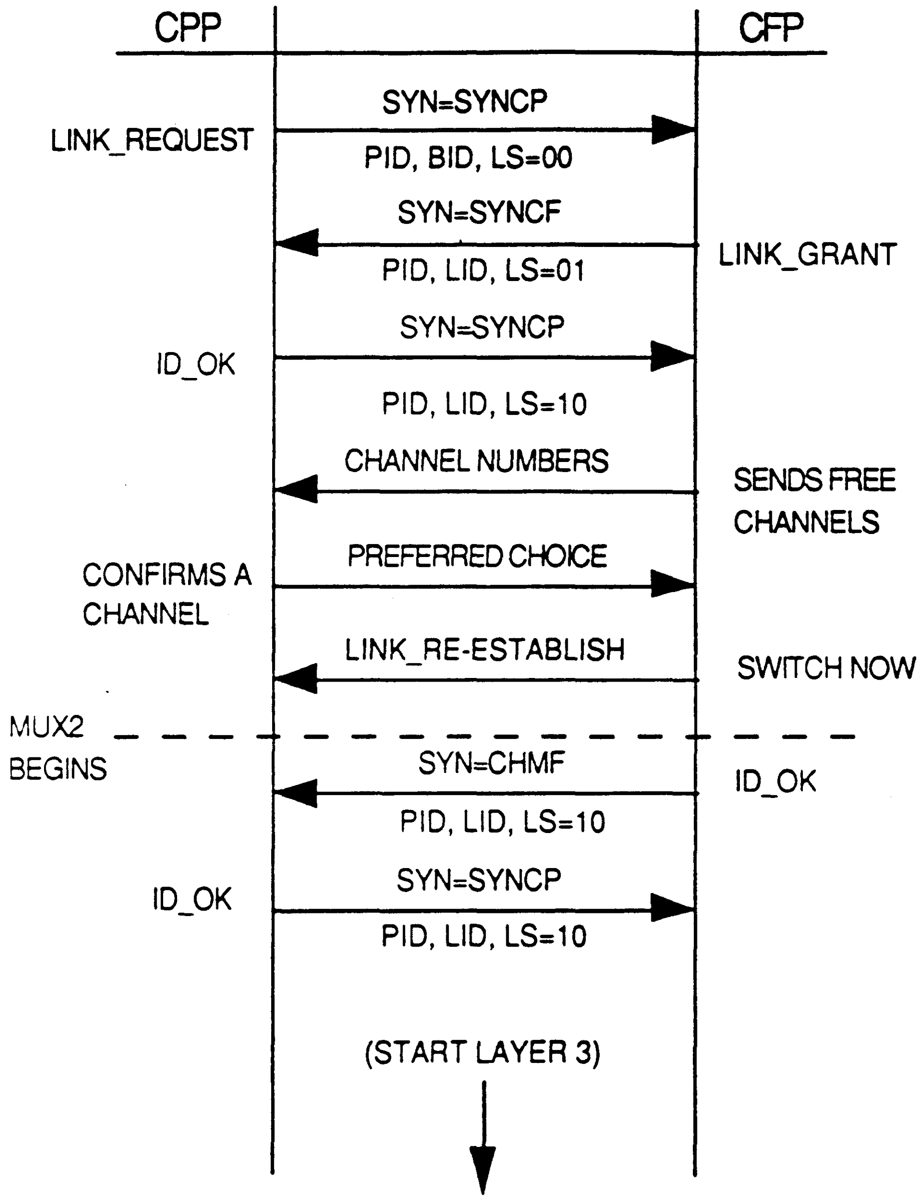



Figure 2.5 Call Set-Up From CPP

2.6.4 Value-Added Services

The CFP may send layer 3 broadcast messages to CPPs in either broadcast or emergency broadcast mode, as described in section 2.4, above.

CPPs may send layer 3 messages to the CFP, without having to establish a traffic channel, by following the registration procedure.

## 3. Hand-over

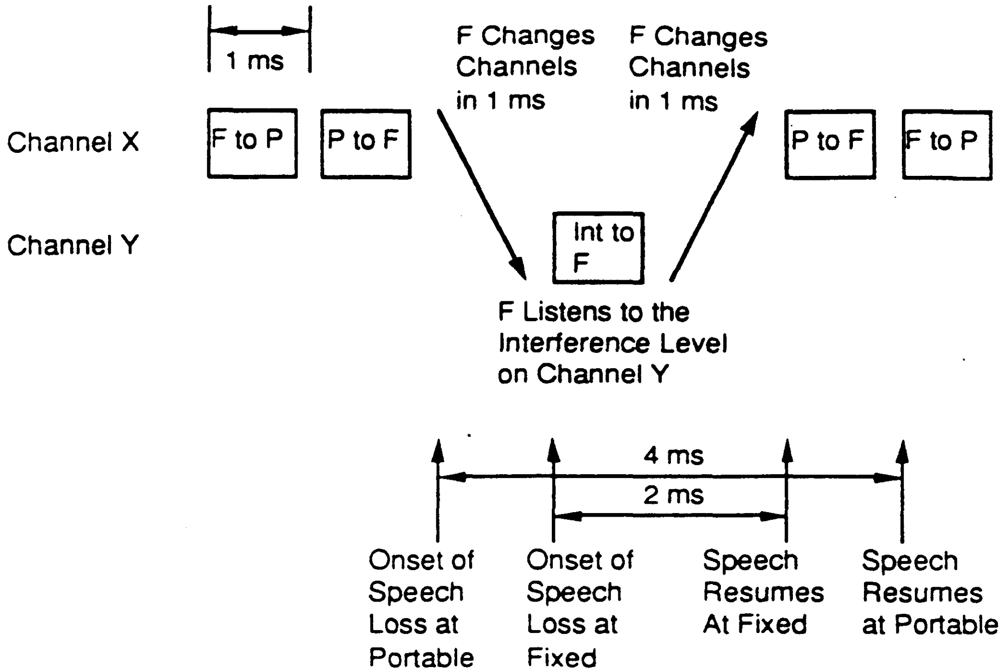
### 3.1 Link Re-establishment in the Same Base Station (Intra-cell hand-over)

This type of hand-over, i.e., to a new frequency on the same base station to avoid interference, is caused by changes in channel usage. (A base station is defined as a CFP containing a number of radio fixed parts (RFPs) and associated antennas which are under common control). Typically, the interference occurs instantaneously with no warning. For example, another call established on the same or adjacent channel in a distant cell may lead to unacceptable interference for a call in progress.

The CFP and CPP maintain a list of up to five candidate free channels to hop to if and when interference suddenly arises. This list is maintained routinely, not just when a hand-over is required. If there is an idle RFP at the base station, the idle RFP maintains the list. If there is no idle RFP available, then the RFPs servicing calls occasionally hop away from their calls to check the interference level on candidate channels, then hop back to their calls. These interruptions may be about 4 ms in duration as illustrated in Figure 3.1. (This case, however, seldom occurs. The probability that there is no idle radio at the base is approximately equal to the blocking probability, i.e. < 1 % for a business communication system.) The CFP keeps the CPP informed of the list of free channels via D-channel messages. The CPP checks one or more of the candidates and confirms to the CFP over the D channel the candidate channel with the lowest field strength from its perspective.

Link re-establishment on a different channel in the same base station may occur upon request from either end in an existing link. The CPP and/or the CFP may try to re-establish a link at any time when the received signal quality is degraded for longer than $T_{pq}$ ($T_{pq}$=40 ms). Link re-establishment is permitted only after a period of at least 300 ms from a previous link establishment or re-establisment.

Figure 3.1: **Checking for a Free Channel**




Action at the CFP:

After transmission or reception of a "Link Re-establish on a Given Channel" message (CAIS, part 2, section 3.5.6), the CFP immediately switches to the given channel and begins transmitting ID_OK in MUX2 over that channel (with CHMF in the SYN channel, PID, and the last received link reference in the LID field in the D channel). The transmission should last for a minimum of $T_{re}$ ($T_{re}$ = 100 ms) unless a response from the CPP is received. Two eventualities exist:

i) The link is re-established when the CFP accepts a MUX2 response (ID_OK) from the target CPP before the expiry of the timeout. The B-channel connection is then re-established.

ii) No recognized response is received before the expiry of the timeout. In this case a new RF channel is selected (from the list of candidate free channels) and the CFP sends ID_OK on this channel for a period of $T_{re2}$ ($T_{re2}$=50 ms). This process continues for a total of up to five free channels.

Action at the CPP:

After transmission or reception of a link re-establishment message, the CPP checks the given channel (and the list of candidate free channels) for the presence of CHMF and the appropriate IDs in the D-channel for a time not exceeding $T_{re} + 4 \cdot T_{re2}$. Two eventualities exist:

i) The CPP detects CHMF in the SYN channel and the expected ID_OK in the D channel. The CPP then responds in MUX2 with SYNCP in the SYN channel and ID_OK in the D channel, completing the handshake.

ii) No recognized response is received before the expiry of the receive time. The CPP may then rescan the Common Signalling Channels and initiate a call set-up procedure to the base station with the maximum relative received signal strength. On successful re-establishment of the radio and signalling links the call is re-routed to the appropriate base station by the CCFP.

Link re-establishment attempts must cease when the 10 s handshake timeout ($T_{hlost}$) expires.

### 3.2 Link Re-establishment to a Different Base Station (Inter-cell Hand-over)

This type of hand-over is typically caused by movement of the CPP out of a cell. The received signal strengths at the CFP and CPP gradually decrease as the CPP moves out of the coverage area of the base station.

Link re-establishment to a different base station may be initiated from either end in an existing link.

Action at the Origination CFP/Destination CFP:

The origination CFP alerts the CCFP of the possible need of a hand-over to a different base station. Adjacent base stations are instructed to monitor and report on the quality of the received signal from the CPP. The base stations also identify one or more free channels up to a maximum of five. The CCFP selects the best base station (i.e., the destination CFP) and free channels and reports this information to the origination CFP.

The origination CFP issues a D-channel message (Monitor Channel(s)) to the CPP to check a list of candidate free channels. The CPP responds on the D-channel with its preferred free channel. The destination CFP is sent this channel number and commences transmitting (and receiving) in MUX2 over this channel (with CHMF in the SYN channel, PID and the last received link reference in the LID field in the D channel). On receipt of a signal indicating that the destination CFP has begun transmitting in MUX2, the origination CFP issues a D channel link re-establishment message (Link Re-establish on a Given Channel To a Different Base Station) and sends a signal to the destination CFP indicating that the hand-over has begun. The destination CFP continues to transmit in MUX2 after receipt of this signal for a period of at least $T_{re}$. The origination CFP continues to operate on its original frequency but switches to transmitting (and receiving) in MUX2 (with CHMF in the SYN channel, PID and the last received link reference in the LID field in the D channel) when the link re-establish message is acknowledged. Speech is muted. Three eventualities exist:

i) The destination CFP accepts an ID_OK ACW from the CPP. The link is re-established on the destination CFP. The CCFP signals the origination CFP to release the link.

ii) No recognized response is received before the expiry of the timeout. In this case the destination CFP selects a new RF channel (from the list of candidate free channels) and the CFP sends ID_OK on this channel for a period of $T_{re2}$ ($T_{re2}$=50 ms). This process continues for a total of up to five free channels.

iii) The origination CFP accepts a MUX2 response with the correct ID code from the target CPP. The B-channel connection is then re-established. (The hand-over to the destination CFP failed.)

Action at the CPP:

After reception of the message to check for free channels, the CPP transmits its preferred free channel to the origination CFP. Normally, this will be the channel having the lowest field strength as measured by the CPP. The CPP may need to briefly hop to candidate channels to evaluate their field strengths, interrupting the call. After reception of a link re-establishment message, the CPP checks the given channel (and the list of free channels) for the presence of CHMF and the appropriate IDs in the D-channel for a period of up to $T_{re} + 4 \cdot T_{re2}$.

Three eventualities exist:

i) The CPP detects CHMF in the SYN channel and a matching PID and LID in the D channel. The CPP then responds with MUX2 with SYNCP in the SYN channel and PID and LID in the D channel. The B-channel connection is re-established.

ii) No recognized response is received before the expiry of the receive time. The CPP then attempts to re-establish the connection with the origination CFP and checks the original channel for the presence of CHMF and the appropriate IDs in the D-channel for a period of up to $T_{re}$.

iii) No recognized response is received before the expiry of the receive time. The CPP may then rescan the Common Signalling Channels and initiate the call set-up procedure to the base station with the maximum relative received signal strength. The call is re-routed to the appropriate base station by the CCFP.

Link re-establishment attempts must cease when the 10 s handshake timeout ($T_{hlost}$) expires.