Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db338

Title	**Confessions of a Phone Phreak**
Publication	*Undercurrents*
Date	1974-09-00
V/I/P	No. 7, p. 15
Abstract	Overview of phone phreaking from a British perspective.
Keywords	British phreaking; British Post Office (BPO); subscriber toll dialing (STD); AC9 signaling system; blue box; international subscriber dialing (ISD); ACI signaling system
Notes	Issue 7 was Sept./Oct. 1974. This is a reprint of "Phone Phreaking" by Mike Brookfield published in "Interface", April 1974.
See also	db340
Source	Alan Rubinstein

CONFESSIONS OF A PHONE PHREAK

TELEPHONES are interesting, and fun to play with. People whose hobby is playing with telephones are known as 'phone phreaks' in the USA, a term which is not very popular in this country. The polite term 'telephone enthusiast' is sometimes used instead.

Anyone interested in amateur radio can go to his local library and find a shelf of books telling him how to annoy his neighbours by interfering with their television pictures. Unlike such normal hobbies it is not so easy to find information on the subject of 'phone phreaking'. When I first became interested in telephones I was more or less on my own and I spent a lot of time trying to find other telephone enthusiasts. This was an interesting exercise, full of odd surprises. On one occasion I spent a lot of time tracking down rumours of one individual who turned out to be no other than myself. Some people get interested in telephones simply by meeting established 'phone phreaks. I feel that one misses something by this.

To understand what 'phone phreaking is all about one needs to know a little about telephone systems.

The British Telephone System

Telephone exchanges in the UK are arranged in a hierarchical structure based on about 40 zones switching centres, 350 group switching centres and about 6,000 minor exchanges. Each group switching centre (GSC) is a member of a zone and its zone switching centre is its primary route to the trunk network. Similarly, each of the minor exchanges has a GSC as its parent.

In addition to this basic structure there are further circuits, GSC to GSC, minor to minor exchange and so on, provided that there is a sufficient demand to justify them.

Until the introduction of Subscriber Trunk Dialling (STD) in 1959, telephone operators handled all trunk traffic. By *this time* most of the network was automatic in the sense that one originating operator could complete a call by dialling, over the trunk network, codes which routed the call from one centre to another.

Following the introduction of STD, the responsibility for the setting up of the call was placed upon the subscriber. Now the most costly part of a telephone system is the provision and maintenance of circuits between exchanges and this dictates the philosophy behind the working of the system.

The STD equipment dials calls over the trunk network automatically and in this way replaces the local operator. The equipment is full of safeguards which ensure that, either by accident or misuse, a subscriber does not waste time on trunk circuits. For example, a subscriber cannot let a call ring indefinitely: he will be automatically disconnected after about 3 or 4 minutes.

Most of the automatic switching equipment in the UK is based upon the older type of electromechanical switching known as the Strowger (or step by step) system. This type of equipment responds directly to the impulses set up as one dials. As a result, there is a very close relationship between the codes dialled and the way in which the call is routed.

If one looks at the dialling code booklet issued to subscribers one will find that it is divided into two parts. The first gives dialling codes for 'local' calls and the main part of the booklet gives the dialling codes for 'local' calls and the main part of the booklet gives the dialling codes for trunk calls.

The local codes operate Strowger switching equipment. If one studies the local dialling codes published for a few neighbouring exchanges it is possible to break them down into their component routings. It is then possible to string them together to reach distances of up to about 70 miles. It is through discovering this that many people, myself included, first became interested in telephones. This stringing together of local codes is known as 'chaining' and is of restricted interest since the lines are unamplified and of low quality.

The STD codes consist of the digit zero followed by a three digit 'area code' and, in the case of minor exchanges, further routing digits. The initial zero connects a subscriber to the STD routing equipment. The next three digits bear no relation to the routing digits actually needed to set up the call and are the same all over the country. They were allocated as a mnemonic in the days when telephone dials had letters on them.

The heart of the STD equipment is a *register translator* (RT). This splits off the area code and translates it into the appropriate routing digits, indeed the same ones that an operator would dial. Meanwhile the remaining dialled digits are stored in a register. The equipment first pulses out the routing digits got from the translator and follows them with the digits stored in the register, these being the final routing digits (for minor exchanges) and the called number. Having done this the equipment switches through the speech path and the register translator releases itself in preparation for the next call, leaving control to a piece of equipment called a register access relay set. This piece of control equipment has obtained the appropriate metering rate for the call from the translator, and when the call is answered it steps the subscriber's meter at this rate.

Trunk Access

Theoretically, the only way that a subscriber has of obtaining a trunk circuit is either via the local operator or through the STD equipment. Neither of these two methods allow one to explore the telephone network, which is what the 'phone phreak wants to do. In practice there are other ways of gaining access to the trunk network. For a variety of reasons there are ways of dialling from the local codes, to which a subscriber has proper access, onto trunk routes. One way in which this can happen is that occasionally a local route can terminate at a GSC with the same status as an incoming trunk route. When this happens one may dial the appropriate local code followed by the digit '1' and gain access to the trunk circuits at the distant GSC.

Another type of trunk access arises when Post Office engineers within an exchange wire up their own irregular circuits. One of these came to light last year in Bristol as a result of a Post Office prosecution. One dialled 173 and received a continuous 'number unobtainable' tone (as one should, it is a spare code). However, if one waited for 30 seconds, this would switch through to Bristol trunks. One person who was prosecuted was apparently running an air charter company and making all his telephone calls abroad free of charge.

A more common type of concealment occurs when, instead of waiting as above, one has to dial a further code, most commonly a digit zero. If more than one such digit is required then the access becomes difficult to find.

In spite of such attempts at concealment a large list of these was compiled. To explore the trunk network using one of these one would use the 'chaining' method to the nearest exchange providing such a trunk access. If one was lucky, one's own exchange would possess one.

As a result of recent publicity the Post Office has tightened up on its own internal security and now only relatively few of these accesses are left. Fortunately, there is a more powerful way of gaining access to trunks and this involves simulating the control signals that are used on trunk routes. To explain how this can be done it is necessary to describe first the principles of telephone signalling.

Telephone Signalling Systems

Dial pulses, which originate at the subscriber telephone on dialling, periodically interrupt the DC path between the telephone and the exchange. This is known as *loop disconnect* signalling and is also used over local links between exchanges. It is not suitable for signalling over longer links because the pulses get distorted, or over microwave links where there is no DC path. Over the majority of trunk routes a type of signalling known as *AC9* is used. This employs a single signalling frequency of 2280 Hz which is within the audio pass band of the circuit. Digits are transmitted as impulses of this frequency sent at dial pulse speed (10 pulses per second). Control signals are also at 2280Hz. For example, on completion of a call a continuous tone at this frequency is sent to clear down the circuit.

The STD system as so far described is inadequate in many ways. It is capable of providing only relatively simple translations and this is why subscribers who have STD cannot dial all of the exchanges on the automatic trunk network. Further, if congestion is met on any of the links within a routing then the call will fail whereas an operator would either redial or try an alternative routing. It was decided from the outset that it would be uneconomical to extend the planned STD system to cope with these problems and so a different approach known as *transit working* was planned. Accordingly, a completely independent trunk network is being built and is now gradually coming into operation. This is known as the *trunk transit network*.

In the transit mode the area code is examined by the originating RT as before, but instead of producing a complete set of routing digits it simply seizes the first free circuit to the most likely switching centre capable of handling that call. If there are no free circuits then it tries its next choice of switching centre.

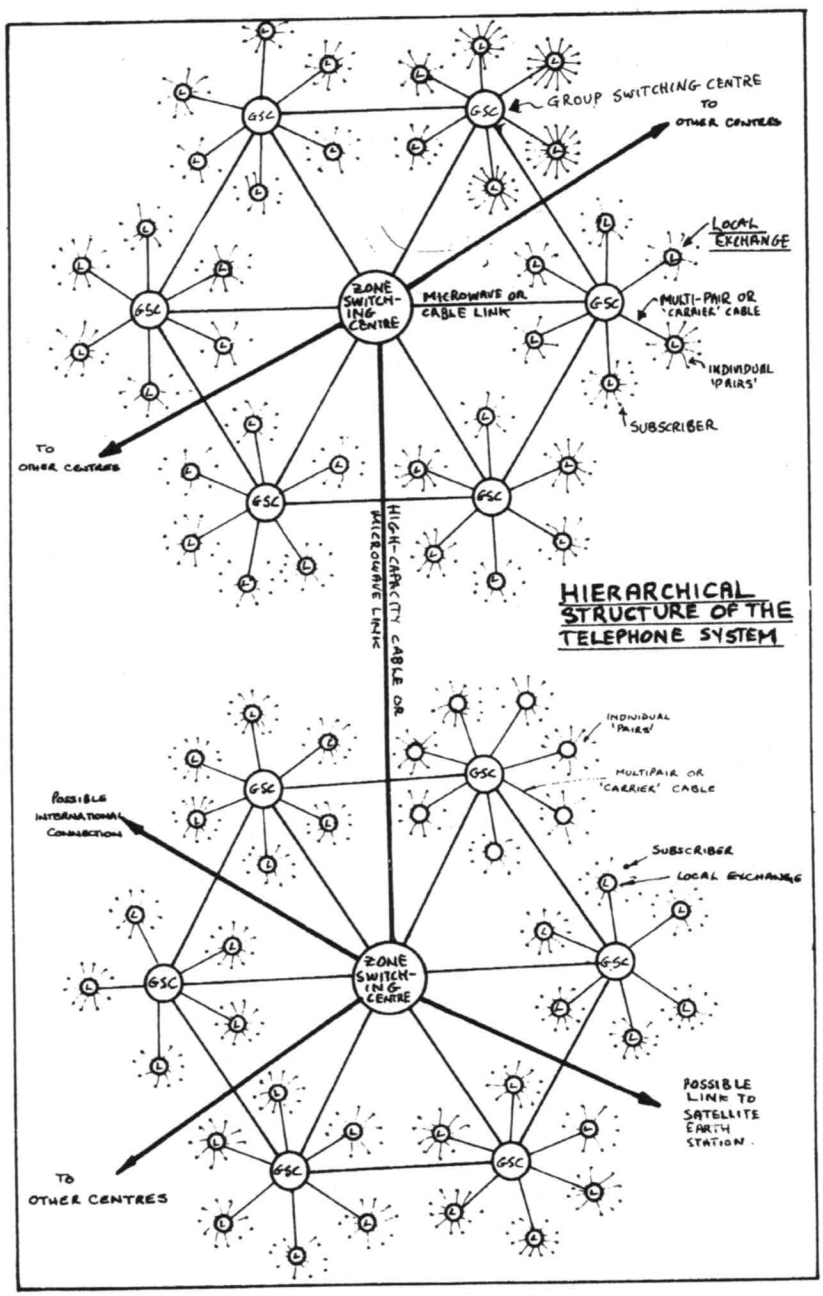
This distant switching centre then requests the original area code and upon receipt of this from the originating RT it will set up the next link in the same way. The intermediate RT is then released and plays no further part in the connection of the call. This process continues until the call reaches its required destination whereupon the distant RT sends back a signal to initiate the transfer of the contents of the originating register to the final register and the call is then established as before.

The area code has to be repeated by the originating RT to each of the intermediate switching centres and a slow signalling system such as AC9 is unsuitable. A high speed signalling system is therefore used and is known as SSMF2. This uses a combination of two frequencies out of a total of six to represent digits.

With SSMF2, a digit may be sent in 160 milliseconds, compared to a maximum of 1 second when using AC9. Signals in the backward direction are needed, for example to request the area code, and these are based on a further six frequencies. Supervisory signals are again at 2280Hz in most cases, these including the *forward clear* for example.

The Blue Box

It has been seen that the control signals employed within the inland trunk network are audio signals within the passband of the telephone circuit. Armed therefore with a set of audio oscillators and some means of playing combinations of these into one's telephone one can imitate these signals. A device capable of doing this is known as a 'blue box' in the USA and as a 'bleeper' in this



country. With such a device the entire telephone system of the world is then at your command.

To imitate signalling system AC9 all that one needs is a single oscillator running at 2280Hz and a method of interrupting this at dial pulse speed. A second telephone dial is a simple and convenient method. In practice one would start by dialling an ordinary STD call and then, before the call is answered, send a short burst of tone. This 'clears down' the call and one is left with an outgoing trunk route. This first link is not released because the telephone is still 'off the hook' and the DC holding conditions are still applied at the local GSC. A second burst of tone will then 're-seize' in the sense that the switching equipment is reconnected at the distant GSC in preparation for the receipt of routing digits. These are sent using the auxilliary telephone dial just as if one was an operator or was using a trunk access.

Simulation of the MF2 signals requires, of course, six oscillators and the procedure is more complicated. However, one does not need to know any internal trunk routing digits.

Once one has unrestricted access to the trunk network in this way it is possible to gain access to the international circuits as well. Over these circuits different signalling systems are employed and these too are normally 'in-band' systems, in that they use tones with frequencies within the normal voice band of 300 to 3000 Hz. More sophisticated 'blue boxes' allow one to simulate these as well and one can go even further and simulate the signalling used internally in other countries. This is the subject of Part II of this article.

Having acquired a 'blue box', the way one explores the network is very much a question of personal taste and people tend to specialise—as in any hobby. To start with, most 'blue box' owners just play around and enjoy the novelty of having the world at their fingertips. Calls to various information services are popular as are calls to international operators, who are very friendly. It is a pleasant diversion on a winter evening to discuss surfing with the Honolulu operator or to chat about the weather with the Sydney operator.

One type of circuit that is quite popular is the *conference call* whereby a number of enthusiasts are connected together: here the conversation often tends towards 'phone phreaking. This type of circuit arises either by accident or by design. One example of the 'accidental conference' was Derry. One of its dependent exchanges got demolished by a bomb and all circuits from Derry to this exchange were connected together onto a recorded announcement. This recorded announcement became disconnected and a conference was born. Conferences also occur on an international scale and are very popular in America, where they are sometimes very sophisticated.

So far nothing has been said about the legality (or otherwise) of 'phone phreaking. Using a blue box one can make a 'phone call to virtually anywhere in the world at the cost of a local call or even free of charge. To make a 'phone call to somebody in this way is clearly fraudulent and if caught you would face prosecution. On the other hand, to use a 'blue box' for the purpose of exploring or studying the telephone system the situation is by no means so clear. When using an AC9 simulator, the very first forward clear causes the equipment to start metering the call and it does so, at the rate appropriate to the initial STD call, for as long as the telephone is off the hook. This occurs because the equipment mistakes the forward clear for an answer signal. For this reason the initial STD call is chosen to give a low metering rate. If one now restricts one's activities to such areas as, for example, experimenting with different signalling systems then the law is very unclear on the subject. There is certainly a good argument against one's activities being illegal.

It is so easy to make STD or international calls free of charge, even with no electronic aids, that anyone wishing to do so would certainly not use a 'blue box'. In this country at least, the 'blue box' user is generally a telephone enthusiast and fairly harmless.

The world is but a Blue Box away

This part of the article describes the extension of the art of phone phreaking from a national to an international scale. As already mentioned, once one has unrestricted access to trunk routes then one may also gain access to international routes. The way in which one can achieve this varies between countries.

In large countries possessing an advanced telephone system such as Australia or the USA, there are centres from which operators can originate international calls. Today, most of the world's telephone network is automatic—which means that these originating operators can complete their international calls without the assistance of an operator in the distant country. The automatic switching equipment giving access to international circuits is located at centres known as Gateway Exchanges, and operator-originated international traffic is first of all routed over a country's internal network to these gateway exchanges. Since the internal network therefore, carries both national and international traffic, it is easy to see that with the unrestricted access to this network provided by a *Blue Box*, the telephone enthusiast can himself route calls via Gateway Exchanges (provided of course, that he knows the appropriate routing codes).

In *this* country, however, the situation is different. Until quite recently the only international operators were those located at the gateway exchange itself—that is, at London's Faraday House—and subscribers were connected to these operators by the local operator in their own exchange or Group Switching Centre. There were no 'shared traffic' routes terminating at the automatic equipment in the Gateway exchange, as in the USA. It was therefore impossible for the telephone enthusiast to gain access to international routes until 1963, when subscribers were themselves allowed to dial international calls. And as a result, such access requires a knowledge of the workings of *International Subscriber Dialling*.

International Subscriber Dialling

International Subscriber Dialling (ISD) is the logical extension of STD. It enables subscribers to dial their own international calls and was first introduced in this country in 1963, between London and Paris. Other areas of Europe soon became available and later still, North America. The service was also made available to other areas within the UK.

One major problem associated with the introduction of ISD was not a technical one but concerned the agreements which had to be made between different countries regarding the charging of calls.

ISD works as follows. By international agreements, every country is allocated a 'country code' (CC) examples being France (33), the UK (44), Israel (972) and the USA (1). In the UK a standard area code (10) is allocated to ISD and the call is handled by the register-translators (RT's) at the subscriber's local exchange, in much the same way as for an ordinary STD call, the subscriber dialling an initial digit 0 to gain access to this equipment. The complete ISD dialling code is then the prefix 010 followed by the country code and then the area code within the distant country.

Upon receipt of the ISD prefix, the originating RT examines the country code to check its validity and to determine the appropriate metering rate. For a valid country code, the call is then routed over the GSC trunk exchange onto direct circuits to the automatic

equipment at the London International Exchange, the originating RT being then released.

Until recently, one could dial, either over a trunk access or by AC9 simulation, the appropriate routing code which gives GSC's access to the International exchange. By by-passing the RT's in this way, the equipment did not 'screen' the country code that you sent and so you could enjoy full international operator status. One example of this was Edinburgh, where the trunk routing code 515 gave you the International RTs in London. Such direct methods are no longer available owing to considerable misuse, apparently by Post Office employees.

It is not obvious, by the way, why one would route the call via Edinburgh instead of going directly to London. The reason is that London is sufficiently large to justify the provision of special trunk exchanges to handle STD and ISD calls exclusively and the only routes onto these is via originating RTs at the local director exchanges: there is no way to bypass these or even gain access to them incoming into London.

It was Post Office policy to introduce ISD at provincial non-director areas only over the trunk transit network, so that it was not until early 1973 that the first of these (Cardiff) had ISD. Other exchanges soon followed but for the sake of illustration we shall consider Cardiff.

In September 1972 the first circuits between Cardiff and the London International Exchange appeared. By dialling Cardiff trunks and then the code 12 one received a signal intended to initialise the transfer of digits, in SSMF2 form, from the Cardiff RT to the international registers. If one's Blue Box was capable of sending SSMF2 one could respond to this signal, send whatever country code one pleased into the international registers, and again achieve international operator status. Those lucky enough to possess an SSMF2 Blue Box enjoyed the novelty of this new route to the rest of the world.

The Post Office was disconcerted at this traffic appearing as soon as the circuits were installed and very quickly (ie a year later) took steps to prevent such misuse. By the following February the Cardiff RTs had been programmed to accept ISD calls and the service became available to the public. (Coin boxes in Cardiff, incidentally, could not handle the high metering rate on calls to North America and so these were free of charge).

TELEPHONE SYSTEMS IN OTHER COUNTRIES

Once a call has been set up to another country it is possible to simulate the signalling employed over the international route and to explore the internal network of the distant country.

The two most important signalling systems used over international circuits are known as CCITT4 and CCITT5.

In the signalling system CCITT4 digits are sent as four-bit binary numbers using two frequencies, 2400 H3 and 2040 H3, to represent 0 and 1 respectively. The control signals also use these frequencies. Digits are sent in response to signals received from the distant equipment, and the transit method of working is generally employed between different countries. (The principles of the transit-working have been described in the first part of this article, as they apply to the internal trunk network in the UK). This signalling system is unsuitable for use over satellite circuits since these introduce a return signal path of about 100,000 miles in length—corresponding to a time delay of some 600 milliseconds. In a 'compelled' signalling system such as CCITT4 this delay is added to the sending time of each digit which makes the overall setting-up time for a call for too high, bearing in mind the need for efficient use of expensive satellite circuits. CCITT4 finds its main application over shorter international routes, the main areas being Europe, South America and Africa.

Over intercontinental and satellite circuits the system CCITT5 is normally used. This is a high speed signalling system. Digits are sent in multifrequency (MF) form similar to the SSMF2 system already described but using different frequencies. The CCITT5 frequencies are the same as those used by the American Telephone and Telegraph Company (AT & T) for the North American internal signalling system, which is very convenient for the Blue Box user. The two signalling systems differ only in the supervisory or control signals.

The simulation of CCITT4 was of great interest to the telephone enthusiast in the early days of ISD when the international RT's handing ISD traffic had access only to those countries to which ISD was allowed. For example, Russia was first reached in this way; a call to Switzerland (which was allowed) was made and then extended to Moscow via the Warsaw transit.

Since then, the equipment known as International Common Access (ICA) over which international operators connect calls, has become available for ISD traffic and most countries are now directly available to the enthusiast by the methods described above. With the availability of ICA interest in CCITT4 simulation has diminished.

Simulation of CCITT5 is simpler than for CCITT4 since one does not have to respond to backward signals and the procedure is simpler. Furthermore, with the addition of a single frequency, 2600 Hz, the simulator can be used within North America. If one is actually in North America then the procedure is indeed very simple and it requires very little effort to make calls free of charge to almost anywhere in the world. This accounts for the tremendous popularity of Blue Box in that continent, the vast majority being primarily interested in saving money on telephone bills. There are only a handful of enthusiasts interested in telephones for their own sake.

It is possible to simulate the North American signalling system from the UK. The procedure is best described by means of an example. Suppose you felt inclined to telephone an adjacent 'phone box via America you would proceed as follows. First set up a call to, say, the Philadelphia weather forecast. Having done this you would send a short burst of 2600 Hz. This is a 'tone on idle' supervisory frequency—that is, the application of this tone will 'clear down' the US internal circuit and its removal will reseize a circuit, the international circuit from the UK to the USA being unaffected. Next you would send (in MF form) the following digits—KP212—183ST. The signals KP (Key Pulse) and ST (Start) are MF signals which must enclose blocks of digits sent. This will connect you to area 212 (New York) and to the 'overseas sender' in that Gateway, the code 183 being its internal access code. When this equipment is ready to receive digits it returns a continuous tone whereupon you send KP0441 838 7062 ST . The initial zero is a dummy digit, 44 is the country code for the UK, 1 is the area code for London and this is followed, in this example, by the required London number.

I find the Australian telephone system much more interesting than the American. There are two independent trunk networks. Down Under—the MFC (multifrequency compelled), and the 2VF (two voice frequency), handling STD and operator-originated traffic respectively.

As far as I know, nobody outside of Australia has managed to simulate the MFC signalling, the difficulty being that the control signals are 'outband' (sent outside the normal 3000 Hz voice frequency band). But provided that one is incoming into Australia with operator status one can gain access to the 2VF network at centres such as Melbourne or Brisbane. This assumes that one knows the appropriate access codes. The 2VF network employs the AC1 signalling system, which uses two signalling frequencies: 600 Hz and 750 Hz. Digits are sent in a similar way to AC9 signals but use the 600 Hz frequency. The supervisory signals are

different, the forward clear for example, consistency of the 750 Hz tone applied for 2 seconds followed by 0.7 seconds of the 600 Hz tone. This signalling system preceded AC9 in this country and is still used to some extent. One can sometimes hear its very characteristic 'forward clear' tone over UK trunk routes when crosstalk occurs between channels using AC1.

Australia has one Gateway exchange, located in Sydney, and a second coming into operation shortly. Modern Crossbar switching is employed at the Gateway, and this has the facility of restricting the access to the outgoing circuits in the transit mode to the appropriate incoming routes. This means, for

instance, that if you were incoming from London, the country code 44 for the UK would not be accepted, because the equipment can recognise that calls from one part of the UK to another are not normally routed via Sydney, even though a telephone enthusiast might consider it a reasonable thing to do. In practice, transit access from Sydney to New Zealand, Hong Kong and Malaga is all that is allowed to UK traffic—which is of restricted interest to the UK telephone enthusiast since these countries are available directly via the International Common Access System.

From the enthusiasts point of view it is therefore fortunate that there is a way of gaining unrestricted access to the international exchange and this works as follows. Operators in certain large exchanges, such as Adelaide, can dial their own international calls, rather than having to rely upon the international operators in Sydney. This traffic is routed over the 2VF network and, as has been mentioned above, it is possible to gain access to this network incoming into Australia. This makes it possible to set up a telephone call all the way round the world.

Firstly, set-up a call to Adelaide via New York (or some other US Gateway) and then send the 2VF access code and the 2VF routing for Sydney, all using CCITT5/USA signalling. Having allowed this connection to complete, the distant 2VF circuit will now accept AC1 signals. Using the pulsed 600 Hz signalling for the digits, one next sends the digits 99 1 44 2 1.838 7603 followed by a short burst of tone at 750 Hz to indicate end of signalling. The digits 99 are the access code for the Gateway exchange, the digit 1 is used for discrimination purposes and the country code 44 is for the UK. The next digit, 2, is known as a language digit and indicates in this case that the call is being set up by an English speaking operator. The area code for London is 1 and this is followed by the required London number. This rather cumbersome procedure follows from difficulty in interfacing an older type of signalling, AC1, with the international routing equipment. A call set up in this way will be routed, via the Indian ocean satellite, back to London This feat was first achieved in the June of 1972.

The term 'language digit' referred to above is rather a misnomer and originated in the days when most of the international circuits were operated manually. This meant that an originating international operator could not in general complete a call but would require the assistance of an operator in the distant country and the purpose of the language digit was to ensure that the call was routed to an assistance operator speaking a specified language. Today, the bulk of international traffic is switched automatically and furthermore the English language has become more or less universarlly used by international operators. A few countries such as France and Russia insist on using the French language. Spanish is used to some extent within South America but in the vast majority of cases the language digit has become redundant. Its use is however mandatory by international agreements and must be used. Many countries now have ISD and with the increase in subscriber originated traffic international agreeements have come into force that require such traffic to carry the language digit zero. This is to allow discrimination by the incoming equipment to prevent certain types of call. For exampler, a subscriber is not allowed access to an assistance operator. When ISD was first introduced to New York from London one could dial New York using the published dialling code 0101 212, followed by the New York number. But instead of dialling a New York number, one could dial a further North American area code and follow this by 1211 to reach the incoming assistance operator in that area. free of charge. This gave interesting possibilities. You could call the Montreal operator and ask for Sydney, then ask Sydney for Hong Kong..... All of this is possible to a Blue Box user but in those days it was quite novel, and required no special equipment or dialling codes. Today, discrimination by means of the language digit '0' prevents all this. This language digit is automatically inserted by the London ICA equipment when accessed via ISD routes and it follows, therefore, that traffic to, say Australia (a non-ISD country) having this language digit can only have originated from a telephone enthusiast. In an attempt to thwart such activities the Australian authorities have arranged for the incoming equipment to reject incoming traffic from London with this language digit. This can only be a temporary measure since ISD to Australia will be introduced in two or three years time. In the meantime, one can route calls via the USA or, say, Copenhagen, using methods described above. Throughout the world the various telephone administrations are making increasing efforts to prevent the activities of the telephone enthusiast and it is this, I think, that will keep the hobby alive as new areas of exploration diminish. After all it is nice to beat the system but even nicer to beat the people trying to stop you. . . ●