PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: SECURITY IN TELECOMMUNICATIONS NETWORK GATEWAYS
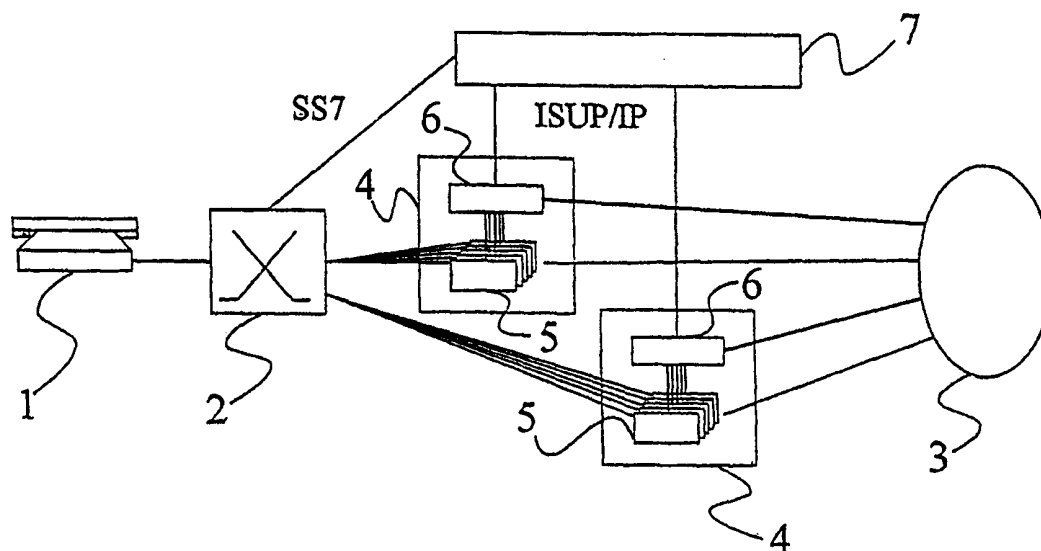
(57) Abstract

A method of transferring signalling messages between an Internet Service Provider (ISP) (4) and an exchange (2) of a telecommunications network for the purpose of allocating and controlling circuit switched communication channels between the exchange (2) and the ISP (4). The method comprising routing the signalling messages via an SS7/IP gateway which provides for conversion of messages between an SS7 protocol used in the telecommunications network and an IP based protocol used in the network which connects the SS7/IP gateway 7 to the ISP 4. For each message received at the SS7/IP gateway 7 from the ISP 4, the SS7/IP gateway 7 confirms the right of that ISP 4 to control a circuit switched communication channel identified in the message.

SECURITY IN TELECOMMUNICATIONS NETWORK GATEWAYS

Field of the Invention

4

The present invention relates to security in
telecommunications networks and in particular to a
method and apparatus for preventing one Internet Access

8   Provider from interfering with telephone circuits
allocated to another Internet Access Provider by a
common telecommunications network operator.

12 Background to the Invention

At the present time, in order to access the Internet, a
user typically has to make a connection (possibly via a

16 modem) to a local telephone exchange of a telecom
operator. The exchange then sets-up a circuit switched
connection between the user and an input device of an
Internet Service Provider (ISP) identified by a

20 telephone number (B-number) dialled by the user. In
some cases, the connection may be routed via one or more
intermediate exchanges. In either case, the telephone
network treats the connection as it would any normal

24 telephone-to-telephone connection, i.e. it is not aware
that the connection serves as an Internet access
connection.

28 The European Telecommunications Standards Institute
(ETSI) has recently established a project under the
acronym TIPHON (Telecommunications and Internet Protocol
Harmonisation Over Networks) to support the market for

32 voice communication and related voiceband communication
(e.g. facsimile) between users connected to both circuit
switched networks and IP based networks. As part of
TIPHON, it has been proposed to more closely integrate

36 the ISPs into the telecommunications networks and in
particular to provide for the exchange of signalling

information between ISPs and the exchanges of telecommunications networks, for the purpose of setting up and managing the circuit switched connections between exchanges and the input devices of the ISPs.

The current TIPHON proposal provides for a signalling gateway which acts as the interface between the signalling network of the telecom operator and the ISP. It is expected that the signalling network of the telecom operator will typically be a Signalling System No.7 (SS7) network which carries messages of the ISDN User Part (ISUP) protocol, whilst communications between the signalling gateway and the ISP are expected to be carried over an IP network. One of the roles of the signalling gateway is therefore to seamlessly relay ISUP messages from the Time Division Multiple Access (TDMA) SS7 network to the ISP over the packet switched IP network, and *vice versa*. The signalling gateway is generally referred to as an SS7/IP gateway.

It is likely that the SS7/IP gateways will be under the control of the telecom network operator, and that a single gateway may provide a signalling interface to the telecom network for a plurality of independently operated ISPs.

Summary of the Present Invention

The inventors of the present invention have discovered that under the current TIPHON proposals it is possible for an ISP connected to an SS7/IP gateway to interfere with the control of another ISP, and in particular with circuits allocated to that other ISP, connected to the same SS7/IP gateway.

It is therefore an object of the present invention to overcome or at least mitigate this problem of fraudulent (or accidental) cross-ISP interference.

This and other objects are achieved by including functionality in the SS7/IP gateway for authenticating signalling messages received from ISPs connected thereto on the basis of the message content and the origins of the messages.

According to a first aspect of the present invention there is provided a method of transferring signalling messages between an Internet Service Provider (ISP) and an exchange of a telecommunications network for the purpose of allocating and controlling circuit switched communication channels between the exchange and the ISP, the method comprising:

routing said signalling messages via a signalling gateway which provides for conversion of messages between a first transmission protocol used in the telecommunications network and a second transmission protocol used in the network which connects the signalling gateway to the ISP; and

for each message received at the signalling gateway from the ISP, confirming the right of that ISP to control a circuit switched communication channel identified in the message.

By authenticating signalling messages received at the signalling gateway from the ISP, the signalling gateway is able to prevent fraudulent messages from being passed from the ISP to the exchange which might otherwise interfere with those circuits allocated by the exchange to another ISP.

4

Preferably, a record is maintained at the signalling gateway, of the circuit switched communication channels allocated to each ISP coupled to the signalling gateway.

Preferably, the telecommunication network comprises a Signalling System No.7 (SS7) based signalling network which is interfaced to the ISP via the signalling gateway. More preferably, the network coupling the signalling gateway to the ISP is an IP based network, such that the signalling gateway provides a conversion between at least the Message Transfer Part protocols (i.e. said first transmission protocol) of the SS7 network and the IP based protocols. This arrangement allows ISUP messages to be transferred, transparently, between the exchange and the ISP.

In certain embodiments of the invention, the ISP from which a signalling message originates is identified at the signalling gateway by virtue of the source IP address associated with the IP datagram in which the message is delivered to the gateway. Typically, each ISP coupled to the signalling gateway is allocated a unique IP address. The signalling gateway maintains a record of those circuits which are allocated to a given ISP/IP address.

In other embodiments of the invention, each of the ISPs connected to a given signalling gateway is allocated a unique Point Code in the signalling network of the telecommunications network, Point Codes being included in the header of a signalling message to indicate the destination and source of the message. The signalling gateway screens messages received from an ISP to confirm that the source Point Codes contained therein correspond to the actual ISPs from which they originated. Again, the originating ISP for a message may be identified on

the basis of the source IP address of the message containing datagram.

4   In other embodiments of the invention, the ISP from which a signalling message originates is identified by virtue of the input port/device of the signalling gateway at which the message. Thus input port/device

8   identity may be used as an alternative to the source ISP IP address.

According to a second aspect of the present invention

12   there is provided apparatus for transferring signalling messages between an Internet Service Provider (ISP) and an exchange of a telecommunications network for the purpose of allocating and controlling circuit switched

16   communication channels between the exchange and the ISP, the apparatus comprising a signalling gateway coupled between a signalling network of a telecommunications network and a network connected to an Internet Service

20   Provider (ISP) and arranged to:
         convert messages between a first transmission protocol used in the telecommunications network and a second transmission protocol used in the network which

24   connects the signalling gateway to the ISP; and
         for each message received at the signalling gateway from the ISP, to confirm the right of that ISP to control a circuit switched communication channel

28   identified in the message.

Brief Description of the Drawings

32   For a better understanding of the present invention and in order to show how the same may be carried into effect reference will now be made, by way of example, to the accompanying drawings, in which:

Figure 1 shows a signalling gateway coupling a signalling network of a telecommunications network to a number of ISPs;

Figure 2 illustrates schematically the protocol stacks implemented at the signalling gateway of Figure 1; and

Figure 3 is a flow diagram illustrating the method of operation of the signalling gateway of the network of Figure 1.

Detailed Description of Certain Embodiments

In Figure 1 there is illustrated a subscriber telephone 1 connected to a local access exchange 2 of a telephone network. This network is assumed to be a conventional network employing PSTN, ISDN, or certain other known communication protocols. Within the network, circuit switched channels over which voice or data may be transmitted are set up and controlled using a Signalling System No.7 based signalling network (e.g. CCITT No.7). More particularly, inter-exchange signalling messages carried by the SS7 network conform to the ISDN User Part (ISUP) protocol.

The present example is concerned with the setting-up and control of a voice communication channel between the telephone network subscriber terminal 1 and a remote terminal (not shown in Figure 1) coupled to the Internet 3. The remote terminal may be for example a multi-media PC connected via a modem and a local access network to the Internet 3, or it may be a telephone network subscriber telephone similar to the telephone 1. In either case, voice data is communicated between the two terminals/telephones over the Internet 3.

A number of ISPs 4 are each allocated a large number of circuit switched channels by the access exchange 2, and

each of these channels has an identification number (CIC) unique to the exchange 2. In order to access the Internet, it is necessary to establish a connection over one of the allocated channels between the subscriber telephone 1 and an Internet interface device 5 (via the access exchange 2) provided by one of the ISPs 4.

The interface device 5 is known in the art as a "Media Gateway" and is arranged to convert voice information received from the telephone 1 into a form suitable for transmission over the Internet (involving for example transcoding, formatting, etc) and to perform the reverse transformation for data received over the Internet and destined for the telephone 1. It is noted that the Media Gateway 5 may communicate with a remote Media Gateway, or with a remote IP terminal, using the ITU multi-media protocol H.323 although this will not be considered here in further detail.

Each ISP 4 has a "Media Controller" 6 which is analogous to a conventional telecommunications network switch, i.e. it is responsible for the general management of Media Gateway resources and in particular for allocating Media Gateways to subscribers (or rather to circuits originating at the access exchange 2).

The Media Controller 6 is arranged to exchange signalling information with a signalling gateway 7, referred to hereinafter as an SS7/IP gateway, which is under the control of the telecommunications network operator and can thus be considered secure from the point of view of the operator. The SS7/IP gateway 7 is connected to the SS7 network and as such is typically allocated a unique Point Code within the visibility area of the SS7 network, which Code provides a destination (and source) address for messages within the network. The physical connection between the Media Controllers 6

and the SS7/IP gateway 7 is provided by an IP network
which may be the Internet but which is more probably an
intranet having no public access.

4

Figure 2 illustrates the communication protocol layers
implemented at the SS7/IP gateway 7 in order to allow
ISUP messages carried by the SS7 signalling network to
8 be relayed over the IP network to the Media Controllers
6, and *vice versa*. ISUP messages received at the SS7/IP

gateway 7 from the access exchange 2 over the SS7
network are processed through a Message Transfer Part
12 (MTP) layer 8 (see "Understanding Telecommunications",
vols. 1 & 2, Studentlitteratur, Lund, Sweden (ISBN 91-
44-00214-9)) before being passed to a processing and
control part 9. Messages are relayed through this part
16 9 before being processed by a TCP/IP part 10 to provide
IP datagrams suitable for transmission over the IP
network to the Media Controllers 6. Messages received
at the SS7/IP gateway 7 over the IP network are
20 processed in the reverse direction, with the processing
and control part 9 performing an additional message
authentication operation as will now be described.

24 For the purpose of routing datagrams over the IP network
between the SS7/gateway 7 and the Media Controllers 6 of
the various ISPs 4, each Media Controller 6 is allocated
an IP address (unique in that IP network). The IP
28 address allocated to a Media Controller 6 is
incorporated into all datagrams sent by that controller
6 to the SS7/IP gateway 7 and enables the SS7/IP gateway
7 to confirm the source of a received packet.

32

When a signalling message is received by the SS7/IP
gateway 7, the processing and control part 9 identifies
the IP address associated with the message. The gateway
36 7 maintains a record of the IP addresses allocated to
the various Media Controllers 6 as well as a record of

the circuits (CICs) allocated to each ISP. Each
signalling message contains in its header part the CIC
to which the message relates. The processing and

4   control part 9 confirms that the originating ISP 4,
identified from the source IP address, is allocated the
CIC to which the signalling message relates. If the
result is positive, the message is passed to the MTP 8

8   for relaying to the access exchange 2. If the result is
negative, i.e. the signalling message relates to a CIC
not allocated to the originating ISP 4, then the message
is not relayed further and is discarded. In this event,

12   an error message may be returned to the originating ISP
4 and also possibly to the access exchange 2.

Figure 3 is a flow chart illustrating the message

16   authentication and relay steps performed at the SS7/IP
gateway 7 upon receipt of a signalling message from an
ISP 4.

20   It will be appreciated that modifications may be made to
the above described embodiment without departing from
the scope of the present invention. For example, each
Media Controller 6 may be allocated a Point Code in the

24   SS7 network of the telecommunications network. Thus, a
Media Controller 6 may be made the destination node for
an SS7 message rather than the SS7/IP gateway (although
signalling messages are still routed through the SS7/IP

28   gateway). As the Point Code is included in the header
of an ISUP message, the SS7/IP gateway 7 may authorise a
received signalling message by matching the Point code
included in the message header with the source IP

32   address.

Whilst the embodiment described above includes only a
single exchange 2 to which the subscriber telephone 1,

36   the SS7/IP gateway 7, and the ISPs 4 are all directly
connected, it will be appreciated that this need not be

the case.   Indeed, a more likely scenario involves a
number of transit exchanges through which signalling
data and circuit switched channels are routed.   It will

4   also be appreciated that the present invention is not
limited to voice communications and is also applicable
to general data communications.

8   The above description has also been concerned with the
use of ISPs to connect subscribers to the Internet.   The
present invention may also be employed in connection
with ISPs which connect subscribers to one or more

12 closed intranets.

Claims

1.   A   method   of   transferring   signalling   messages
between   an   Internet   Service   Provider   (ISP)   and   an
exchange   of   a   telecommunications   network   for   the   purpose
of   allocating   and   controlling   circuit   switched
communication channels between the exchange and the ISP,
the method comprising:

    routing   said   signalling   messages   via   a   signalling
gateway   which   provides   for   conversion   of   messages
between   a   first   transmission   protocol   used   in   the
telecommunications   network   and   a   second   transmission
protocol   used   in   the   network   which   connects   the
signalling gateway to the ISP; and

    for   each   message   received   at   the   signalling   gateway
from   the   ISP,   confirming   the   right   of   that   ISP   to
control   a   circuit   switched   communication   channel
identified in the message.

2.   A   method   according   to   claim   1   and   comprising
maintaining   a   record   at   the   signalling   gateway   of   the
circuit   switched   communication   channels   allocated   to
each ISP coupled to the signalling gateway.

3.   A   method   according   to   claim   1   or   2,   wherein   the
telecommunication   network   comprises   a   Signalling   System
No.7   (SS7)   based   signalling   network   which   is   interfaced
to the ISP via the signalling gateway.

4.   A   method   according   to   any   one   of   the   preceding
claims,   wherein   the   network   coupling   the   signalling
gateway to the ISP is an IP based network.

5.   A   method   according   to   claim   4   when   appended   to
claim   3,   wherein   the   signalling   gateway   provides   a
conversion   between   at   least   the   Message   Transfer   Part
protocol of the SS7 network and the IP based protocols

enabling ISUP messages to be transferred, transparently, between the exchange and the ISP.

6.   A method according to claim 4 or 5, wherein the ISP from which a signalling message originates is identified at the signalling gateway by virtue of the source IP address associated with the IP datagram in which the message is delivered to the gateway.

7.   A method according to claim 3 or to any one of claims 4 to 6 when appended to claim 3, wherein each of the ISPs connected to a given signalling gateway is allocated a unique Point Code in the signalling network of the telecommunications network, Point Codes being included in the header of a signalling message to indicate the destination and source of the message, and the signalling gateway screens messages received from an ISP to confirm that the source Point Codes contained therein correspond to the actual ISPs from which they originated.

8.   A method according to claim 3 or to any one of claims 4 to 6 when appended to claim 3, wherein the ISP from which a signalling message originates is identified by virtue of the input port/device of the signalling gateway at which the message arrives.

9.   Apparatus for transferring signalling messages between an Internet Service Provider (ISP) and an exchange of a telecommunications network for the purpose of allocating and controlling circuit switched communication channels between the exchange and the ISP, the apparatus comprising a signalling gateway coupled between a signalling network of a telecommunications network and a network connected to an Internet Service Provider (ISP) and arranged to:

convert messages between a first transmission
protocol used in the telecommunications network and a
second transmission protocol used in the network which
connects the signalling gateway to the ISP; and

5   for each message received at the signalling gateway
from the ISP, to confirm the right of that ISP to
control a circuit switched communication channel
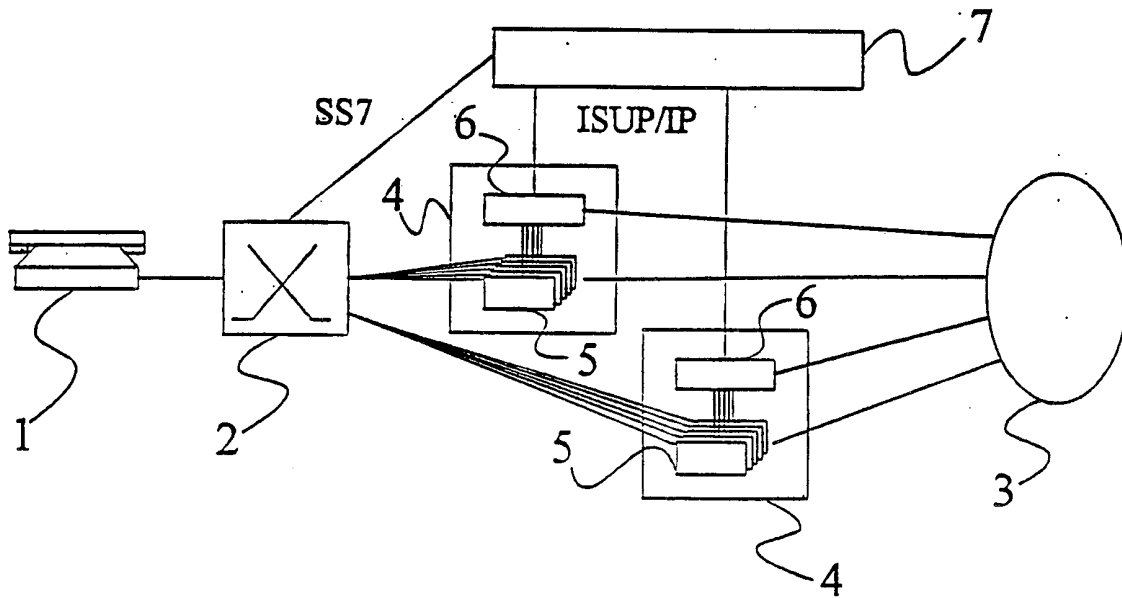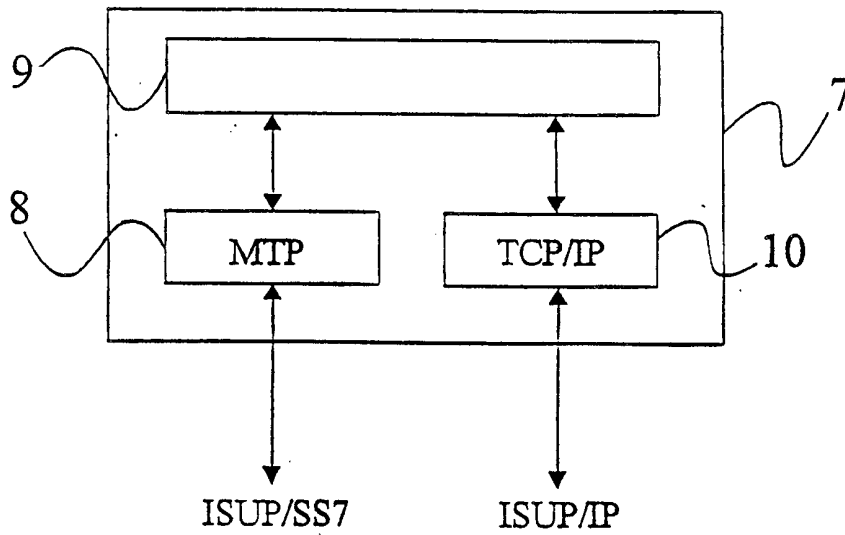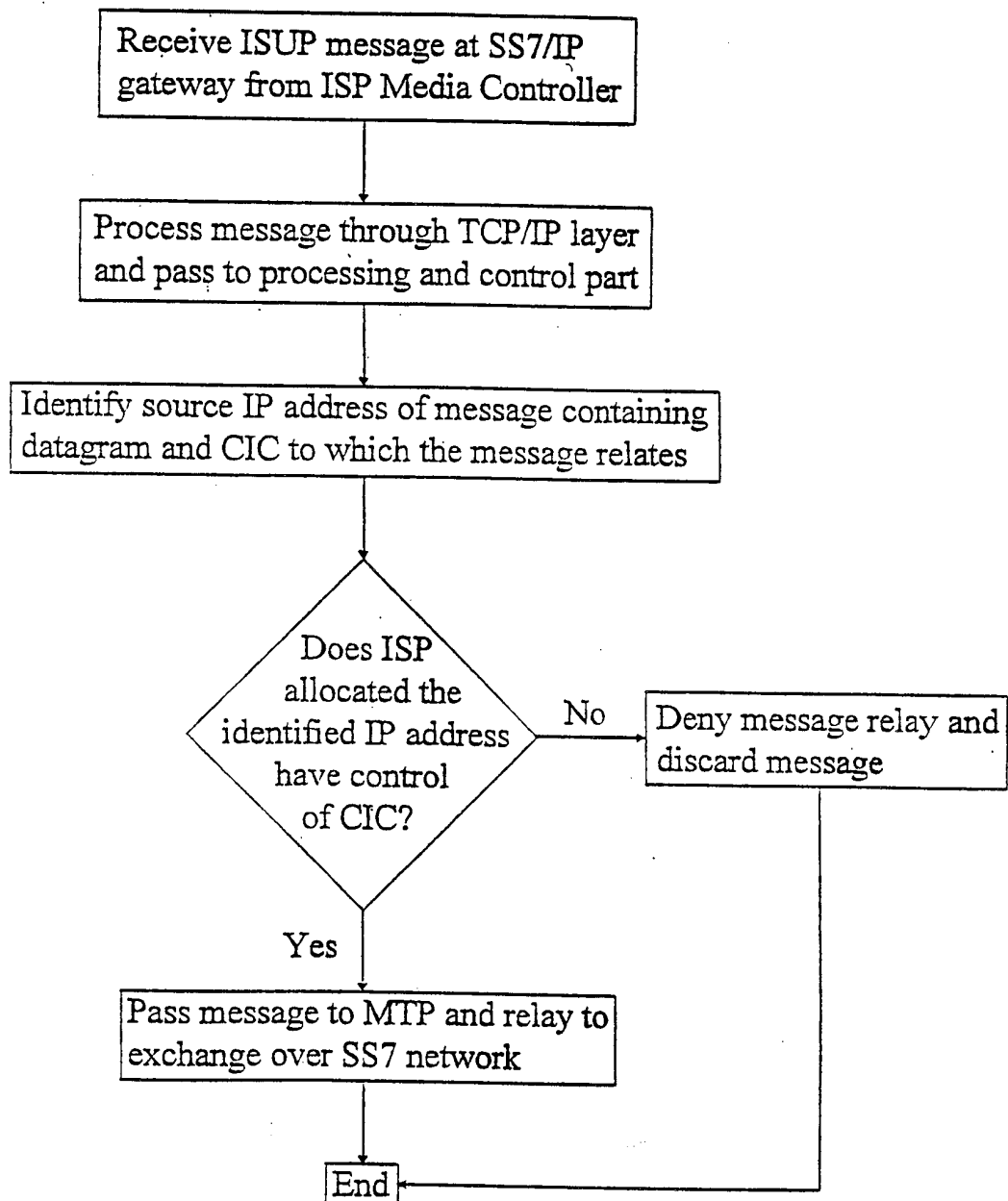identified in the message.

SS7

ISUP/IP

7

6

4

6

5

5

1

2

3

4

Figure 1

9

7

8

| MTP | | TCP/IP | 10 |

ISUP/SS7   ISUP/IP

Figure 2

Receive ISUP message at SS7/IP
gateway from ISP Media Controller

Process message through TCP/IP layer
and pass to processing and control part

Identify source IP address of message containing
datagram and CIC to which the message relates

Does ISP
allocated the
identified IP address   No   Deny message relay and
have control   discard message
of CIC?

Yes

Pass message to MTP and relay to
exchange over SS7 network

End

Figure 3

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04Q3/00   H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04Q   H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 38018 A (TELEFONAKTIEBOLAGET LM ERICSSON) 28 November 1996 (1996-11-28) abstract page 1, line 24-36 page 5, line 11-35 page 7, line 19 -page 12, line 17 claims 1-7,11; figures 1,2	1-5,9
A		6-8
X	WO 98 17048 A (BRITISH TELECOMMUNICATIONS PLC) 23 April 1998 (1998-04-23) abstract page 4, line 1 -page 5, line 16 claims 1,2,10-12; figures 2-5,8	1,2,4,9
	-/--	

| X | Further documents are listed in the continuation of box C. | | X | Patent family members are listed in annex. |

Date of the actual completion of the international search	Date of mailing of the international search report
30 March 2000	10/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gijsels, W

INTERNATIONAL SEARCH REPORT

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 28885 A (TELEFONAKTIEBOLAGET LM ERICSSON) 2 July 1998 (1998-07-02) abstract page 2, line 17-26 claims 1,7,8; figures 1,2	1-9
A	EP 0 851 653 A (LUCENT TECHNOLOGIES INC) 1 July 1998 (1998-07-01) column 4, line 31 -column 5, line 21 claims 6-8; figures 1-7	1,4,6,8,9
A	EP 0 203 614 A (FUJITSU LTD) 3 December 1986 (1986-12-03) page 6, line 32 -page 7, line 8 page 8, line 24-36 page 10, line 7-17 figures 1,4-8,10A-12B	1,7,9
P,X	WO 99 34613 A (BELL CANADA) 8 July 1999 (1999-07-08) abstract page 8, line 11 -page 14, line 19 claims 1,4-6,13-15; figures 1,2,5	1-4,9
P,X	EP 0 909 064 A (KOKUSAI DENSHIN DENWA CO LTD) 14 April 1999 (1999-04-14) abstract page 3, line 31 -page 4, line 52 figures 1A,1B,3	1,2,4,9
E	WO 99 67928 A (TELEFONAKTIEBOLAGET LM ERICSSON) 29 December 1999 (1999-12-29) the whole document	1-4,6,7,9
E	EP 0 966 145 A (NORTEL NETWORKS CORP) 22 December 1999 (1999-12-22) abstract claims 1-7; figures 1,3,5,6,22-25	1,3,4,9

1

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9638018	A	28-11-1996	FI	961690 A	25-11-1996
			AU	708519 B	05-08-1999
			AU	5916696 A	11-12-1996
			BR	9609190 A	11-05-1999
			CA	2221183 A	28-11-1996
			CN	1185268 A	17-06-1998
			EP	0829181 A	18-03-1998
			JP	11505973 T	25-05-1999
			NO	975343 A	21-01-1998
WO 9817048	A	23-04-1998	AU	4630597 A	11-05-1998
			EP	0932972 A	04-08-1999
WO 9828885	A	02-07-1998	AU	5352098 A	17-07-1998
			EP	0958684 A	24-11-1999
			NO	992963 A	20-08-1999
			SE	9604784 A	21-06-1998
EP 0851653	A	01-07-1998	CA	2221218 A	23-06-1998
			JP	10210182 A	07-08-1998
EP 0203614	A	03-12-1986	JP	1672772 C	12-06-1992
			JP	3032946 B	15-05-1991
			JP	61276465 A	06-12-1986
			CA	1287152 A	30-07-1991
			CN	1006436 B	10-01-1990
			HK	46792 A	03-07-1992
			KR	9001156 B	27-02-1990
			SG	45592 G	12-06-1992
			US	5182550 A	26-01-1993
WO 9934613	A	08-07-1999	AU	1865099 A	19-07-1999
EP 0909064	A	14-04-1999	JP	11068851 A	09-03-1999
WO 9967928	A	29-12-1999	FI	981354 A	12-12-1999
EP 0966145	A	22-12-1999	NONE		