



(22) Date de dépôt/Filing Date: 2005/07/14

(41) Mise à la disp. pub./Open to Public Insp.: 2006/05/30

(45) Date de délivrance/Issue Date: 2009/01/27

(30) Priorités/Priorities: 2004/11/30 (US60/631,633);  
2005/01/12 (US11/033,930)

(51) Cl.Int./Int.Cl. *H04L 12/56* (2006.01),  
*H04L 12/24* (2006.01)

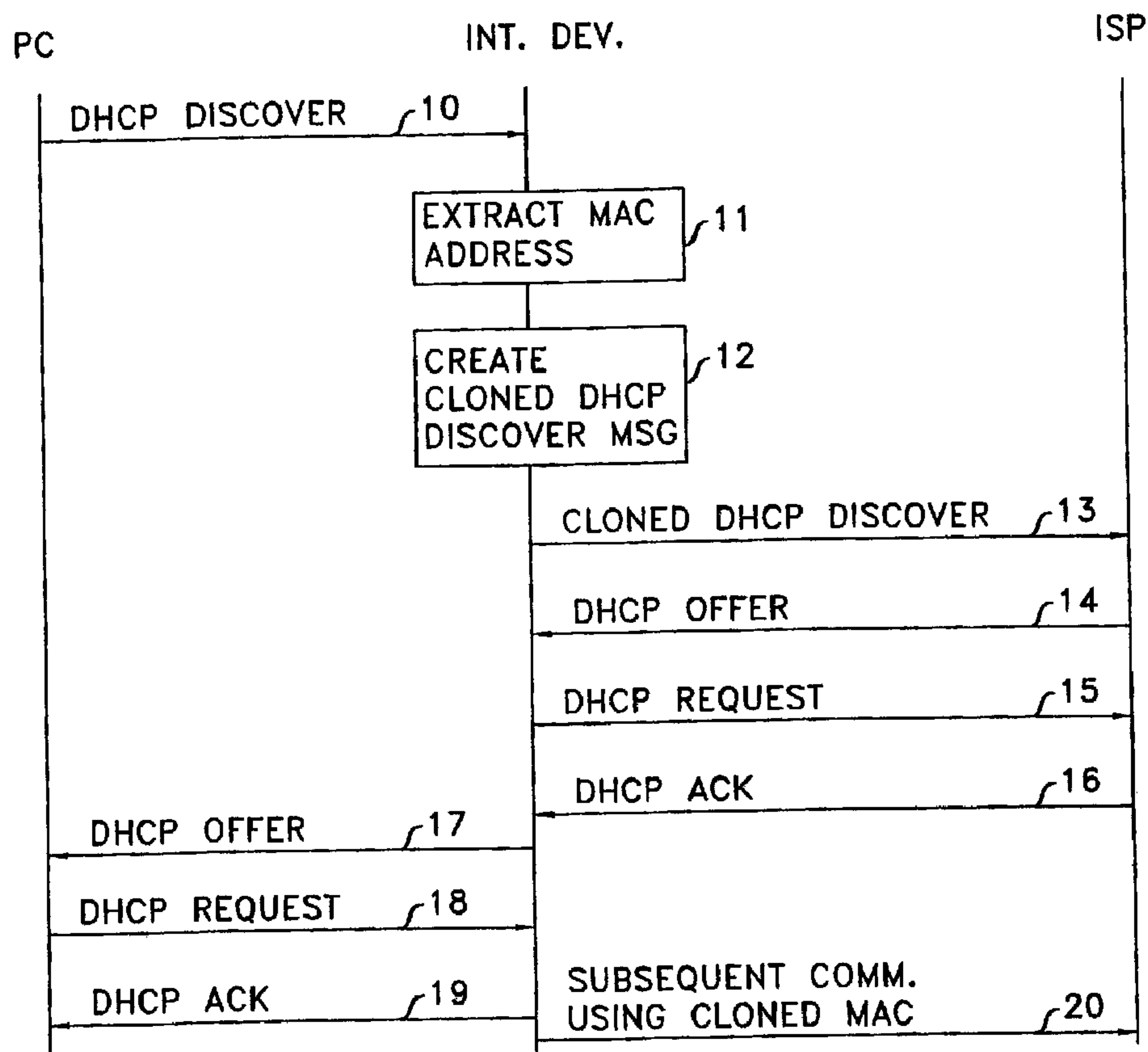
(72) Inventeurs/Inventors:  
CHERCHALI, ALI, US;  
GUDELIS, MARIUS J., JR., US;  
LESTER, WILLIAM G., US;  
MCLAUGHLIN, ROBERT J., US

(73) Propriétaire/Owner:  
AT&T CORP., US

(74) Agent: KIRBY EADES GALE BAKER

(54) Titre : TECHNIQUE DE CLONAGE AUTOMATIQUE D'ADRESSE MAC

(54) Title: TECHNIQUE FOR AUTOMATED MAC ADDRESS CLONING



(57) Abrégé/Abstract:

In an arrangement where the device that is known to an ISP is communicating with the ISP through an interposed device that is not known to the ISP, the interposed device captures the known device's MAC address upon startup and clones the captured MAC address in all standard packets that it sends to the ISP.

Cherchali 0318

**Abstract**

**[022]** In an arrangement where the device that is known to an ISP is communicating with the ISP through an interposed device that is not known to the ISP, the interposed device captures the known device's MAC address upon startup and clones the captured MAC address in all standard packets that it sends to the ISP.

## Technique for Automated MAC Address Cloning.

### **Background**

- [001] This application claims priority of United States Application Serial No. 11/033,930 published under No. US 2006/0114894 A1.
- [002] This invention relates to communication over the Internet, and more particularly to establishing IP addresses for subscriber devices.
- [003] Internet Service Providers (ISPs) supply a public IP address upon request to a subscriber's IP device (e.g., PC NIC card). This request is most commonly made at startup of the IP device, when the device sends a Dynamic Host Configuration Protocol (DHCP) Broadcast Discover message, requesting IP Address offers from any DHCP server that is listening. In response to the DHCP Broadcast Discover message one or more DHCP Offer messages are received at the subscriber's IP device, the IP device chooses the offer of one of the responding servers, and sends a DHCP Request message to the chosen server. The chosen server sends back an Acknowledgement (ACK) message, and communication thereafter proceeds.
- [004] Cable companies that offer Internet access through cable modems bridge DHCP Discover messages that are received by a modem onto a Data Over Cable System Interface Specification (DOCSIS) channel, where the cable modem identifies itself to a cable modem termination system (CMTS) by providing its Media Access Control (MAC) address. The CMTS thus receives both the DHCP Discover message from an IP device that is connected to the cable modem and the cable modem's MAC address. When a subscriber's IP device, such as a PC, connects to the cable company's ISP server, the cable company can therefore establish a correspondence between the MAC address of the subscriber's cable modem and the MAC address of the subscriber's IP device. Thereafter, knowing the MAC address that is expected to be found in DHCP Discover messages coming from the subscriber's cable modem, a cable company can choose to decline providing an IP address in response to a DHCP Discover message with an unexpected MAC address. Declining to provide an IP address is a measure of security that prevents an interloper's IP device from obtaining service. Consequently, however, when a legitimate subscriber wants to change the IP device or add an interposed device,

the subscriber needs to contact the ISP (e.g., by telephone), and have the ISP clear the existing MAC addresses association, so that a new association can be established.

- [005] The fact that anytime the subscriber wants to add a new IP end-device such as a new PC, a home-router, or some other device, the subscriber needs to contact the ISP represents a significant inconvenience. A solution is to mimic, or clone, the MAC address of the old device in the new end-device, but this also presents a hassle for the subscriber because currently available devices need to be manually configured to perform such cloning.

### **Summary**

- [006] An advance in the art is achieved in an arrangement where the device that is known to the ISP is communicating with the ISP through an interposed device that is not known to the ISP by having the interposed device automatically clone the known device's MAC address in its communications with the ISP. This is achieved by the interposed device capturing the MAC address of the known device at startup and employing the captured MAC address in all standard packets that are sent to the ISP. Certain exemplary embodiments may provide a method executed in an interposed IP device having an upstream side for communicating with an ISP and a downstream side for communicating with one or more user IP devices, comprising: receiving a DHCP Discovery message from one of said user IP devices; extracting a MAC address that is known to said ISP from said DHCP Discovery message; forming an outgoing DHCP Discovery message that includes said extracted MAC address; sending the formed DHCP Discovery message to said ISP as part of a protocol that results in an acknowledged public IP address and a DNS address being available; sending a DHCP Offer message to the user device from which said DHCP Discovery message was received, offering a private IP address for communication between said user device and said interposed IP device; and communicating with said ISP with packets that carry said extracted MAC address.

**Brief Description of the Drawing**

- [007] FIG. 1 presents a messages flow chart in accord with the principles disclosed herein;
- [008] FIG. 2 presents an alternate messages flow chart ; and
- [009] FIG. 3 shows an arrangement of an interposed device that supports both a PC and an IP telephone.

**Detailed Description**

- [010] Many ISPs track a user's MAC address as a crude security measure, but the idea of cloning a MAC address has made this security measure more of a hassle than an effective measure. Home Router manufacturers embraced the idea of cloning in order to keep their buyers from having to reset this MAC with the ISP. However, the subscriber has to locate and identify the MAC address of his or her PC, and use this information to manually set up cloning in the router. To a novice this setup can be challenging, and circumventing it would provide a much better customer experience.

Cherchali 0318

- [011] The present disclosure relates to an arrangement where a subscriber's PC (or other IP device) has already been configured to work with the ISP, and where the subscriber interposes a new device between the subscriber's PC and the cable modem. Home Routers (HR), Media Terminal Adapters, and Telephone Adapters are examples of such interposed devices, each possessing its own MAC address.
- [012] Although interposed devices have their own MAC addresses, to meet the objective of this invention an interposed device needs to automatically assume the MAC address of the PC that is already known to the ISP's server whenever the interposed device communicates with the ISP server.
- [013] In accordance with the illustrative approach depicted in FIG. 1, when the user's IP device is powered on at step 10, the TCP/IP interface of the IP device sends out a DHCP Discover message to acquire an IP address. It is a request to receive an IP address by selecting from one or more DHCP Offer messages that might arrive from listening DHCP servers. In step 11 the interposed device captures the DHCP Discover message and extracts therefrom the MAC address. In step 12 the interposed device creates its own DHCP Discover message, places the MAC address that was extracted from the DHCP Discover message sent by the IP device instead of its own MAC address, and in step 13 forwards the modified DHCP Discover message to the ISP. In step 14 the ISP sends to the interposed device a DHCP Offer message containing a public IP address and a DNS address, in step 15 the interposed device sends a DHCP Request message to the ISP, which effectively confirms its acceptance of the offered IP address, and in step 16 the ISP sends an ACK message, confirming the IP address that will be used. Thereafter, according to step 20 communication proceeds between the interposed device and the ISP, with the continued use of the cloned MAC address. The continued use of the cloned MAC address prevents an ISP from raising an alarm should it choose — in the course of the communication session — to check the MAC address of the device with which it is communicating.
- [014] Following step 16, or concurrently therewith, at step 17 the interposed device sends a DHCP Offer message to the subscriber's IP device, offering to the IP device a private IP address, and at steps 18-19 the interposed device and the IP device complete

the IP acquisition protocol vis-à-vis the private IP address in the conventional manner described above.

[015] FIG. 2 shows a slightly different approach. Specifically, as soon as the interposed device receives the initial DHCP Discover message in step 21, in step 22 it immediately offers the subscriber's IP device a private IP address, but with no DNS listed. The offer contains a very short lease time; for example, 10 sec. or fewer. In step 23 the IP device follows up with the DHCP Request (since this is the only offer it received), and the interposed device completes the transaction with a DHCP ACK message in step 24.

[016] The interposed device then turns to its task of establishing a connection to the ISP, extracts the MAC address of the IP device in step 11, creates its own DHCP Discover message with its MAC address replaced with the extracted MAC address of the IP device in step 12, and presents its created DHCP Discover message (with the cloned MAC address) to the ISP in step 13.

[017] In the illustrative signal flow chart of FIG. 2, the lease time for the private IP address provided to the IP device expires shortly after the interposed device sends its created DHCP Discover message to the ISP. When the lease time thus expires, in step 25 the IP device sends a DHCP Request Renew message to the interposed device, asking to renew the lease. Since the interposed device has not yet received an IP address from the ISP, the interposed device sends a DHCP ACK message to the IP device in step 26, renewing the lease for another short interval.

[018] Eventually, the communication between the interposed device and the ISP (steps 14, 15, and 16) completes, and the interposed device is in possession of a public IP address and DNS address. Thereafter, when the IP address lease of the IP device expires again and the IP device sends a DHCP Request Renew message in step 27, the interposed device responds in step 28 with a DHCP NACK message that denies use by the IP device of the previously provided private IP address. Having received a negative acknowledgement message, the subscriber's IP device sends a new DHCP Discover message in step 29, in response to which in step 30 the interposed device sends a DHCP Offer message that is complete with DNS address(es), and the same or a different private IP address. The IP device then sends a DHCP Request message in step 31, and the interposed device responds with a DHCP ACK message in step 32.

Cherchali 0318

**[019]** The interposed device can be viewed to have an upstream side that is connected to the ISP through a modem, and a downstream side that is connected to a subscriber's IP device with a MAC address that is known to the ISP. On the upstream side the interposed device behaves like a client relative to the ISP. On the downstream side the interposed device behaves like a server relative to the subscriber's IP device, and any other device that is connected to the interposed device on the downstream side thereof, such as illustrated for example in FIG. 3 where a PC and a telephone are connected to the downstream side of the interposed device. For sake of simplicity, it is assumed that the telephone shown in FIG. 3 is an IP device. Of course, the shown telephone can be a conventional POTS telephone if the circuitry that is necessary for converting it to an IP device is included within the interposed device.

**[020]** It is noted that the above-disclosed approach requires the PC with the MAC address that is known to the ISP to send a DHCP Discover message to the interposed device before any other of the IP devices that are connected to the downstream side of the interposed device. When this is done, other devices can send their own DHCP Discover message, obtain their own private IP address from the interposed device and communicate in a conventional manner. It is noted, however, that the communication with the ISP, as far as the ISP is concerned, is with the PC that is known to the ISP because, as shown in step 20 of both FIG. 1 and FIG. 2, subsequent communication from the interposed device to the ISP is with packets that employ the cloned MAC address.

**[021]** The above discloses two illustrative approaches for automatically cloning the MAC address of a device that is known to an ISP, but it should be realized that other approaches can be implemented without departing from the spirit and scope of this invention. To illustrate, the private IP address that is provided to the PC (sans a DNS address) is shown in FIG. 2 to be provided immediately upon receipt DHCP Discover message 21, but it could just as validly be provided sometime later, such as after the MAC address is extracted.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method executed in an interposed IP device having an upstream side for communicating with an ISP and a downstream side for communicating with one or more user IP devices, comprising:

receiving a DHCP Discovery message from one of said user IP devices;

extracting a MAC address that is known to said ISP from said DHCP Discovery message;

forming an outgoing DHCP Discovery message that includes said extracted MAC address;

sending the formed DHCP Discovery message to said ISP as part of a protocol that results in an acknowledged public IP address and a DNS address being available;

sending a DHCP Offer message to the user device from which said DHCP Discovery message was received, offering a private IP address for communication between said user device and said interposed IP device; and

communicating with said ISP with packets that carry said extracted MAC address.

2. The method of claim 1 where said protocol comprises:

receiving a new DHCP Offer message from said ISP that includes said public IP address;

sending a DHCP Request offer informing said ISP of acceptance of said public IP address; and

receiving an acknowledgement message from said ISP.

3. The method of claim 2 where said new DHCP Offer message includes a DNS address.

4. The method of claim 1 where said step of sending said DHCP Offer message is executed following completion of said protocol, including in said DHCP Offer message a DNS address provided by said ISP.

5. The method of claim 1 where said step of sending said DHCP Offer message is executed prior to completion of said protocol, including in said DHCP Offer message no DNS address, and specifying lease duration of less than 10 or fewer seconds.

6. The method of claim 5 further comprising the steps of:  
receiving a DHCP Request from said primary user IP device in response to said sending of the DHCP Offer message;  
sending a DHCP ACK to said primary user IP device message if said protocol has not completed; and  
sending a DHCP NACK to said primary user IP device message if said protocol has completed.

7. The method of claim 6 further comprising the steps of:  
receiving a new DHCP Discover message from said primary user IP device following the sending of said DHCP NACK message; and  
sending a new DHCP Offer message to said primary user IP device in response to said new DHCP Discover message, which offer includes a private IP address and said DNS address.

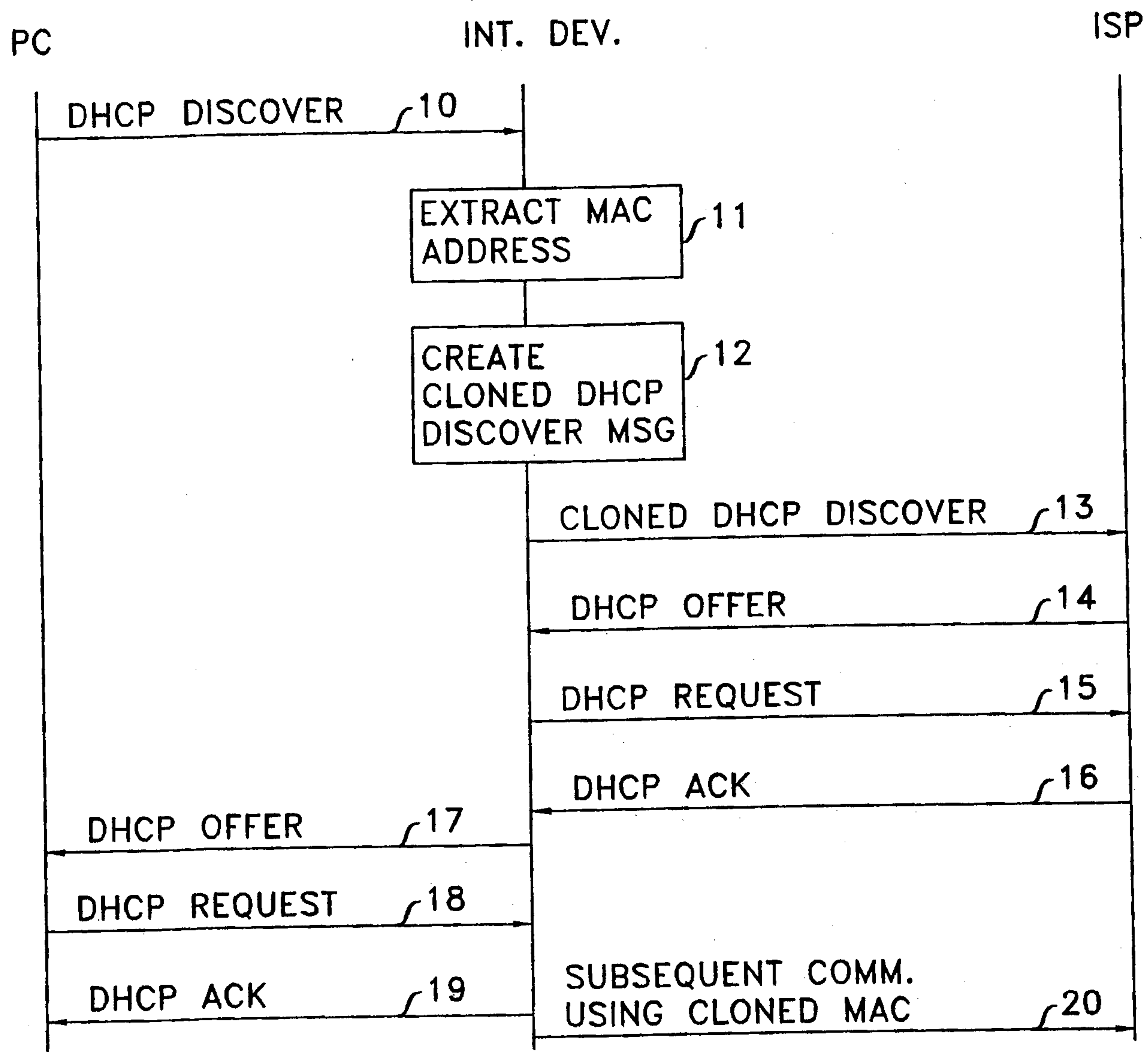
8. The method of claim 5 further comprising the steps of:  
receiving a DHCP Renew message from said primary user IP device in response to said sending of the DHCP Offer message;  
sending a DHCP ACK to said primary user IP device message if said protocol has not completed; and  
sending a DHCP NACK to said primary user IP device message if said protocol has completed.

9. The method of claim 8 further comprising the steps of:  
receiving a new DHCP Discover message from said primary user IP device following the sending of said DHCP NACK message; and

Cherchali 0318

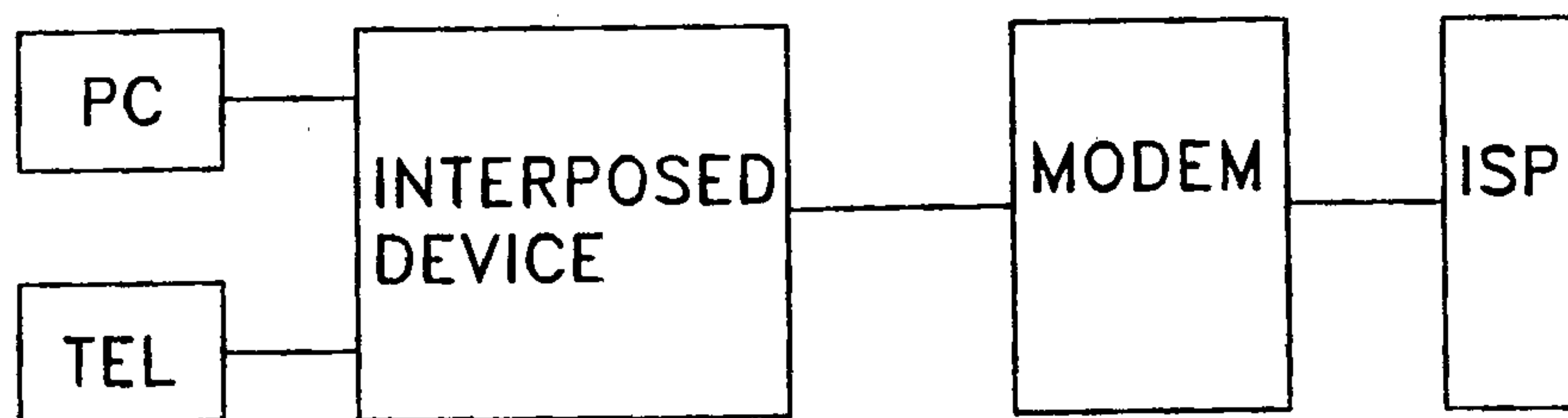
sending a new DHCP Offer message to said primary user IP device in response to said new DHCP Discover message, which offer includes a private IP address and said DNS address.

FIG. 1





*FIG. 3*



PC

INT. DEV.

ISP

