Title: IP ADDRESS ALLOCATION IN A MOBILE COMMUNICATIONS SYSTEM

Abstract: The invention relates to mobility management in an Internet-type protocol traffic in a mobile communications network. At least one of mobile exchanges (DXT1, DXT2) in the mobile communication network is arranged to dynamically allocate an IP address to a mobile host (MH) from an address space of the mobile communications network for a lease period and to associate the allocated IP address with a user identity (SSI) and a data equipment identity (NSAPI) used for identifying the mobile host (MH) in the mobile communication network.
Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
IP address allocation in a mobile communications system

Field of the Invention

The invention relates to address allocation for Internet-type protocol traffic in a mobile communications system.

Background of the Invention

Mobile communications system refers generally to any telecommunications system which enables wireless communication when users are moving within the service area of the system. A typical mobile communications system is a Public Land Mobile Network (PLMN). Often the mobile communications network is an access network providing a user with wireless access to external networks, hosts, or services offered by specific service providers.

One of the main targets in the development of mobile communications networks is to provide the user with IP (Internet Protocol) service, i.e. access to the Internet through a mobile communication network. It is desired that the IP will be implemented as an overlay of the mobile network while maintaining backwards compatibility with present systems, assuming minimal modifications in the present standards. However, a problem is that the basic IP concept does not support the mobility of the user: IP addresses are assigned (allocated) to network interfaces in dependence on their physical location. In fact, the first field of an IP address (the NETID) is common to all interfaces that are linked to the same Internet subnet. This scheme prevents the user (the mobile host) from keeping its address while moving over different Internet subnets, i.e. while changing the physical interface.

In order to enhance mobility in the Internet, a Mobile IP protocol for IP version 4 has been introduced by the Internet Engineering Task Force (IETF) in the standard RFC2002. Mobile IP enables the routing of IP datagrams to mobile hosts, independently of their point of attachment in the subnet. Mobile Node MN' (also called Mobile Host MH) refers to a host that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address. In the mobile IP concept, a datagram is encapsulated and routed to a known decapsulation agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination. Each mobile node is connected to a home agent over a unique tunnel, identified by a tunnel identi-
fier which is unique to a given Foreign Agent/Home Agent pair. In the mobile IP, the mobile host is identified with respect to its home IP network. Thus, the Mobile IP solves the mobility management problem of the basic IP by adapting to the inflexibility of the IP address, but IP the mobile host is still identified with respect to its home IP network.

The prior art mobile IP schemes are not very suitable for a mobile communication system which does not employ IP as a network protocol. The TETRA network, which tunnels IP traffic through a non-IP protocol, is an example of such a system. The TETRA system is a digital mobile communication system developed primarily for professional and governmental users, such as the police, military forces, oil plants, etc. Figure 1 illustrates one scenario of a TETRA network connected to the Internet. The TETRA network comprises digital exchanges DXT and TETRA base stations TBS. There are two possible configurations of how a DXT can be connected to the internet. In the first configuration each DXT unit may have its own direct "exit" via an adjacent router, such as router 1 for DXT1 and router 2 for DXT2 in Figure 1, for forwarding IP packets from the TETRA network to the Internet and vice versa. In the second configuration, only one or some of the DXT units, referred to as gateway DXTs herein, are connected to an Internet router (e.g. DXT1 to router 1 in Figure 1), the other DXTs being connected to the Internet over these gateway DXTs.

In mobile communications systems mobile hosts are able to move from one cell to another and thereby arbitrarily roam between the DXTs. The mobile host may start an IP data exchange in one network and complete it in another. The movement of the mobile hosts among TETRA networks leads to a situation where the netid identifier in the IP address of the mobile does not necessarily correspond to the current network.

There are two ways of how an IP address can be allocated to the host: 1) an IP address can be permanently configured in the mobile host, or 2) the host can acquire an IP address either at the system start-up or at the start of an IP service. The second way is preferable for two reasons.

There may be over sixteen thousand IP users bound to the same DXT. The users may be spread over a wide geographical area. If the static IP address configuration is adapted, changes to the network configuration require a manual reconfiguration of each host in the network. In other words, the IP network management becomes inflexible.
The exponential growth of the Internet results in exhaustion of the unique IP address space. It becomes harder for organizations to acquire additional unique address space. This means that the amount of users in an organization may be higher than the amount of available IP addresses. In such a case, a dynamic IP address allocation provides most of the users with IP service.

There is a dynamic address allocation method called the Dynamic Host Configuration Protocol (DHCP). The DHCP is defined in RFC 1541. It is intended for use in local area networks (LANs) over a TCP/IP protocol stack, i.e. in the Internet environment, and thus it is not fully applicable to mobile communications networks which do not employ IP as a network protocol, such as the TETRA. For example, the DHCP communicates address information between the end host and the DHCP client, which introduces an additional load on the air interface in the TETRA. Secondly, the DHCP utilizes the UDP protocol as a transport protocol, which adds an overhead in form of the IP and a UDP header to each DHCP message. Also, due to air link failures, a part of the DHCP server replies will probably be lost, causing often address re-allocations. Thirdly, the DHCP client broadcasts a DHCP DISCOVER message on its local physical subnet, which is not a normal broadcast in the TETRA infrastructure. In addition, the DHCP restricts address acquisition to the local network. In a mobile environment, such as the TETRA, it is worthwhile to allow address acquisition also from remote networks.

Disclosure of the invention

An object of the invention is a new dynamic address allocation method and a mobile communication system which overcome or alleviate the above described problems.

This and other objects of the invention are achieved with a method and a system which are characterized by what is disclosed in the attached independent claims. Preferred embodiments of the invention are disclosed in the attached dependent claims.

Each mobile communication network is assigned a set of unique IP addresses (IPv4 or IPv6 addresses, for example), so the Internet routers will see the mobile networks as ordinary local IP networks. An IP address is a pair of the network and host identifiers. The network identifier (netid) specifies a mobile IP network and the host identifier specifies a mobile host in the mobile network. The addresses available under the assigned network identifier are
collectively referred to as the address space. IP addresses are allocated to
to users from the available address spaces. The address space may be divided
into static and dynamic address subspaces. Static IP addresses are individu-
ally assigned to particular users. The dynamic subspace may be further di-
vided into multiple address pools. An address pool is defined with a pair of
lower and higher edge addresses. The address pools may be shared by sev-
eral organizations and, in such a case they are referred to as organization ac-
cess rights to acquire IP addresses. In a mobile network, an IP subnetwork
can be formed around one or multiple switches, such as DXTs. In the latter
case, several switches will be logically organized under the same netid prefix
and will share the same host address space. The possibility to distribute the
organization address space among multiple networks and to interactively ac-
quire an IP address from them increases the robustness of the address acquisi-
tion method; the user does not depend on a single address distribution cen-
ter. This also increases the address hit rate; if a particular address space is
exhausted, the user may try another network.

The mobile host is identified by a unique pair of a user identity and
a data equipment identity which are bound to an IP allocated to the mobile
host in the mobile communications network. The user identity enables to bind
the allocated IP address to a specific end user or to a specific mobile station in
the mobile communication network and to verify his/her permission to use the
IP service. In the preferred embodiment of the invention, the user identity is a
mobile subscriber identity. The end data equipment identity enables to distin-
guish between several data equipments connected to the same mobile station.

In the preferred embodiment of the invention, a network service access point
identifier (NSAPI) is used for this purpose. As used herein, the term ‘end data
equipment’ refers to any data equipment or IP application connected to, inte-
grated into or associated with a mobile station. The use of the user identity
and the data terminal identity provide a unique identification for the mobile
host, without any relation to the IP network. Further, in most communication
systems, such as TETRA, this allows to re-use the identities already available
in the communication system.

The IP address is preferably allocated for a predetermined period,
called a lease period. The allocated IP addresses with their associations, such
as the user identity and the data equipment identity, are stored in a data
structure called an address table. When the lease period has elapsed, the IP address is deallocated (freed) or the allocation is renewed.

According to a first embodiment of the invention the information about the subnets, address pools and user rights are configured to databases in the network entities. A network entity may have an assigned address space or not. If a network entity does not have an assigned local address space, or it is not able to allocate an IP address to a mobile host for some other reason (e.g. the local address pool is currently exhausted, or the mobile host or user is not permitted to acquire IP addresses from the local address pool), the network entity may acquire an IP address from a remote network entity. In the latter case the local network entity functions as a client and the remote network functions as a server from the point of view of IP address allocation. The client network entity leases the IP addresses from the remote servers on behalf of local users, i.e. mobile hosts. This minimizes signaling taking place over the air interface.

According to a second embodiment of the invention the information about the subnets, address pools and user rights are configured to databases in the network entities but an end-to-end allocation protocol is used to communicate address information between a network entity allocating IP addresses (an address server) and the mobile host itself. If the local network entity is not able to allocate an IP address (e.g., it has no local address pool, or the local address pool is exhausted), the local network entity acts like a "proxy" server trying, on behalf of the mobile host, to acquire an IP address from a remote address server. This approach requires a specific protocol entity residing in the end data equipment in a network layer. Further, in the worst case, more messages may be transmitted over the air interface due to the allocation process than in the first embodiment. On the other hand, mobility management may be less complex.

**Brief description of the Drawings**

In the following, the invention will be described in greater detail by means of preferred embodiments with reference to the accompanying drawings, in which

Figure 1 illustrates a TETRA network connected to the Internet,
Figure 2 illustrates the difference between AIP and DAAP approaches of the present invention,
Figure 3 shows an address table,
Figures 4, 5, 6 and 7 are signaling diagrams showing illustrative scenarios of the AIP address allocation,
Figure 8 is a state diagram illustrating the operation of APC,
Figure 9 is a state diagram illustrating the operation of APS,
Figure 10 illustrates the network entities and protocol entities involved with DAAP protocol,
Figures 11, 12 and 13 are signaling diagrams showing illustrative scenarios of the DAAP address allocation,
Figure 14 is a state diagram illustrating the operation of DAAPC, and
Figure 15 is a state diagram illustrating the operation of DAAPS.

Preferred Embodiments of the Invention
The present invention can be generally applied to mobile communications systems for providing IP mobility. The invention is particularly suitable used for providing IP mobility management in a mobile telecommunications system that employs a non-IP protocol for routing IP traffic, the TETRA network being an example of such a system. In the following, the preferred embodiments of the invention will be described by means of the TETRA system without limiting the invention to this particular mobile communications system.

A mobile host MH may consist of a laptop computer PC connected to a mobile station radio. Alternatively, the MH can be an integrated combination of a small computer and a cellular telephone, similar in appearance to the Nokia Communicator 9000 series. Yet further embodiments of the MH are various pagers, remote-control, surveillance and/or data acquisition devices, etc.

An example of the possible TETRA architecture is described above with reference to Figure 1. It should be understood that Figure 1 shows only a simplified architecture which is suitable for the description of the present invention. In practice, the TETRA system may include any number of TBSs, DXTs, MHs and routers, as well as other network elements which are relevant to the present invention. As used herein, the TETRA IP network is a collection of DXTs that share the same IP address network prefix. One TETRA network may be subdivided into two or more TETRA IP networks. According to the current scenarios, each TETRA network is assigned a set of unique IP addresses (IPv4 or IPv6 addresses, for example), so the Internet routers will see TETRA networks as ordinary local IP networks. The IPv4 address is composed of 32
bits and presented as a pair of the network and host identifiers. The network identifier (netid) specifies a TETRA IP network and the host identifier specifies a mobile host in the TETRA network. In the TETRA network, an IP subnetwork can be formed around one or multiple DXTs. In the latter case, several DXTs will be logically organized under the same netid prefix and share the same host address space. In the example illustrated in Figure 1, a TETRA subnetwork is formed around DXT1 and assigned a netid ‘192.1.1.0’, and a TETRA subnetwork 2 is formed around DXT2 and assigned a netid ‘192.1.2.0’. Organization of IP networks around DXTs requires routing capabilities on the links between them. Each single- or multi-DXT network must be able to forward datagrams addressed to other TETRA IP networks. In Figure 1 the DXT1 and the DXT2 are interconnected by a link 10.

In the following, two different approaches embodying the present invention will be described: an Address Information Protocol (AIP) and a Dynamic Address Allocation Protocol (DAAP). The DAAP and the AIP apply a similar technique to dynamic address management, i.e. an address lease mechanism. The difference between the DAAP and the AIP lies in protocol architecture. The AIP protocol has been designed in compliance with the existing TETRA packet data standard, while the DAAP protocol requires a new protocol entity in the mobile host as well as new messages sent over the air interface. Figure 2 demonstrates the difference between the two approaches. The grey-coloured rectangles (black boxes) show the elements that the AIP or the DAAP do not see. In the case of the AIP, the APC and APS units on local and remote DXTs maintain the address information. The APC leases IP addresses, on behalf of local users from remote APS servers. The DAAP, in turn, is an end-to-end protocol, which means that the address information is communicated between the address server (DAAPSG) and the host itself (DAAPC). The DAAPP acts as a forwarding machine: The DAAPP simply directs the control messages to correct destinations.

The AIP and DAAP protocols will be now described in more detail.

**The AIP protocol**

The AIP protocol manages the IP service in the TETRA and it includes IP mobility management. The AIP protocol resides on the top of the TETRA transport layer; consequently, it exchanges control messages with peers utilizing the underlying transport service. The protocol is not required to route datagrams over the shortest path. Local processes can request IP ad-
dress information from the AIP at least in two cases. In the first case, when the user is requesting the IP service, the process that is responsible for resource allocation requests an IP address from the AIP. Second, before the TETRA routing process forwards the IP datagram, it requests the current location associated with the destination IP address from the AIP. The location of the mobile host may be specified with the identification number of a TETRA network node. In the preferred embodiment, in the IP service, location is defined with the identity (address) of the DXT exchange.

The AIP entities allocate IP addresses to users from the available address spaces. Allocated IP addresses with their associations are stored in a data structure called an address table. The address space may be divided into static and dynamic address subspaces. The static IP addresses are individually assigned to particular users. An AIP entity which is assigned an IP network identifier is called an Address Pool Server (APS) and an AIP entity without an IP network identifier is called an Address Pool Client (APC). Both the APS and APC may co-exist in the AIP process unit. The AIP entity acts as the APC in the following cases: 1) The AIP is not assigned an address space (the AIP is a pure APC), 2) the AIP is assigned an address space; however, the address pools are currently exhausted, and 3) The user has no permission to acquire IP addresses from local address pools. If for some reason the AIP cannot allocate an IP address from the local address space, it may acquire an address from a remote APS.

When the APS or APC issues an IP address to the user, it creates an entry in the address table storing the IP address and the user current location. In order to allocate an IP address, the AIP must know both the user identifier and the identifier of the end data equipment or application. The former identifier is necessary to bind the IP address either to the end user or to the end mobile station. The Individual Short Subscriber Identity (SSI) number may serve for this purpose. The latter identifier is necessary to distinguish between several data equipment (or applications) connected to the same mobile station. The Network Service Access Point Identifier (NSAPI) may be used for this purpose. An example of a possible address table with a minimal set of fields is shown in Figure 3. The IP Address entry field lists all of the allocated IP addresses. The Location DXT field indicates the current locations of the IP users. The Static/Dynamic field shows whether or not the address is permanently assigned to the user. The User Identifier field associates IP addresses with end
users. The NSAPI (Network Service Access Point Identifier) field identifies the end data equipment. In the TETRA network, the user may simultaneously use up to 13 data equipment. Number 0 is reserved for a special use and number 15 for multicast. As a result, there may be more than one entry for the same user, i.e. the same SS1 (like SSI A in Figure 3) but different NSAPIs and IP addresses (like IP address '192.1.1.1' and NSAPI 1 as well as IP address '192.1.1.52' in Figure 3).

In this context the entry (entries) of a single user in the table of Figure 3 is called a user IP context of the respective user. The IP context of the user may contain several entries. As noted above, the user IP context is created, when the APC or the APS issues an IP address to the user. Normally the IP address is issued in response to an address acquisition request from the user. The address acquisition request contains the user and data equipment identifiers SSI and NSAPI. When the APC or APS receives the address acquisition request from the mobile host, it looks up the address table for an entry whose user and data equipment identifiers match with ones in the received request. If the APC or the APS finds such an entry, it completes the request process by returning the IP address back to the caller. Otherwise, the APC or the APS will attempt to allocate an IP address from the local address space. If there is no spare IP address in the address pool, the APC or APS sends an address acquisition request to the remote APS server. The remote APS server obtains an IP address from an address pool and sends it back to the requesting entity. The address may be issued for a predetermined period of time which may be renewed with a specific renewal procedure. The default period may be 12 hours, for example. However, the default time should preferably be such that the IP address would not change during the time the mobile host is registered to the system. When the user no longer needs an IP address, the user requests the entry or the IP context in the address table to be deleted and the IP address to be returned back to the address pool. If the IP address is permanently allocated, it cannot be allocated to another mobile host. The IP context may also be transferred from one DXT to another in the handover situation.

Figures 4, 5, 6 and 7 show illustrative scenarios of the AIP address allocation.
Example 1

Figure 4 shows how the host acquires an IP address from the local address space (the address space on the same DXT where the user is located). The numbering refers to that used in Figure 4.

1. The mobile host connected to a mobile station acquires an IP address. It sends an IP address request over the air interface.
2. The IP address request arrives at the DXT, at the IP context manager. The IP context manager forwards the address request to the local AIP.
3. The local AIP, after successful validation of the user permission, picks up a spare IP address from an address pool. It associates the IP address with an user identifier SSI and a network service access point identifier NSAPI, thus leasing the IP address to the mobile host for a lease period. The local AIP sends an IP address response back to the IP context manager.
4. On receipt of the response, the IP context manager allocates the IP context to the user and sends an IP address response back to the mobile host.

Example 2

Figure 5 shows how the mobile host acquires an IP address from a remote address space (an address space on a DXT other than the one where the user is located). Referring to Figure 5 the following steps take place.

1. The mobile host connected to a mobile station acquires an IP address. It sends an IP address request over the air interface.
2. The IP address request arrives at the DXT, at the IP context manager. The IP context manager forwards the address request to the local AIP.
3. The local AIP, after successful validation of the user permission, attempts to acquire an IP address from an address pool, but it fails. The local AIP obtains from the database a list of APSs from which the user may acquire an IP address. The local AIP interactively sends an IP address request to APSs until it receives a positive response from one of them.
4. On receipt of the IP address request, an APS associates the IP address with user identifier SSI and network service access point identifier NSAPI thus leasing the IP address to the AIP-sender for a total lease period. The total period of time may be twice the lease period, for example. The APS sends an IP address response back to the AIP-sender.
5. On receipt of the IP address response, the local AIP associates the IP address with an user identifier SSI and a network service access point identifier NSAPI, thus leasing the IP address to the mobile host for the lease period. The local AIP sends an IP address response back to the IP context manager.

6. On receipt of the response, the IP context manager allocates the IP context to the user and sends an IP address response back to the mobile host.

**Example 3**

Figure 6 shows how the local AIP renews address lease (in this context, the local AIP is an APS on the same DXT where the user is located). Referring to Figure 6 the following steps take place.

1. The address lease has expired. The local AIP sends an address use verification request to the IP context manager.

2. The IP context manager sends the address use verification request to the mobile host.

3. If the IP address is in use, the mobile host responds with a positive response back to the IP context manager.

4. On receipt of the response, the IP context manager sends a positive response to the local IP. The AIP leases the IP address for the next lease period. On receipt of negative response or no response, the AIP deletes the allocation of the IP address.

**Example 4**

Figure 7 shows how the APC renews an address leased from the APS. Referring to Figure 7 the following steps take place.

1. The address lease has expired. The AIP sends an address use verification request to the IP context manager.

2. The IP context manager sends the address use verification request to the mobile host.

3. If the IP address is in use, the mobile host responds with a positive response back to the IP context manager.

4. On receipt of the positive response, the AIP sends the APS an address lease renewing request.

5. On receipt of the address lease renewing request, the APS renews the total lease to the APC-sender and replies with a positive lease re-
newing response. On receipt of this response, the AIP renews the address lease to the user.

Figure 7 also shows an alternative case where the lease renewing request is lost between the local AIP and APS. The alternative steps are:

5. The AIP sends the APS an address lease renewing request. The request is lost. While waiting for a response, the AIP sets the timer to 80% of the lease period.

6. When the timer expires, the APS removes the IP address and the AIP sends the APS a second lease renewing request. The request is lost. While waiting for a response, the AIP sets the timer to 20% of the lease period.

7. When the timer expires, the AIP deletes the IP address and sends the IP context manager an address remove request. When the timer expires on the APS, the APS removes the IP address.

8. On receipt of the address remove request, the IP context manager forwards the address remove request to the mobile host. The mobile host stops using the IP address.

**Operation of the APC**

The AIP sends two messages in each address acquisition exchange. Normally, the originator sends a request and the destination will reply to that request by sending either a positive or negative response.

When the AIP has received a dynamic address acquisition request from the local service user it checks whether there is a spare IP address in one of its address pools. If a vacant IP address is found, the AIP will complete the request without acquiring an IP address from a remote APS server. Otherwise it must interactively send address acquisition requests to other known APSs.

The behaviour of the originating APC, when leasing addresses from the remote APS, is illustrated by a generalised state diagram shown in Figure 8. The NO_ENTRY state is an imaginary state that represents no state at all. The first state transition occurs when the server user on the local DXT invokes the AIP address acquisition function. It is assumed that the AIP will create a temporal entry associated with a local call and assign it the ACQUIRING_ADDRESS state. In this text, the temporal entry will be referred to as an address entry or an entry. If the AIP has no a spare IP address in a
local address pool it will choose an APS server, and send an ADDRACQreq request to it.

In the ACQUIRING_ADDRESS state, the AIP is waiting for a response. If a positive ADDRACQres response arrives, the AIP updates the address table entry, assigns the ASSOCIATED state and completes the local request. If the AIP receives a negative ADDRACQres, it selects another APS, if any is left, and retransmits the same ADDRACQreq.

In both the ACQUIRING_ADDRESS and ASSOCIATED states, the AIP may receive more than one positive ADDRACQres response. The AIP always chooses the first response arrived. If a response arrives at the ACQUIRING_ADDRESS state, the AIP moves the entry to the ASSOCIATED state, sets the lease timer, and completes the local request. If a late response arrives at the ASSOCIATED state, the AIP discards it.

The AIP leases IP addresses to users for a certain period of time, which is referred to as a lease period. The default lease period is equal to 12 hours. On the other hand, the APS leases IP addresses to other AIPs for a total lease period which is twice the lease period. If the user releases an IP address before a total lease expiration, the AIP sends an address release request ADDRELreq to the appropriate APS and deletes the address table entry associated with the released address.

When the lease timer has reached the lease period, the AIP attempts to renew the lease of the IP address. It sends an address lease renewing request ADDREREq and moves the address table entry to the RENEWING_1 state.

Before transition to the RENEWING_1 state, the AIP must verify whether the user still has the IP address. It sends an address verification request to the user and moves the address entry to the VERIFYING_ADDRUSE state. If the AIP receives a negative address verification response in this state, it releases the IP address. Otherwise the AIP sends an address lease renewing request LEASERENreq to the APS, sets the address entry timer to a value that is equal to 80% the lease period, and moves the entry to the RENEWING_1 state.

The address entry timer expiration in the RENEWING_1 state causes the AIP to send the second address lease renewing ADDREREq request, set the address entry timer to a value equal to 20% of the lease period, and move the entry to the RENEWING_2 state.
In the RENEWING_2 state, on the timer expiration, the AIP releases the IP address by sending an address release request to the user and deleting the address entry.

If the AIP in any state receives a positive lease renew request LEASRENreq, it sets the address entry timer to the lease period, and moves the entry back to the ASSOCIATED state.

**Operation of the APS**

Referring to Figure 9, when the APS receives an address acquisition request ADDRACQreq, it allocates an IP address and assigns the address entry the ASSOCIATED_REMOTE state. The APS holds the IP address in this state for the total lease period. If the APS receives a lease renewing request LEASRENreq, it resets the lease timer and responds with a LEASRENres response. On the lease timer expiration, the APS releases the IP address.

When the APS allocates an IP address to a local user, it assigns the address entry the ASSOCIATED_LOCAL state and sets its timer to the lease period. When the timer expires, the APS moves the address entry to the VERIFYING_ADDRUSE_LOCAL state, and verifies IP address usage by sending the local user an address verification request. If the APS receives a positive verification response, it returns the address entry back to the ASSOCIATED_LOCAL state. Otherwise it deletes the address entry.

On the RESTOREReq request receipt, in the ASSOCIATED_LOCAL state, the APS resets the entry timer, and completes the request, in the VERIFYING_ADDRUSE_LOCAL state, the APS moves the entry to the ASSOCIATED_LOCAL state, and completes the request.

**II The DAAP protocol**

The three entities involved in the DAAP protocol are illustrated in Figure 10: DAAP Client (DAAPC), DAAP Proxy (DAAPP), and DAAP Server (DAAPS). The DAAPC is a protocol entity residing on the end data equipment in the network layer. Figure 10 also illustrates how the DAAP protocol is situated in the protocol stack in different entities. The DAAPC acquires an IP address from the DAAPS after a logical link between the mobile host and the mobile station has been established. The information about the subnet, address pools and user rights are configured to the network database. The DAAP, which is assigned an IP network identifier, is called the DAAPS, and a DAAP without a network is called the DAAPP. Both the DAAPS and the DAAPP co-exist in the DAAP protocol unit. The DAAP acts as the DAAPP in
the following cases: 1) the DAAP is not assigned an address space (the DAAP is a pure DAAPP), 2) the DAAP is assigned an address space; however, the address pools are currently exhausted, or 3) the user has no permission to acquire IP addresses from local address pools. If for some reason an IP address cannot be allocated from the address space on the local DXT, the local DAAP entity on this DXT acts like a proxy (DAAPP) trying, on behalf of the DAAPC, to acquire an IP address from a remote DAAPS server. When the DAAP on the DXT has received an address acquisition request, it checks whether there is a spare IP address in one of its address pools. If a vacant IP address is found, the DAAP will complete the request without acquiring an IP address from a remote DAAPS server. Otherwise it must interactively send address acquisition requests to other known DAAPS servers. When the DAAPS issues an IP address to the host, it creates an entry, which is called an address table, saving the IP address and the user current location. In order to allocate an IP address, the DAAPS must know both the user identifier and the identifier of the end data equipment. The former identifier is necessary to bind the IP address either to the end user or to the end mobile station. The Individual Short Subscriber Identity (SSI) number may serve for this purpose. The latter identifier is necessary to distinguish between several data equipment connected to the same mobile station. The Network Service Access Point Identifier (NSAPI) may be used for this purpose. The DAAPS leases the IP address to the DAAPC for a total lease period. The DAAPC renews the lease when the lease period has expired.

Figures 11, 12 and 13 show illustrative scenarios of the DAAP address allocation.

**Example 5**

Figure 11 shows how the mobile host acquires an IP address from the local address space (the address space on the DXT of user location). Referring to Figure 11 the following steps take place.

1. The mobile host connected to the mobile station acquires an IP address. The DAAPC sends an IP address request over the air interface.
2. The IP address request arrives at the DXT. The local DAAPS, after successful validation of the user permission, picks up a spare IP address from an address pool. The local DAAPS associates the IP address with user identifier SSI and network service access point identifier NSAPI, thus leasing
the IP address to the mobile host for a total lease period. The local DAAPS sends an IP address response back to the DAAPC.

Example 6
Figure 12 shows how the mobile host acquires an IP address from a remote address space (the address space on a DXT other than the one where the user is currently). Referring to Figure 12 the following steps take place.

1. The mobile host connected to a mobile station acquires an IP address. The DAAPC sends an IP address request over the air interface.

2. The IP address request arrives at the DXT. The local DAAP, after successful validation of the user permission, attempts to acquire an IP address from an address pool, but fails. It then acts as a DAAPP, and obtains from the database a list of DAAPS servers from which the user may acquire an IP address. The local DAAP interactively sends an IP address request to the DAAPS servers until it receives a positive response from one of them.

3. On receipt of the IP address request, a DAAPS associates the IP address with a user identifier SSI and network service access point identifier NSAPI, thus leasing the IP address to the DAAPC for a total lease period. The total period of time may be twice the lease period, for example. The DAAPS sends an IP address response back to the DAAPP.

4. On receipt of the IP address response, the DAAPP sends the IP address response to the DAAPC.

Example 7
Figure 13 shows how the DAAPC renews address lease from the DAAPS. Referring to Figure 13 the following steps take place.

1. The address lease, which is a half of the total lease period, has expired. The DAAPC sends an address lease renew request to the DAAP on the local DXT. While waiting for a response, the DAAPC sets the timer to 30% of the total lease period.

2. On receipt of the request, the DAAPP sends the DAAPS an address lease renew request.

3. On receipt of the address lease renew request, the DAAPS renews the total lease to the DAAPC and replies with a positive lease renew response.

4. On receipt of this response, the DAAPP forwards it to the DAAPC. On receipt of the response, the DAAPC resets the lease timer.
Figure 13 also shows an alternative case where the lease-renewing request is lost between the local DAAPP and the DAAPS:

1*. The address lease, which is half of the total lease period, has expired. The DAAPC sends an address lease renew request to the DAAP on the local DXT. While waiting for a response, the DAAPC sets the timer to 30% of the total lease period.

2*. On receipt of the request, the DAAPP sends the DAAPS an address lease renew request. The request is lost.

3*. The timer has expired on the DAAPC. The DAAPC sends second address lease renew request to the DAAPP. While waiting for a response, the DAAPC sets the timer to 20% of the total lease period.

4*. The DAAPP forwards the DAAPS an address lease renew request. The request is lost. After the total lease period has elapsed, both the DAAPC and the DAAPS remove the IP address.

**Operation of the DAAPC**

The behaviour of the originating DAAPC when leasing addresses from the remote DAAPS is illustrated by a generalised state diagram shown in Figure 14. The NO_ENTRY state is an imaginary state that represents no state at all. The first state transition occurs when the server user on the mobile host invokes the DAAPC address acquisition function. The DAAPC will create an address entry and assign it the ACQUIRING_ADDRESS state. The DAAPC sends an address acquisition request to the DAAP on the local DXT. If that DAAP has no spare IP address in a local address pool, it will choose a DAAPS server, create an temporal address entry in the cache, assign the state ACQUISITION to it and send an ADDRACQreq request to it.

In the ACQUISITION state, the DAAPP waits for a response. If a positive ADDRACQres response arrives, the DAAPP deletes the temporal address entry and completes the local request by forwarding the ADDRACQres response to the DAAPC. If the DAAPP receives a negative ADDRACQres, it selects another DAAPS, if any is left, and retransmits the same ADDRACQreq.

The DAAPP may receive more than one positive ADDRACQres response. The DAAPP always chooses the first response arrived and discards late responses.

The DAAPC leases the IP address to the user for a certain period of time, which is referred to as a lease period. It obtains the value of the lease
period from the ADDRACQres response. The default lease period is equal to 12 hours.

On the other hand, the DAAPS leases IP addresses to the DAAPC for a total lease period which is twice the lease period. If the user releases an IP address before a total lease expiration the DAAPC will delete the address and send an address release request ADDRELreq to an appropriate DAAPS.

After lease timer has reached lease period, the DAAPC attempts to renew the lease of the IP address. It sends an address lease renewing request ADDRENreq, moves the address table entry to the RENEWING_1 state, and sets the address entry timer to a value that is equal to 80% the lease period.

The address entry timer expiration in the RENEWING_1 state causes the DAAPC to send the second address lease renewing ADDRENreq request, set the address entry timer to a value equal to 20% of the lease period, and move the entry to the RENEWING_2 state.

In the RENEWING_2 state, on the timer expiration, the DAAPC releases the IP address by sending an address release request to the user and deleting the address entry.

In any state, if the DAAPC receives a positive lease renew request LEASRENreq, it sets the address entry timer to the lease period, and moves the entry back to the ASSOCIATED state.

**Operation of the DAAPS**

Referring to Figure 15, when the DAAPS receives an address acquisition request ADDRACQreq, it allocates an IP address and assigns the address entry the ALLOCATED state. The DAAPS holds the IP address in this state for the total lease period. If the DAAPS receives a lease renewing request LEASRENreq, it resets the lease timer and responds with a response LEASRENres. On the lease timer expiration, the DAAPS releases the IP address.

The description only illustrates preferred embodiments of the invention. The invention is not, however, limited to these examples, but it may vary within the scope and spirit of the appended claims.
Claims

1. A method of allocating an Internet Protocol-type, or IP-type, address to a mobile host in a mobile communication network comprising mobile exchanges (DXT1, DXT2) and a plurality of mobile hosts (MH), said method being characterized by the steps of
dynamically allocating an IP address to a mobile host (MH) from an address space of the mobile communications network for a lease period,
associating the allocated IP address with a user identity (SSI) and a data equipment identity (NSAPI) used for identifying the mobile host (MH) in the mobile communication system.

2. The method according to claim 1, characterized by the steps of
defining the location of the mobile host by the identity of a mobile exchange (DXT1, DXT2) currently serving the mobile host (MH),
associating the location information of the mobile host with the allocated IP address.

3. The method according to claim 1 or 2, characterized by the steps of
sending an IP address request from the mobile host to the serving mobile exchange (DXT) functioning as an address allocation server incapable of allocating IP addresses,
allocating an IP address from the address pool for said lease period,
associating said allocated IP address with the user identity (SSI) and the data equipment identity (NSAPI) of the mobile host (MH),
sending said allocated IP address to the mobile host (MH).

4. The method according to claim 1, 2 or 3, characterized by the steps of
sending an IP address request from the mobile host to the serving mobile exchange (DXT) functioning as an address allocation client incapable of allocating IP addresses,
sending a further IP address request from the serving mobile exchange to a remote address pool server,
allocating an IP address from the address pool for said lease period and associating said allocated IP address with the user identity (SSI) and the data equipment identity (NSAPI) of the mobile host (MH),

sending said allocated IP address to the serving mobile exchange (DXT),

associating said allocated IP address with the user identity (SSI) and the data equipment identity (NSAPI) of the mobile host (MH) at the serving mobile exchange,

sending said allocated IP address to the mobile host (MH).

5. The method according to claim 4, characterized by allocating said IP address at the remote address allocation server for a second lease time which is longer than said lease time used at the serving mobile exchange.

6. The method according to any one of claims 1-5, characterized by the steps of

sending an address use verification request to the mobile host at expiration of said lease period,

reallocating the IP address for said lease period when a positive address use verification response is received from the mobile host,

deleting the IP address allocation when no positive address use verification request is received.

7. The method according to claim 6, characterized by the steps of

sending, in response to said positive address use verification response, an address renewing request to said remote address allocation server,

renewing said second lease period for said IP address at said remote address allocation server,

sending an address renewing response to the serving mobile exchange.

8. The method according to claim 1, 2 or 3, characterized by the steps of

providing an address allocation protocol (DAAP) client at the mobile host,
providing an address allocation protocol server at said allocation server,
establishing a logical connection between the DAAP client and the DAAP server,
using an end-to-end DAAP protocol over said logical connection between the DAAP client and the DAAP server.

9. The method according to claim 8, characterized by a step of
   a serving mobile exchange which is not able to provide an IP address for the requesting mobile host locally acting as a proxy forwarding communication between a remote DAAP server and the DAAP client.

10. The method according to claim 8 or 9, characterized by the steps of
   sending an address use renew message from the DAAP client to the DAAP server in response to an expiration of a predetermined portion of said lease period,
   renewing said lease period for said IP address at said DAAP server,
   sending an address renewing response to the DAAP client,
   resetting a lease period timer at the DAAP client in response to a receipt of a positive response,
   removing the IP address at the serving mobile exchange. DAAP client in response to a receipt of a negative response or no response.

11. The method according to claim 10, characterized in that the user identity is a mobile subscriber identity (SSI) and the data equipment identity is a network service point access identifier (NSAPI).

12. A mobile communication network, comprising
a plurality of mobile hosts (MH),
mobile exchanges (DXT1,DXT2), and
an Internet Protocol-type, or IP-type, service for the mobile hosts,
characterized in that
at least one of the mobile exchanges (DXT1, DXT2) is arranged to dynamically allocate an IP address to a mobile host (MH) from an address space of the mobile communications network for a lease period and to associate the allocated IP address with a user identity (SSI) and a data equipment
identity (NSAPI) used for identifying the mobile host (MH) in the mobile communication system.

13. The network according to claim 12, characterized in that the user identity is a mobile subscriber identity (SSI) and the data equipment identity is a network service point access identifier (NSAPI).
### Fig. 3

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Location DXT</th>
<th>Static/Dynamic</th>
<th>User Identifier</th>
<th>NSAPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.1.1.1</td>
<td>DXT2</td>
<td>S</td>
<td>SSI A</td>
<td>NSAPI 1</td>
</tr>
<tr>
<td>192.1.1.52</td>
<td>DXT3</td>
<td>D</td>
<td>SSI A</td>
<td>NSAPI 2</td>
</tr>
<tr>
<td>192.1.1.62</td>
<td>DXT4</td>
<td>D</td>
<td>SSI B</td>
<td>NSAPI 1</td>
</tr>
</tbody>
</table>

### Fig. 4

1. Host
2. IP Context Manager
3. Allocate ip context
4. ip address response
5. Lease ip address for lease period
6. ip address request
7. ip address response

### Fig. 5

1. Host
2. IP Context Manager
3. Allocate ip context
4. ip address response
5. Lease ip address for lease period
6. ip address request
7. ip address response

### Fig. 6

1. Host
2. IP Context Manager
3. Allocate ip context
4. ip address response
5. Lease ip address for lease period
6. ip address request
7. ip address response
INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00674

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/22, H04Q 7/38, H04L 12/28
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)

IPC7: H04Q, H04L

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

SE, DK, FI, NO classes as above

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5708655 A (TOTH ET AL.), 13 January 1998 (13.01.98), column 7, line 41 - line 46; column 8, line 12 - line 15; column 19, line 34 - line 44</td>
<td>1-5, 8, 9, 12, 13</td>
</tr>
<tr>
<td>E,X</td>
<td>WO 0059252 A1 (NOKIA NETWORKS OY), 5 October 2000 (05.10.00), page 10, line 13 - page 12, line 36, figures 1, 2</td>
<td>1-4, 8, 9, 12, 13</td>
</tr>
<tr>
<td>A</td>
<td>WO 9921379 A1 (TELEFONAKTIEBOLaget LM ERICSSON (PUBL)), 29 April 1999 (29.04.99), page 4, line 16 - page 5, line 30; page 7, line 30 - page 8, line 26</td>
<td>1-13</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

Date of the actual completion of the international search: 5 December 2000

Date of mailing of the international search report: 08-12-2000

Form PCT/ISA/210 (second sheet) (July 1998)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>EP 0483547 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 6 May 1992 (06.05.92), column 6, line 51 - column 7, line 32; column 8, line 35 - column 10, line 21</td>
<td>1-13</td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (continuation of second sheet) (July 1998)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 5708655 A</td>
<td>13/01/98</td>
<td>AU 718114 B</td>
<td>06/04/00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 3199797 A</td>
<td>07/01/98</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9709572 A</td>
<td>10/08/99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2257981 A</td>
<td>18/12/97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1228228 A</td>
<td>08/09/99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0904665 A</td>
<td>31/03/99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9748246 A</td>
<td>18/12/97</td>
</tr>
<tr>
<td>WO 0059252 A1</td>
<td>05/10/00</td>
<td>FI 990694 D</td>
<td>00/00/00</td>
</tr>
<tr>
<td>WO 9921379 A1</td>
<td>29/04/99</td>
<td>AU 9562498 A</td>
<td>10/05/99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 0009108 D</td>
<td>00/00/00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2346515 A</td>
<td>09/08/00</td>
</tr>
<tr>
<td>WO 9832301 A1</td>
<td>23/07/98</td>
<td>AU 5684698 A</td>
<td>07/08/98</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9806769 A</td>
<td>16/05/00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1250578 T</td>
<td>12/04/00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0953265 A</td>
<td>03/11/99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6061346 A</td>
<td>09/05/00</td>
</tr>
<tr>
<td>EP 0483547 A1</td>
<td>06/05/92</td>
<td>DE 69119353 D,T</td>
<td>07/11/96</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2516291 B</td>
<td>24/07/96</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4227149 A</td>
<td>17/08/92</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 5159592 A</td>
<td>27/10/92</td>
</tr>
</tbody>
</table>