Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 76 (1998)

Heft: 7-8

Artikel: New internet service opportunities offered by Mobile-IP

Autor: Jung, Pierre

DOI: https://doi.org/10.5169/seals-877310

From the Exploration-Programmes of Corporate Technology (3)

New Internet Service Opportunities offered by Mobile-IP

The proposed standard "Mobile-IP" offers the opportunity for a new type of mobile IP services. Whereas today, a mobile user may already rather easily establish a connection to any user on the fixed IP-network, it is not possible to access a mobile IP-user without knowing at which point of the fixed IP-network he is connected to. In the near future, Mobile-IP will allow accessing any user without having to care whether he is underway or connected to his home network.

PIERRE JUNG, BERNE

Let us start with the present situation of mobile data services. Today, Internet mobile services mostly appear as "polling services". As soon as the mobile user has spare time (e.g., back in the hotel room after a conference), he logs onto his home network via a modem (eventually a mobile GSM data modem) and retrieves his information (typically E-mail and Scheduling information) from his home network. We will refer to the mobility underlying this kind of minimal and unidirectional (communication initiated by the mobile user) service provision as "nomadic mobility".
We now want to introduce a new vision of Internet services, providing a lot of added value for the customer. Let us consider the situation, where a mobile user is a VIP who needs to be warned immediately of the presence of new information destined to him and the latter should most probably be forwarded to him. In other words, this information needs here to be "pushed" to this mobile user. In order to provide such new services, we need a new kind of Internet mobility, which we will refer to as "true network mobility".
The latter bi-directional service vision closely relies on the notion of mobile user "accessibility". In this paper, we will see why the notion of accessibility is not yet efficiently supported in the Internet with the widely deployed protocol IPv4 and how we can solve this problem with the implementation of Mobile-IP.

Typical Usage Scenarios

In our project, we concentrate on three concrete secure mobile services where both the aspects of security, in terms of authentication and encryption and those of a bi-directional mobile IP communication are of central interest. The fact, that users are allowed to be mobile, makes security a more complex issue. Therefore, security and mobility aspects have to be considered together.
The first service considered is a secure mobile centralised scheduler service with remote warning and reply feature, based on e.g., the Lotus Notes Calendar or Microsoft-Scheduler, which every authenticated customer can access, and where he can modify company-shared scheduling data. The other users (whether mobile or not) get informed of the modifications if they are concerned. The customer's platform for such a service could be a palm-top computer or a Personal Digital Assistant (PDA) like the Palm Pilot from 3Com and IBM. The latter pocket computer would then be switched in standby mode until a warning notice arrives. The mobile user may then either reply immediately or later. While moving around, the system must be able to switch from one network to another, or even change the service provider, requiring a connection to the new network, discard the old one and be authenticated again for seamlessly providing this service.
The second service considered is a secure mobile centralimed priority E-mail service, e.g., Lotus Notes Mail or Microsoft-Exchange Mail, where the customer gets informed as soon as new mail arrives, and may retrieve it. As previously, this service may run on a customer's small-sized pocket computer operating in stand-by mode for providing a full accessibility.
The third service involves a secure communication between two mobiles in a foreign network. A typical application would be to send messages from one mobile to another; the latter warning the customer of the message arrival so that

Within the frame of the exploration programme* EP97-3, called "Internet Services", we watch the technology trends in the Internet world in order to get aware of new business opportunities for Swisscom. In the fast growing Internet, innovation is going on at a speed never seen before and mostly at a global scale. Nevertheless, medium-term trends can be observed, such as: demand for guaranteed quality of service, demand for an easy-to-use terminal, the forming of virtual communities of common interests and related business, or the demand for mobile IP services, described in the attached paper.

* Exploration programmes are carried out by Corporate Technology. They are approved by the Konzernleitung and are regularly reviewed. The activities are scheduled to meet medium- to long-term demands of Swisscom (two to seven years from now).

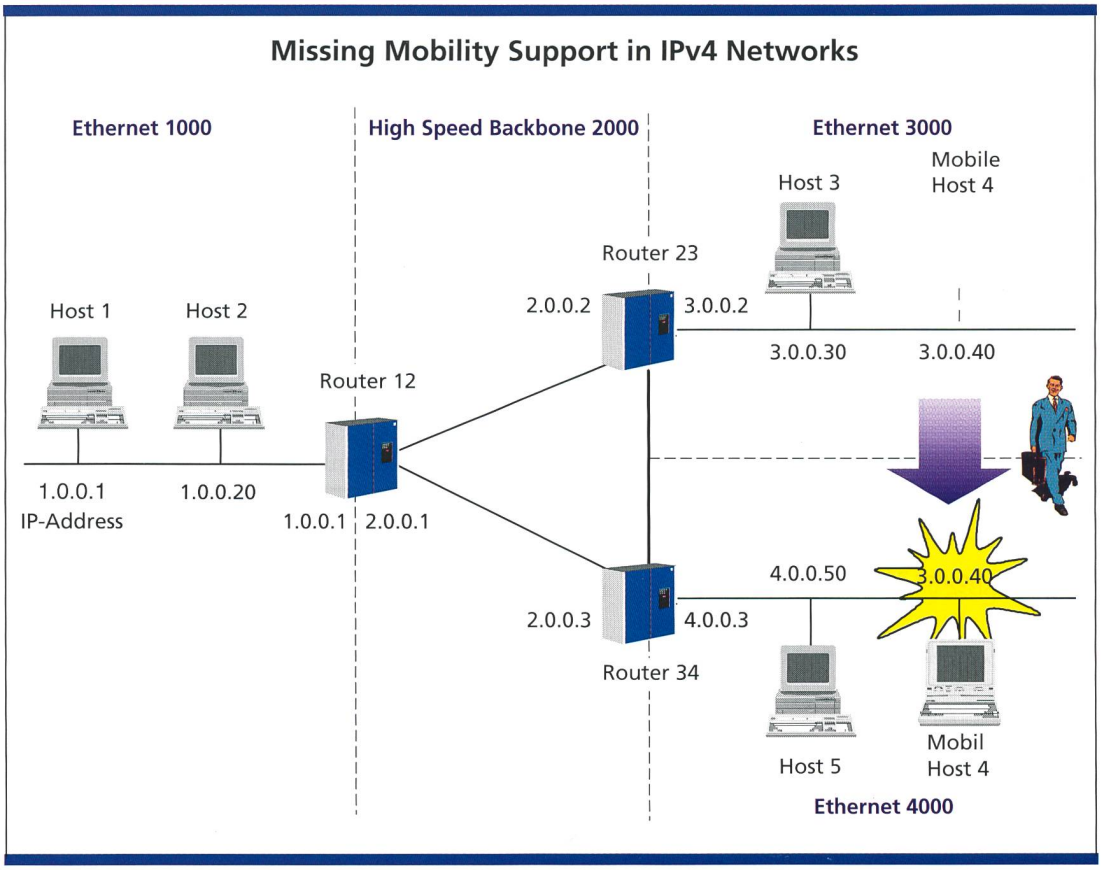

Figure 1. Mobile host 4 looses its connectivity in both originating and terminating directions, while moving in a classical IPv4 network environment.

he may reply immediately. The goal of this task is mostly to figure out and to analyse situations where the security and mobility protocols may "interfere" with each other.

IP Routing Fundamentals

For already a long time, the version 4 of the Internet Protocol (IPv4) has been used in the Internet. There is a broad consensus about the next generation of the Internet protocol, called IPv6. IPv6 will provide some support for mobile nodes. Nevertheless, we will still have to deal for years with IPv4. Therefore, in this paper, we consider IPv4 to be the Internet protocol in use.

IP addresses consist of two parts: the network prefix, followed by the host address. The total length of the address is fixed, but the division between network prefix and host address can be configured as desired. This means that a short network prefix corresponds to a large network (big address space for hosts available), whereas a long network prefix corresponds to a small network. Network addresses are not distributed randomly, but in a hierarchical way.

Between different networks, we have so called routers connecting the latter together. These routers maintain routing tables, telling them which networks can be accessed through any of the router's physical ports. So, when a router receives an IP packet, it will compare the destination address of the packet with the entries in its routing table. The router will then choose the route with the longest matching network prefix. This might even be the route directly to the host, in case of a full match between destination address and routing table entry.

The entries of these tables may be carried out manually or dynamically, based on automatic routing information exchange. In the latter procedure, after an initial configuration, the routers discover their neighbours and thereafter begin to interchange information about known routes via routing updates. When a router sends a routing update to another router claiming that it can reach several addresses, that router is "advertising accessibility" to these target addresses.

Now, let us analyse what happens when a node is moved from one network to another while keeping its fixed IP address, and without network-layer support for mobility. In IP networks, packets destined to a specific address will be routed towards the router which advertises accessibility to the network-prefix of that address. Thus if such a node moves away from the router which advertised its accessibility, the packets will still be attracted by that router, but can no longer be delivered to the mobile node. The packets are discarded and a corresponding Internet Control Management Protocol ICMP message is sent back to the source of the packet. This situation is represented in figure 1, where a mobile host 4 looses its connectivity in both originating and terminating directions, while moving in a classical IPv4 network environment from Ethernet 3000 to Ethernet 4000 and keeping its original IP-Address 3.0.0.40.

In other words, with classical IP routing, a node must not move from one network to another without changing the network-prefix of its IP address in order to reflect its attachment to the new network. Unfortunately, overlaying protocols (TCP, UDP) do not allow to change the IP address during an ongoing session. Therefore, we need new routing mechanisms to provide the feature for a mobile node to communicate and to be accessible while it moves from one network to another.

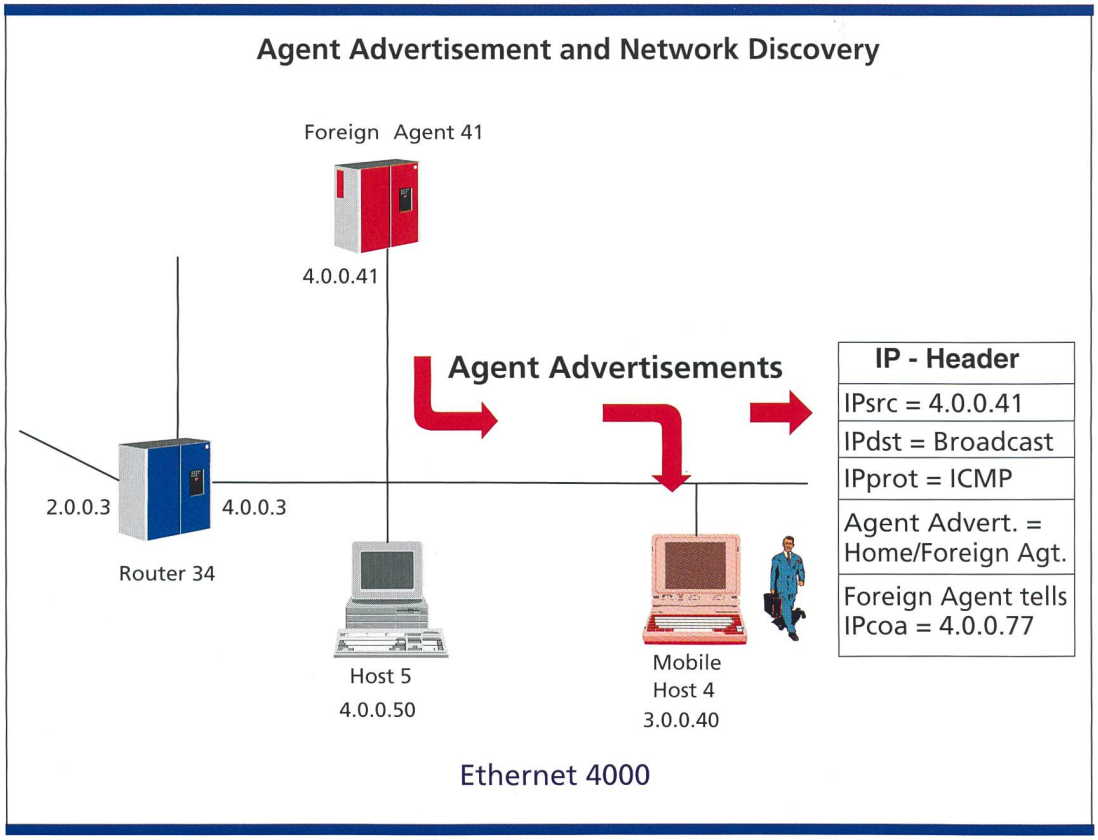

Figure 2. Foreign agent 41 broadcasts agent advertisement messages. Mobile host examines the advertisement and, since detecting a foreign network, it gets the foreign agent's care-of address.

True Network Mobility vs. Nomadic Mobility

In Nomadic Mobility, communications are basically initiated by the mobile node. Nomadic mobility is primarily not conceived for communications towards the mobile user. The mobile user has to log-on and start his communications applications each time he accesses a different network (either a geographically different network or the same network but interfaced through a another media), and he needs to get a fixed IP-address each time. As the mobile user moves out of the range of his link layer connection, he will have to log-on and start his communications applications again, even if he simply wants to remain remotely connected to the same network. Nomadic mobility is already widely available in many operating systems, e.g., Microsoft Windows, Apple OS, IBM, or Linux. They convey the IP data from the applications over the Point-to-Point Protocol (PPP), itself running on top of the link layer, which is very often composed of a GSM data modem connected to a GSM mobile phone.

This solution is sufficient if the mobile-user does not need to connect often to his home network and if he does not need seamless mobility, i.e., being accessible at anytime and anywhere on the globe under the same IP address. But as soon as other users (either fixed or mobile) need to communicate with the mobile user, or the mobile user needs to change the link layer during a session, nomadic mobility is no longer sufficient and only true network mobility is the solution.

By True Network Mobility, we mean the mobile node being able to communicate with one sole permanent IP address without dropping the ongoing communication while moving from one network to another. On top of mobile originated communications as described in the section above, the true network mobility allows any other users in the network to initiate communications towards the mobile user. True mobility allows the mobile user to remain connected while changing the network and to keep the same IP-address. True mobility may be implemented with Mobile-IP, an IETF (Internet Engineering Task Force) standard of which the first part has just been finalised. True mobility is preferable to nomadic mobility in many cases such as applications basing on IP address databases, e.g., network licensing systems relying on a range of IP-addresses or security-related applications.

Mobile-IP

Mobile-IP addresses the network-layer mobility and has been published by the Internet Engineering Steering Group (IESG) in November 1996 as a proposed standard. It was developed by the IP Routing for Mobile Hosts (Mobile-IP) working group of the Internet Engineering Task Force (IETF), which was formed in June 1992. Mobile-IP is a scaleable and robust solution for true mobility, allowing to maintain ongoing communications.

Mobile-IP is a network-layer solution for node mobility in the Internet. Mobile-IP sets up routing tables only in some appropriate nodes, such that IP-packets can be sent to mobile nodes not connected to their home network. As a network-layer protocol, Mobile-IP is completely independent of the media (link-layer) over which it runs. It is therefore able to switch from one type of media to another without loosing connectivity, e.g., moving from an Ethernet connection to a Wireless LAN based connection without service disruption for the communications application.

Mobile-IP solves the problem of routing IP-packets to mobile nodes. It is not yet a complete solution for mobility since enhancements on other, higher, levels of the OSI- communications protocol stack still need to be performed, e.g., modifications on the Transport Control Protocol (TCP), taking into account the raw bandwidth, the bit error rate, and the congestion rate on the lower OSI layers for improving the overall system performance.
The three most important characteristics of Mobile-IP are:

- The ability for a mobile node to communicate with other nodes after changing its point of attachment in the Internet by using only its home (permanent) IP-address, regardless of the point of attachment to the Internet.
- The ability to communicate with other computers, that do not have an implementation of the Mobile-IP protocol. In other words, no protocol changes are needed on fixed hosts and routers.
- Some protection against new security threads due to mobility. Specifically, Mobile-IP is designed to prevent trivial denial of service attacks from hackers by a basic authentication mechanism.

Mobile-IP has been designed also in order to comply with expensive and/or slow wireless links. As a routing protocol, Mobile-IP requires routing updates between the various nodes implied in the mobile communication. The size of the corresponding messages as well as their frequency has therefore been reduced to a minimum. On the other hand, the mobile node processes have been designed as simple as possible, in order to implement them on very low-power small devices like Personal Data Assistants (PDAs), smart cellular phones or palmtop computers.
Mobile-IP assumes that unicast packets, i.e., packets destined to a single recipient, are routed without regard to their IP source address, thus only routed, based upon their IP-destination address. It furthermore makes use of the routing functionalities available in the Internet infrastructure as well as of its underlying scaleability in order to be used by a large number of users.
In order to understand the concept of Mobile-IP, we have to define some expressions:

Home Address
The home network initially assigns the Mobile Node a permanent IP address, the home address. This address does not

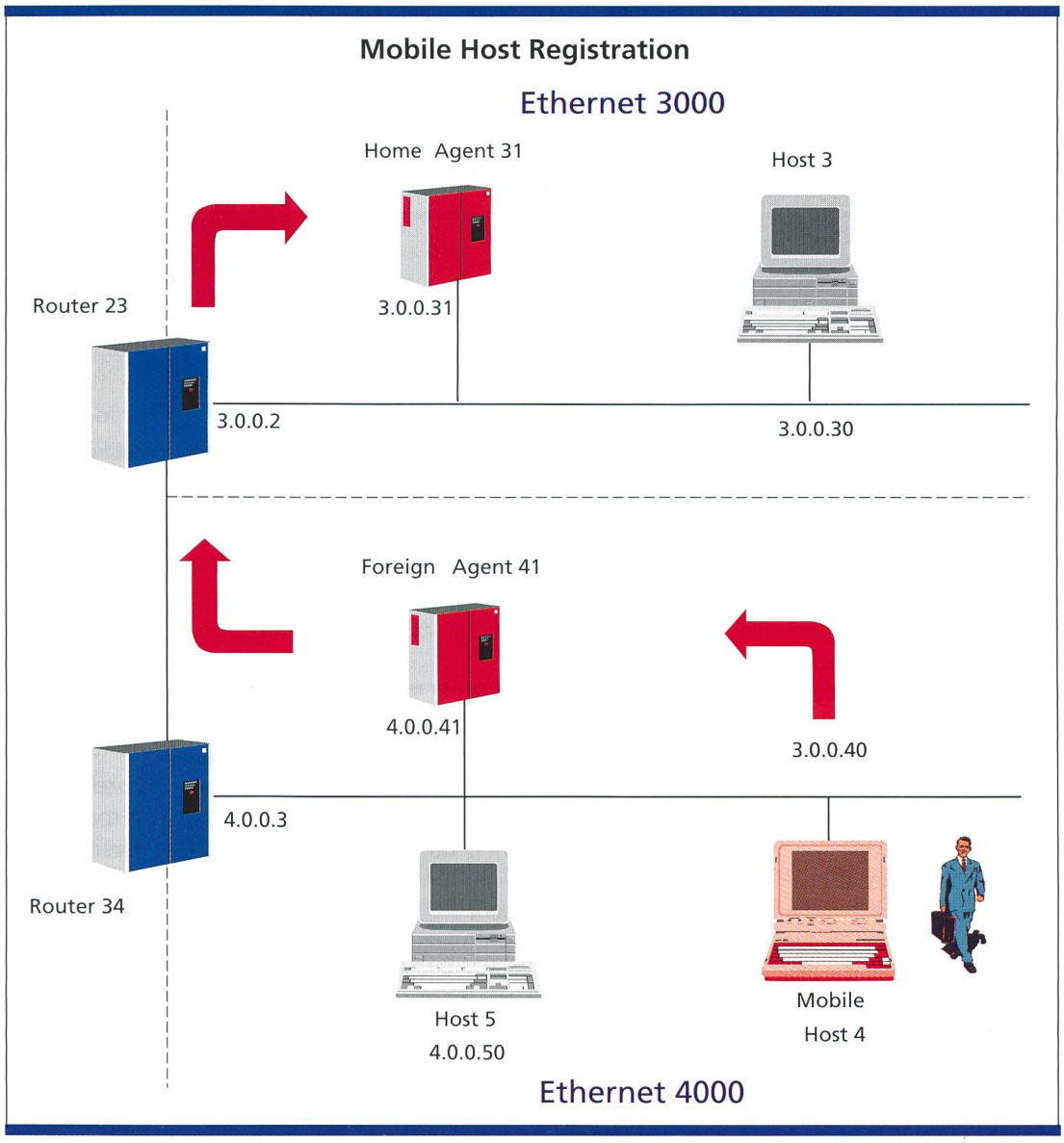

Figure 3. The mobile host registers the care-of address just acquired in the previous step to his home agent.

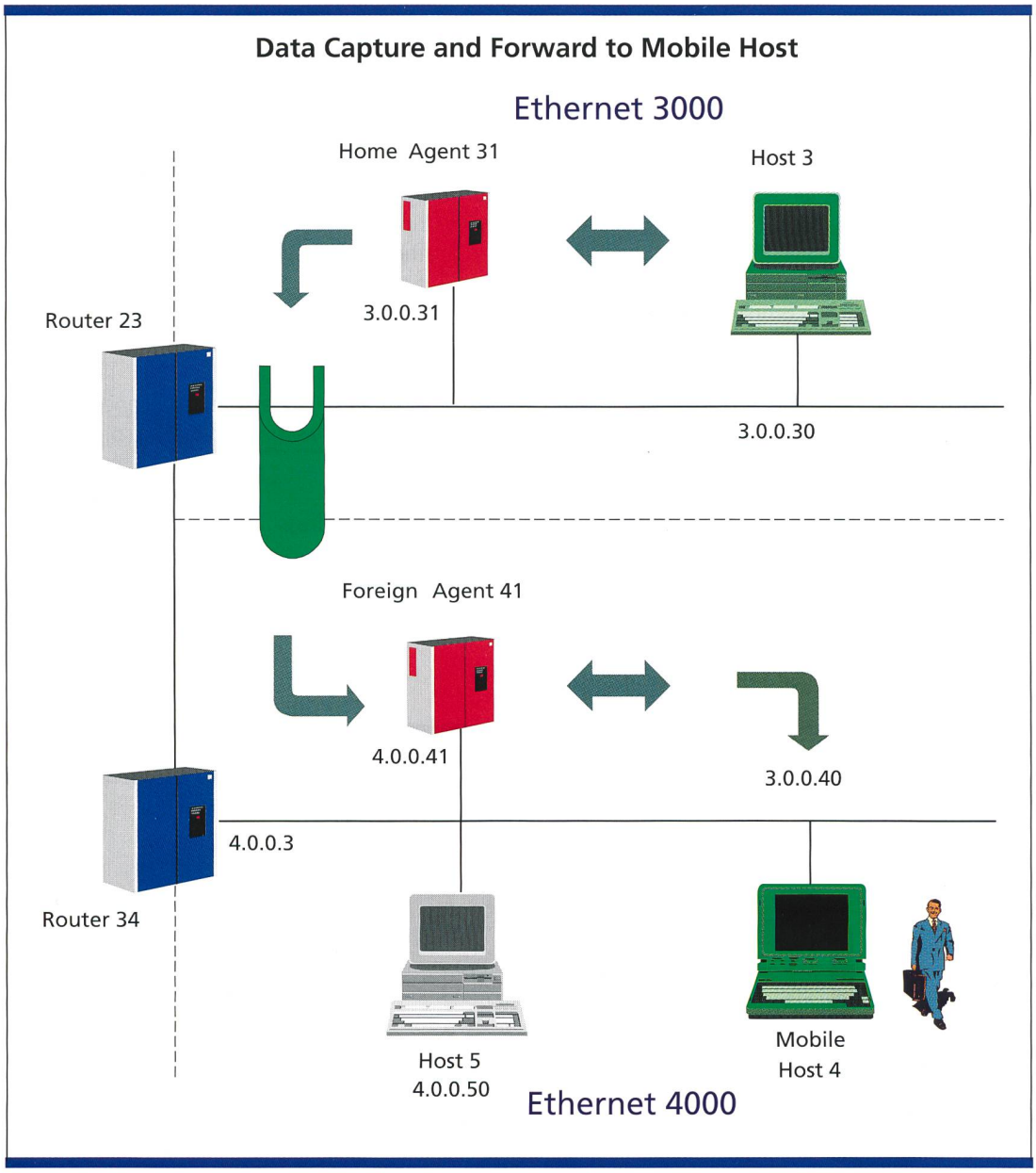

Figure 4. The home agent intercepts the packets destined to the mobile host and tunnels them to it via its acquired the care-of address.

change while the Mobile Node moves from network to network. The network-prefix of this address defines the home network. In virtually any communication with other nodes, the Mobile Node uses its home address.

Care-of Address
The care-of address is an IP address associated with a Mobile Node that is visiting a foreign network. It is specific to that foreign network and it changes every time the Mobile Node moves from one foreign network to another. A care-of address is almost never used as the IP source or destination address during a data communication.

We identify the most important components:
Mobile Node
A node which may change its point of attachment to the Internet from one network to another while maintaining ongoing communications and using only its permanent IP home address.

Home Agent
A router with an interface on the mobile node's home network. The Home Agent is always kept informed about the current location of the Mobile Node. This information is stored as the care-of address of the Mobile Node. The Home Agent is responsible for attracting packets destined to the Mobile Node's home address and for tunnelling them to the Mobile Node's current location; i.e., to the Mobile Node's care-of address.

Foreign Agent
A router on the Mobile Node's current foreign network. The Foreign Agent assists the Mobile Node in informing its Home Agent of its current care-of address. It provides a care-of address to the Mobile Node and de-tunnels packets for that Mobile Node, which have been tunnelled by its Home Agent. It serves as a default router for packages generated by the node while connected to this foreign network.

Home Agents and Mobile Nodes are usually operated by the same administrative entity. Foreign Agents, however, may typically be owned and/or administrated by Internet service providers, as soon as an offsite mobility is required.

Routing with Mobile-IP

A new connection between a mobile node (also called host) moving to a new network is established in a step-by-step way as follows:

- Home agents and foreign agents advertise their presence on their attached networks by periodically broadcasting special messages called Agent Advertisements. This is depicted in figure 2, where foreign agent 41 broadcasts Agent Advertisement messages to all the nodes on Ethernet 4000, telling the availability of a Mobile-IP service.
- Mobile nodes listen to these Agent Advertisements and examine their contents in order to determine whether they are connected to their home network or to a foreign network. While connected its home network, a mobile node acts as stationary node, without making use of any other Mobile-IP functionality. The message header which is examined appears on the right of figure 2, where mobile host 4 examines the advertisement of foreign agent 41. It determines that is on a the foreign Ethernet 4000 network and gets foreign agent's 41 care-of address, i.e., 4.0.0.41.
- The mobile node registers the care-of address (4.0.0.41) just acquired in the previous step to his home agent 31, as appears in figure 3. If available, the mobile host uses the foreign agent to assist it in the registration procedure. An authentication phase will take place in order to prevent remote denial-of-service type attacks from hackers.
- Home agent 31 advertises the accessibility of mobile host 4, as if the latter would be attached to its home network. Doing this, packets sent to the mobile node are sent to its home network. The home agent intercepts these packets, and tunnels them to the care-of address of the mobile node as depicted in figure 4.
- At the care-of address, the packets are extracted from the tunnel and are delivered to the mobile node.
- In the reverse direction, packets sent from the mobile are directly routed to their destination, with the foreign agent serving as the default router for all packets generated by the visiting mobile node. In the case this is not allowed on the foreign network, the messages use a reverse tunnel to the home agent and are forwarded from there on to their destination.

Conclusions

In this paper, we introduced an innovative concept for the mobility, considering the two-way feature for initiating a communication. In nomadic mobility (the classical way), the mobile user initiates his data retrieval (polling) when he thinks of it. In true network mobility, the mobile user is reachable across networks, under a single, fixed IP-address. In the latter case, the data communication is no more only an information polling but data can be sent to the mobile user whenever it is necessary (scheduling information, priority E-mail, ...).

We briefly described the routing problems caused mobile users moving across networks within the existing IP-world and how the latter problems could be solved by Mobile-IP.

The new Mobile-IP proposed protocol solves the routing problem already in existing IPv4 networks with a very little amount of supplemental resources (3 supplemental components). Upwards, it has been integrated in IPv6 and downwards, it is fully compatible with older IPv4 networks that do not support Mobile-IP, it is scaleable, and a provision for basic security mechanisms has been provided. The security issues (authentication and privacy and network protection) are very important aspects where research is ongoing.

These topics are currently being investigated in several Exploration- and Application Projects at Swisscom Corporate Information and Technology in Berne.

References

Perkins C., ed., IP-Mobility Support IETF RFC-2002, Oct 1996.

Perkins C., Mobile-IP, IEEE Communications, Vol. 35 N° 5, 1997.

Perkins C., Mobile Networking through Mobile-IP, IEEE Internet Computing, Jan./Feb. 1998.

Zusammenfassung

Mit dem vorgeschlagenen Standard «Mobile-IP» ergeben sich Möglichkeiten für eine neue Klasse von IP-Diensten für mobile Benutzer. Während es bereits problemlos möglich ist, eine Verbindung von einem mobilen Benutzer zu irgendeinem Benutzer am festen IP-Netz aufzubauen, ist es heute noch nicht möglich, einen mobilen Benutzer zu erreichen, ohne den genauen Ort seiner Anbindung an das feste IP-Netz zu kennen. In naher Zukunft wird uns Mobile-IP aber ermöglichen, jeden IP-Benutzer zu erreichen, ohne uns darum zu kümmern, ob er gerade mobil oder am festen IP-Netz angeschlossen ist.

Pierre Jung *received his diploma in Electrical Engineering at the Swiss Federal Institute of Technology (ETH), Lausanne, in 1986. He then joined Siemens-Albis in Zurich, where he was involved in the digital switch development area. He thereafter went to Ascom Radiocom, as responsible for the digital mobile radio technology transfer from Asea Brown Boveri Corporate Reseach Labs. In 1992, he joined Swisscom. Since then he has been project leader in several research and application projects in the field of Mobile Communications and Network Quality Management. He is currently leads the activities in the areas of Internet Service Enabling Technologies within the Internet Services Exploration Programme.*