Internet-To-Go, Now With Mobile IP

by Peter Rysavy
Published November 1, 1997, Network Computing

Two trends in the computing industry are converging. One is the expanding scope of the Internet. The other is the surge in use of mobile computers for telecommuters and other remote users. These workers need access to IP-based networks--both corporate intranets and the Internet at large. A new Internet standard, Mobile IP, will help keep mobile computers seamlessly connected, independent of location. And Mobile IP supports any underlying medium--wireless or wired.

Using distributed routing tables, Internet routers pass on IP datagrams based on IP address, part of which specifies the destination computer's subnet. This addressing scheme, however, prevents a computer with a fixed IP address from connecting to a different subnet. The simplest way around this is to not assign fixed IP addresses, and instead, let computers obtain an IP address dynamically by using DHCP, for example. This approach also simplifies the management of IP addresses.

But a temporary address has two major limitations: Other nodes cannot easily originate transmissions to the mobile node because they cannot effortlessly learn its new IP address, and each time a mobile computer obtains a new IP address, Internet client software applications must be restarted. If your TCP/IP stack engages DHCP only at startup, you'll have to restart it as well. Moreover, temporary addresses do not let you roam seamlessly from one IP subnet to another. This is a handicap especially for wireless LANs--a doctor with a wireless LAN connection needs to maintain IP connections throughout the hospital as he or she accesses patient records.

Mobile IP was invented to let hosts with a fixed IP address connect to any IP subnet and immediately be reachable from the Internet.

How It Works Mobile IP, an extension to IP, is a recent Internet standard specified in RFC 2002, "IP Mobility Support." The idea behind it is conceptually simple, though a number of complications may arise when using it. Mobile IP consists of three components: the mobile node, a home agent and a foreign agent. The mobile node is built into a TCP/IP stack or can exist as a "shim" under a TCP/IP stack. The home agent operates on a router or a workstation

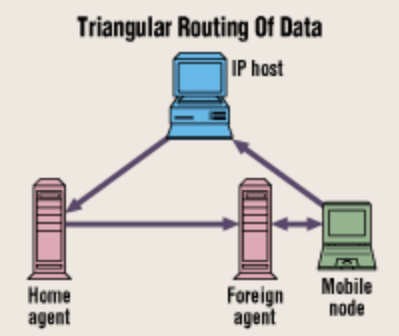
on the mobile node's home subnet. The foreign agent operates on a router or workstation on a foreign network where the mobile node is visiting, or on the mobile node itself under certain conditions. The beauty of Mobile IP is that these are the only elements required. No other changes are needed in any other part of the Internet, including routers or other systems, such as DNS.

When a mobile node comes up on a network, it first determines whether it is on its home network or on a foreign network. It does so by listening for a local broadcast message from a home agent or foreign agent. Alternatively, it can solicit an agent advertisement message. These initial and subsequent registration messages are based on extensions to Internet Control Message Protocol (ICMP) Router Discovery specified by RFC 1256.

When the mobile node is on its home subnet--the one specified by its IP address--the mobile node informs the home agent of its presence. From there, IP addressing and datagram delivery work as they would without Mobile IP. The situation changes when the mobile node connects to a foreign network. There it obtains a "care of address," which is the foreign agent's IP address. The mobile node registers with its home agent and gives the home agent its care of address. Alternatively, if DHCP is available on the foreign network, the mobile node can obtain a temporary address, register this with the home agent and act as its own foreign agent.

Once the mobile node has registered with the home agent, IP traffic addressed to the mobile node is received by the home agent, encapsulated in another IP datagram and then "tunneled" to the foreign agent. The foreign agent forwards the datagrams to the mobile node. Two forms of encapsulation are specified in related standards RFC 2003 (IP Encapsulation within IP) and 2004 (Minimal Encapsulation within IP).

In the reverse direction, the mobile node can bypass the home agent and send datagrams directly to their destination (see "Triangular Routing of Data,"). This results in a triangular routing of traffic, which is not necessarily efficient but is effective. In addition, when a mobile node changes its location, it can register with a new foreign agent, though traffic directed by the home agent to the "old" foreign agent will be lost until the new mobile node has registered its location.



The home agent must know that the mobile node is legitimate, so security is an important issue with Mobile IP. Similarly, the mobile node must be able to trust the home agent. IPsec, a series of Internet security standards, can be used in conjunction with Mobile IP to provide authentication and encryption.

Is It for You? So, should you rush out and get Mobile IP? First ask yourself how often you connect into another company's network. When were you last able to jack into a network, other than by using a phone connection, in your hotel room or at the airport? As desirable as this might be, it is not yet an option. Mobile network connections are not part of mainstream computing today, but as the demand for connections to the Internet increases, that will likely change.

A more immediate need for many companies is to allow their workers to connect to the corporate network from other locations--such as a different building on a campus or at a remote office. Mobile IP makes this possible. Meanwhile, Mobile IP is increasingly being used in specialized applications, particularly vertical market applications involving wireless LANs, such as car rental depots, freight handling and supermarket inventory.

Mobile IP also is being designed into the infrastructure of some new wireless WANs. Cellular Digital Packet Data (CDPD), the dominant wireless WAN that routes IP, provides its own IP mobility service. Like Mobile IP, it forwards packets from a home network to a foreign network.

You should consider Mobile IP if you have computers that need to stay connected with IP applications running as they roam from one subnet to another.

Using Mobile IP Mobile IP is easy to use, but, unfortunately, few commercial implementations of it exist. FTP Software, the only company currently offering Mobile IP, combines the home agent and foreign agent into one Windows application as part of its Secure Client 3.0. A workstation is required to house the home agent, and one is needed for the foreign agent at every network the mobile node will visit.

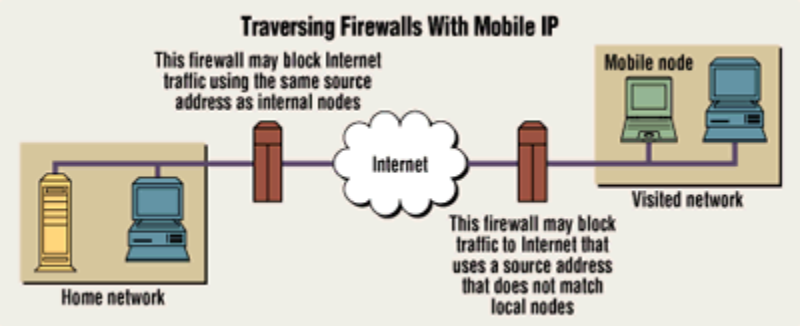
Using a different approach, Telxon Corp. has integrated home and foreign agents directly into Aironet Wireless LAN access points. To configure Mobile IP, you specify the home agent and security parameters at the mobile node and a list of authorized mobile nodes at the home agent. You also can specify mobile node authentication information at each foreign agent.

Once demand for Mobile IP increases, vendors can build home and foreign agents directly into routers, though no such products have been announced. This would simplify Mobile IP's use, since all you would need is the mobile node. Keep in mind that while the Mobile IP standard has been completed, revisions are under way, and work on related standards is continuing. Until all this work is done, you may run into compatibility problems among products.

Keeping Connections Secure The biggest issue facing Mobile IP is security. Strong authentication is needed because the mobile node may be accessing corporate resources from

the Internet. Fortunately, standards are available for authentication. For example, FTP Software's Mobile IP implementation provides mutual authentication of the mobile node and the home agent.

The thornier security problem is one of traversing firewalls. This problem is twofold because it involves firewalls both at the home network and at the foreign network. Many firewalls rely on packet filtering to implement some or all of their security. If the mobile node is trying to communicate with the home agent or other hosts on its home network, the firewall there may reject datagrams from the mobile node because the datagrams have the source address of an internal node, but appear on an external port (see "Traversing Firewalls With Mobile IP").



A similar problem can occur at the foreign network. Many firewalls are configured so that they will not pass datagrams from inside a network to the Internet if the source address differs from what is expected. The intent is to prevent the internal network from being a haven for malicious users spoofing source addresses and perpetrating mischief on the Internet. Unfortunately, the Mobile IP node's address does not belong on the internal network, so its transmissions may be blocked.

Although these firewall problems usually will arise during Internet communication, they also may come up in corporate intranets as companies increase their use of internal firewalls. For instance, you may need to configure the firewall protecting the home network to allow ICMP datagrams addressed to the home agent, which will allow the mobile node to register its new location.

Going Places Mobile IP is not standing still. The core standard may be done, but a revision is in the works, and work is continuing with related standards to address security, improve routing efficiency and provide mobility in IPv6. In fact, most of Mobile IP is incorporated into IPv6. This inclusion, along with other enhancements to IPv6, will result in excellent support for mobile devices. For example, IPv6 will let Internet nodes associate a mobile node's home address with its care of address and send packets directly to the care of address rather than via the home address. This will eliminate any triangular routing.

Another IPv6 improvement comes from two associated standards, "Neighbor Discovery for IP Version 6" (RFC 1970) and "IPv6 Stateless Address Autoconfiguration" (RFC 1971). These ensure that a mobile node can obtain a care of address, eliminating the requirement for foreign

agents. Yet another improvement relates to the standard "IP Authentication Header" (RFC 1826), which will assure fixed nodes that messages from a mobile node are authentic--something that is particularly important if the message includes crucial information such as a new care of address.

Should you wait for IPv6 to be deployed before looking at mobility? No. Your need to support mobile workers working at multiple locations will probably grow faster than your need for IPv6. The good news is that mobility protocols for IPv4 and IPv6 are nearly identical, so migrating from one to the another should be relatively straightforward.