Mobile Internet Protocol in the Solaris™ 9 Operating Environment

Enabling mobile devices to use two IP addresses.

Sun™ ONE
Open Net Environment

Sun microsystems

Key feature highlights

Enables transparent access to the Internet from wired and wireless devices, such as laptops, PDAs, handhelds, and digital cellular phones.

Allows users to roam through and beyond their enterprise, while maintaining their home IP address.

Delivers enhanced server availability.

Adheres to IETF standards.

Enables seamless communication in various locations.

Easy to configure and use.

Today's explosive levels of growth — in terms of bandwidth, networks, and digital devices — are driving an even greater shift towards a services model of computing. The Services on Demand approach moves the burden of a computing infrastructure from end users and their PCs to the organizations that provide the services. Since its inception in 1982, Sun has been driven by a singular vision — The Network Is The Computer™ — and has helped businesses harness the transforming power of the network in order to create, deploy, and deliver reliable Services on Demand.

As the foundation for the Sun™ Open Net Environment (Sun ONE) — Sun's vision, architecture, platform, and expertise for delivering Services on Demand — the Solaris™ 9 Operating Environment provides an integrated yet open architecture for building and deploying Services on Demand. The Solaris 9 Operating Environment (OE) offers new levels of performance in scalability, availability, manageability, and security, and delivers a complete and highly refined environment designed to enable customers to increase service levels while decreasing costs and reducing IT risks.

Mobile Internet Protocol (IP)

Mobile IP enables the transfer of information between mobile computers — laptops, personal digital assistants (PDAs), wireless Internet devices, etc. With Mobile IP, a mobile computer can change its location to a foreign network and still be able to communicate as if it were located on its home network.

Current versions of the Internet Protocol (IP) assume that the point at which a computer connects to the Internet or a network is fixed, and that the IP address of the computer identifies the network to which the computer is attached. Due to these assumptions, datagrams are sent to a computer based on the location information contained in the IP address.

Many of today's widely-deployed internet protocols require that a node's IP address remain unchanged. This means that if a computer or wireless device moves to a new network while keeping its IP address unchanged, the IP address no longer reflects the device's location. Consequently, network routing protocols cannot route datagrams to the device correctly. To communicate, the device would have to be reconfigured with a different IP address representing its new location every time it moves.

Besides being cumbersome, changing the address means the application will fail and will need to be restarted. Under the current Internet Protocol, if the device moves without changing its address, it loses routing. If the device does change its address, it loses any current connections.

Mobile IP solves this problem by allowing the mobile node to use two IP addresses. The first address is its normal home address. The second address is a "care-of address" that the device borrows at each new network location.

The Mobile IP feature in the Solaris Operating Environment facilitates the transfer of information between mobile computers — laptops, personal digital assistants (PDAs), wireless Internet devices, and more — by allowing them to have two addresses.

In this way, Mobile IP enables a mobile device to roam freely on the Internet while allowing it to use the same home address. Consequently, communication activities are not disrupted whenever the device changes its point of attachment because the device is provided with a valid IP address wherever it goes, and the network is provided with information about the device's new location.

Mobile IP Functional Entities

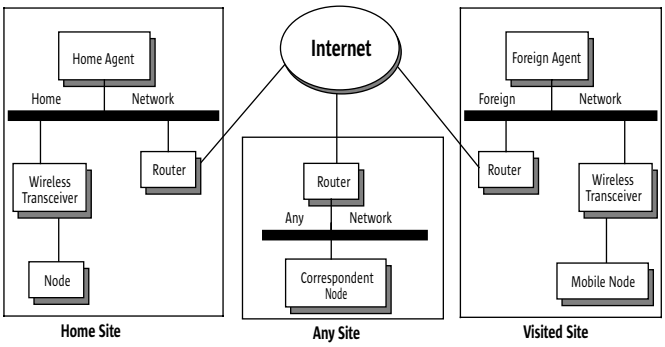
Mobile IP introduces new functional entities that include:

- A mobile node host or router that changes its point of attachment from one network to another
  - Maintains all existing communications by using its home IP address
- A home agent server or router on the home network of a mobile node
  - Intercepts datagrams that are destined for the mobile node
  - Maintains current information on the location of the mobile node
  - Delivers the datagrams to the care-of address
- A foreign agent server or router on the foreign network that the mobile node visits
  - Provides host routing services to the mobile node
  - Provides a care-of address to the mobile node
  - Provides "first-hop" routing services for the mobile node

Mobile IP Data Communication

The following diagram illustrates how a datagram moves from one point to another using Mobile IP.

Figure 1: Mobile IP Data Communication



By using the above illustration's Mobile IP topology, the following scenario shows how a datagram moves from one point to another within the Mobile IP framework.

- The correspondent node (node on any network) sends a datagram to the mobile node by using the mobile node's home address (normal IP communication).
- If the mobile node is not on its home network, the home agent knows to intercept the datagram.
- The home agent forwards the datagram to the foreign agent. The home agent must "tunnel" the datagram so that the foreign agent's IP address appears in the outer IP header.

- The network routes the datagram as it would any other datagram.
- The foreign agent receives the datagram, sees it contains the datagram originally addressed to the mobile node, and delivers it to the mobile node.
- Datagrams sent from the mobile node to its correspondent node are sent through the foreign agent by normal IP routing procedures. Either the foreign agent forwards the mobile node's datagram to its router as it would any other datagram, or if the agents are using a reverse tunnel, the foreign agent "tunnels" the mobile node's datagram to the home agent, which then sends it to the correspondent node exactly as it would any other datagram.

Reverse tunneling is used in cases where "Ingress Filtering" is present on any of the networks between the foreign agent and the correspondent node. Ingress Filtering provides defense from hackers and would cause the datagram to be discarded since its source address is easily identified as being foreign to that part of the network.

In the case of wireless communications, the illustration depicts the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all communications between the correspondent node and the mobile node use the home address of the mobile node, even when the mobile node is located on the foreign network. The care-of address is used only for communication with mobility agents, and is never seen by the correspondent node.

Solaris Mobile IP Implementation

Mobile IP has been available in the Solaris Operating Environment since June 2000. It supports IP version 4 (IPv4) and is easy to configure. Sun continues to track IETF standards and is committed to expanding Mobile IP functionality in the future.

Mobile IP for the Solaris Operating Environment supports the RFCs as defined by the IETF.

- RFC 2002: IP Mobility Support (Agent Only)
- RFC 2003: IP Encapsulation Within IP
- RFC 2794: Mobile IP Network Access Identifier Extension for IPv4
- RFC 3012: Mobile IP Challenge/Response Extensions
- RFC 3024: Limited Private Address and Reverse Tunneling Support for Mobile IP

The functionality in the following IETF drafts are also supported in the Solaris implementation of Mobile IP:

- IP Mobility Support for IPv4, Revised: draft-ietf-mobileip-rfc2002bis-03.txt
- Mobile IP Vendor/Organization-Specific Extensions: draft-ietf-mobileip-vendor-ext-09.txt

As part of a commitment to providing scalable, secure solutions to its users, the Solaris home and foreign agents support dynamic control of IPSec policies. Introduced in the Solaris 9 Operating Environment, this functionality enables authentication and encryption protection algorithms of mobile node traffic through IPSec.

The Solaris 9 Operating Environment also introduces foreign agent support for mobility advertisements and connection over dynamic interfaces. This feature is useful when a mobile node requests a connection through a newly created PPP interface.

Mobile Internet Protocol in the Solaris™ 9 Operating Environment

About Sun ONE

The Sun Open Net Environment (Sun ONE) is Sun's vision, architecture, platform, and expertise for delivering Services on Demand today and in the future. Based on open standards such as Java™ and XML technology, Sun ONE provides a highly scalable and robust framework for building and deploying a variety of Services on Demand — from traditional Web-based applications to future context-aware Web services. By simplifying the way Web services are created, assembled, and deployed, the Sun ONE platform can enhance productivity, speed time to market, and increase business opportunities for enterprises worldwide.

System Requirements

Mobile IP is a feature of the Solaris Operating Environment

For More Information

To learn more about Mobile IP and the Solaris 9 Operating Environment, visit sun.com/solaris.

Mobile IP-related questions can be sent to mobileip-questions@sun.com.

For additional information on Sun ONE, visit sun.com/sunone.

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA **Phone** 800 786-7638 or +1 512 434-1577 **Web** sun.com

We make the net work.

Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India–Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand–Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China–Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland–German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44 0 1252 420000, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800

5/02 DE1692-0