

# Cisco IOS Mobile IP

## *Enables Transparent Mobility*

—Stacey O'Rourke

### Executive Summary

The ability to provide ubiquitous mobility limited only by the scope of the Internet can be enabled with the availability of mobile IP in IOS™ software. This protocol provides users the ability to roam through and beyond their enterprise while maintaining their home IP address. This Internet Engineering Task Force (IETF) proposed standard protocol enables transparent routing of IP datagrams to mobile users despite their physical movement. The mobile IP protocol itself is very straightforward and based on IP tunneling. Valuable data can be constantly forwarded to mobile users wherever they roam. Packets originated by a mobile users can either be sent normally, without a tunneling requirement, or they can be forwarded back to a user's enterprise for increased security. The benefits of mobile IP include transparent mobility and the low per-packet overhead, which make this solution very attractive for wireless applications. Cisco Systems will be integrating mobile IP support in the IOS software Release 12.0(1)T.

### Background

#### Movement toward Boundless Networking

With the advent of new technologies the communications and networking paradigm is changing. The most important pieces of information reside on users' networks, with e-mail and Web servers containing all of the information needed for daily business operations. "Road warriors" are in need of connectivity to their home networks and the Internet from just about anywhere, and wireless services are sprouting up to meet this demand. Devices to enable these communications, such as personal digital assistants (PDAs), are getting smaller, smarter and more efficient. They are also more reliable in performing useful business functions with their extended battery lifetimes. The need for nonstop networking from areas where there is no wired connectivity is becoming a requirement for many users who find themselves away from their own networks. Cisco IOS software now provides the networking technology that will enable this cutting-edge connectivity.

#### Wireless Services

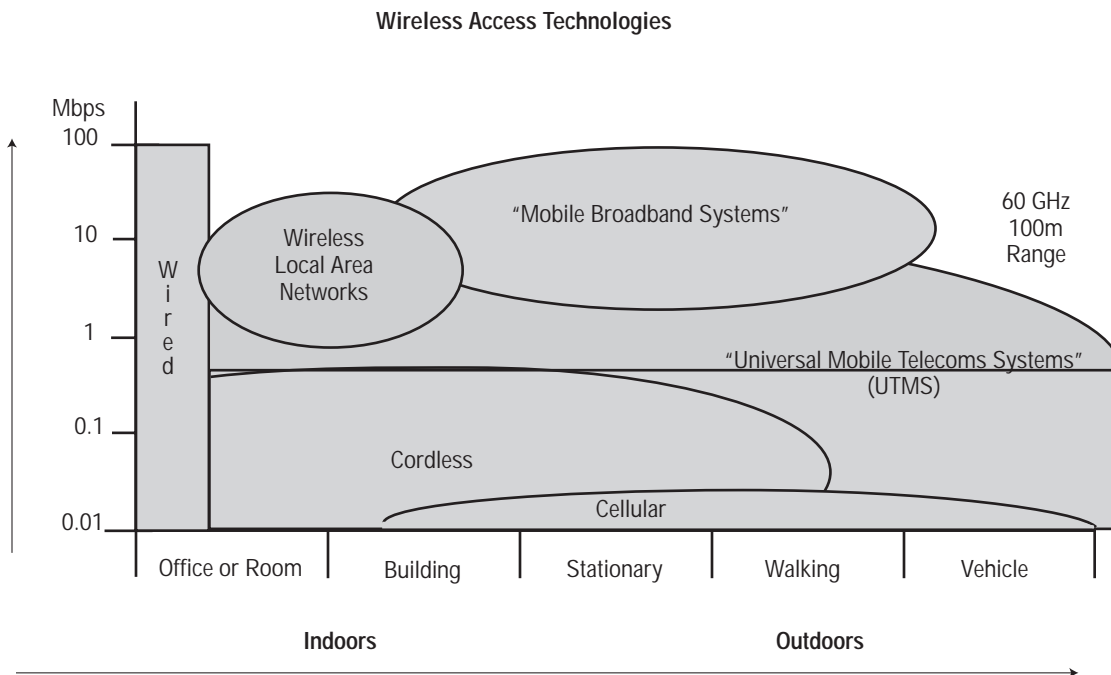
The applicability of mobile IP is not restricted to wireless applications. However, it is likely to be deployed in this arena first. It is an ideal way to enable data services unencumbered by the wired infrastructure. There are many wireless technologies that offer customers alternative data solutions from the low-earth orbit (LEO) satellite constellations currently being launched that offer traveling users voice and data services anywhere on the planet to the household wireless LAN. Some service providers are using microwave to offer local microwave distribution service (LMDS), multipoint microwave distribution service (MMDS), and similar services to users that include voice, data, and video functionality. Cellular technologies also offer voice and growing amounts of data service to customers to connect them to the Internet. Cellular phone networks are well established to support the voice needs of customers, and now these providers are anxious to start offering the data services that their users have long sought.

Although cellular service has been around for quite some time, only recently have technological advances allowed cellular service providers to offer compelling data services. The first generation of cellular data service is circuit-switched and utilizes resources in much the same way as traditional voice services. This type of service is inefficient at utilizing the carrier network, and more importantly, wasteful of scarce air-link resources. Further, the accompanying billing model is somewhat cost-prohibitive for the majority of subscribers. As second- and third-generation cellular offerings emerge, such as those being referred to as personal communication systems (PCS), the model is evolving into a packet-based data service, enabling better use of resources in the network and especially the air-link. Packet data enables more efficient use of the air-link which means per packet, rather than per circuit, consumer charging.


**Special Needs are Emerging**

With the advent of these new offerings and the availability of new devices, users are beginning to see real uses for these wireless services. These services can enable users to connect to their enterprise networks. While business professionals wait in airports, sit in conferences, commute on trains, or visit customers and vendors, they don't need to be out of touch with their home office. The extension of the enterprise network, in the form of mobile virtual private networks (VPNs), is a truly compelling use of these new wireless services. Corporations are willing to pay for services that make employees more productive. Just as 42 percent of business professionals now carry a cellular phone to stay in touch with their offices while they are on the road, it is likely that a similarly large number of professionals would be eager to carry a device that would tie them into their corporate network.

Figure 1 Wireless technology applicability by bandwidth and situation



A special set of requirements emerges from this new set of connectivity services. When devices and users don't have wires there is the likelihood that they will move from one location to another. This is apparent when users are on trains or in cars, but can also be an issue when users are stationary. As increased data rates are offered, there is a corresponding shrinkage in coverage area. Users are even more likely to move from one cell to another, sometimes without physically moving, because as conditions change in the area, such as having a large truck roll by, a cell hand-off can take place. The rerouting of data packets will need to be dealt with for both directions of data flow. Loss of sessions due to street traffic conditions can not occur and emerging push applications will require constant knowledge of a device's location. There must be a way to adequately deal with these relocation and rerouting issues.



## Mobile IP: Solutions for Emerging Networking Needs

Mobile IP, request for comment 2002 (RFC 2002), enables a host to be identified by a single IP address even while the device physically moves its point of attachment from one network to another, allowing for the transparent forwarding of data packets to a single address. This IETF proposed standard functionality provides the unique ability to maintain sessions, regardless of movement between locations on different networks, because there are no address changes to be dealt with. Mobility becomes an issue that the mobile IP protocol can transparently negotiate to allow users new freedoms. Movement from one point of attachment to another is seamlessly achieved without the intervention or the knowledge of the user. Mobile IP is the first protocol to offer such mobility transparently to applications. Roaming from a wired network to a wireless or wide area network can also be achieved with ease. Therefore, mobile IP provides ubiquitous connectivity for users whether they are within their enterprise networks or away from home. Access to the resources within the network remains the same from the perspective of the user. This allows for truly transparent mobility with respect to all devices that communicate with the mobile node and all intermediate devices within networks.

An added benefit of mobile IP is that it allows users to gain access to their enterprise networks and the Internet in the same way no matter where they are physically. They can access resources in the same way while they are within the bounds of their enterprise network and also when they dial in from hotel rooms or customer sites. Mobile IP provides a solution that can work in all connectivity situations. It enables users to connect to media of any kind, automatically locate a mobility agent, and register their current location with a home gateway. The home gateway will then forward any traffic received for this mobile user to his current location. Should the user move, since the mobile IP software is automatically monitoring for this condition, it will notify the home gateway of the move. In this way sessions can be seamlessly maintained despite movement. When the user returns home, the mobile IP protocol will automatically discover this and informs its home gateway that it has arrived home, and the host will behave as any other IP device normally would.

Cisco IOS software increases the overall offering of this mobility solution since many value added features can be used in conjunction with mobile IP. All IOS features for differentiation of services, accounting, traffic engineering and queuing can be used in conjunction with mobile IP. By always being able to identify a user by an IP address it is also possible to simplify certain configurations within the network. Access lists and queuing or traffic shaping configurations could remain static, for example. Netflow statistics and accounting data would be obtained in a straightforward manner. And it could be possible to manage the mobile IP functionality in the network in the same way the rest of the IOS platform elements are monitored. Cisco has implemented full MIB support for mobile IP as specified in RFC 2006.

## Emerging Examples where Mobile IP is Applicable

### Delivery Vehicles

The need for wireless data communication is not new. Today there are several industries that rely on it to save time and money. One of the places where it is absolutely necessary is in the delivery industry. These people need to be in touch with schedule changes or road conditions. Drivers need to be updated immediately when pickup schedule changes occur or when there are hazards to be aware of. Drivers require directions in order to arrive at the new destination on time. A tremendous amount of time can be wasted printing schedules, updating them with changes and trying to ensure that the drivers have correct information. If this data is constantly kept current on a device in the vehicle, the drivers can plan accordingly and immediately contact home base when they have questions. This save a tremendous amount of time, allows more deliveries to be made efficiently, and ensures that the schedule is kept at all times. Most of the systems that are performing these functions today were developed specifically for each organization's applications in a proprietary manner. The pressing need to make a generalized solution for the expanding service industry is rapidly emerging. This will enable even greater savings, by using standard protocols and off-the-shelf platforms that can be managed in conjunction with the rest of the network elements.

### The Business Traveler

As the pace and frequency of business communication increases, time spent out of touch hurts businesses. "Road warriors" often find themselves wasting valuable workday hours without any communication with the home office. Business travelers could make better use of time spent while in cabs, in a hotel lobbies, and in an airport terminals, or even on an airplane. Availability of services to tie users back into their corporate network could prove invaluable. Even more compelling would be a service that would allow

users to be automatically notified of new developments as they occurred. If users could carry a device that would allow them to constantly receive relevant information it would be very liberating. This information could include stock and news updates as well as sports scores and entertainment schedules. If users then had the ability to access any Web pages referenced in e-mail and immediately reply directly from this same device, users could be as effective on the road as they are at their desks. This would go a long way toward ensuring that communication would not break down when users have to visit customers or attend conferences. Services that will allow this sort of communication can be offered in the very near future.

#### **Wired/Wireless VPN**

One benefit of this new era of communication is the extension of the wired VPN into the emerging wireless world. Paging services that require users to call back into the office are less compelling. More compelling will be the new class of services that enable users to carry a small device that is always on and always connected and gives users the capability to be tied directly into what is going on in their home environment. New products are coming to market that will have the ability to recognize whether a user is at home or away and adapt the forwarding of information to fit a profile the user sets up to match different situations. These will provide users with the ability to get what they need when they need it, with mobile IP providing the underlying network service.

### **Detailed Protocol Overview**


#### **Location Discovery**

Mobile IP works because the mobile node is able to discover whether it is at home or away from home. A host determines whether it is on its home network by using extensions to ICMP Router Discovery Protocol (IRDP) (RFC 1256). These IRDP extensions indicate mobility agent information that facilitates agent discovery. Routers acting as home agents (HAs) or foreign agents (FAs) will advertise their existence. HAs are routers located on the mobile node's home network that are capable of tunneling the mobile node's datagrams to it while it is away. FAs are devices on a network that are capable of acting as a detunneling point for datagrams to the mobile node. Agent discovery, like router discovery, works through advertisements, solicitations, and responses. A mobile aware host, which is a host that is capable of utilizing mobile IP, will listen for agent advertisements or solicit them. An agent advertisement will indicate a mobility agent's IP address as well as whether it is able to serve as an HA or FA. Agents will also advertise the registration options they are capable of supporting, as well as their availability, by using the appropriate fields. If the mobile node notices its own HA's advertisement, it knows it is at home and does not need to register or do anything special in order to receive its datagrams.

If, on the other hand, a mobile node receives an IRDP advertisement from another mobility agent, it will be able to determine it is not on its home network. When this is the case, a mobile node will need to register with its own home agent in order to receive datagrams, since they would not otherwise be directed to the host at its current location. The mobile node will try to locate a suitable foreign agent. It can find one if the IRDP advertisement contains mobility information, and then it can register its location via this foreign agent if it desires. If this IRDP advertisement does not contain mobility information, or if the FA does not support the options the mobile node desires, the mobile node can register directly with its home agent. In either case the MN will send a registration request to its HA.

#### **Care-Of Addresses and Registration**

While away from home, the mobile node will be associated with a care-of address. This address will identify the mobile node's current, topological point of attachment to the Internet and will be used to route packets to the mobile node while the user visits other locations. Either a foreign agent's address or an address obtained by the MN for use while it is present on a particular network will be used as the care-of address. The former is called a foreign agent care-of address and the latter a co-located care-of address. After the MN decides on his care-of option he sends a registration request to his HA. In this request he lists the options he would like for his registration. Tunneling to mobile nodes can be done via IP in IP encapsulation (RFC 2003) or generic route encapsulation [GRE (RFC 1701)]. Cisco IOS has also implemented tunnel "soft state" as described in RFC 2003 to aid in path maximum transmittable unit (pMTU) discovery. Tunnel soft state allows the tunnel head to keep track of the tunnel path MTU and return this value to senders of larger packets via internet control message protocol (ICMP) type 4 responses. The registration requests and replies are required to have an authentication extension that includes a keyed MD5 hash of the registration packet as well as a timestamp to ensure the origination of the request and the time it was sent, to prevent replay attacks.



When the home agent receives a registration request, it determines whether the authentication hash is valid, if the timestamp is within an acceptable range, and if it can honor the request in terms of resources as well as options. It then sends a reply to the mobile node. When the MN and the HA agree upon a set of service options then a mobility binding is put into the HA's binding table and used to associate the mobile node's home address with the care-of address. This binding will allow the mobile node to receive tunneled datagrams destined for its home address when it is not physically connected to that network. Since the HA is attached to the home LAN of the MN it will merely accept and forward traffic destined for the registered MN.

When this binding is first added to the table the HA sends a gratuitous ARP on the MNs home LAN so that all directly connected devices can continue to communicate with the mobile node through the HA. While the mobile node is registered with the home agent the home agent will proxy ARP for the home address of the mobile node and tunnel packets to it using the care of address in its mobility binding. When the mobile node moves its point of attachment to the Internet it will notify the home agent and indicate its new care-of IP address. This change in location is only known to the HA and all other devices can continue to communicate with the MN transparently. When a mobile node returns to its home network it will send a gratuitous address resolution protocol (ARP) responses in order to indicate its return and allow devices to send packets directly to the MN on its home subnet.

#### Cisco IOS Enhancements to Mobile IP

The Cisco IOS implementation of mobile IP has enhancements to ensure scalability, resiliency, and security. IOS platforms can function as HAs or FAs or both simultaneously. Since it is possible for large numbers of devices to be mobile, the number of keys needed to perform the authentication function could become very large. For this reason, IOS software allows for the mobility keys to be stored on an authentication, authorization and accounting (AAA) server that can be accessed via either TACACS+ or RADIUS. This allows for scalability to large numbers of potentially mobile users and provides a single place for maintenance. For security, IOS has the ability to use registration filters to restrict who is allowed to register. This mechanism can be used on both the FA and the HA to prevent certain MNs from registering and to prevent registration via some mobility agents. This provides the further ability to restrict usage to only to areas where administrators have trust relationships in place.

Because of the many years of internetworking experience, Cisco recognized the fact that the mobile IP architecture could benefit from additional built-in redundancy. The base specification could allow the failure of an HA to interrupt data flow to the mobile node. This is the case since there is no "keepalive" mechanism between the HA and registered MNs. If MNs fail to receive traffic tunneled from their home agent it may be because there was no traffic. On the other hand, if there were some sort of failure on the HA due to a power failure or a software upgrade, the binding table could have been lost, and there is no mechanism to alert the MNs. Because of this situation, IOS software has implemented home agent redundancy, leveraging de facto Hot Standby Router Protocol (HSRP). This feature allows for one or more home agents to back one another up in the event of any kind of a failure. The active HA sends binding updates to the backup HA every time a new registration is entered into the binding table, which keeps the binding tables in sync. If a new HA boots up on the LAN it can have the entire binding table loaded into its memory so that it can be ready in the event of any network failure. This enables the nonstop networking that customers have come to rely on Cisco to provide.

#### Standardization Status

Mobile IP is the Internet proposed standard mechanism for dealing with mobility. It is outlined in RFCs 2002 to 2006:

- 2002: IP Mobility Support
- 2003: IP Encapsulation within IP
- 2005: Applicability Statement for IP Mobility Support
- 2006: The Definitions of Managed Objects for IP Mobility Support using SMIPv2

All of these RFCs are all in proposed standard status with multivendor support. Cisco, as the market leader, has identified mobile data as one of the most significant emerging opportunities. Cisco IOS has the first implementation of IETF standard mobile IP available on a router platform with the 12.0.1T release.

### Mobile Host Requirements

The mobile IP protocol requires the use of mobility-aware clients. This means that a piece of software needs to run on the hosts that are mobile. This is much the same as the requirement that when hosts dial in to a PPP network today they have support of PPP and the ability to negotiate an IP address. The mobile IP support that is needed can be very minimal; hosts only need to determine whether or not they are at home and be able to register with their home agents. On the other hand, it is possible that these hosts will want to de-tunnel their own packets. They will need to have the ability perform this function also in that case. Cisco Systems is the networking leader, providing the infrastructure to enable roaming directly within the IOS software running on platforms in networks today. Similarly, client software will be manufactured by host market leaders. There are currently many freeware versions of mobile node software available, and some enterprising companies have written software for their own internal use as well. There are a number of vendors who are beginning to offer software to support this functionality, including, Sun Microsystems, Toshiba and NetManage.

### Other Important Issues

#### Security Concerns

Security concerns are heightened when corporate network resources are accessed from beyond enterprise bounds. Therefore Cisco's implementation of mobile IP has some additional security features. IOS software has support for the mandatory and both of the optional authentication parameters within mobile IP. These are the mandated mobile-home authentication, and the optional foreign-home and mobile-foreign authentications. The authentication procedures performed are keyed MD5 hashes, which cover all registration requests and replies. The registration requests and replies are all time-stamped to ensure that there can be no replay attacks also. This attack might occur if a registration packet is sniffed off the wire and then reused by an impostor in order to gain access to network resources. This timestamp is also protected by the hash. Cisco has implemented access list functionality to enable an administrator to permit the registration of certain users and prevent the registration via certain mobility agents. Reverse tunneling has been implemented in our home agent to allow for the optional tunneling of datagrams back to the home agent from the MN or the FA. This will allow for communication through firewalls, for example. Communication beyond a firewall can be an issue when ingress filtering is performed on firewalling devices or boundary routers. The logging of any type of mobile IP security violation can be performed with IOS software as well, such as an attempt to register which fails authentication. In the future, it will be possible to utilize IPSec encryption with mobile IP in IOS software. This will further ensure that corporate communications can remain private for mobile VPNs.

### References

1. RFC 2002: IP Mobility Support
2. RFC 2003: IP Encapsulation within IP
3. RFC 2005: Applicability Statement for IP Mobility Support
4. RFC 2006: The Definitions of Managed Objects for IP Mobility Support Using SMIv2
5. RFC 1701: Generic Routing Encapsulation (GRE)
6. RFC 1702: Generic Routing Encapsulation over IPv4 networks
7. RFC 1256: ICMP Router Discovery Messages





Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe s.a.r.l.  
Parc Evolic, Batiment L1/L2  
16 Avenue du Quebec  
Villebon, BP 706  
91961 Courtaboeuf Cedex  
France  
<http://www-europe.cisco.com>  
Tel: 33 1 69 18 61 00  
Fax: 33 1 69 28 83 26

Americas  
Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Headquarters  
Nihon Cisco Systems K.K.  
Fuji Building, 9th Floor  
3-2-3 Marunouchi  
Chiyoda-ku, Tokyo 100  
Japan  
<http://www.cisco.com>  
Tel: 81 3 5219 6250  
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Connection Online Web site at <http://www.cisco.com/offices>.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia  
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore  
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela