White Paper

Birdstep Intelligent Mobile IP Client v2.0, Universal Edition
Seamless secure mobility across all networks

Copyright ©2002 Birdstep Technology ASA
Table of Contents

1 Introduction ....................................................................................................................... 3
2 Scope ............................................................................................................................... 4
3 Application Areas ............................................................................................................ 4
   3.1 Enterprise deployment .............................................................................................. 4
   3.2 Public deployment ...................................................................................................... 5
4 Mobility vs. Security ........................................................................................................ 5
   4.1 Mobile IP and Security ............................................................................................ 5
   4.2 Proprietary Solutions vs. Open Standards ............................................................ 6
   4.3 Mobility requirements ............................................................................................. 7
5 Mobile VPN alternatives .................................................................................................. 8
   5.1 Basic models ............................................................................................................. 8
   5.2 Seamless VPN models ............................................................................................ 11
   5.3 Deployment and configuration ............................................................................... 15
   5.4 Automatic client configuration .............................................................................. 18
6 Conclusion/Summary ..................................................................................................... 19
1 Introduction

With Mobile IP, the enterprise and public operator can provide seamless “always-on” network access to the mobile professional. For the enterprise user, this means “hassle-free” connectivity both inside and outside the office environment. It also means the ability to control cost of network charges by always choosing the best available connection. For the operator, Mobile IP enforces the operator-customer relation, and enables the operator to provide a mobility service for the user not only on the operator’s own network but also when the user is connected to the enterprise network, or even to the access network of a different network operator.

The common theme for both enterprise and operator deployment, is the need for security. Virtual Private Network (VPN) technologies protect the integrity of communication for the mobile user when outside the office environment. Enterprises that already rely on market leading VPN solutions for external access of the corporate information, and want to provide seamless mobility find it crucial to mobilize the existing VPN in order to protect existing investment and to leverage the security and functionality of the market leading VPN solutions.

The Birdstep Intelligent Mobile IP client has followed an open and standards-based approach to provide seamless roaming for operators and enterprises. Experience gathered through work with various customers has provided us with the know-how to improve this standard-based, VPN-independent roaming model. With the next generation of our Mobile IP client, based on a ground breaking “best-of-breed” VPN design approach, we have been able to maintain our tradition of supporting the existing standards and existing network infrastructure. In addition we have solved key issues for offering mobility support of 3rd party VPN solutions.

The most important features requested from both network operators and enterprises have been the following:

1. Ability to turn VPN off when the user is connected using a secure connection to his or her intranet (such as Ethernet or corporate Wireless LAN with dynamic WEP key) and ability to turn on the VPN when the user is connected using an external network such as a private WLAN or public Wireless LAN hotspot or using a public cellular service such as GSM or GPRS.

2. Automatic configuration of the client to simplify large-scale deployment of mobility service for non-technical users. This has been supported until now with distribution of XML configuration files to the terminal at installation time. Now, parameter management is directly supported by the client itself. Standard, secure, web-based parameter download is now the simplest way to manage a large number of Mobile clients using the existing enterprise or operator web server backend infrastructure.

The new Birdstep Intelligent Mobile IP client, v2.0 Universal Edition solves both these requirements, and caters to both operator and enterprise deployments. A corresponding v2.0 Standard Edition will replace the exiting v1.4 of the Birdstep Intelligent Mobile IP client. Since the latter edition does not include the VPN on/off feature, it is a simpler and cheaper deployment alternative for users who spend most of their working day outside the enterprise.
2 Scope

This whitepaper starts by outlining application areas (this includes requirements for enterprises and operators), then it describes some of the existing approaches to solve such requirements, it then explains how the Birdstep Mobile IP client is designed to solve the requirement of seamless VPN and finally it explains the automatic configuration features of the Mobile IP client. This paper focuses exclusively on the Universal Edition of the new Mobile IP client from Birdstep. This whitepaper does not describe the basic concepts back Mobile IP; there is a wide range of articles on the subject. If you need to refresh your knowledge, you should read some of the documentation available at the web site from the Internet Engineering Task Force (www.ietf.org).

3 Application Areas

In the last years major technology developments have directly changed our way of working. The increased reliance on the Internet as a business tool and the development of sophisticated wireless communications systems have freed employees from the need to remain at their desk when doing productive work.

Mobility and productivity are the current trends in all business practices. Enterprise users are spending more time traveling and on meetings at other places than in their own offices. More than ever they want to be able to connect from any location to their corporate network.

3.1 Enterprise deployment

We assume that enterprises want their users to roam internally (between any combinations of LAN and/or WLAN subnets, where the WLAN subnets can be secured using for example WEP/LEAP or other security mechanisms), and externally to public networks such as public WLAN hotspots, public locations with Ethernet/ISDN or analog line connections such as hotel rooms, and home users with an ISDN/ADSL or analog line connection. Two important application areas for Mobile IP inside the enterprise is (1) when the enterprise WLAN is deployed as an unsecured network outside the company firewall and (2) when the enterprise WLAN due to its size needs to be segmented in separate subnets. In both cases Mobile IP cater for the need to move seamlessly between any enterprise networks.

For enterprise users, we assume that communication is encrypted with market leading VPN clients, with VPN concentrators placed in the enterprise DMZ. We also assume that the enterprise wants to enable VPN when the user is roaming on public or unsecured networks as listed above to maintain security, while they want to disable VPN when users are connected to their secured intranet to avoid unnecessary load on the VPN concentrator and corporate firewall. (However, for small enterprises with a small number of users, the load on VPN concentrator may be regarded as acceptable since the VPN concentrator is not a bottleneck.)

We further assume that the enterprise IT management wants to control all Mobile IP parameters from a central location controlled by the IT management.
3.2 Public deployment

3.2.1 Mobile operators

We assume that mobile operators have deployed a 2.5G cellular network, such as GPRS or IS95B networks, and may have licenses for 3G (UMTS/CDMA2000) networks. We also assume that the operators operate a switched cellular network (such as GSM or CDMA) and that the operator is in the process of deploying WLAN zones, or go in alliance with Wireless ISPs. Some of these operators might also either be ISPs or have alliances with ISPs. Most of the mobile operators fall today under this category.

3.2.2 ISPs

ISPs that currently serve dial-in ISDN/POTS pools and operate xDSL/CATV/LMDS broadband networks may be interested in offering their customers mobility to wireless technologies. The ISPs may become Wireless ISPs by providing public or enterprise WLAN hotspots, but the ISPs may also partner with existing WISPs or mobile operators with WLAN plans. Trends in the market to offer wholesale of local WLAN access zones to existing ISPs confirm this category.

3.2.3 Operators catering enterprise customers

We further assume that the operators want to target not only to the individual user, but they also want to cater their enterprise customers. Such target market has two requirements in the MIP arena. The first requirement is the need to provide seamless roaming to their users to keep them loyal and increase their use of the operator’s offerings, the second requirement is to cater to the enterprises that require access to the network for their employees while these are on the road. In this case, the operator provides a public mobility service, independent of the enterprise IT infrastructure. In this case, the enterprise handles its own VPN infrastructure and out-sources mobility to the operator, which becomes a public network mobility provider.

3.2.4 Configuration

We assume that the enterprise want to control all parameters of their own enterprise users from a central location and that service registration shall be as simple as possible. We also assume that operators want to offer the parameters to the enterprises, which can then supply to their users for roaming in the public space. We also assume that the operators want to control centrally all the parameters offered to their private clients.

4 Mobility vs. Security

4.1 Mobile IP and Security

The need to protect the integrity of communication for the mobile user introduces the requirement for a seamless mobile VPN solution. It is important to note that Mobile IP is secure but does not protect your data. Mobile IP includes protection of mobility handling with the following key mechanisms:
- Authentication of registration messages
- Prevents hi-jacking of traffic
- Ensures integrity of binding list
- Accommodates any authentication algorithm

Data security is not part of Mobile IP, and security can be handled either by running traffic over a secure link (such as a wired Ethernet or a Wireless connection with layer2 encryption), or security can be overlaid using VPN technology. The use of VPN is enabled by placing a VPN concentrator in the DMZ of an enterprise network and a VPN client installed in the terminal. When VPN is used together with Mobile IP, Mobile IP can be used inside the VPN tunnel, or VPN can be overlaid the Mobile IP connection. What is important on both cases is that the VPN is in control of security.

4.2 Proprietary Solutions vs. Open Standards

When it comes to providing VPN mobility there are two completely different implementation approaches in the market. The first approach is a proprietary bundle with Mobile IP and VPN client from the same vendor with vendor-specific signaling between the two clients. The second alternative, pioneered by Birdstep has been to interoperate with product offerings from major VPN vendors. The figure below outlines both alternatives. Since there is no bundle between Mobile IP and VPN on the client side of open design approach, there is no need for bundle between the MIP and VPN on the agent/server side either. The closed design normally requires a bundle on the agent/server side also.

![Figure 1: Closed vs. open mobility design](image)
The proprietary bundled implementation alternative often requires investment in new server side components, introduction of new elements in the network topology that either can compromise the established security rules of the enterprise or compromises the scalability and redundancy already implemented at the network. This approach can be justified at small-scale installations where such requirements are not a real concern.

The open standards implementation alternative requires interoperability with existing software and hardware components. The Birdstep message has always been to develop a Mobile IP client that can coexist with any Mobile IP Home Agent (such as a Cisco router, Solaris Server, Linux server, etc) and mobilize the existing market leader VPN solutions (such as Checkpoint, Nortel, Cisco and Microsoft). This approach leverages on existing VPNs, provides a scalable solution to the market and does not force the user to replace existing and proven infrastructure.

4.3 Mobility requirements

Before going into a detailed description of different solutions that combine Mobile IP and security, it is important to understand the mobility requirements arising from enterprise users. There are three different areas of concern regarding network handover and seamless operation:

- Between subnets internally
- Between subnets externally
- Across the security boundary

Since external access to internal resources is always via a secure VPN tunnel solution it is in fact the VPN that must be made mobile when moving between subnets externally as pointed in the second bullet above. The challenge to meet the requirement described in the third bullet is to turn the VPN on or off as required.
5 Mobile VPN alternatives

Secure mobility using VPN can be handled in various ways as discussed in the next four subsections. The two first models are classified as basic since they do not support seamless operation across a security boundary. In contrast, the last two models manage to solve the seamless VPN operation across a security boundary. The approach taken by Birdstep is to use a best-of-breed approach combining the best from the two basic models and turn the combination into a seamless VPN solution that works across a security boundary.

5.1 Basic models

5.1.1 Mobile IP inside VPN

If Mobile IP is placed inside of the VPN, this is called the Mobile IP in VPN approach. It leverages a VPN solution to reach the enterprise intranet, and has the advantage that VPN is only used when the user terminal is connected to an external network. Mobile IP works fine for handovers between different access networks within the intranet (e.g. WLAN and Ethernet), but the session is lost when the client wants to roam from an intranet connection to a public network connection. The solution does not provide mobility between different access networks, since the VPN session is broken for every network change.

![Diagram of Mobile IP in VPN](image)

To be able to access the enterprise intranet from outside, figure 4 shows how the VPN client is placed below the Mobile IP client. The VPN terminate the IPSEC tunnel from the VPN client, and pass packets onto the intranet through the enterprise firewall. Packets from the Mobile node can now reach the Mobile IP Home Agent on the intranet.
For internal access within the intranet, the VPN client becomes inactive, and the VPN overhead is not incurred for internal communication (see figure 5.) Note that seamless handover can now be achieved across heterogeneous internal access networks in the enterprise intranet.

The solution provides the following advantages:

- The Mobile IP Home address is internal, and the Mobile Node is part of the intranet.
- The VPN is only used when the client connects from public networks, and no VPN overhead is incurred when the user is connected to the intranet.

The solution has the following disadvantages:

- The VPN tunnel breaks at every handoff, and the VPN session must be re-established (this is normally a manual process due to security policies).
- Tunnel re-establishment incurs performance penalty.
- Enterprises must deploy mobile IP service, and cannot rely on an operator managed mobility service.
5.1.2 VPN overlaid Mobile IP

If VPN is placed on top of Mobile IP, we call this solution the “VPN overlaid MIP approach”. Until now, this approach has been the preferred way to mobilize a VPN solution. This is the model supported by Birdstep as well in the version 1.4 of the Mobile IP client. The strength of the Birdstep solution, compared to other such solutions, has been to interoperate with products from major VPN vendors instead of pushing a proprietary solution.

When the VPN client software is overlaid a Mobile IP system, the Mobile IP is an external system with the Mobile IP Home Agent placed outside the intranet, usually on the enterprise DMZ. In this way, Mobile IP mobilizes the existing VPN solution, and any application can now run securely over VPN and the session will not be altered as access networks are changed.

![Figure 6: VPN overlaid Mobile IP](image)

To be able to access the enterprise intranet from outside, figure 7 shows how the VPN client is placed overlaid to the Mobile IP client. The Mobile IP client must be able to reach the Home Agent that must be placed in the DMZ in the same way as the VPN concentrator.

![Figure 7: Overlaid VPN outside access](image)
For internal access within the intranet, (see figure 8.) the Mobile IP client is still forced to reach the Mobile IP Home Agent placed in the DMZ. It is also forced to reach the VPN concentrator.

![Diagram](image)

**Figure 8: Overlaid VPN inside access**

The solution provides the following advantages:

- VPN tunnel survives handoff, bound to MIP address
- Enterprises can rely on a public mobile IP service

The solution has the following disadvantages:

- Home address is external, not part of intranet
- Must always use VPN, also when on intranet
- Traffic loops via outside HA when on intranet

### 5.2 Seamless VPN models

#### 5.2.1 The Mobile IP Proxy

Using this model, the Mobile IP system will allow seamless mobility across security boundaries of the enterprise. Until recently, the standardization efforts in IETF has focused on introducing a new component called the proxy-Home Agent which is deployed on the external DMZ and synchronized with the real Home Agent which is placed securely on the enterprise intranet. However, the proxy Home Agent and the Home Agent must use a signaling scheme that may or may not be proprietary depending on who implements such solution.
At this time the proxy Home Agent is not yet standardized.

Figure 9: Mobile IP with the proxy agent model

Figure 10 shows the sequence needed for your client to connect from the outside to the enterprise network when using the Mobile IP Proxy implementation. As shown in the figure there is an increased complexity of the communication that needs to take place between all the components involved to be able to reach the enterprise from the outside.

Figure 10: Proxy Mobile IP solution access from the outside
Figure 11 shows the sequence needed for your client to connect to the enterprise network when using
the Mobile IP Proxy implementation and the client is on the inside. This case is a simpler case
compared to reaching the enterprise network from the outside. The VPN client becomes inactive and
the VPN overhead is not incurred for internal communication.

![Figure 11: Proxy Mobile IP solution access from the inside](image)

The solution provides the following advantages:

- Solves the seamless VPN problem
- Little extra overhead

The solution has the following disadvantages:

- Requires a new type of component (the proxy)
- Not yet standardized, probably implemented using proprietary protocols between proxy and Home
  Agent.
- Several components share control over same address range
- Requires careful design-in to maintain security
- Restricted deployment flexibility

### 5.2.2 Seamless VPN using existing, standard components

Instead of introducing a new, not-yet-standardized network component that is likely to be
implemented by various vendors with proprietary signaling protocols, Birdstep has developed and
submitted a patent for a new generation Mobile IP client that can utilize legacy Mobile IP Home Agent
components and eliminate the need for proprietary protocols. This solution is the foundation for
Birdstep's mobility offering which solves the requirements described in the initial sections. To
understand the new mobility solution from Birdstep, it is important to understand how the mobility
solution solves the seamless mobile VPN problem. This problem is simply "how can a 3rd party VPN be
turned on and off when the mobile unit moves between insecure internet connections and secure
intranet connections without interrupting the connection?".

The key to this solution is to establish two separate Mobile IP systems. Both mobility systems can be
handled from a single client, and standard Mobile IP Home Agent components can be used on the
server side. Note that there is no need for new network components such as the proxy Mobile IP Home Agent. The two mobility systems are isolated by the VPN, ensuring security using the existing enterprise VPN solutions. This solution represents a best-of-breed approach, where the two mobility systems take care of the following tasks:

- The internal (HA on intranet) Mobile IP system mobilizes your application (using the advantages of the method described in Mobile IP inside VPN model).
- The external (HA on DMZ) Mobile IP system mobilizes your VPN (using the advantages of the method described in the VPN overlaid Mobile IP model)

![Figure 12: Mobile IP using standard components](image)

Note that this solution requires a Mobile IP client software with dual system capabilities, which is the key feature of the Birdstep Universal mobility solution described below.

For access to the enterprise intranet from the outside, figure 13 shows how the VPN client and the two instances of the Mobile IP client operate. When the VPN is in use, the external instance of the MIP client communicates to the MIP HA outside the intranet, while the internal instance of the MIP client communicates through the VPN to the internal MIP HA.

![Figure 13: Protocol flow, outside access to enterprise intranet (VPN in use)](image)

For internal access within the intranet, the VPN client becomes inactive, and the VPN overhead is not incurred for internal communication (see figure 14.) Note that seamless handover can now be
achieved across heterogeneous internal access networks in the enterprise intranet and the internal instance of the MIP client is the only active element, the external instance of the MIP client and the VPN client are completely transparent.

![Diagram](image)

*Figure 14: Protocol flow, inside access to enterprise intranet (VPN not used)*

The most important characteristic of the dual-MIP approach is that the two systems are completely isolated by the VPN solution. Moreover, the VPN solution is still in full control of all access to the Intranet. No changes are required to any infrastructure components such as agents, firewall rules or VPN gateways.

The solution provides the following advantages:

- Solves the seamless VPN problem
- No specific design requirements
- Your VPN solution is (still) in control of all external access
- High deployment flexibility

The solution has the following disadvantages:

- Incurs minimum of extra overhead

5.3 Deployment and configuration

In the following sections, we will discuss deployment alternatives for the new Mobile IP client, focusing on the configuration aspects of the client software such that enterprises or operators can enable mobility for their users without manual configuration steps required by such users.
The Birdstep Intelligent Mobile IP version 2.0, Universal Edition focuses both on enterprise, and operators who want to provide a total mobility and security solution to enterprises. In the following sections, enterprise-controlled and operator-controlled universal mobility solutions are presented. These solutions differ in which entity provides the management of the Mobile IP Home Agent and the automatic Mobile IP client configuration.

5.3.1 Enterprise-controlled universal mobility solution

In the enterprise-controlled universal mobility model, two Mobile IP Home Agents are used as shown in Figure 15. Note that one Home Agent (HA) is placed on the DMZ where it can be reached from public networks, while another HA is placed on the enterprise Intranet. The enterprise VPN controller is placed on the DMZ or integrated in the firewall.

Figure 15: Universal mobility model requires two Mobile IP Home Agents and is focused towards enterprise deployment.

Enterprises want to offer their employees seamless roaming inside the premises to increase productivity. In addition, they want their employees to use the best and preferably lowest cost access when outside the enterprise. When the client terminal is attached to an intranet access network (e.g. wired LAN or LEAP-based WLAN), it registers itself with the intranet HA. When the client terminal is attached to an external access network (such as insecure or public WLAN, ADSL at home, GPRS or other public networks) it registers with the external HA.

In this case, traffic generated within the enterprise network does not use VPN and does not go through any VPN concentrator. On the other hand, traffic generated from terminals connected to public networks goes through a VPN tunnel to secure such traffic. Note that traffic is always tunneled through the Home Agents, be it the external or the internal HA. It is important that the Mobile IP HA is dimensioned according to the projected traffic volume.
The typical user case for this package is an enterprise that wants to provide seamless mobility to its users when roaming seamlessly between GPRS, public WLAN and wired LAN.

The following components are required in the central enterprise infrastructure: Two Mobile IP Home Agent’s, a VPN concentrator and a web server to provide configuration information to the clients (see configuration chapter), and the enterprise firewall. On the terminals, a VPN client and the Birdstep Mobile IP Client, Universal Edition (version 2.0) is used.

5.3.2 Operator-controlled universal mobility solution

Operators interested in providing a total solution to enterprises that do not have the internal staff/infrastructure/focus to do it themselves, but that require roaming as described above, can offer a universal mobility solution based on this package. In this case the operator assists the enterprise to setup the internal infrastructure and provides the profile information to be installed at the employee’s workstations to allow roaming in the inside (on the enterprise network,) as well as on the outside (on the operator’s owned public network.) The operator, in this case, provides the client configuration information to the enterprise. An example configuration of this scenario is shown in Figure 16.

Figure 16: Operator providing a managed mobility service for enterprises using the Mobile IP client, Universal edition
The operator may manage the enterprise intranet HA (if the enterprise chooses to allow such management). The operator manages the public HA and provide configuration for both HAs. (The operator may also manage the enterprise VPN solution, but this is not required).

The operator can now offer a managed mobility service providing seamless mobility between the enterprise LAN, operator GPRS/GSM and operator public WLAN hotspots.

The following components are required in the central operator infrastructure: One Mobile IP Home Agent and a web server to provide configuration information to the clients (see configuration chapter). The following components are required in the enterprise infrastructure: One Mobile IP Home Agent, a firewall and a VPN concentrator. On the terminals, a VPN client and the Birdstep Mobile IP Client, Universal Edition (version 2.0) is needed.

Note that this configuration can also be used for enterprises that subscribe to a public mobility service from an operator, but want to configure the terminals themselves. In this case, the client configuration information is maintained by the enterprise.

5.4 Automatic client configuration

An important new feature of the Mobile IP client is automatic client configuration. Figure 17 outlines how the configuration server is used to remote configure the Mobile IP client.

![Figure 17: Automatic Mobile IP client configuration]

Note that the configuration server is a standard web server, where configuration files can be stored. The minimal requirement to this configuration server is that it provides HTTPS using Secure Socket Layers (SSL) or even plain HTTP. Configuration files can be stored in this web server.
The client downloads the configuration file specified in the configuration URL. Construction of the URL is implementation specific, but it should be possible to support a large number of configuration files based on one or more of the following parameters:

- Command line parameter
- User-specified URL path extension
- Username / password

### 6 Conclusion/Summary

The new Universal Mobility solution from Birdstep solves the key issue of mobilizing your standard VPN solution while turning it on only when the user is connecting from an external insecure network. In this way, the load on the VPN concentrators and the Firewall network components are kept as low as possible. Since the existing VPN solution can be utilized also for highly mobile workers, the investment in VPN is protected, and existing security policies can be enforced. The enterprise can now use the best available VPN solutions knowing that the Universal mobility solution can mobilize the VPN of your choice. The Birdstep Intelligent Mobile IP Client, Universal Edition (version 2.0) represents a breakthrough in the development of a standard-based seamless VPN solution.

With the Birdstep Universal mobility solution, users are able to move seamlessly both between different internal networks, between different external access networks, and across the security boundary protected by VPN and Firewall technologies. The VPN is turned on or off as required. VPN is turned on when public networks are used, and VPN is turned off when the terminal is connected to the intranet.

Very importantly, VPN on/off feature depends only on existing standard-based components such as industry standard VPN components, industry standard Mobile IP Home Agents together with the Birdstep IETF-standard based Mobile IP client. Using this architecture, you can rely on well-proven network components, and do not need any proprietary signaling between any of the components in the solution.

Further more, large-scale deployment of Mobile IP is now possible using the standard-based web infrastructure of the operator or enterprise to automatically configure the client with no manual configuration steps needed by the end user. This feature enables the organization to quickly introduce seamless and secure mobility for their existing user base, without extra technical requirements to the end user.

Please refer to our web pages for more detailed product information and fact sheets.