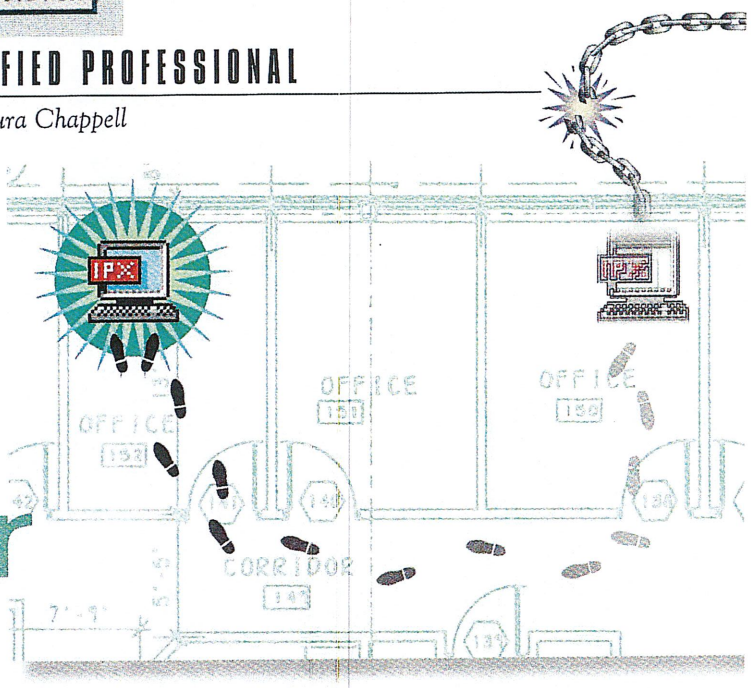
Laura Chappell

Mobile IPX

Unshackle Your Computer



During the past couple of years, Novell has implemented several technologies that have caused a big stir, such as Novell Directory Services (NDS) and Novell Embedded Systems Technology (NEST). In all of the hubbub, you may not have noticed one of Novell's most interesting new technologies: Mobile IPX. With Mobile IPX, you can physically move a Mobile IPX client from one location on a network to another without severing the client's NetWare Core Protocol (NCP) connection. You can even hot-swap your network interface board and maintain the client's NCP connection the entire time.

Because Mobile IPX maintains your NCP connection, you can move a Mobile IPX client from one place on the network to another without rebooting your workstation and logging in to the network again. For example, if a law firm does not use Mobile IPX, attorneys must plug their laptop into a 10Base-T jack in their office wall when they arrive at work, and they cannot unplug their laptop without losing their NCP connection. With Mobile IPX, on the other hand, these attorneys can take their laptop to the firm's library and plug it into a 10Base-T jack at that location to perform research on a case, or they can move to a conference room or to a colleague's office and plug in their laptop there—all while maintaining their NCP connection.

WHAT IS MOBILE IPX?

Mobile IPX is not a product; rather, it is a technology that is available with NetWare MultiProtocol Router (MPR) 3.1. You can install NetWare MPR 3.1 as a dedicated router on any Intel-based computer connected to a NetWare 3.12 or a NetWare 4.1 network. You can also install NetWare MPR 3.1 on the NetWare 3.12 or NetWare 4.1 file server that your Mobile IPX clients will use most often. By installing NetWare MPR 3.1 on this server, you eliminate unnecessary traffic and ensure that the clients' request packets and the server's reply packets do not have to travel an extra hop before reaching their destination.

The Mobile IPX technology that is included with NetWare MPR 3.1 consists of two parts: the Home Router and the Mobile IPX client software. The Home Router is simply a process that runs on NetWare MPR 3.1. When you install NetWare MPR 3.1, the Home Router feature is disabled by default, so you must enable it using the MPR INETCFG utility.

To take advantage of Mobile IPX, you must use IPXODI 3.02 or higher. Both NetWare MPR 3.1 and NetWare Client for DOS and Windows 1.20b include IPXODI 3.02. If you are not running IPXODI 3.02, you can install the Mobile IPX client software included with NetWare MPR 3.1, or you can download NetWare Client for DOS and Windows 1.20b from the *NetWare Connection* FTP site (ftp://ftp.nwconnection.com/pub/nwc-online/utilities/vlmup4.exe). Then you can configure the client software as a mobile client, which will notify Mobile IPX of any changes in the client's location or address.

CONNECTING WITHOUT MOBILE IPX

Before you can appreciate the capabilities that Mobile IPX offers, you must know how a client establishes and maintains an NCP connection without Mobile IPX. For example, why does a client lose its NCP connection when you move the client from one network location or address to another?

Getting the Network Address

When you set up a network, you must assign it a network address such as AA-BB-CC-DD. During the configuration process, you must bind this address to the network interface board (such as an NE2000 board) in every server on network AA-BB-CC-DD using the following command:

```
BIND IPX TO NE2000 NET=AA-BB-CC-DD
```

When you connect a NetWare client to a network, the client does not know its network address. However, the client must include this address in the IPX header's source network address field for any packets the client sends across the network. To determine its network address, the client immediately sends a Get Nearest Server request, placing 00-00-00-00 in the IPX header's source network address field. The appropriate

```
ipx: = = = = = = = = = = = Internetwork Packet Exchange = = = = = = = = = = =
     Checksum: 0xFFFF
     Length: 34
     Hop Count: 0
     Packet Type: 17(NCP)
     Network: AA-BB-CC-DD      --->    AA-BB-CC-DD
     Node: 00-00-1B-1E-F2-2C   --->    FF-FF-FF-FF-FF-FF
     Socket: 0x4006            --->    RIP
```

Figure 1. *After the client learns its network address, it can include that address in the IPX header's source network address field.*

NetWare server responds to this request by sending the client a reply packet, which contains the network address. The client learns its network address (AA-BB-CC-DD in our example) from this packet and can begin to use the address in the IPX header's source network address field. (See Figure 1.)

After the NetWare client logs in to a NetWare server and begins sending NCP requests, the server uses the NCP Watchdog process to monitor the client's connection. If the server does not receive any requests from the client within the Watchdog timeout period, the server will send a Watchdog packet to that client. (Five minutes is the default Watchdog timeout setting for both NetWare 3.12 and NetWare 4.1.)

A Watchdog packet is simply an IPX packet that contains a connection number and a question mark (?) in the data portion of the packet. If the client's NetWare shell or NetWare requester is still loaded, the client responds with a Y, indicating that the connection is valid. If the client does not respond, the NetWare server sends another Watchdog packet every minute for ten minutes (again, the default setting for both NetWare 3.12 and NetWare 4.1). If the server does not receive a reply to these packets, it terminates the client's connection.

Moving a NetWare Client

If you moved a NetWare client from network AA-BB-CC-DD in Building 1 to network DD-CC-BB-AA in Building 4 without using Mobile IPX, two things would prevent you from maintaining your NCP connection: the static network address and the NCP Watchdog process.

- **The Network Address Is Static.** If you disconnect a NetWare client from network AA-BB-CC-DD in Building 1 and connect it to network DD-CC-BB-AA in Building 4, the client still thinks its network address is AA-BB-CC-DD. As a result, the client places this address in the IPX header's source network address field whenever it sends a packet across the network.

  When a server responds to the client's NCP request, the reply is sent to network AA-BB-CC-DD. Because the client is no longer at that address, however, it never receives the server's reply. Therefore, the client continues to send its request until it reaches the maximum number of retries set in the NCP Retry Counter, and the client times out waiting for a reply.

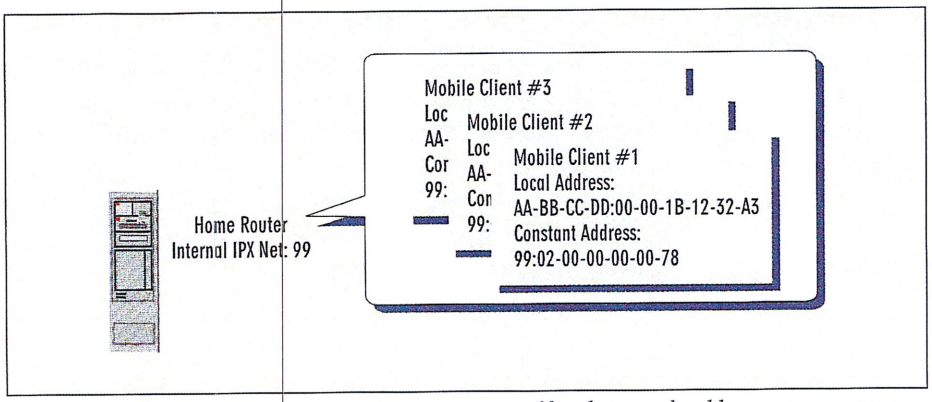


Figure 2. *The Home Router maintains a mapping of local network addresses to constant network addresses.*

To prevent this problem, you must unload the NetWare client software and reboot the workstation you have moved. The client then sends a Get Nearest Server request packet and learns its new network address from the Get Nearest Server reply packet.

- **The NetWare Watchdog Process Can Time Out the Connection.** If you take longer than 15 minutes (or whatever amount of time has been specified in the server's NCP Watchdog settings) to move the NetWare client from network AA-BB-CC-DD in Building 1 to network DD-CC-BB-AA in Building 4, the NCP Watchdog process times out the client's connection.

CONNECTING WITH MOBILE IPX

When I examined the protocol-layer performance of Mobile IPX, I discovered that its implementation is both simple and elegant. Mobile IPX does not add a new protocol to NetWare's existing protocol suite; it simply uses standard Routing Information Protocol (RIP), Service Advertising Protocol (SAP), and NCP communications. Because Mobile IPX uses these protocols to send Mobile IPX client packets across the network, these packets appear as typical, nonmobile client packets. As a result, both NetWare MPR 3.1 and third-party routers can automatically forward these packets just as they forward other client packets.

In addition, Mobile IPX uses NetWare's existing internal and external IPX network addressing scheme to define the destination of Mobile IPX client packets. In effect, Mobile IPX just uses some simple trickery to remove the network location dependence. In this way, Mobile IPX is an ingenious use of the natural behavior of NetWare.

As mentioned earlier, the Mobile IPX technology consists of two main parts: the Home Router and the Mobile IPX client software. The Home Router handles all communications between the destination server and the Mobile IPX clients. To do this, the Home Router assigns each Mobile IPX client a unique *constant network address*, which is a virtual address that exists on the Home Router. This address consists of the Home Router's internal IPX network number and a fictitious node address for the client.

A Mobile IPX client also has a local network address, which is the address of the physical network to which the client

is attached (or to which it dials in). As shown in Figure 2, the Home Router maintains a mapping of local network addresses to constant network addresses.

A Mobile IPX client sends an NCP request directly to the destination server, placing its constant network address in the source network address field of the IPX header. The server then processes this request and sends an NCP reply to the constant network address—the Home Router's internal IPX network number.

The Home Router, in turn, forwards the server's NCP reply to the Mobile IPX client via the best route using the client's local network address. The Home Router determines the best route by referring to its internal Router Information Tables and looking for the router that requires the lowest number of ticks to send the reply to the client. (A tick is approximately 1/18 of a second.) Figure 3 shows a typical data path for Mobile IPX. (See p. 30.)

In addition, the Home Router performs Watchdog spoofing for Mobile IPX clients. In Watchdog spoofing, the Home Router replies to NCP Watchdog packets on behalf of a Mobile IPX client. Because the Home Router replies to these packets, a client's NCP connection is maintained even if the client roams out of range of an access point.

Establishing a Connection

To understand how Mobile IPX works, you should understand the Mobile IPX sign-on process. The following steps explain how a Mobile IPX client establishes and maintains an NCP connection:

Step 1: Locate the Nearest Home Router

When a Mobile IPX client boots up, it generates a Get Nearest Server request that indicates the client is looking for the nearest Home Router (SAP number 0x021D). Whereas a nonmobile client sends a Get Nearest Server request looking for the nearest file server or directory services server, a Mobile IPX client must locate the nearest Home Router so that the client can learn its constant network address from this Home Router.

The Get Nearest Server reply packet, then, serves two purposes: It lets the Mobile IPX client know its constant network address, and it identifies the internal IPX network number of the nearest Home Router.

Step 2: Find the Best Route

To determine the best route to the nearest Home Router, the Mobile IPX client sends a RIP route request to the Home Router. After checking its Router Information Tables, the Home Router sends a RIP route reply to the client, indicating which router can forward the client's packets to the Home Router using the lowest number of ticks.

Step 3: Get a Constant Network Address and a Time-To-Live Setting

The Mobile IPX client then sends a sign-on request packet to the nearest

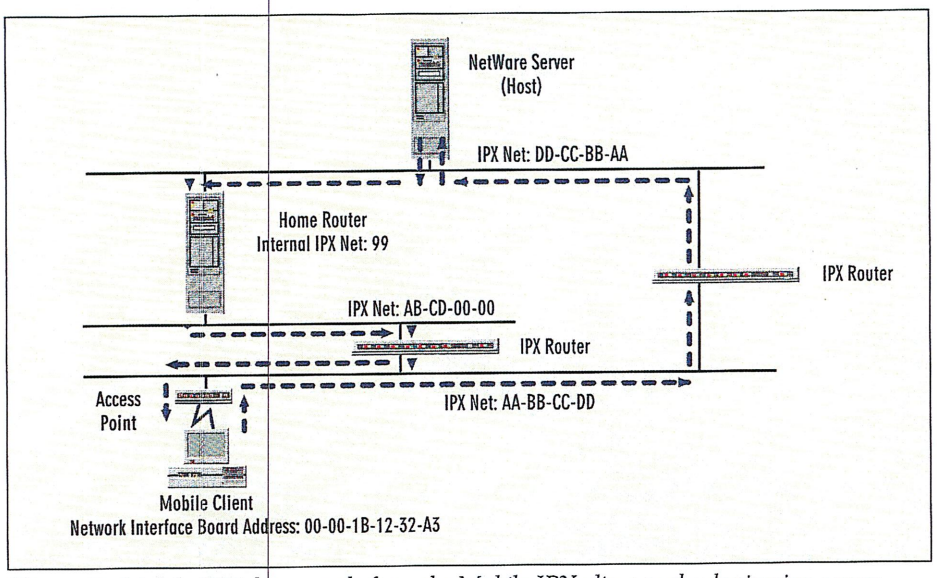


Figure 3. *Mobile IPX data travels from the Mobile IPX client to the destination server. The server's reply is sent to the Home Router, which transmits the response to the client.*

Home Router via the best route. This packet contains the client's local network address (AA-BB-CC-DD:00-00-1B-12-32-A3, for example). The Home Router keeps track of the client's local network address and assigns the client a constant network address. As mentioned earlier, this address is based on the Home Router's internal IPX network number plus a virtual node address that is determined by a combination of variables, such as the number of times the Home Router has been reset and the number of clients to which the Home Router has already assigned a virtual node address.

In addition to the Mobile IPX client's constant network address, the Home Router's sign-on reply packet contains a Time-To-Live (TTL) setting that indicates how long the client can be detached from the network before the Home Router will terminate its NCP connection.

Step 4: Maintain the Connection

Whenever the Mobile IPX client detects a change in its local network address, it sends a Bind Update request packet containing its new local network address to the Home Router. The client can detect such a change when it sends a RIP route request packet across the network and receives a response. The RIP route reply packet includes the client's local network address.

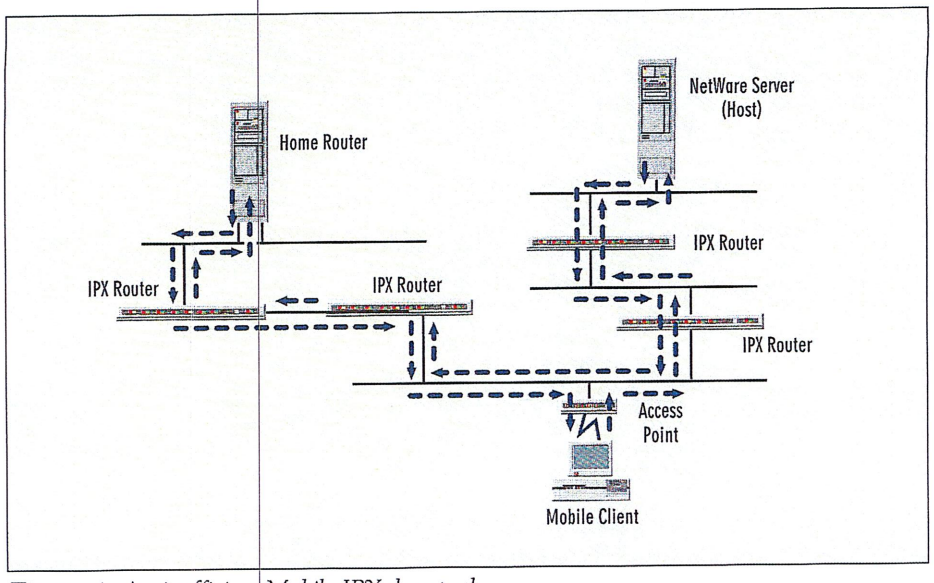


Figure 4. *An inefficient Mobile IPX data path*

The Mobile IPX client sends a RIP route request packet and a Bind Update request packet approximately one minute before the TTL timer is set to expire. The Bind Update request packet contains the client's local network address in the source network address field of the packet's IPX header.

Upon receipt of the Bind Update request packet, the Home Router determines whether the Mobile IPX client has been moved by comparing the local network address in the client's Bind Update request packet to the local network address in the Home Router's mapping of local network addresses to constant network addresses.

If the Mobile IPX client has not been moved, the Home Router resets the TTL timer to zero and sends a Bind Update reply packet to the client's existing local network address. If the client has been moved, however, the Home Router maps the client's new local network address to the client's existing constant network address and sends a Bind Update reply packet to the new local network address.

DESIGNING A NETWORK FOR MOBILE IPX

Because all reply packets must travel through the Home Router on their way to a Mobile IPX client, you should pay particular attention to where you place the computer running NetWare MPR 3.1 with the Home Router enabled. If you place this computer across the network from the client's destination server and the client's local network, reply packets must traverse the entire network to get to the Home Router before being rerouted to the client, as shown in Figure 4.

In Figure 5, on the other hand, the intermediate computer running NetWare MPR 3.1 is being used as the Home Router. (See p. 32.) This path is logical because it does not require any additional hops, and it does not place an additional load on unrelated network segments.

CONFIGURING A MOBILE IPX CLIENT

Before you configure a Mobile IPX client, you must ensure that the client has a Mobile IPX-aware network driver. (To find out whether your network driver is Mobile IPX aware, you will need to contact the vendor that made your network interface board.) To be Mobile IPX aware, a network driver must include the following features:

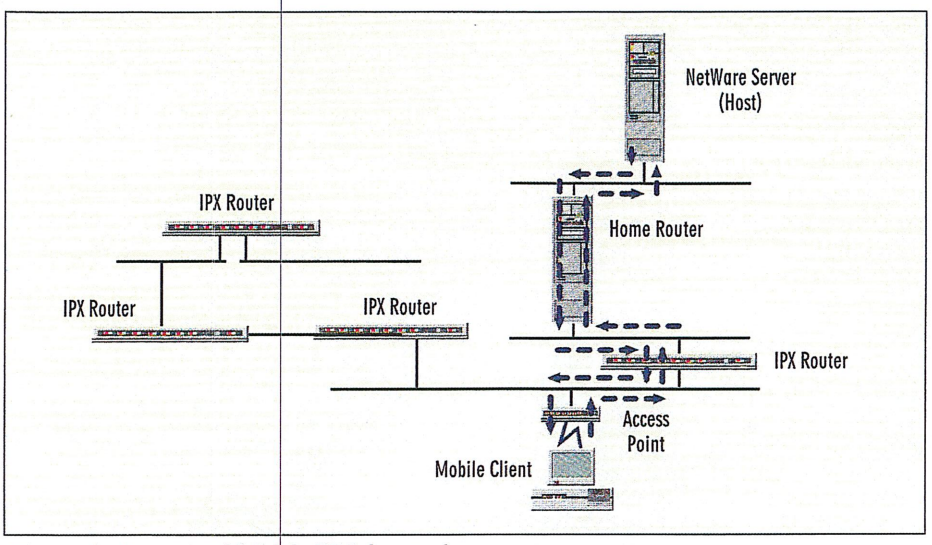


Figure 5. *An optimal Mobile IPX data path*

- The ability to detect when a PC card is inserted in or removed from a wireless Mobile IPX client
- The ability to detect when a wireless Mobile IPX client is within range or out of range of an access point
- Support for the NetWare Event Service Layer (NESL)

A Mobile IPX-aware driver can detect specific changes that occur with a Mobile IPX client, such as if a PC card is removed from a client or if a wireless client travels out of range of an access point. When the driver detects a change, it notifies IPX of the change through NESL. NESL then triggers the Mobile IPX process to take the necessary steps to maintain the client's NCP connection.

For example, suppose that you hot-swap a Mobile IPX client's network interface board. The client's Mobile IPX-aware network driver uses NESL to notify IPX of a change in the network interface board and the board's hardware address. NESL, in turn, triggers the Bind Update process to ensure that the client's local network address remains current in the Home Router's Router Information Tables. In this way, the client's NCP connection is maintained.

To configure a Mobile IPX client, install the client software that comes with NetWare MPR 3.1 or the NetWare Client for DOS and Windows 1.20b. Then you must make the following changes to the workstation's STARTNET.BAT file:

```
@ECHO OFF
SET NWLANGUAGE=ENGLISH
CD \NWCLIENT
LSL
NESL
driver
    (alternate driver)
IPXODI /M
VLM
```

The IPXODI /M switch enables the Mobile IPX client software, which includes the NESL executable file. NESL notifies IPX of any changes in the network interface board's hardware address (the media access control, or MAC, address) or the client's local network address.

CONFIGURING THE HOME ROUTER

On NetWare MPR 3.1, load the INETCFG utility, select Protocols, and then select IPX. The IPX Protocol Configuration screen appears. Choose Mobile IPX Support, and then select Enable.

Finally, select Mobile IPX Configuration to define the following parameters:

- **Time-To-Live Override.** This parameter overrides a Mobile IPX client's TTL setting, which specifies how long a Home Router will maintain the client's NCP connection without receiving an NCP reply from the client.

  You can specify 1 to 10,080 minutes for this parameter; the default setting is 30 minutes.
- **Watchdog Spoofing.** This parameter determines whether the Home Router can respond to a server's NCP Watchdog communications on behalf of a Mobile IPX client. If the Home Router responds to these communications, the Mobile IPX client will not lose its connection if it roams out of range of an access point.

  You can enable or disable this parameter; the default setting is Enabled. (You would disable this parameter if you wanted the Watchdog process to allow a Mobile IPX client only 15 minutes of out-of-range time before terminating its NCP connection.)
- **Broadcast to Virtual Network.** This parameter defines whether broadcast packets (such as a server's broadcast of its Server Information Tables) are sent by the Home Router to a Mobile IPX client. Unless a client requires these packets, you can reduce traffic by forcing the Home Router to discard them.

  However, if a client is running software that monitors servers, that client will require broadcast packets. If the client stops receiving broadcast packets from the servers it is monitoring because the Home Router is discarding these packets, the software assumes the servers have gone down and may trigger an alarm. (An alarm is triggered only if the software is designed to send an alarm.)

  You can choose to forward or discard broadcast messages; the default setting is Forward.

After you have configured the Home Router, press the Escape key and save your changes when prompted. Then select Reinitialize System to make the changes effective immediately.

CONCLUSION

Because Mobile IPX uses the existing NetWare protocol suite, you can install and configure Mobile IPX on a NetWare network quickly and easily. Mobile IPX clients can then roam from one place on the network to another without losing their NCP connection. The possibilities are endless: In fact, you might want to look out for users who are logging in to the network from their laptop—poolside!

For more information about NetWare MPR 3.1, visit Novell's World-Wide Web (WWW) site (http://iamg.novell.com/iamg/products/mpr/nwmprtoc.htm).

Laura Chappell researches, writes, and lectures on NetWare protocol performance, troubleshooting, and optimization. You can reach Laura at lchappell@imagitech.com.

Special thanks to Terry Bailey, Novell associate software engineer, for his help with this article.