Bell Laboratories IOTA Technology

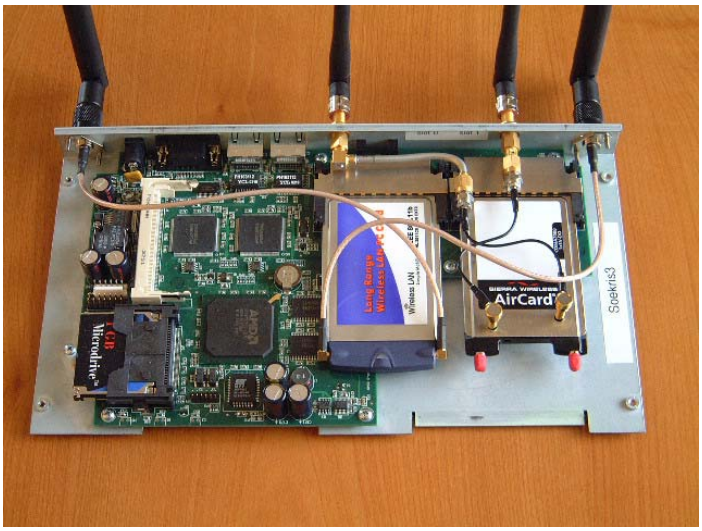
Scott Miller
(scm@lucent.com)
Lucent Bell Labs
Dept. of High Speed Mobile Data

The Lucent Technologies Bell Laboratories Research IOTA team has developed the necessary components for allowing a 3G wireless carrier to offer integrated service across 802.11 and 3G wireless networks. The technology also works in an 802.11 only deployment and is tailored for use in public 802.11 deployments. Currently we have advanced prototype versions of:

802.11 Access Gateway

The 802.11 Access Gateway is connected behind the 802.11 access points in an 802.11 deployment and allows the backend infrastructure deployed for 3G networks (AAA, MobileIP Home agents, billing servers) to be used for public 802.11 service. The 802.11 gateway simultaneously supports both the SimpleIP (portability) and MobileIP (full mobility) modes of operation, as well as several IP services such as QoS, DHCP, NAT, dynamic packet filtering, web caching, and HTTP/DNS redirection. The gateway would support the 3GPP2 and WECA standards for MobileIP and Radius support and provides the means to provide security and accounting in a public 802.11 deployment. The gateway is a software solution that runs on the Linux operating system and uses off-the-shelf hardware.

MobileHotSpot Gateway



Combines an 802.11 Access Point, 1xEV-DO 3G wireless data backhaul and the public access gateway networking functionality of the 802.11 Access Gateway into one small appliance-like box. This single box solution simply needs power to enable easy

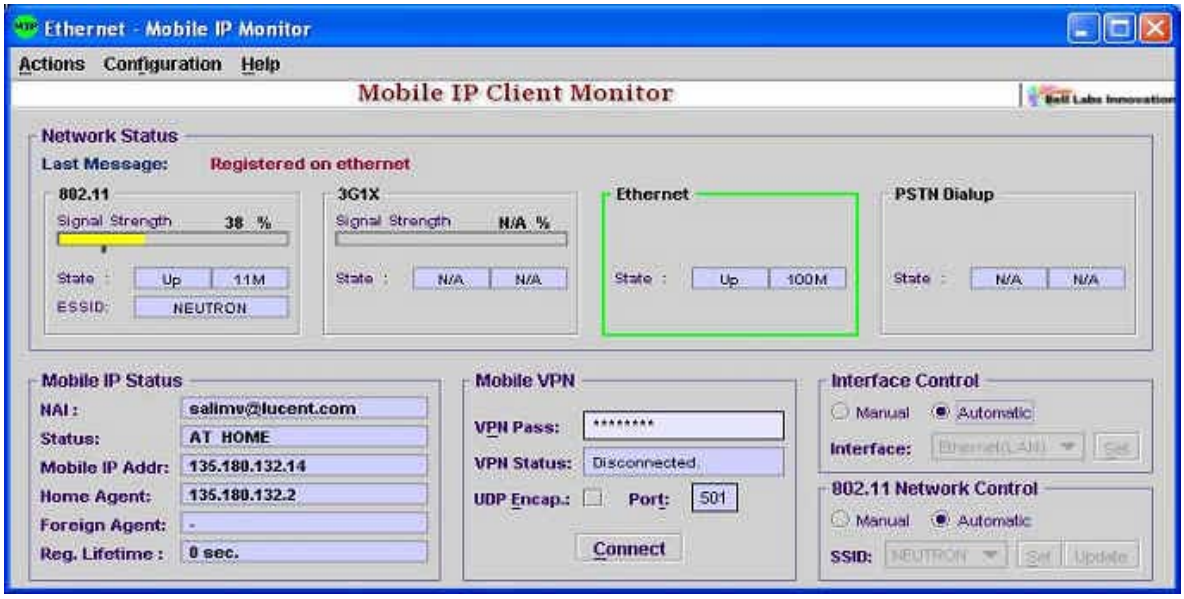
installation of an 802.11 hotspot using the 3G data backhaul. This would enable 802.11 hotspots on buses, trains, and for other temporary network setups (outdoor events, ships in port, temporary building moves, conference room network access, emergency setups, etc) without requiring wired network access.

The gateway may also function in a mobile environment where the backhaul is established via a wireless data channel such as UMTS, 1xRTT, GPRS, or other such wireless packet data channel. The wireless modem for the backhaul is embedded into the gateway or connected externally (e.g. ethernet, USB, etc). In this instance, the gateway is responsible for initiating the connection over the wireless backhaul channel using configured information required for authentication such as network access identifier (NAI), password/shared secret, access point name (UMTS/GPRS), and dial string required to establish the packet data channel via a PPP connection. The IP address used for this wireless backhaul channel may be statically configured or may be obtained dynamically from the wireless access network during the PPP negotiation. When the IP address is obtained dynamically the gateway lautoconfigures, based on the obtained address, the foreign agent care of address for MobileIP mode of operation and the address to NAT to, for SimpleIP mode of operation. Since the wireless backhaul channel may be lost depending on coverage and interference conditions, the gateway constantly monitors the status of the connection and re-establish the connection if it is dropped. The gateway requests the IP address that it previously received in the last successful establishment of the channel, however, the network may not be able to allocate the same IP address on re-establishment. In that case, the gateway again reconfigures itself to the newly obtained IP address. In the MobileIP mode of operation, the gateway then starts advertising the new foreign agent care of address, which appears to MobileIP clients as if they moved to a new network with a different foreign agent, and reinvoke the MobileIP registration procedures. For SimpleIP mode of operation, the NAT reconfiguration causes existing TCP and UDP flows to fail due to the IP address change. However, any new flows are NATed to the new IP address and the subscriber is able to continue the data session without reauthentication needed.

The gateway also obtains the local DNS server IP address on backhaul establishment. All DNS requests from clients are redirected to this optimal local DNS server by the gateway regardless of the clients prior DNS setting.

The gateway supports an ethernet backhaul connection using DHCP and doing a similar autoconfiguration process as outlined above for the wireless backhaul case. In this instance, the gateway obtains the IP address and DNS server addresses dynamically by initiating a DHCP exchange on the connected local network

Multi-Interface MobileIPv4 Client software



Offers MobileIP support and intertechnology handoff across multiple interfaces (e.g. ethernet, 802.11, 3G1X, 1xEV-DO). The client selects the best interface based on an algorithm so that the user does not have to constantly adjust their wireless setting and pick interfaces and relogin. The client software also selects the best 802.11 ESSID (network name) without requiring Windows XP support or user interaction. The client's graphical user interface controls the Lucent IPSec client software (if installed) and supports MobileIP over IPSec. It is expected that the client will interoperate with other vendors' IPSec clients. This enables users to connect securely to their enterprise networks from a public 802.11 or 3G wireless connection and then switch between subnets or even between the two technologies without interruption to the running applications. The client runs under the Windows operating system. A detailed description of the IOTA client software follows:

A. **Management of the 802.11 wireless interface**. The code contained in the Bell Labs client overrides the default control of the 802.11 wireless interface by the Windows operating system. These features are:

- Selection of new BSSID (i.e. access point) whether on same subnet or different subnet
- An algorithm based on signal strength and preferred networks that the client software uses to automatically select the best 802.11 network from those that the client detects in the current location. This allows switching to a new access point before losing connectivity completely to the current access point. The algorithm contains a bounce protection algorithm to prevent rapid switching between interfaces or access points. Also provided is a tunable means to average several signal strength samples before making the final decision to pick a new network.

- A preferred network list containing an ESSID list optionally with the associated WEP key for the ESSID entry. The list is ordered such that networks at the beginning of the list are selected over those below. The setting of the WEP key for the network is done automatically and an association with the access point is forced.

B. **Management of multiple profiles**. The client will allow the user to select a particular profile before logging in. The profile contains items such as:
   - User name/login/Network Access Identifier
   - A shared key or certificate used for authenticating the user or a pointer to where this information is stored
   - A preferred network list per profile
   - For mobile IP support, mobile IP configuration parameters such as Home Agent address, Home address, registration lifetime, authenticator information, etc.

C. **Management of multiple interfaces**. The client will automatically select based on priority and signal strength rules which physical interface will become the primary interface for sending network traffic. The interface may be 802.11, 3G1X, 1xEV-DO, UMTS, PPP variants, Ethernet. The client software may choose to suppress notification of the absence of one of these interfaces from upper layer protocol stacks. A graphical user interface is provided to show the current status of all the configured interfaces.

D. **Multi-interface Mobile IP protocol support**. The client will perform Mobile IP procedures compliant with RFC 3220, RFC 3012, and the wireless standard IS-835. The Mobile IP support will also span multiple interfaces so that the same IP address can be used even when switching physical interfaces on the client device. For example, this allows seamless inter-technology handoff between 802.11 and 3G or 802.11 and Ethernet. A graphical user interface is provided to show which interface is currently active as well as a summary of the Mobile IP parameters currently in use.

E. **Support for IPSec over MobileIP.** By inserting the NDIS intermediate driver below the IPSec NDIS layer, IPSec over MobileIP is achieved by allowing all MobileIP signaling to be done outside of the normal kernel packet flow in Windows. Integration with the Lucent IPSec client is provided. This feature allows a user to maintain their VPN connection even when crossing subnets or using a different physical interface.