

Purpose

The purpose of this whitepaper from TapRoot Systems, Inc. is to discuss mechanisms for affordable and secure access to the internet from a laptop using a mobile phone as the conduit. While there are many different mechanisms and products currently providing internet access via a mobile phone to the laptop, it is important to understand that not all access methods are equal. This white paper will provide some perspective on the different technologies that are currently in use to provide access to the internet for a laptop via the mobile device.

The Challenges of Mobile Connectivity

People conducting business on the go face challenges of staying connected to office systems that ultimately hamper productivity and although cell phones and mobile email devices have made strides, the simple fact is, they do not give the full experience that one gets from a laptop or larger screen device.

In addition to getting connected there is also an argument brewing about which network is best for connectivity: 3G wireless wide area networks (WWAN) or wireless local area networks (WLAN) that run on the 802.11x standards. TapRoot Systems see the two networks as complementary rather than competitive alternatives. The 3G WWANs are great at broad coverage while the Wi-Fi™ networks have great penetration for connectivity to laptops, MP3 players, gaming devices, and a host of new “connected” devices.

Finding hotspots: For those needing to sync up, the endless pursuit of a Wi-Fi hotspot can be a frustrating ordeal. This may suffice for those familiar with the local hotspots but for those visiting an unfamiliar area, the quest for connectivity can become a daunting and somewhat costly task. In today’s world, the idea not having access at any given time or location is unacceptable. Having to physically travel to find a hotspot or waiting to sync up is something that is not only a waste of time but also something that can easily be avoided.

About TapRoot Systems, Inc.

TapRoot Systems, Inc. provides software products and services for the mobile device marketplace. The company specializes in foundational software solutions and creative applications for the industry's major mobile operating systems: Microsoft® Windows Mobile®, Microsoft Windows CE®, Linux® Mobile, and Symbian OS®. TapRoot is a Microsoft Development Partner, a MontaVista™ Mobilinux™ Partner, a Symbian Platinum Partner, a S60 Contractor and a S60 Wireless Technology Provider. TapRoot Systems is headquartered in the Research Triangle Park area of North Carolina, USA with development facilities around the world. For more information, please visit www.TapRootSystems.com or email marketing@taprootsystems.com.

About the Author

Mike Linstrom is the VP of Carrier Technologies for TapRoot Systems, Inc. Mike has over 22 years of experience in software, product development and management. Prior to joining TapRoot, Mike was head of the Enterprise Solutions, Mobile Devices Business Unit for Nokia in Irving, Texas. Mike leads TapRoot’s efforts in the development of applications positioned to assist wireless carriers in satisfying subscribers needs.

Non-standard implementations: After the pursuit of the hotspot ends successfully, there is still the challenge of connecting successfully. Hotspots are configured differently depending upon the wireless internet service provider (WISP). At times just accessing the home splash screen or captive portal to authenticate or log on can be problematic. Any failures put unnecessary burdens on IT departments. Resolutions to connectivity or usage issues must be resolved on a case-by-case basis. However, when a user is at home, wireless connections to the internet are fast and easy regardless of the WLAN router security settings. This is because the connection has been done before and is a “known” entity. No logging in, no looking through settings to make a connection work, in short it is a “fast track” to connectivity.

Security: While typical public networks offer the easiest connectivity they also have the least security or control. These WLAN hotspots are typically unsecure and the data is transmitted as clear text and while some authenticate users, the data transmission is still unsecure enabling hackers to see everything that is transmitted. Closed public networks utilize software, either on the router or a server, to control the network and limit it to only authorized users and while WPA does provide additional security, it also can bring headaches for IT managers as it does and can conflict with certain enterprise configurations. These closed public hotspots typically force the user to make payment via credit card. The transmission of that information over a potentially un-secure network plus the storage of that information increases the exposure to identity or personal information theft.

Availability: Unfortunately availability is still an issue. It is not always feasible to travel to a public hotspot and most areas are still not covered by public or private access networks. When visiting a business client’s location, many times the network access at their facility is secure but limited to employees and it is simply not feasible to run down the street for internet access. With a mobile solution the user could access the internet to get the needed information anywhere there is cellular coverage.

Other solutions: While many of today’s Smartphones include modem functionality and can be connected either by cable or wirelessly via Bluetooth or IrDA, the solution is typically too complicated for the average user. The cabled solution forces a user to have the cable with them at all times and the wireless solutions are limited to either line-of-sight (IrDA) or distance (Bluetooth). All of these solutions offer just a single connection to the internet despite their complexity. In addition to the limitations mentioned above, the user must traverse the phone menus to turn on the wireless radio and then go to another menu to tether the Smartphone to the device. Additionally software, either drivers and/or synchronization, must be loaded and maintained on the target laptop. All of this makes for an overwhelming experience that is just not acceptable for the average user.

A Solution for Secure and Easy Mobile Internet Access

Ideally, one could turn a Smartphone with an integrated Wi-Fi radio into a mobile router or hotspot with just a simple press of a button. As important as the functionality is, the solution must be both intuitive (easy-to-use) and secure. The 3G (or faster) WWAN could be utilized as the backhaul while the 802.11x radio would be used to set up an ad hoc WLAN. Utilizing an ad hoc network would enable connectivity via the mobile phone to any Wi-Fi enabled device that needs internet access. This solution would offer simultaneous connectivity to more than one device. The bottom line is that fast, secure internet access would be available when needed and where wanted since the mobile router would be, well, truly mobile!

The Benefits of Mobile Internet Access

The solution would, in a sense, extend a carrier's network to fulfill broader access while allowing the carrier to maintain control of the data pipe. This would give the end-user a familiar umbrella in which to operate. It would also give the IT manager a consistent mobile interface to the internet that would decrease cost, complexity, and support while enabling increased productivity.

Affordability: Where public hotspots can be costly from a month-to-month contract for a single license, the proposed solution would be a low cost, high availability solution. Since most road warriors already have data plans on their mobile phones, the delta cost would be small to have full access to the internet anywhere a cellular call can be placed.

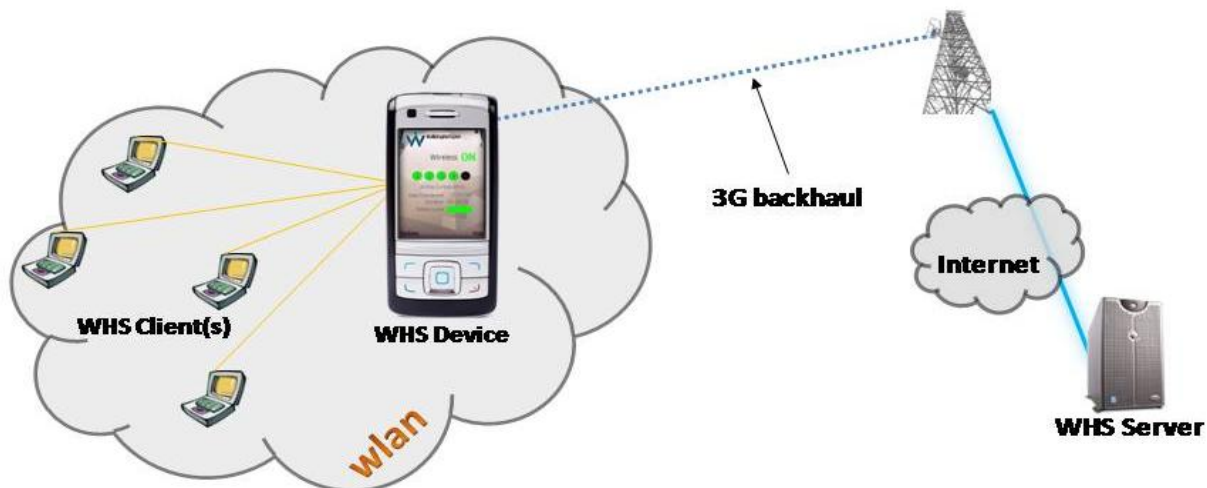
Productivity: Having a mobile hotspot when and where needed would enable connectivity to pertinent data at any time and location. There would be no need to wait to get to the office, hotel, or home to connect. There would also be no need to seek out a public hotspot; simply start the application and connect. Another key feature for the proposed solution would be that not only would it allow connectivity virtually anywhere but it would be truly mobile, which means connectivity in motion: on trains, on buses, and in cars, etc. The nature of the carrier networks allow hand-offs from tower to tower as you move about the city or from city to city. In the event of a network drop, the WLAN could stay persistent and the WWAN connection would be self healing; meaning it comes back up automatically when available.

The TapRoot Solution: *WalkingHotSpot*™

The *WalkingHotSpot* solution from TapRoot Systems is a carrier grade solution that bridges the two radios in a Smartphone to create a truly mobile router. It enables connectivity for end-users while providing a secure extension of a carrier network. Various service levels are available to provide differentiation in both features and number of concurrent users and can be tailored to various operating models such as carriers, enterprises, WISP replacement/extension, and rural WISP coverage.

The application is robust but light, meaning it can easily run in the background servicing a number of connected clients to the internet while making calls or running other applications. It is an after-market application, which means it is downloadable or upgradeable over-the-air. As can be seen in the system diagram below the *WalkingHotSpot* solution utilizes a client server architecture. The WHS server (i.e., the authentication server portion of the solution) provides seamless connectivity while enforcing security methods required by mobile network operators (MNOs). The server can even be integrated into a carrier or enterprise network or it can be hosted outside and communicate via secure channels. Some of the other benefits of this architecture are explained in the following paragraphs.

WalkingHotSpot Solution System Architecture



Security: and usability are built in from the ground up and not just an afterthought. Like the public networks, the *WalkingHotSpot* solution offers very easy access to known clients, but utilizes the WHS server to control network access via common security methods in use today with some key enhancements that are made possible and enforced by the WHS server. As an additional authentication safeguard, the owner of the Smartphone controls who can and cannot connect. Overall, access is very easy to obtain via a true standard pipe utilizing HTTPS and SSL for secure communication. Additionally this solution allows VPN traffic making the overall solution one that even IT managers willingly embrace.

Usability: means the application is easy to download, setup, and use. Start to finish – the data entry (sign-up) to provision the application, download, install, and setup takes less than five (5) minutes to complete. But the real evidence is when connectivity is needed, simply start the application and point any Wi-Fi enabled device at the newly created WLAN – it is that simple! If a device is connecting for the first time, a pop-up dialog will appear on the Smartphone running the *WalkingHotSpot* application, asking the owner if access is allowed. Security, ease of use, speed of service, and mobility a powerful combination of features in a small package enable productivity on the go.

Mobility: For locations that have wired broadband access, it is easy to create a WLAN. All that is needed is for the user to purchase a wireless access point, connect it to the broadband gateway and connect. While this solution does indeed provide wireless access, it does so in a fixed location or perimeter. The *WalkingHotSpot* solution is the next step in mobility by enabling the user to take the hotspot with them. No longer does an end-user need to find a hotspot by traveling to a fixed location network and unlike tethering via cable, IRDA, or Bluetooth connectivity can be shared by multiple client devices. This solution will fundamentally change the way people access the internet by focusing on three main components, mobility, security, and ease of use. No longer will people need to wait to connect or share data. Full internet access will now be available in remote areas that were previously without broadband access. The *WalkingHotSpot* solution is an option to consider when purchasing a WLAN access point but with one huge advantage, it is mobile!

With an already very large installed base, greater than 200 million, the number of devices that have embedded Wi-Fi continue to grow at ever increasing rates due to low costs and complexity. Conversely, the promise of free municipal Wi-Fi has not materialized due to a questionable business model. This undoubtedly will mean that free hotspots will continue to grow but the lack of security will weigh heavily on the user as they transmit private information. This will undeniably pave the way for a new generation of personal, secure wireless access led of course by the *WalkingHotSpot* solution.