WHITE PAPER NOVEMBER 2012

MITIGATING CARRIER MOBILE TRAFFIC JAMS

WHY WI-FI IS THE DATA OFFLOAD OPTION OF CHOICE

MOTOROLA

INTRODUCTION

MANAGING CROWDED MOBILE NETWORKS

The rapid uptake and now mainstream use of wireless smart phones and tablets have led to an explosion in mobile data consumption. These massive consumption levels have created requirements for substantially more wireless network capacity to transport mobile traffic. Users already expect high-speed wireless access anywhere and anytime, and their usage is only expected to multiply as smart phones, tablet computers and other mobile devices continue to proliferate.

For example, while the United Kingdom's Portio Research reports that smart phone shipments reached 485 million in 2011, it expects that number to top 655 million in 2012 and leap to 1 billion in 2016. And International Data Corporation has upwardly revised its tablet-shipment forecasts for 2012 to 107.4 million and for 2013 to 142.8 million. By 2016, IDC expects worldwide tablet shipments to reach 222.1 million.

It goes without saying that these and other usage trends are stressing mobile operators' networks nearly to exhaustion. And the potential for network traffic jams will continue even as carriers upgrade their infrastructures to support faster 3G and 4G speeds. The main contributors include the rapid increase of new subscribers running bandwidth-intensive data and video applications combined with limited spectrum availability. And if history is any indicator, application development and consumer usage volumes will naturally rise to meet – and then exceed – the capacity of the network.

Mobile service providers need a strategy to successfully handle mobile traffic demands so they can continue to deliver high-quality mobile experiences to subscribers, attract new customers, and retain happy ones.

PRIMARY OFFLOAD OPTIONS FOR MOBILE OPERATORS

Mobile operators have three primary options available to increase their mobile capacity: 1) additional spectrum, 2) femtocells, 3) Wi-Fi.

1) BUYING/LICENSING ADDITIONAL SPECTRUM

This is a difficult and costly alternative, because spectrum is a finite resource and one that is scarce. Getting more of it often entails attempting to buy or barter for spectrum from an existing license-holder. Another option in the United States is lobbying the Federal Communications Commission to move spectrum away from an existing set of services and instead make it available for 3G/4G services. This is a time-consuming and political process. If successful, the would-be license-holder must then compete with others at a federal auction for the spectrum and, if victorious there, must pay considerable license fees costing millions or even billions of dollars.

2) USING FEMTOCELLS

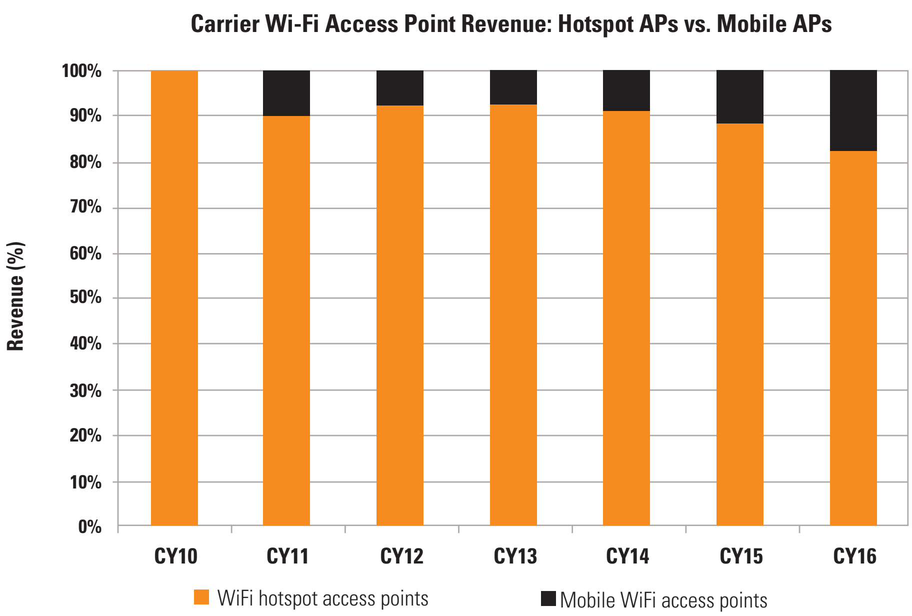
This option involves supplementing the macro-cellular network of large outdoor cell towers. Femtocell equipment is relatively new, constituting very small cellular base stations that support small numbers of users (compared to traditional cell towers). Because they are smaller, they are far less expensive than full size cell towers and can be quickly and easily installed exactly where signal sources are needed to plug coverage gaps. But there are some downsides to femtocells:

- They require the use of the same costly and scarce licensed spectrum as the cell towers.
- They are generally used indoors only and might interfere with operation of the macro network.
- They currently each support relatively limited coverage areas of up to about 30 feet (compared to a cell tower's reach of 20 to 45 miles, depending on terrain).

3) OFFLOADING CELLULAR TRAFFIC ONTO WIRELESS LANS (WI-FI)

Mitigating the traffic problem by moving mobile WAN traffic onto Wi-Fi networks is proving easier and more economical for carriers than the above two alternatives. Wi-Fi networks operate at multimegabit speeds in unlicensed, rather than licensed, spectra. This means that use of these airwaves is free of charge to whoever builds the Wi-Fi infrastructure. Because most smart phones and tablets contain both cellular and Wi-Fi radios, subscribers can use either type of network. If the mobile network operator has put the appropriate back-end infrastructure in place, subscribers can move between the two network types automatically as traffic loads warrant without having to do anything special. Wi-Fi infrastructure equipment is orders of magnitude less expensive than cell tower equipment and has been reinforced with carrier-grade features and redundancy. Because Wi-Fi can be installed inexpensively, swiftly and without spectrum licenses, it has emerged as a particularly attractive strategy to address today's immediate 3G offload and looming 4G offload requirements.

Figure 1. Industry Poised for Mobile and Wi-Fi Core Integration



Source: Infonetics Research, Inc., 2012

OFFLOAD SOLUTION REQUIREMENTS

There are several important requirements for supplementing a network of cell towers with other bandwidth sources. They relate to unifying the disparate network infrastructures into one system with consistent security, user convenience/transparency, billing and management. The necessary components include the following:

1. A common authentication method that works across multiple mobile access networks, including GPRS, EDGE, CDMA, UMTS, HSPA, LTE and Wi-Fi. This is important because at any given time, a subscriber might be using any one of these radio access network (RAN) types. The authentication mechanism should ensure that there is no gap in security as users seamlessly move from one network type to another. This keeps user access secure regardless of which RAN is in use while keeping the log-on experience consistent and simple for subscribers. Users who have to change their behavior to accommodate network differences often abandon the task, and their productivity suffers as does their satisfaction with their mobile service operator.

2. A unified subscriber management system, billing system and user database that are accessible by both cellular and Wi-Fi connections. If multiple network types are to be used, in effect, as "one big network," subscribership management and billing systems must be combined to share information at the back end.

3. Unified subscriber policies for 3G/4G and Wi-Fi to ensure a consistent user experience on both cellular and Wi-Fi networks.

4. Ability of client devices to automatically select 3G, 4G or Wi-Fi connectivity depending on various parameters like signal strength and traffic load. Again, it is important that these decisions be made automatically by the device, without user intervention, to keep user experiences simple, consistent and satisfactory.

5. Ability of client devices to seamlessly roam between 3G, 4G and Wi-Fi networks without dropped connections when crossing network borders. This transparent handoff is sometimes called fixed mobile convergence (FMC) or, perhaps more accurately, mobile-to-mobile convergence (MMC).

6. Enough available capacity in the Wi-Fi network to handle offloaded traffic from the service provider's 3G/4G network, both in terms of the number of concurrent client sessions that can be supported and aggregate throughput.

CHALLENGES OF WI-FI DEPLOYMENT

Wi-Fi is currently the offload favorite of operators because of its low expense and ability for quick deployments. Still, building the network does have its challenges. The primary reason is that there are a number of moving parts in the mobile landscape. Below is a summary of the primary challenges of building a cellular offload network using Wi-Fi:

HETEROGENEOUS MIX OF NETWORK DEVICES

Service providers have limited control over subscribers' client devices that use Wi-Fi and 3G/4G network connections. The various devices that users might choose include feature phones, smart phones, tablets, laptops and netbooks. These devices all have different characteristics and signal strengths. This means that Wi-Fi AP placement and power levels that work just fine for reaching certain clients at a given distance might not be adequate for other, lower-power client devices.

In addition, devices might support 802.11b/g connections, which operate in the 2.4GHz band; 802.11a, which operates in the 5GHz band; 802.11n, which runs in both frequency bands, or, eventually, emerging 802.11ac slotted for the 5GHz band. Moreover, devices could be running any number of operating systems, including Android, BlackBerry, iOS, Linux, Mac OS, Symbian, Windows, Windows Mobile, Windows CE and Windows Phone X. There are multiple releases of each of these operating systems, further complicating the features, capabilities and power levels in use.

While designing a 3G/4G Wi-Fi offload solution, mobile network operators must realize that users might have any combination of these devices and operating systems. Because of this mix, the carrier's offload solution must be able to accommodate this wide range of platforms and their behaviors.

VARIATIONS IN DEPLOYMENT ENVIRONMENTS

Wi-Fi offload deployment scenarios could vary, depending on whether they address indoor or outdoor coverage, high or low densities of users, the size of the desired coverage areas and so on. In some locations, there might be no wired backhaul options available, so the solution will have to rely on a wireless backhaul mechanism such as 3G/4G or WiMax. Or there could be a physical restriction as to where Wi-Fi access points (APs) can be deployed. The restriction could be related to the terrain of the environment or stem from the need for a permit from a local municipality to mount an AP on a light pole. As you can see, there is no "single size fits all" solution, so service providers must consider a wide range of Wi-Fi AP products to meet the special requirements of each of their varied deployment scenarios.

THE UNLICENSED SPECTRUM ENVIRONMENT

The Wi-Fi offload network is built in an unlicensed spectrum environment. This is advantageous because of the cost and ease of deployment. On the other hand, the unlicensed airwaves are equally available to all parties who might wish to use them. This means that there could be interference from other operators' Wi-Fi networks or other devices operating in the 2.4GHz and 5GHz bands. This interference can be avoided and mitigated using the rich and sophisticated Wi-Fi RF management tools available today. However, the sources of interference cannot be entirely eliminated, given that everyone has equal rights to use of the spectrum.

INTEGRATION WITH EXISTING 3G/4G BACK-END SYSTEMS

Because mobile network operators have made a substantial investment in the back-end infrastructure of their broadband (3G/4G) networks, it would be most cost-effective for the Wi-Fi offload infrastructure also to make use of that existing infrastructure for the following activities:

- Single sign-on capabilities for subscribers across 3G/4G and Wi-Fi
- Single billing and subscriber management system
- Reuse of existing database on the home location register (HLR)

All of these require tight integration with the 3G/4G back-end systems and Wi-Fi access network.

REMOTE MANAGEMENT AND TROUBLESHOOTING

Since a service provider's Wi-Fi infrastructure deployment is geographically dispersed, administrators should have a centralized management console in place to monitor and troubleshoot APs deployed at remote sites. Wi-Fi infrastructure downtime means loss of revenues for service providers; if skilled engineers and technicians must travel to AP sites to troubleshoot problems, both downtime and maintenance costs increase. Remote troubleshooting tools, by contrast, give network maintenance personnel the ability to troubleshoot and fix problems without having to be physically present at the remote sites, saving time and expense.

HIGH DENSITY

Most Wi-Fi offload deployments are characterized by higher user density than a typical enterprise deployment, especially in crowded urban locations. With lots of people close together using bandwidth-intensive mobile applications such as social networking, IP conferencing, and video streaming, network capacity requirements expand quickly. Usage loads might require more Wi-Fi APs with power turned down so as to reuse spectrum frequently while avoiding co-channel interference. Wi-Fi infrastructure should be designed to handle multiple concurrent user sessions and to be able to transfer large volumes of data in both the uplink and downlink directions.

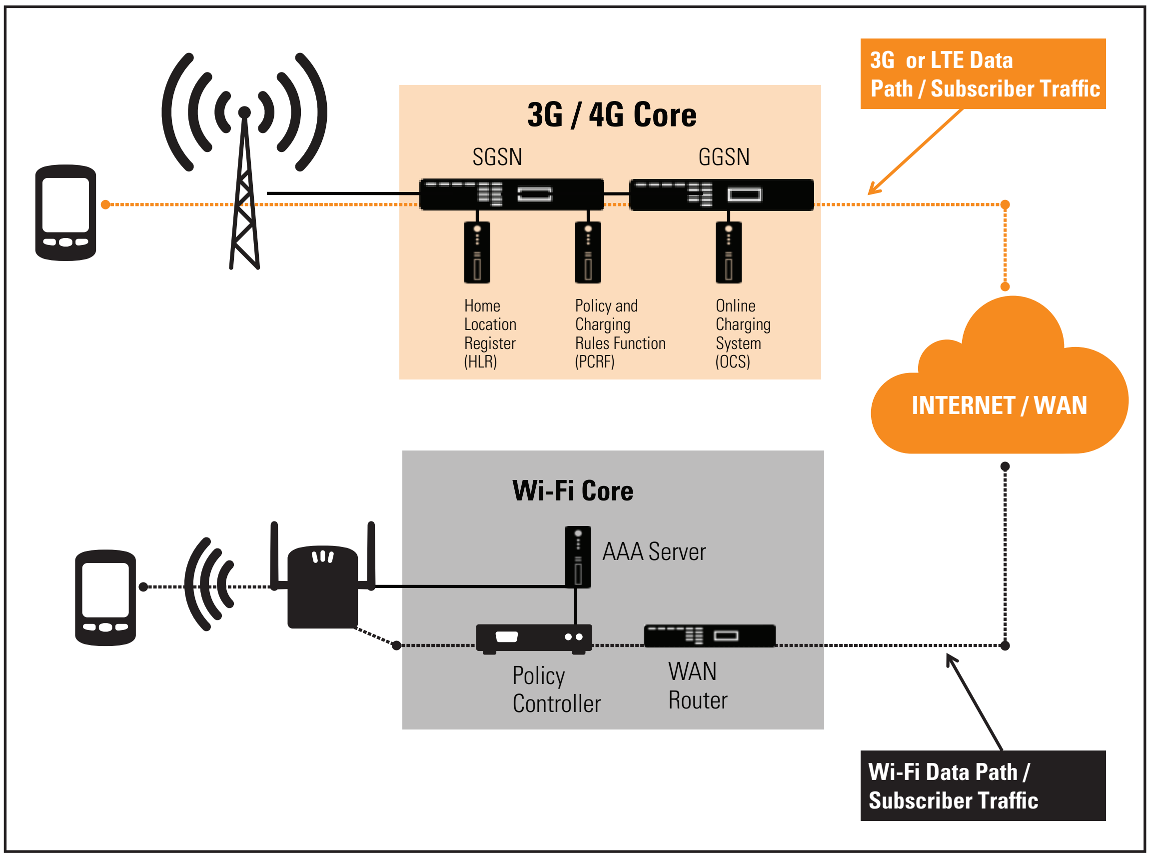
WI-FI OFFLOADING: INTEGRATION OPTIONS

Wi-Fi offloading solutions can range from basic data offload straight to the Internet to more complex integration with the provider's 3G/4G core network and subscriber management and billing systems. The descriptions and diagrams below reflect three different integration approaches: 1) entirely decoupled; 2) coupled by integrating subscriber management databases (control plane) only; and 3) fully coupled, with integrated control and data planes.

1) DECOUPLED SCENARIO

The most basic form of data offloading, this is where the Wi-Fi network and the 3G/4G cellular network simply run in parallel. The mobile traffic is offloaded to the Wi-Fi network through a separate network, and there is zero integration between the two networks. Separate subscriber databases are maintained for both the networks, and the subscriber management systems are disparate. In this case, end users are responsible for manually moving back and forth from 3G (or 4G) to Wi-Fi (see Figure 2).

Figure 2. Fully Decoupled Wireless Infrastructures (No Integration)



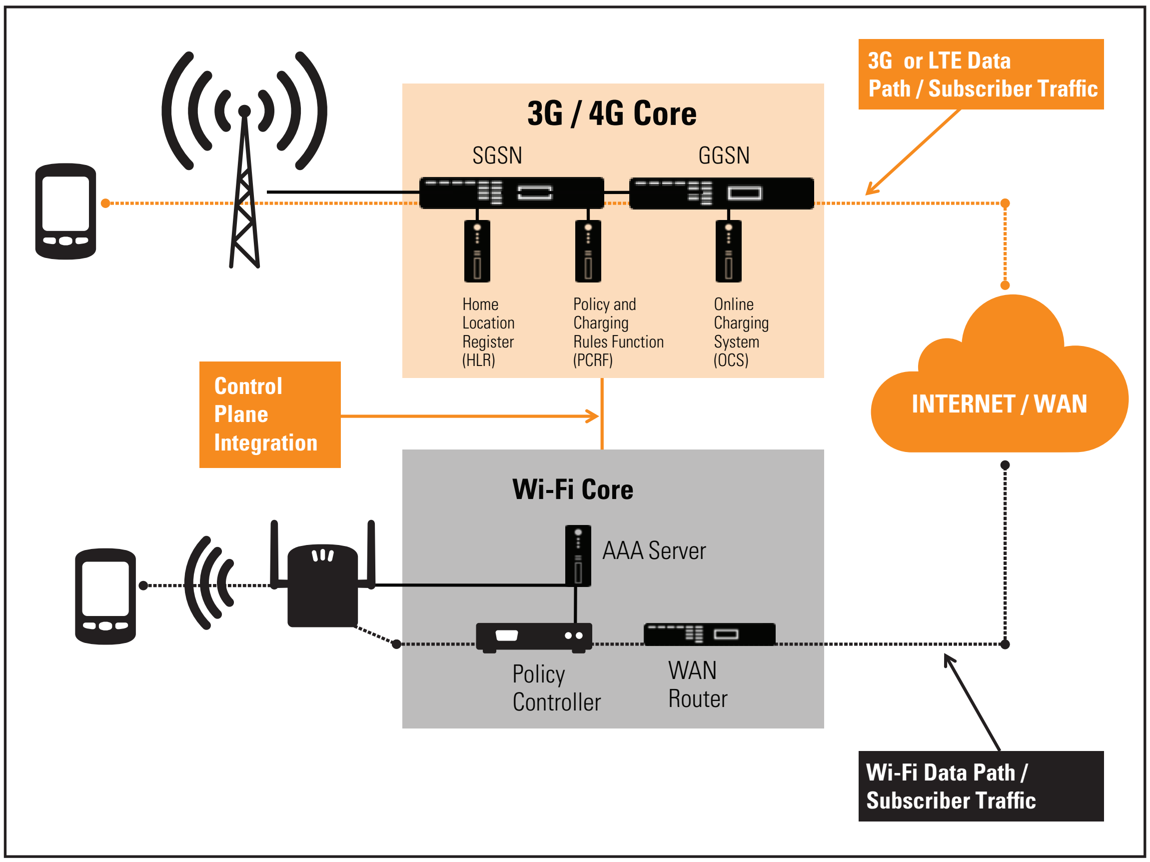
In this scenario, two entirely separate customer databases are in play and must be managed and maintained as such. Operators are inhibited from mixing and matching new service offerings that span both types of networks, because there is no way to link the platforms so that services run over both transparently. Instead, customers must subscribe to two separate services using separate authentication methods, credentials and log-ins, a situation that users will likely find onerous and that will generally inhibit service usability.

2. COUPLED SCENARIO: SUBSCRIBER MANAGEMENT ONLY

In this "loosely coupled" form of Wi-Fi offloading, the subscriber management function of the Wi-Fi network is integrated with that of the core 3G (or 4G) cellular network. The AAA server in the Wi-Fi network core communicates with the 3G (or 4G) HLR for user authentication. At the front end, users authenticate using the EAP-SIM communication mechanism between the subscriber identity module (SIM) on the mobile device and the operator's authentication center. For users without EAP-SIM device capabilities, a separate subscriber database is maintained in the Wi-Fi network core.

In this scenario, the control planes of the two network types are integrated. The policy and charging rules function (PCRF) component talks to the subscriber policy database, for example, and assigns an appropriate quality of service (QoS) priority marking. The QoS parameters are passed to the Wi-Fi APs through RADIUS messages so that QoS levels can be enforced at the edge of the Wi-Fi network. The accounting and billing are also integrated to provide a unified subscriber management platform. While the control planes of both networks are merged, however, the Wi-Fi traffic still takes a separate data path than the 3G (or 4G) traffic (see Figure 3).

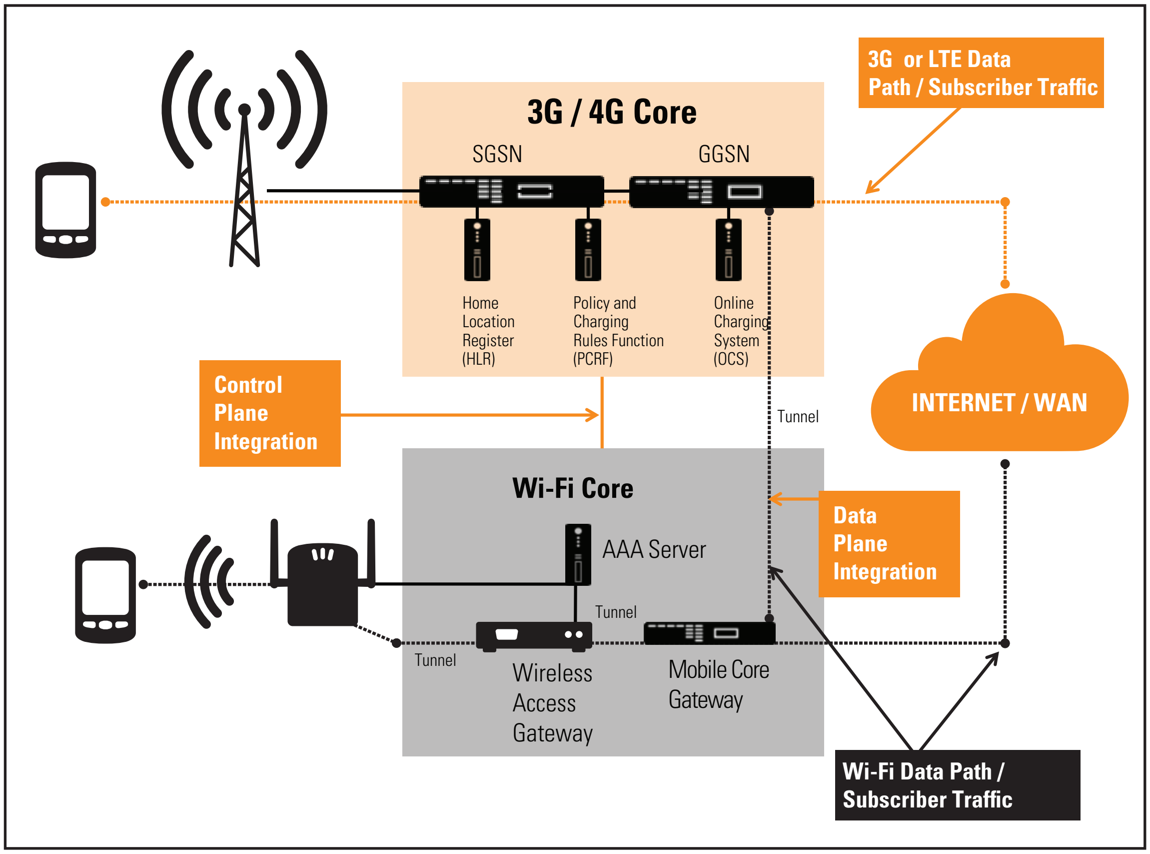
Figure 3. Integrated Control Planes



3. FULLY COUPLED SCENARIO

In this scenario, both the control and data planes of the core cellular and core Wi-Fi networks are fully integrated. By injecting data traffic from subscribers' mobile devices into the operator's mobile core, 3G (and 4G) services can be routed directly to Wi-Fi access networks, without requiring separate logons or any other manual functions on the part of the user. In effect, the WLAN becomes a seamless extension of the cellular network, supporting not only data, but voice, content, television and any other services that the operator might wish to offer.

Figure 4. Integration of Control and Data Planes



Two primary methods of achieving the control and data plane integration shown in Figure 4 have emerged:

1) **Interworking Wireless LAN ("iWLAN"),** a 3GPP specification (TS 24.327). Using this mechanism, the mobile client device opens an IPsec-based VPN tunnel from the device to the dedicated iWLAN server in the operator's core mobile network. This approach has met with some resistance, because it requires special software on each mobile device and can be resource-intensive, consuming considerable battery power.

2) **S2a Mobility based on GPRS Tunneling Protocol (SaMOG),** release 11, a 3GPP specification (TS 23.402). Using this mechanism, the Wi-Fi access point (AP) sets up the secure tunnel, rather than the client device. This approach eliminates the need for each mobile client to run any special software or unique features in order to be a part of the combined cellular / Wi-Fi network environment. As such, it is currently the frontrunner for integrated offload approaches.

ADDITIONAL FMC AND ROAMING CONSIDERATIONS

In addition to the carriers' mobile and Wi-Fi networks being able to exchange subscriber identity information and data traffic, it is important that the user be seamlessly and securely transferred to the "best" network when appropriate. The ability to move on and off networks in the background, securely, without any manual requirement on the part of the subscriber, constitutes the FMC / MMC function described earlier, and is often called "roaming."

The Wi-Fi Alliance, an industry group that certifies interoperability among products, recently announced a new certification program, called Passpoint, which contributes to seamless, secure inter-network roaming. The main elements of Release 1 of the Passpoint program are to provide automatic Wi-Fi network discovery and seamless network selection. By adding additional parameters to the Wi-Fi beacon and probe response frames, the mobile device can learn the capability of each wireless network before authenticating to it. The client device can, based on this information, choose the best Wi-Fi network to connect to.

The Wi-Fi Alliance began certifying Passpoint equipment in June 2012.

PHASED APPROACH RECOMMENDATION

When approaching a 3G/4G offload project, mobile network operators should plan to deploy in multiple phases. The first phase is to combine the authentication and billing functions of Wi-Fi and cellular network operations in order to create a unified subscriber management system. This allows the Wi-Fi infrastructure back end to integrate with the 3G/4G back-end for common authentication, billing, policies and so forth. The result is streamlined operations, lower complexity and reduced cost, compared with running two separate operational infrastructures and billing/subscriber platforms.

Service providers should consider data coupling as a long-term Phase-2 deployment, which will support seamless roaming between Wi-Fi and 3G/4G networks. Without this unification, end users will lack a transparent roaming experience among different network types, which will hamper their mobility experiences and reduce their service satisfaction.

For more information about how Motorola Solutions can help you mitigate mobile traffic jams, visit us at motorolasolutions.com/services.

Part number WP-CARRIER-OFFLOAD. Printed in USA 11/12.

MOTOROLA