WHITE PAPER

Sharing the Load:

- The Value of Subscriber, Service, and Policy Control in Mobile Data Traffic Offload

bridgewater SYSTEMS

THE MOBILE PERSONALIZATION COMPANY

Contents

1. Introduction – It's all about data

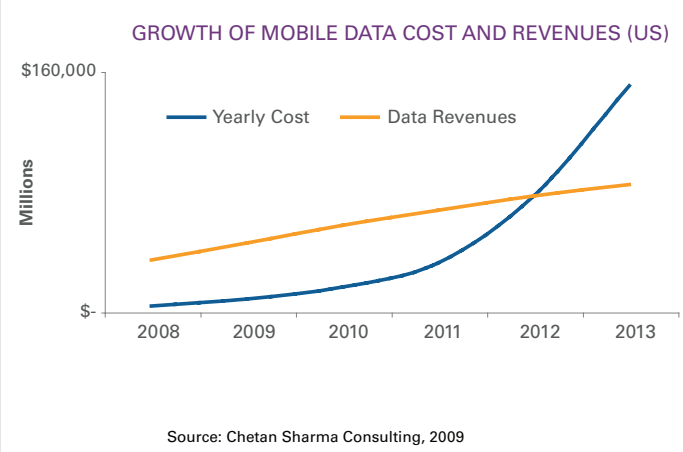
The mobile data industry has evolved rapidly over the past two years, resulting in exponential growth in data traversing service provider networks globally.

Growing 3G penetration, lower-cost smartphones and USB laptop dongles, together with the popularity of mobile applications and flat-rate data plans have fueled the increase in mobile data usage. The impact of that usage is now being felt by service providers and consumers alike.

Service Providers are having to contend with congested networks and the resulting impacts on service delivery — both new and very real consequences of mobile data growth. As a result, subscribers are often not getting the level of service they expect. As mobile data usage continues to climb, service providers are faced with the challenge of improving user experience levels and preventing the unacceptable — dropped data sessions, slow network speeds, and pent up subscriber frustration.

Service providers are also faced with the prospect of mobile data delivery costs outweighing revenues by 2011 (see Figure 1).

Many service providers are beginning to adopt a range of strategies including optimization of 3G networks using intelligent policy control, mobile data traffic offload, and transformation to 4G to reduce costs and alleviate congestion. Together, these strategies could reduce data delivery costs by more than 60 per cent over the next three years.[1] In an era of huge mobile data growth, this holistic approach to the congestion management conundrum is vital to long-term success.



Source: Chetan Sharma Consulting, 2009

Figure 1: Growth of Mobile Data Costs and Revenues

The purpose of this paper is to profile the value of subscriber, service, and policy control in delivering a transparent and personalized mobile experience when implementing a mobile data offload strategy. It highlights the key challenges facing fixed and mobile service providers, and profiles the role of Bridgewater's solutions in the following offload scenarios — 3G to Wi-Fi, 3G to femtocells, and mobile data onload.

INTRODUCING MOBILE DATA OFFLOAD

Offload — the ability to move mobile data traffic from one network to another in a way that is transparent to the subscriber — is a key component of an effective network congestion reduction strategy.

Mobile data offload will reduce costs and improve economies of scale by balancing traffic requirements across networks. The cost savings are significant. Service providers deploying a multi-access offload strategy can expect savings in the range of 20 to 25 per cent per annum. In the US market, service providers could save between $30 and $40 billion per year by 2013.[2]

1 Chetan Sharma Consulting, 2009.
2 Chetan Sharma Consulting, 2009

Service providers are looking to implement data offload to address the following congestion pain points:

- Overburdened Core Network Elements — routing traffic directly to the Internet before it reaches core network elements (such as the SGSN, the GGSN, and service grooming servers) offloads these elements, thereby reducing backhaul costs.
- Congested Cell Sites — One option is to deploy intelligent policy controls that reside in the core network to offload subscribers attached to congested cell sites based on a real-time knowledge of cell-site conditions, subscribers and their respective entitlements, and device and applications usage.

An offload strategy has the added benefit of supporting new business models including revenue-sharing partnerships between 3G and Wi-Fi service providers, and enabling fixed operators to leverage their infrastructure to offer mobile data services via Wi-Fi.

Regardless of where data offload is implemented in the network, Bridgewater's solutions provide service providers with carrier-grade authentication, authorization, accounting, and interworking support that ensures a transparent and secure single-sign-on experience to subscribers as they move between 3G, 4G, Wi-Fi, and femtocells. The addition of dynamic policy control allows operators to leverage flexible business rules to govern granular decisions regarding when, where, and under which circumstances subscribers, devices, and applications should be offloaded to alternate networks.

PROTECTING THE MOBILE USER EXPERIENCE

Flat-rate data plans, together with smartphones such as the iPhone and USB dongles, have encouraged users to change their relationship with mobile data. Far from treating mobile data as a scarce resource, some users are now opening the tap and leaving it on. For example, it is now common for just five per cent of users to be responsible for over 50 per cent of data traffic on the mobile network.

Service providers also face the challenge of cell-site-specific congestion in urban centers or during specific events. Operators have reported that in many urban centers, 80 per cent of data traffic is being managed by just 10 per cent of cell sites. Furthermore, it is no longer feasible from either a cost or societal perspective to construct more cell towers in many areas.

There is the role of bandwidth-hungry services to contend with as well. For example, video is expected to account for 64 per cent of mobile data traffic on the network within the next three years.[3]

The overall result is a degradation of service for mobile customers. To alleviate the problem, service providers need to ability to correlate congested cell sites with subscribers, their service plans, and usage behavior in real time. Armed with that level of knowledge, they can employ data offload strategies that will ensure a high quality experience for all subscribers, whether they use the mobile internet on-the-go or access services over a Wi-Fi network.

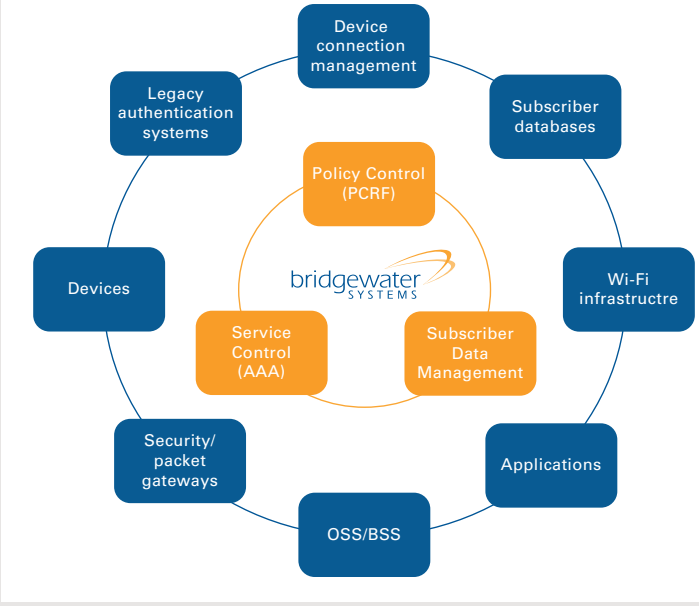
2. Mobile data offload ecosystem

As with many other parts of the mobile industry, the ecosystem for mobile data offload is both complex and symbiotic. As shown in Figure 2, the mobile data offload ecosystem comprises the following key elements:

- Security and packet gateways;
- Devices including handsets and femtocells;
- Device connection managers to support re-direction of traffic from one network to another and to detect alternate Wi-Fi networks;

3 Cisco Systems, 2009

- Service control or AAA (authentication, authorization, and accounting) systems to securely authenticate and authorize subscribers and femtocell devices for access to networks, and to manage usage tracking based on accounting records;
- Subscriber databases including legacy HLRs and subscriber data management systems;
- Policy control for granular real-time controls over which subscribers, devices, and applications are offloaded;
- Wi-Fi infrastructure; and
- Radio access network (RAN) infrastructure to support offload when congestion is experienced.



Source: Bridgewater Systems, 2010

Figure 2: Mobile Data Offload Ecosystem

3. Challenges of offload

Mobile data offload to Wi-Fi and femtocells presents a number of challenges to service providers that must be overcome if successful deployment is to follow. These include:

- **Consistent user experience** — Service providers must ensure that subscribers receive a comparable user experience regardless of access network. Service portability, parity, and continuity across multiple access networks is essential whether users are on 3G, Wi-Fi, or using a femtocell device in the home.
- **Transparent sign-on** — Lack of single sign-on across network types impacts the user experience and creates barriers to service use. Service providers require a single sign-on process to ensure barriers are kept to a minimum.
- **Authentication access issues in Wi-Fi** — Subscriber authentication data often resides in the Home Location Register (HLR) in 3GPP networks. This is not easily accessed from non-3GPP networks, such as Wi-Fi. An integrated solution that can federate subscriber data from existing systems is essential to the user experience.
- **HLR is load sensitive** — HLRs are struggling to handle high traffic volumes. An offload solution that caches subscriber data for authentication and authorization on multiple access networks offers distinct advantages.
- **Is Wi-Fi Switched On?** — Smartphone users do not always have Wi-Fi turned on due to the heavy battery drain on their handsets. Moreover, network systems cannot force a device to switch on Wi-Fi, which presents challenges for service providers who want to offload traffic to Wi-Fi.
- **What hotspots? Which subscribers?** — The handset's connection manager requires knowledge of Wi-Fi hotspot locations, in particular those in the vicinity of high-traffic cell sites that typically experience congestion. An offload solution also needs to be subscriber-aware, including subscriber location as it relates to available hotspots.
- **Subscriber, device, and application awareness** — Solutions should distinguish between different subscriber segments and different network conditions. When should some customers be offloaded versus others, and which applications and devices are most important at what time?

4. Bridgewater's data offload solutions

Bridgewater's mobile data offload solutions allow service providers to deliver a transparent and secure experience for subscribers as they move between access networks. They also enable 'selective offload' whereby policies can be applied to move certain subscribers, devices, and applications to Wi-Fi or move traffic based on network conditions and subscriber location.

The cornerstones of Bridgewater's solutions include the Bridgewater® Service Controller (AAA), Policy Controller (PCRF), and Subscriber Data Broker™. Together they provide a seamless, efficient, and precise offload solution for over-burdened 3G networks.

The solutions perform the following critical functions in a mobile data offload deployment:

Service Controller — Carrier-grade authentication, authorization, accounting, and interworking support that ensures a transparent and secure single sign-on experience to subscribers as they move between 3G, Wi-Fi, femtocell, fixed, and 4G networks. It also provides comparable AAA services for femtocell devices and integrates with existing network elements such as gateways, Wi-Fi infrastructure, and existing authentication systems.

Subscriber Data Broker — A subscriber data management platform that manages the subscriber experience across multiple access networks, bringing critical real-time awareness of subscriber state (location, context), profile (identity, service entitlements, device type), and usage (behaviors, application patterns, billing) information. This includes the ability to federate existing subscriber authorization data from HLRs in 3GPP networks;

Policy Controller —Intelligent, dynamic policy controls that enable selective offload decisions based on subscriber entitlements, applications, devices, and other parameters. It integrates with policy enforcement points in the network such as device connection managers, the GGSN, PDSN, and DPI.

5. Mobile data offload use cases

3G TO WI-FI OFFLOAD

The increasing prevalence of dual-mode 3G/Wi-Fi devices such as the iPhone, other smartphones, and laptops creates an opportunity to shift mobile data users onto the fixed line network, thereby reducing congestion and opening up new revenue streams.

In urban centers with a high prevalence of public Wi-Fi hotspots — whether service-provider-owned or through revenue sharing arrangements with hotspot providers — offload can relieve 3G network congestion and provide a better user experience. For example, Verizon Wireless is partnering with hotspot provider Boingo, to provide competitive 3G/Wi-Fi packages, attractive bundled services, and common access to services across multiple networks.[4]

The challenge in deploying a 3G to Wi-Fi offload strategy is ensuring a secure and transparent subscriber experience without the need to sign in again when the subscriber moves to another network.

Use Case – 3G to Wi-Fi Offload

Ensuring a seamless user experience is important in any mobile data offload strategy.

Consider a typical premium user with a data plan that enables access to mobile video. In a busy urban location, during times of network congestion, the premium user's mobile video experience may be degraded, resulting in inconsistent streaming and frustration.

However, if the user is in an area with access to the service-provider-owned hotspot, his handset can detect the Wi-Fi network and automatically redirect the device to Wi-Fi using the connection manager on the phone.

Once connected to Wi-Fi, the user's video streaming service runs smoothly with no delays.

The entire experience of moving over from 3G to Wi-Fi is transparent to the user, who now has access to his premium content over the Wi-Fi network with no interruptions and no need to sign in again.

AT&T in the US is one operator taking advantage of an offload strategy. The operator has 20,000 hotspots and allows customers to buy service as a day pass or a monthly service. iPhone users receive it for free.

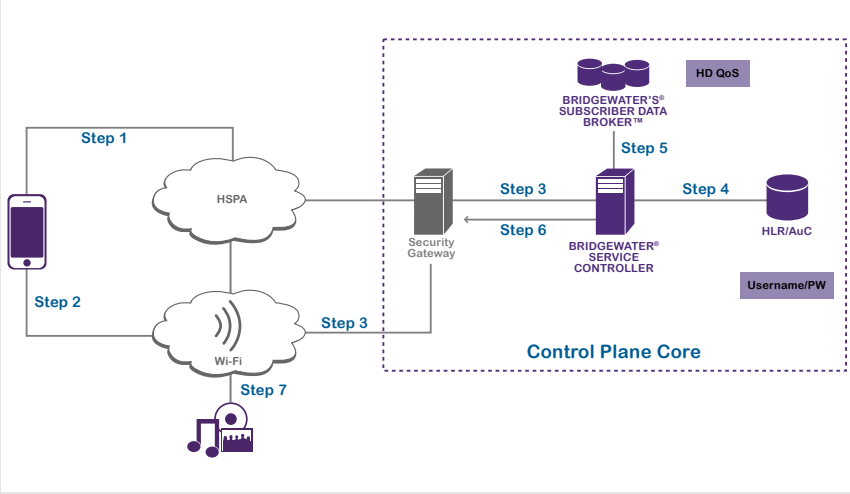
4 Verizon Wireless, December 2009

Service providers require a centralized view of 3G and Wi-Fi user entitlements, while leveraging existing network investments such as the data store or HLR to ensure the most efficient use of network resources and subscriber data.

From a technical point of view, successful 3G to Wi-Fi offload deployments enable seamless inter-working between a service provider's core 3G network and the Wi-Fi network. This includes 3GPP AAA support for Wi-Fi and secure authentication and authorization of 3G subscribers onto the Wi-Fi network. Facilitated by standards-based protocols, this ensures a transparent access experience for the end user while reducing the authentication load on the HLR.

3G TO WI-FI OFFLOAD: HOW DOES IT WORK?

The Bridgewater Service Controller is a key component in this use case, enabling transparent and secure authentication, authorization, and accounting, as well as leveraging existing subscriber data assets. The key steps are shown in Figure 3:



Source: Bridgewater Systems, 2010

Figure 3: 3G to Wi-Fi Offload Network

- The user's dual-mode device, which is attached to the 3G network (step 1), detects a Wi-Fi hotspot nearby (step 2);
- The Security Gateway in the service provider network sends an authentication request to the Bridgewater Service Controller (step 3), which in turn retrieves authentication vectors from the HLR to authenticate the user (step 4). In order to ensure a fast re-authentication, the Service Controller will also pull and cache these authentication vectors, reducing the load on the HLR by removing the need for additional access on each re-authentication;
- The Security Gateway retrieves a Wi-Fi profile from Bridgewater's Subscriber Data Broker to assign a Quality of Service (QoS) profile (step 5), which is authenticated against a user's service entitlements from the HLR (step 6); and
- Finally, the user is allowed onto the Wi-Fi network to continue their service (step 7), without having to access a portal or log in.

The solution also includes multi-access support for a consistent experience across multiple networks, and SIM-based authentication to ensure that the subscriber's entitlements are consistent whether accessing premium services via the 3G or Wi-Fi network.

3G TO FEMTOCELL OFFLOAD

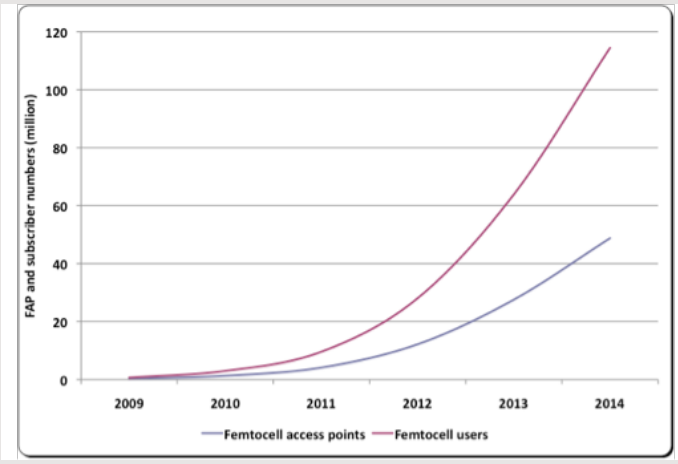
Femtocells — micro-sized cell sites situated indoors — will play an increasingly important role in many service provider strategies as a low-cost method of ensuring both optimal indoor coverage and reduced 3G congestion (see Figure 4). Offload to femtocells can have a profound effect on network performance, with indoor usage having a greater impact on network capacity than outdoor usage.

Regardless of 3G network type, all femtocells must be authenticated onto the network and authorized for access. The challenge for service providers is ensuring a seamless experience for the user in their own home, with a network solution that authenticates and manages the femtocell device while providing the necessary security key exchange and handoff.

Service providers also require a common device management system for femtocells to manage the network securely and efficiently.

3G TO FEMTOCELL OFFLOAD: HOW DOES IT WORK?

Bridgewater's solution for mobile data offload to femtocells, underpinned by the Bridgewater Service Controller and Bridgewater's Subscriber Data Broker, supports multi-access attachment, security, and roaming away from the user's home site. End-to-end security is essential to any deployment, including necessary encryption, authentication, authorization, and key management.



Source: Informa Telecoms & Media, 2010

Figure 4: Global Femtocell Deployment Forecast

Use Case – 3G to Femtocell Offload

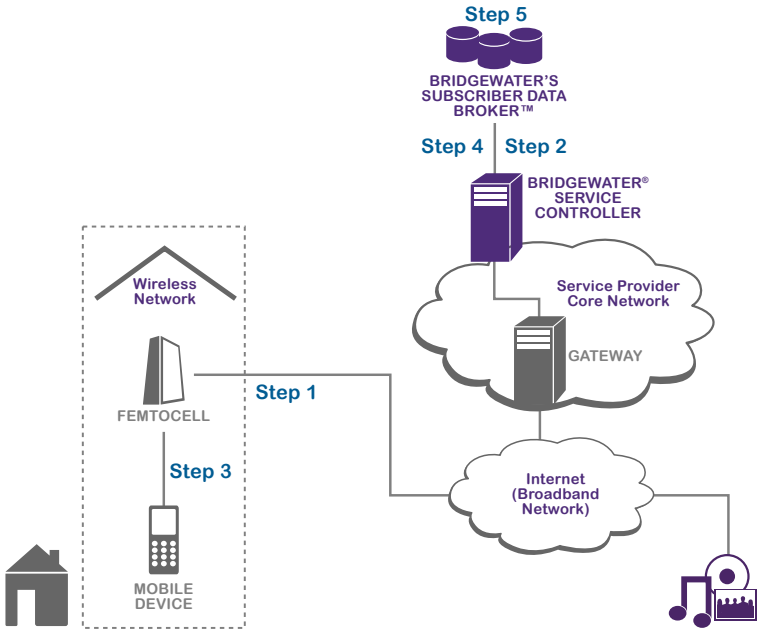
There is a concentration of data traffic in homes and offices, with 60 to 80 per cent of mobile data usage taking place indoors. However, poor voice and data coverage indoors often leads subscribers to switch to wireline usage.

This situation creates both an economic and customer service imperative for service providers to deploy a femtocell strategy. For example, in the UK, Vodafone has recently unveiled a subsidized femtocell package aimed at consumers for a one-time fee of £50.

Femtocells offer users better coverage and faster downloads, streaming, and Internet services.

Service providers benefit from offloading backhaul to a wireline broadband connection, reduced 3G network congestion, and revenue opportunities from expanded indoor coverage.

The key steps are shown in Figure 5:



Source: Bridgewater Systems, 2010

Figure 5: 3G to Femtocell Offload Network

- The femtocell device is activated and sends an authentication request to the Bridgewater Service Controller (step 1);
- The Service Controller then authenticates the femtocell device based on a device profile stored in the Subscriber Data Broker (step 2);
- When the subscriber's mobile device enters into the range of the femtocell, an authentication request is sent to the Service Controller to authenticate the subscriber for femtocell use (step 3);
- The Service Controller authenticates the subscriber based on their profile (step 4). The Service Controller can also retrieve authentication vectors from the HLR to authenticate the user. It will then pull and cache these authentication vectors for fast re-authentication; and
- The Service Controller retrieves a user profile from the Subscriber Data Broker to authorize specific QoS profiles or entitlements while on the femtocell (step 5).

Femtocell entitlement management — provisioning, re-registration, firmware updates, geo-fencing, simultaneous sessions — is incorporated to ensure a superior user experience. For service providers deriving incremental revenue from femtocell deployments, accounting is provided for metered services.

MOBILE DATA ONLOAD — THE CASE FOR CABLE OPERATORS

Cable operators (MSOs) are leveraging the use of unlicensed Wi-Fi spectrum to enable alternative wireless access for their customers. This involves adding Wi-Fi support to cable infrastructure to create Wi-Fi hotspots in urban centers and home environments in order to offer services that compete with existing 3G and 4G services. This strategy allows cable operators to offer a new set of wireless data services for their captive customer base, while leveraging their existing footprint.

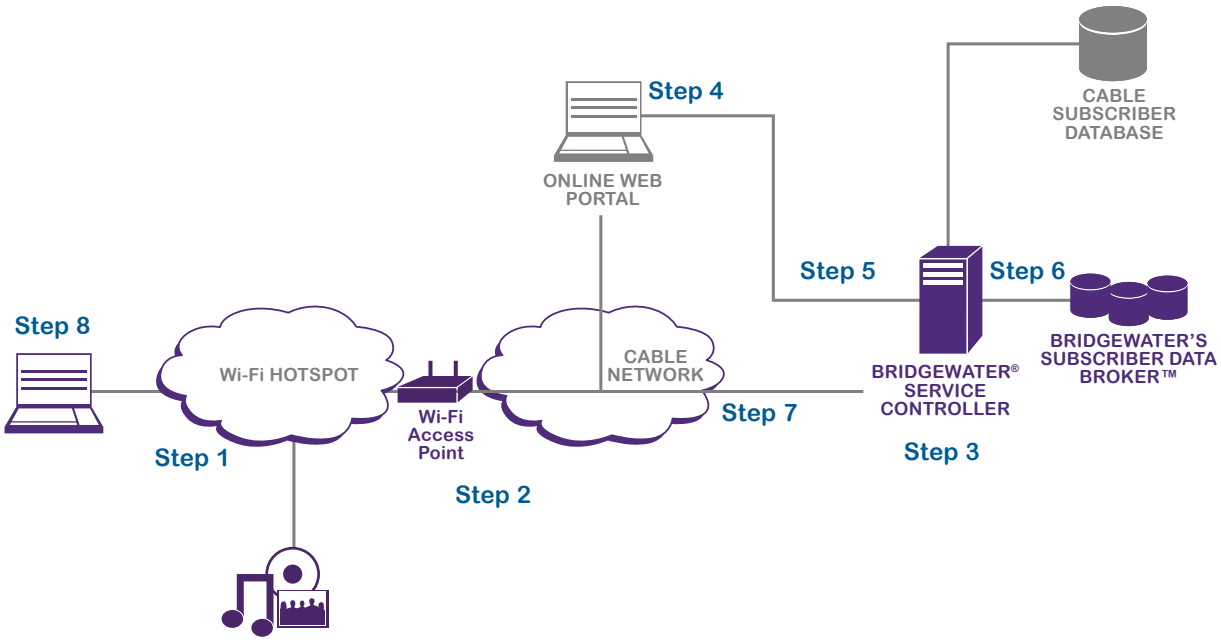
A key challenge is how to manage a secure and transparent subscriber experience across multiple access networks — for example cable to Wi-Fi to 3G.

MOBILE DATA ONLOAD: HOW DOES IT WORK?

The Bridgewater Service Controller and Subscriber Data Broker provide the required multi-access support, security, and roaming capabilities for cable operators to provide transparent access to wireless services. This includes end-to-end security for cable subscribers accessing the Wi-Fi network such as encryption, authentication, authorization, and key management.

This solution allows MSOs to get an additional share of the wireless subscriber wallet by onloading subscribers to Wi-Fi from 3G or cable networks, while leveraging existing backend infrastructure.

The steps required for mobile data onload are shown in Figure 6:



Source: Bridgewater Systems, 2010

Figure 6: Mobile Data Onload Network

- The user's Wi-Fi-enabled mobile device detects a Wi-Fi hotspot nearby and attempts to access Internet service (step 1). This Wi-Fi network can be owned by the cable operator or by a revenue-sharing partner;
- The Wi-Fi access point then sends an authentication request to the Bridgewater Service Controller (step 2);
- The Service Controller checks the subscriber's credentials, including the device's media access control (MAC) address against the existing subscriber profiles stored in the Subscriber Data Broker (step 3);
- If it is the first time the cable subscriber is accessing the Wi-Fi service, the authentication request is rejected and the subscriber is redirected to an online portal to log in (step 4);
- The user logs in via the portal and an authentication request with user credentials including MAC address, is sent to back to the Service Controller (step 5);

- The Bridgewater Service Controller validates the subscriber credentials from the portal against credentials federated from the existing subscriber profile repository (step 6). Within the operator's network, the Bridgewater Service Controller can retrieve authentication vectors from the existing subscriber profile database to authenticate the user and cache these for fast re-authentication;
- The Bridgewater Service Controller then authenticates and authorizes the subscriber for Wi-Fi access (step 7). If there is a subsequent session, the subscriber is automatically authorized on the Wi-Fi network without having to log on through the portal, bypassing steps 4 and 5.
- The user is now granted Internet access on the Wi-Fi network (step 8). If a user travels from one Wi-Fi access point to another on the same MSO network, the Bridgewater Service Controller will automatically check the device MAC ID against the existing subscriber profiles and will authorize the user without having to re-enter any log-in credentials. This built-in mobility access allows a seamless, transparent access experience for subscribers.

FINE TUNING THE APPROACH – SELECTIVE OFFLOAD

There is an increasing need for more sophisticated management of which subscribers, devices, and applications are offloaded and under what circumstances. Dynamic policy control enables selective offload — an intelligent solution to this challenge.

This involves fine-tuning the approach so that users are offloaded from 3G networks based on a range of parameters such as subscription type, services used, location, or previous behavior.

Policy control adds a layer of dynamic management to mobile data offload and far greater control of the subscriber experience, with policy decisions pushed to the mobile device connection manager. This process enables the device client to act as a policy enforcement point.

Dynamic policy control also enables decisions to be made based on real-time RAN congestion levels and the applications being used. Service providers can, for example, re-prioritize subscribers on a congested cell site or offload all mobile video traffic or laptop devices to Wi-Fi, but only during peak congestion periods. Similarly, these decisions can be made based on specific times of day, days of the week or a combination of these factors.

Where Wi-Fi service revenue is a key factor, service providers can make offload decisions based on Wi-Fi assets being in range or not. Prioritization of key traffic — such as machine-to-machine (M2M) and public safety applications — is also possible.

The process gives service providers the ability to balance traffic demands by offloading subscribers, devices, and applications based on service level agreements for specific customer types, network conditions, and entitlements.

Subscriber Experience – Selective Offload

Service providers can treat specific users differently on a granular level. Take for example a subscriber viewing mobile videos in a highly congested urban center. While the subscriber may have Wi-Fi turned off on his device, the service provider has Wi-Fi hotspots in the vicinity.

Dynamic policy decisions can be pushed to the device connection manager to turn on Wi-Fi and selectively offload subscribers. For example, service providers can offload a basic bronze plan subscriber while giving bandwidth priority to a premium gold customer on the 3G network.

The bronze subscriber can then be authenticated onto the Wi-Fi network seamlessly, alleviating congested network conditions and ensuring a quality mobile experience for the subscriber.

6. The Bridgewater advantage

Bridgewater offers several key advantages to service providers deploying a mobile data offload strategy:

- **Extensive and Proven Multi-Access Network Support** — Bridgewater's market-leading products are proven in over 150 Tier 1 deployments globally and have scaled to support millions of subscriber. They are access-network and vendor agnostic, enabling seamless mobility and service portability across network types. This is a critical future-proof capability as service providers leverage multiple access networks simultaneously to support new services, enable data offload across networks, and migrate to 4G. By deploying a best-of-breed solution, service providers can avoid vendor lock-in, exploit economies of scale, and leverage existing investments.
- **Broad Interoperability** — Bridgewater has completed extensive interoperability testing with gateways, Wi-Fi provider access points/infrastructure, connection managers, and femtocell devices.
- **Transparent subscriber experience** — The subscriber does not need to log on to separate services as the solution re-authenticates and re-authorizes across multiple access networks. The user's entitlements in the 3G or cable network are translated into the Wi-Fi network, ensuring service portability across multiple access networks.
- **Service Enablement** — By having a common subscriber view, service providers can offer flexible service bundling options across all networks and devices, allowing for a more unified subscriber experience. For example, users will not have their sessions disconnected while being re-authenticated once they are in range of a new network.
- **Interworking** – Service controls for multi-access networks need to simultaneously support 3G, 4G, and Wi-Fi technologies to manage subscriber access to networks. This includes authorization and important accounting functions required for billing and other purposes. Support for 3GPP AAA functions for interworking between 3GPP and non-3GPP networks such as EVDO, Wi-Fi, WiMAX, and femtocells is also required. Wi-Fi interworking functions between fixed and mobile networks — for example to support data offload to Wi-Fi hotspots — are essential.
- **Common subscriber data management platform** — This allows service providers to use a common approach to managing authentication and authorization for individuals, groups of subscribers, and devices across multiple access networks including single sign-on. It also enables data federation of entitlements from service provider HLRs for Wi-Fi authentication and eliminates the need to provision Wi-Fi services in another subscriber database.
- **Offload the HLR** — The Bridgewater Service Controller pulls and caches authentication vectors, reducing the load on the service provider's HLR and enabling fast re-authentication.
- **Manage femtocell entitlements** — The Bridgewater Service Controller manages subscriber-related data, as well as device specific entitlements for femtocells including location services, device authentication, authorization and accounting, and security key management.

7. Conclusion

Service providers facing congested mobile networks as a result of the rapid growth in mobile data consumption can use mobile data offload to Wi-Fi and femtocells to ease congestion and generate incremental revenue streams. Alternatively, cable operators have the opportunity to onload subscribers to Wi-Fi networks and offer wireless services to cable customers.

Whether offloading or onloading, the importance of delivering a transparent and seamless subscriber experience across multiple access networks using service controls and subscriber data management cannot be underestimated. This includes transparent access to networks and a consistent experience that reflects subscriber entitlements, location, devices, and usage behavior.

Global Service Provider Offload Scenario

One of the world's leading Tier 1 global service providers is leveraging its fixed line infrastructure and Wi-Fi DSL devices in the home for 3G mobile data offload.

The service provider is offloading data from laptops, smartphones, and video applications to alleviate network congestion.

Of primary importance in the offload strategy is to create a seamless subscriber experience between the 3G network and Wi-Fi devices, with a single sign-on process.

The deployment also manages a common set of subscriber entitlements across both 3G and fixed line networks, with authentication and authorization profiles residing in the service provider's HLR being federated to the fixed line network.

The increasingly sophisticated requirements around data offload/onload will require intelligent policy controls that communicate directly with device connection managers and make intelligent real-time decisions to manage the process selectively.

Service providers using an offload or onload strategy need to take into account the following requirements to ensure success:

- A consistent user experience with transparent single sign-on;
- Smart networks with subscriber, device, and application awareness;
- Extensive multi-access network support;
- Broad interoperability between network elements;
- A common subscriber data management capability;
- Simultaneous service and policy control support for 3G, 4G, Wi-Fi, and devices, including femtocells; and
- Wide ecosystem support for offload network elements.

Those service providers deploying an offload strategy face the promise of significant cost savings, revenue opportunities from multiple access networks, and a far better user experience.

Bridgewater Systems, the mobile personalization company, enables service providers to efficiently manage and profit from mobile data services, content and commerce. The company's market leading mobile personalization portfolio provides a real-time, unified view of subscribers including entitlements, devices, networks, billing profiles, preferences and context. Anchored by Bridgewater's Subscriber Data Broker™, the portfolio of carrier-grade and standards-based products includes the Bridgewater® Service Controller (AAA), the Bridgewater® Policy Controller (PCRF) and the Bridgewater® Home Subscriber Server (HSS). More than 150 leading service providers including America Movil, Bell Canada, Clearwire, Cox, Hutchison Telecom, Iusacell, Scartel, SmarTone-Vodafone, Sprint, Tata Teleservices, Tatung, Telmex, Telstra, and Verizon Wireless use Bridgewater's solutions to rapidly deliver innovative mobile services to over 150 million subscribers. For more information, visit us at **www.bridgewatersystems.com.**

Company Headquarters
303 Terry Fox Drive
Suite 500
Ottawa, Ontario
Canada K2K 3J1
P: +1 613 591 6655
F: +1 613 591 6656

European Office
Albany House
324/326 Regent Street,
Suite 404, London,
United Kingdom W1B 3HH
P: 44 (0) 118 925 3298
F: 44 (0) 118 925 3299

Asia Pacific Office
Suite 211/250 Pitt Street
Sydney, NSW,
Australia 2000
P: + 61 2 9283 2313
F: + 61 2 9283 3738

U.S. Office
280 Madison Avenue,
Suite 912
New York, NY
United States 10016
P: +1 866 652 0471
F: +1 613 591 6656

V5.04.10