

# Keeping mobile data flowing

---

## *Mobile data application delivery control*

**February 2010**

Due to competitive pressure and demand from subscribers, mobile network operators have had to handle an ever-increasing volume of data traffic. Much of this is driven by users accessing data applications that may not have been specifically written for mobile environments. Managing the applications and the data they generate is the key to providing a satisfactory experience for subscribers.

This paper discusses how mobile network operators (MNO) can prepare their networks for what is likely to be a continually growing demand for mobile data access. It should be of interest to those tasked with managing mobile data services and those that make a living by providing the applications that drive them.

Bob Tarzey  
Quocirca Ltd  
Tel : +44 7900 275517  
Email: [bob.tarzey@quocirca.com](mailto:bob.tarzey@quocirca.com)

Rob Bamforth  
Quocirca Ltd  
Tel: +44 7802 175796  
Email: [rob.bamforth@quocirca.com](mailto:rob.bamforth@quocirca.com)



*An independent report by Quocirca Ltd.*

[www.quocirca.com](http://www.quocirca.com)

Commissioned by Zeus Technology

quocirca

# Keeping mobile data flowing

---

## *Mobile data application delivery control*

### Executive summary

*The increasing demand for mobile data access alongside traditional telephony services is stressing mobile operators' networks as never before. The extra load from data services is especially hard to manage when there are unexpected peaks in demand. One way to gain better control is to deploy application delivery controllers to manage mobile data applications and the traffic they generate, optimising the user experience and minimising their impact on bandwidth-constrained resources.*

- **Mobile data volumes will continue to soar as users seek access from a range of end user devices**  
As the use of smartphones and cellular connected devices (laptops, netbooks and e-readers) continues to grow, MNOs need to make sure their networks are ready to cope with increasing, and unpredictable, volumes of data traffic. This will include surges caused by sudden rises in popularity of some mobile data applications or the acquisition of many new subscribers in a short period of time through winning new delivery contracts.
- **The demand is from both business and consumer subscribers**  
Employees accessing email and other productivity applications are driving demand as much as consumers uploading photos and videos to popular web sites and downloading new handset applications. MNOs need to understand different traffic types and, in some cases, be able to prioritise depending on the subscriber profile or the particular mobile data application being accessed.
- **MNOs will need to take an increasingly pro-active approach to managing mobile data applications and the traffic they generate**  
First, it is necessary to make sure the applications themselves can respond to varying workloads and then make sure that the traffic they generate is optimised for delivery across bandwidth-constrained networks by intelligently shaping data traffic close to the mobile data application itself. Both of these objectives can be achieved using application delivery controllers.
- **Application delivery controllers (ADC) both help manage the application and ensure efficient communication between mobile data applications and end user devices**  
ADCs are network devices, which can be used to manage traffic to and from mobile data applications and to manage the applications themselves. ADCs can improve the capacity and efficiency of applications by imposing prioritisation and shaping policies on traffic. ADCs also provide load balancing, acceleration, caching, filtering and offload capabilities to improve availability, security and performance, thereby ensuring the successful delivery of data to users of mobile devices.
- **To be effective, ADCs need to be deployed close to mobile data applications**  
Some mobile data applications will be deployed on an MNO's own IT infrastructure, for example subscriber portals; many others will be accessed over the internet. Software-based ADCs (softADC) can be deployed anywhere on the MNO's network, on the same physical or virtual servers as the mobile data application, alongside internet gateways or on partner sites where applications popular with an MNO's subscribers are hosted.

### Conclusions

The hunger, from both business and consumer users, to access data from their mobile devices is only going to increase for the foreseeable future. For MNOs, it will be hard to predict what the new mobile data applications will be and how widely their subscribers will use them. The one thing MNOs can do when providing access to new mobile data applications is to ensure the application itself, and the traffic it generates, is handled as efficiently as possible. In doing so, MNOs can be more responsive to the wide-ranging demands of their subscribers and ensure that they can, at least, meet expected service levels, if not exceed them.

## 1. Introduction—the impact of data access on MNOs

In July 2007, when the iPhone was launched in the UK, a single mobile network operator (MNO)—O2—had been selected as Apple’s exclusive partner to deliver voice and data services to its new handsets. O2 has a solid reputation for data networking despite some breadth of reach concerns regarding EDGE and 3G coverage, and should have been able to handle the uncertain demands of the iPhone launch. The iPhone was expected to be popular, given Apple’s iconic status, but how fast demand would grow, especially for data services (access to the internet, email and other data applications), was uncertain.

More than two years on, the iPhone has taken a respectable share of the smartphone market and this has generated a big demand for mobile data access. However, in the UK, at least, this has not been without problems; there have been a few service outages that have led to adverse press coverage for Apple and O2. Apple has now reached agreements with other operators to extend iPhone services in the UK. This was going to happen anyway as demand grew; however, this increased the pressure on O2 to sustain a high level of performance and subscriber satisfaction, reducing the risk of subscriber churn. Ensuring they can cope with surges in demand for data access—be they temporary or permanent—is clearly important to all MNOs.

Service problems caused by increased demand from one set of subscribers, such as iPhone users, also impact on subscribers of other mobile phone services—all are served over the same network. MNOs need to be able to be in a position to support a wide variety of new mobile data access demands, whilst maintaining service levels for existing subscribers.

This paper discusses how MNOs can prepare their networks for what is likely to be a continually growing demand for mobile data access. It should be of interest to those tasked with managing mobile data services and those that make a living by providing the applications that drive them.

*“Ensuring they can cope with surges in demand for data access—be they temporary or permanent—is clearly important to all MNOs”*

## 2. The mobile data revolution

The ability to access data services whilst ‘mobile’ has become increasingly commonplace—more and more subscribers are signing up for mobile data tariffs, especially in the developed markets. This is not just to access data from smartphones but also for the use of cellular ‘dongles’, or modems, for data access from laptops, netbooks and e-readers, such as Amazon’s Kindle. If Apple’s new iPad takes off, this will increase the requirement further.

Internet consumption on fixed broadband networks has become an entrenched behaviour that, increasingly, mobile users are taking for granted too. BBC’s ‘iPlayer’ currently consumes around 10% of the UK’s fixed internet capacity; imagine the strain on mobile networks as users increasingly expect to be able to carry out such activities on their mobile devices too.

Mobile data services are serving two principle audiences, which increasingly overlap. First, consumers, with their interest in handset-enhancing applications and internet-based resources, such as social network sites—think of all the pictures and videos being generated using mobile phones and being uploaded to sites like Facebook and YouTube. Second, there are business users, accessing email and other business productivity tools.

On top of all this, MNOs provide their own data services. These include security services that authenticate access rights and filter data traffic to block certain content based on the user’s profile and portal services that allow subscribers to manage their own accounts, reducing overall subscriber management costs.

Finally, fierce competition puts pressure on MNOs to drive down prices and introduce attractive new tariffs, for example more “all-you-can-eat” charging for some types of data access that have been introduced in the last 3 or 4 years. This means that network usage is no longer directly linked to revenue.

Ensuring the maintenance of high quality, predictable performance for all their services is one of the biggest challenges faced by MNOs. To understand what impact data traffic has on the overall performance of an MNO's network requires an understanding of the different elements of that network.

### 3. The profile of a mobile network

As with any service provider, MNOs aim to maximise the use of the infrastructure their services rely on and minimise the need to invest in new equipment. Access is provided from the cell towers over the licensed radio spectrum to the subscriber devices within range. This setup is complicated in that each operator is typically running several different mobile systems—GSM, GPRS, EDGE, 3G—in the same territory, each with different radio, and data delivery, performance and characteristics. Some MNOs are now extending their networks through the use of small-scale consumer electronics, or office-ready 'cell sites'. These femto, pico or micro cells improve coverage in homes, offices, shopping centres and so on; these rely on wired broadband connections to link to the MNO's wireless core, often through a public internet connection.

The backhaul network is a wired infrastructure that links all these cells back to the wireless core. Essentially, this is a private network, although resources are sometimes shared between MNOs or the lines are leased from other carriers. All traditional telephony communication, such as voice calls, MMS (picture messages) and SMS (text messages), from one user to another, is handled within the MNO's wireless core, with connections to other MNOs for calls originating or terminating elsewhere. Data traffic, however, must be routed from the wireless core to communicate with the required services—this is done via the packet core. These services will either be served from the MNO's own IP-based infrastructure (for example an MNO's own portals), by mobile data applications provided by partners, or directly from the internet via gateways provided by the MNO.

The challenge that MNOs face is handling these data communications efficiently. Whilst they can assert quite a lot of control over how a given device/operating system combination interacts with services they have deployed internally—because the MNO owns both the user interface and the backend—in most cases they have no such control. Both components are more often written and owned by third parties whose software developers had no idea about which MNO's network would be used to link the two. However, it is possible to assert some control over any mobile data application through intelligent management of both the application and traffic it generates; but first it is necessary to understand the different meanings of the word 'application' in the mobile world.

### 4. Applications in the mobile world

As the worlds of telecommunications and information technology (IT) have converged, the two industries have had to learn to speak each other's language. Some words had come to mean different things depending on which side of the divide you came from; for example "*application*". To an IT person, an application is a piece of software that runs on a computer and makes it do something useful for end-users; to a telecommunications person, an application is typically a service running across their network, that may do something useful for their subscribers or provide an internal service. There are three categories of applications that impact an MNO's network:

1. Traditional mobile services: those the MNOs have offered for many years—voice calls, voice mail, SMS, MMS etc. The traffic these generate is restricted to the traditional wireless core and is not the focus of this paper.
2. Handset applications: developed to enrich the subscriber's use of devices. Many of these just use the resources on the handset itself, although they are often downloaded over the air, for example from Apple's App Store. Such downloads may seem like one-off events, but many will be automatically updated as new versions appear and the applications themselves may place an ongoing burden on the network if they need to regularly access some backend resource; in which case they fall into the third category (as do services like the App Store itself).

*"As the worlds of telecommunications and information technology (IT) have converged, the two industries have had to learn to speak each other's language"*

3. Mobile data applications: these need a component on the user device (it may be just a web browser), but are only useful when accessing the mobile network and using some backend resource. The most obvious examples are email and web browsing, but business users are coming to rely on mobile data access for productivity applications, for example service engineers ordering spare parts whilst in the field or doctors accessing patient records whilst visiting them in the home.

It is mobile data applications that are of interest in this paper. The volume of data traffic they can generate has the capability to impact the overall performance of an MNO's network, especially when there are surges in demand. In an ideal world, the developers of mobile data applications would write carefully-structured network calls aimed to minimise the impact they have on a given network.

However, the reality is that developers usually have no idea which MNO's network the applications they write will be making data requests over. This is particularly true of applications written for PC devices that might be connected using mobile broadband; they will often have been written assuming higher speed fixed line broadband would be available. So, unless commissioned specifically by an MNO to write an application for its own subscribers, application developers will write generic network calls that pay little heed to an individual MNO's specific network capabilities and make as many network calls as they need to provide the end-user functionality.

Regardless of this, MNOs still have to ensure the applications are capable of responding to the volume of incoming requests and prioritise and control their data traffic they generate. Furthermore, the MNO can never be sure how popular a given application will be and when its usage will peak—so the MNO needs to be able to handle peaks and troughs in demand. One approach is to deploy application delivery controllers (ADCs) that provided intelligent control of application resources, brokering the conversation between the user device and the mobile data application itself.

## 5. Handling backend resources via application delivery controllers (ADC)

Wikipedia defines an ADC as “a network device in a data centre that helps perform common tasks done by web sites in an effort to remove load from the web servers themselves”. However, in the mobile data access scenario they can also be used to broker the communications between the handset and a given mobile data application. So a broader definition is required:

*“ADCs are network devices, which can be used to manage traffic to and from mobile data applications and to manage the applications themselves. ADCs can improve the capacity and efficiency of applications by imposing prioritisation and shaping policies on traffic. ADCs also provide load balancing, acceleration, caching, filtering and offload capabilities to improve availability, security and performance, thereby ensuring the successful delivery of data to users of mobile devices”.*

Using ADCs has obvious benefits when the volume of requests a given application will receive is unpredictable in advance and when responses to data requests need to be returned over bandwidth—constrained mobile networks.

Mobile data applications can be deployed anywhere, so there must be flexibility in how ADCs are deployed too. Some will be in the MNO's own data centres; either to manage traffic to and from its own mobile data applications, such as subscriber portals or a handset application download site, or to manage traffic to and from internet resources such as email gateways and external web sites. Flexible deployment is easiest to achieve using ADCs deployed as software (softADC) rather than appliances; softADCs may be installed on the same server as the target application or, perhaps, for busy applications, on a dedicated physical or virtual server in the same location. SoftADCs can also be installed on partner sites that run applications popular with a given MNO's subscribers.

*“Using ADCs has obvious benefits when the volume of requests a given application will receive is unpredictable in advance and when responses to data requests need to be returned over bandwidth—constrained mobile networks”*

There are many ways in which ADCs can improve the services provided by MNOs, these include:

- **Load balancing:** the distribution of requests across available instances of a mobile data application and, when necessary, invoking new ones. For MNO-owned applications running in a virtualised environment, ADCs may make use of spare compute capacity that the MNOs have locally or call on third party resources at times of extreme load.
- **Network acceleration:** the minimising of traffic being sent from the mobile data application to the end user device using techniques such as de-duplication and compression. The ability to do this will be limited depending on the device's ability to understand the modified traffic, and will have to accommodate the differences between handsets/PCs and/or the operating systems that run on them.
- **Caching:** this is the practice of keeping copies of commonly accessed content as close to the user as possible. For example, a given website that is regularly accessed by users may have content that is relatively static (compared to, say, a news site). This means local copies of many web pages can be cached by an ADC rather than read direct from a central server each time they are required.
- **Coping with intermittent connectivity:** ADCs can also provide short term caching for individual users, even when content is dynamic—for example filling in a web form. This can help re-establish an internet session seamlessly should mobile coverage be lost for a short period.
- **Deep packet inspection:** ADCs can inspect the data and make traffic management and policy decisions based either on the type of data or because a particular type of content is recognised.
- **Filtering:** many MNOs offer security services to their subscribers whereby certain types of content are blocked. With direct internet access this can only be achieved by the MNO filtering content, for example to check it is not likely to be offensive.
- **Content based billing:** knowing what internet applications any given traffic is associated with allows content-based billing to be implemented. For example, email might be sold on an "all-you-can-eat" tariff whilst web access might be based on volume of data accessed—only by inspecting the traffic can the two be distinguished. This is possible in theory, user acceptance is another matter.
- **Mobile data application billing:** understanding application usage allows MNOs to enter into the usage-based charging agreements that could be of interest to some application owners because such information can be used to help monetise their offerings.

In summary, ADCs can intelligently manage application resources and communications with user devices maximising the user's data access experience across a given MNO's network.

## 6. Conclusions and recommendations

The hunger, from both business and consumer users, to access data from their mobile phones and other remotely connected devices is only going to increase. For MNOs it will be hard to predict what the new mobile data applications will be and how widely their subscribers will use them. The one thing MNOs do have control over is how well their networks respond to changing demand in data access requirements and, to do that, they need to build intelligence into the way data applications and the traffic they generate is handled; ADCs help achieve this. In doing so, MNOs can be more responsive to the wide-ranging demands of their subscribers and ensure that they can consistently meet and, in some cases, exceed expected service levels.

*"ADCs can intelligently manage application resources and communications with user devices maximising the user's data access experience across a given MNOs network"*

## About Zeus

Zeus software enables our customers to create, manage and deliver exceptional online services in Physical, Virtual and Cloud environments. Implementing a Zeus solution allows organisations to control and manage the flow of traffic to their web-enabled applications, ensuring a consistently robust application delivery infrastructure.

Zeus Traffic Manager and Zeus Load Balancer software is used by thousands of customers worldwide. It actively manages network traffic to and from applications:

- It improves performance by load balancing and optimising the traffic, caching and offloading to allow the application to run at the most efficient level possible,  
**... thus improving customer experience and your ROI on your infrastructure;**
- It improves reliability of services by actively monitoring the health of each server, detecting server errors or imminent overload and routing traffic away,  
**... thus improving the availability of your services;**
- It improves security of services using anti-denial-of-service and filtering measures. The 'Application Firewall Module' adds a full Web Application Firewall to secure an application to the requirements of PCI DSS and beyond,  
**... thus protecting services and data from malicious attacks;**
- It contains a wide range of capabilities to control, shape and monitor traffic—compression, bandwidth and rate shaping, advanced session persistence, service level monitoring, advanced traffic visualisation and diagnostics, allowing you to  
**... create powerful, innovative solutions to application delivery challenges.**

Zeus powers over one million website infrastructures across the world including BT, Virgin Media, Call Genie, the BBC, ITV, and Comic Relief.

Zeus is in a unique position to assist any business looking to enhance their mission-critical Internet service infrastructure.

For further information, please email: [info@zeus.com](mailto:info@zeus.com) or visit [www.zeus.com](http://www.zeus.com).



#### REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of some of the issues facing mobile network operators as they deploy more and more data applications.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca would like to thank Zeus for its sponsorship of this report.

## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption—the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>