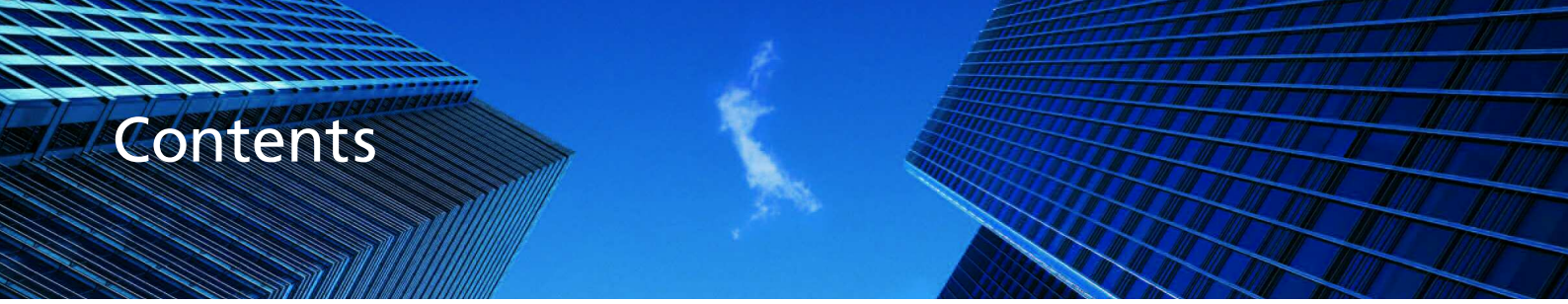
GPRS:
How it works

An O2 White Paper



Contents

1. Executive summary

The General Packet Radio Service (GPRS) is an enhancement to the existing GSM network infrastructure and provides a connectionless packet data service. The same cellular base-stations that support voice calls are used to support GPRS and as a consequence GPRS can be used wherever it is possible to make a voice call. GPRS roaming agreements exist with a large number of countries and this means users can use GPRS devices whilst abroad.

GPRS is based on internet Protocols (IP) and enables users to utilise a wide range of applications – email and internet and/or intranet resources for instance. With throughput rates of up to 40 Kbit/s, users have a similar access speed to a dial-up modem, but with the convenience of being able to connect from anywhere.

GPRS is classed as being a packet switched network whereby radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user for a fixed period of time, the available radio resource can be concurrently shared between several users. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell. The actual number of users supported depends on the applications being used and how much data is being transferred.

The term "always on always connected" is often used when people are describing GPRS and means once users have logged on they can remain connected to the data network for the working day. It should be noted that unlike GSM circuit switched data working, where the cost of the data call is related to the time spent connected to the network, this is not an issue when using GPRS as the cost of a GPRS data session is dependant on the amount of data sent and received not the time spent connected to the network.

2. GPRS network infrastructure

GPRS introduces a number of new functional elements that support the end to end transport of IP based packet data. GPRS was developed by the GSM standards bodies, resulting in a system with defined functionality, interfaces and inter-network operation for roaming support. The GPRS network architecture is shown in Figure 1.

Two major new core network elements are introduced: the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support node (GGSN). The SGSN monitors the state of the mobile station and tracks its movements within a given geographical area. It is also responsible for establishing and managing the data connections between the mobile user and the destination network.

The GGSN provides the point of attachment between the GPRS domain and external data networks such as the internet and Corporate Intranets. Each external network is given a unique Access Point Name (APN) which is used by the mobile user to establish the connection to the required destination network.

The GSM Base Station Subsystem (BSS) is adapted to support the GPRS connectionless packet mode of operation. A new functional node called the Packet Control Unit (PCU) is introduced (as part of the BSC) to control and manage the allocation of GPRS radio resources to mobile users.

In the context of this paper the term mobile station or MS refers to GPRS devices – could be handsets, PC data cards, handheld devices (such as O2's XDA devices) or any other device that incorporates a GPRS radio capability.

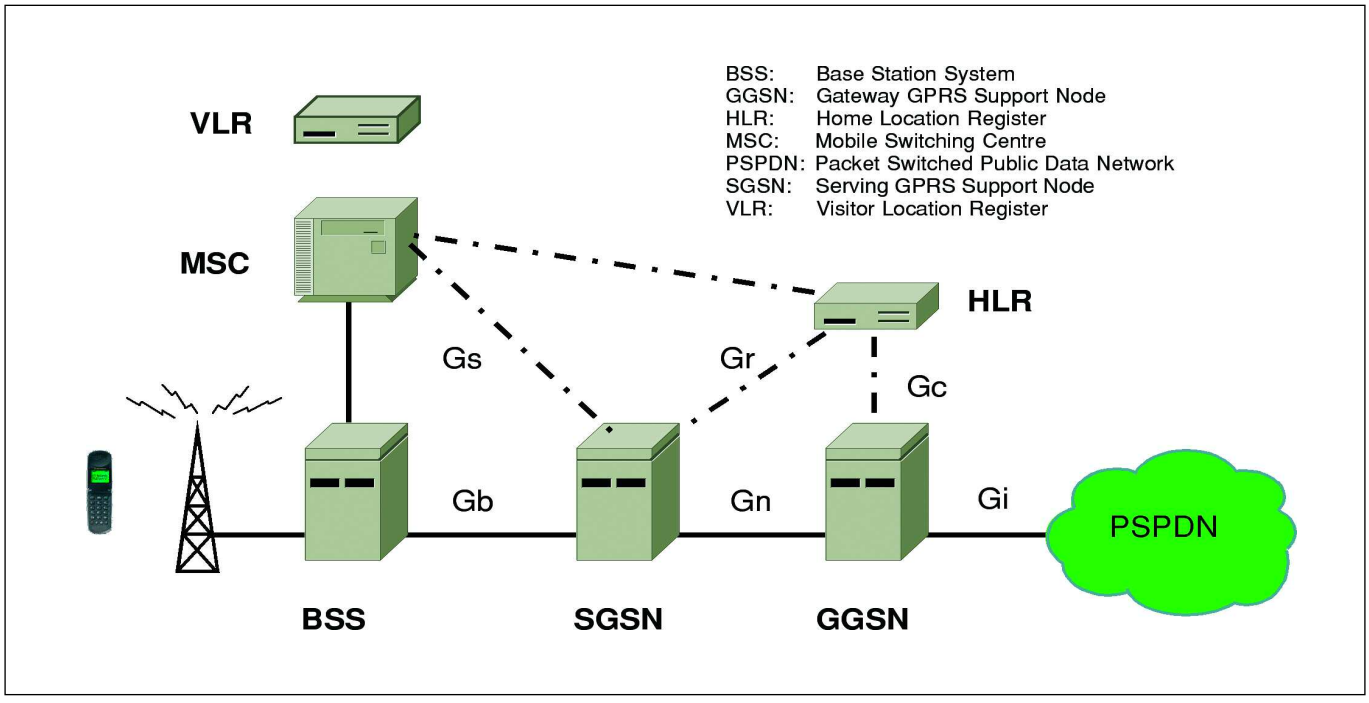


Figure 1:
GPRS Network Architecture.

The architecture diagram shown in Figure 1 shows a number of standardised network interfaces:

- **Gb** – frame relay connection between the SGSN and the PCU within the BSS. This transports both user data and signalling messages to/from the SGSN.
- **Gn** – the GPRS backbone network, implemented using IP LAN/WAN technology. Used to provide virtual connections between the SGSN and GGSN.
- **Gi** – the point of connection between GPRS and the external networks, each referenced by the Access Point Name. This will normally be implemented using IP WAN technology.
- **Gr** – interface between the HLR and SGSN that allows access to customer subscription information.
- **Gs** – optional interface that allows closer co-ordination between the GSM and GPRS networks.
- **Gc** – optional interface that allows the GGSN access to customer location information.

A number of other elements are also introduced (not shown on Figure 1):

- **CG** – the Charging Gateway provides the means to collect and co-ordinate the billing information produced by the SGSN and GGSN before processing by the billing system.
- **DNS** – the IP Domain Name Service is required to enable users to establish a data session with the destination network. It provides the mapping between APNs and GGSN IP addresses.

3. GPRS Operation

3.1. Subscription

The HLR is the repository for all network related subscription information. The functionality of the HLR has been enhanced to include GPRS details. Each user must have at least one GPRS subscription record containing information such as a list of networks (identified using the APN) to which access is allowed and the subscribed Quality of Service (QoS). Further optional information may be stored such as the users' static IP address.

A user may have a subscription for both GSM and GPRS services.

3.2. GPRS Attach

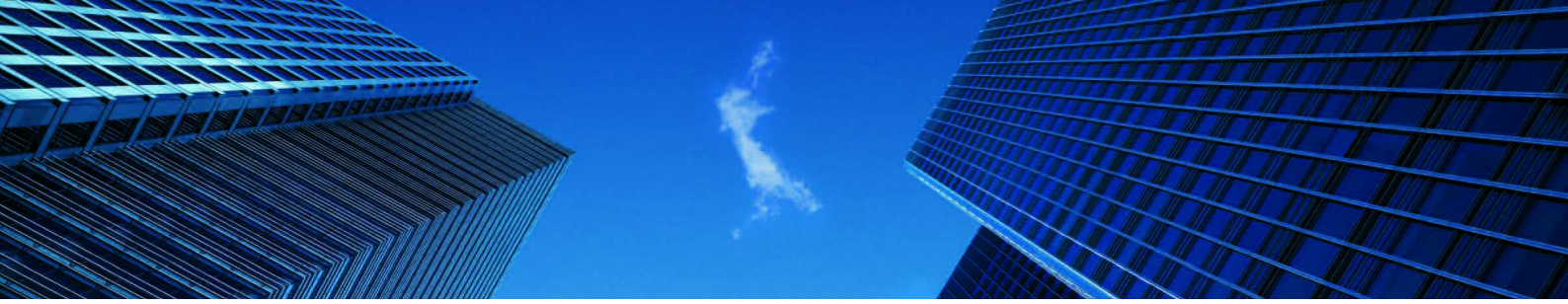
The MS must in the first instance, be known to the network. This is achieved using the GPRS attach procedure. The attach procedure can be summarised as follows:

- The Mobile Station (e.g. GPRS device) first makes a request for enough radio resources to enable the transport of the Attach Request signalling message. Upon assignment of the appropriate radio channel,the Attach Request message is sent.

This contains information about the user's identity, MS capabilities and current location.

- The SGSN constructs an Update Location message that is sent to the appropriate HLR.
- The HLR completes the location updating process and provides the user's GPRS subscription record to the SGSN.
- The SGSN signals to the MS that the procedure is complete.

Upon completion of the Attach procedure, the network is capable of tracking the MS (via subsequent location updates) and is aware of the services and networks that the user may have access to. At this point the user is not able to send or receive data.



3.3. PDP Context Activation

In order to enable user data transfer, a Packet Data Protocol (PDP) Context must be activated in the MS, SGSN and GGSN. This procedure is initiated by the user and is analogous to 'logging on' to the required destination network. The process is illustrated in Figure 2.

1. The user will initiate the 'logging on' process using an application on the PC or MS.

- The MS will request sufficient radio resource to support the Context Activation procedure. Upon allocation of the radio resources, the MS sends the Activate PDP Context Request to the SGSN. This signalling message includes key information such as; the user's static IP address (if applicable), the QoS requested for this context, the APN of the external network to which connectivity is requested, the user's identity and any necessary IP configuration parameters (e.g. for security purposes).
- The SGSN receives the Activate PDP context message and check the user's subscription record to determine if the request is valid.

2. If the request is valid, the SGSN sends a query containing the requested APN to the DNS server.

3. The DNS server uses the APN information to determine the IP address of a GGSN that will provide the required connectivity to the external network. The GGSN IP address is returned to the SGSN.

4. The SGSN uses the GGSN IP address to request a connection (tunnel) to the GGSN.

5. The GGSN upon receipt of this request completes the establishment of the tunnel and returns an IP address to be conveyed to the MS. The GGSN associates the tunnel with the required external network connection.

6. The SGSN sends an Activate PDP context response message to the MS (including IP address) – packet exchange can now commence.

Upon completion of this procedure, a virtual connection is established between the MS and the GGSN. The GGSN also has an association between the tunnel and the physical interface to the external network. Data transfer may now take place between the MS and the external network.

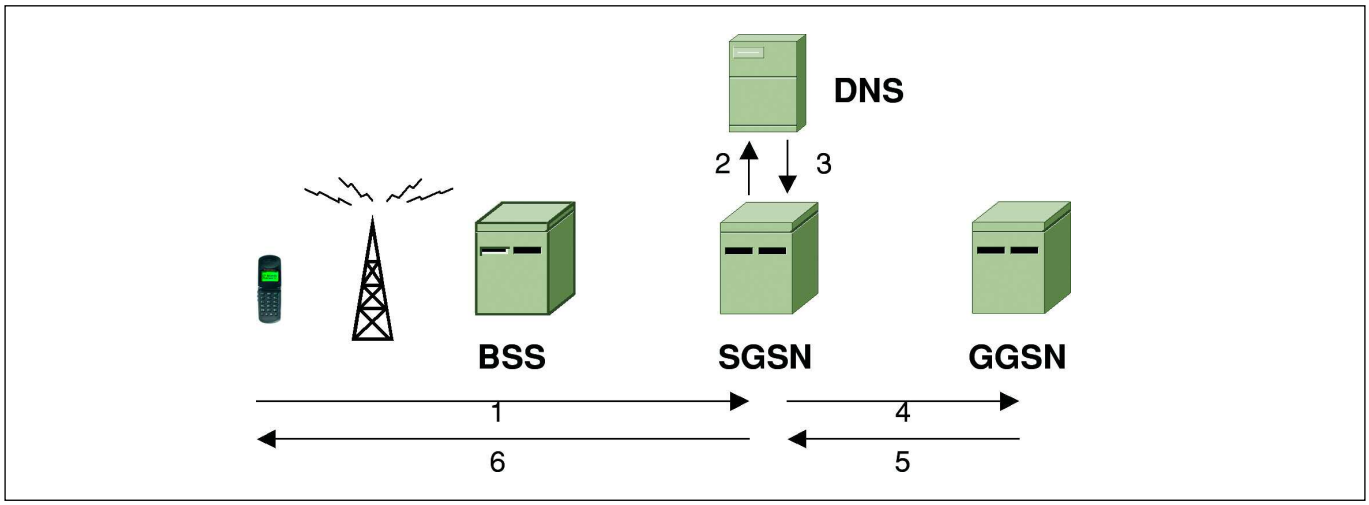
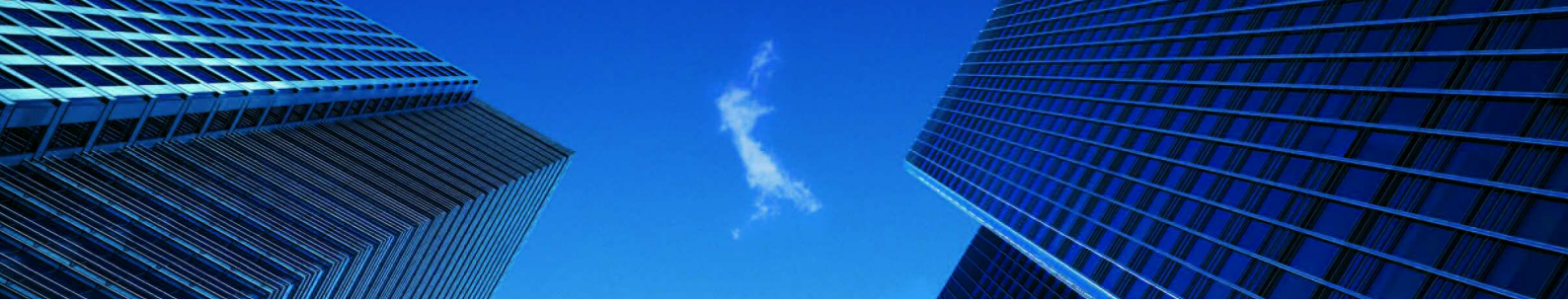


Figure 2:
PDP Context Activation Process.

3.4. GPRS Context Deactivation and Detach

GPRS provides two additional, independent, procedures that enable a PDP context to be deactivated and the MS to disassociate itself from the network (i.e. detach). An implicit context deactivation takes place if the MS invokes the detach procedure. GPRS detach may be performed when:

- The MS is powered off.
- The MS is detached from the network if it stays out of coverage for a period that exceeds the mobile reachable timer (e.g. 3 hours in O2's network).
- User wishes to detach from the GPRS network, but wants to remain attached to the GSM network for circuit switched voice.



3.5. What happens to an incoming voice call during a GPRS data session?

The vast majority of GPRS devices (e.g. mobile handset, laptop datacard, O2 XDAII etc.) are categorised as being Class B mobile devices. Class B devices can be attached to both the GPRS and GSM networks, but they cannot transmit or receive on both simultaneously.

If a mobile is in an active GPRS data session when an incoming voice call is detected, the user will normally be notified by an on-screen message, and will then have the option to suspend the data session and accept the call, or continue with the data session and reject the call.

The diagram shown in Figure 3 illustrates the process. In this example the Call Line Identity (CLI) of the caller has been recognised by the handset of the GPRS user, and therefore the caller's name appears in the display. If the user accepts the call the GPRS data session is suspended until the user ends the call.

If the detach procedure is invoked, any active context will be automatically deactivated.

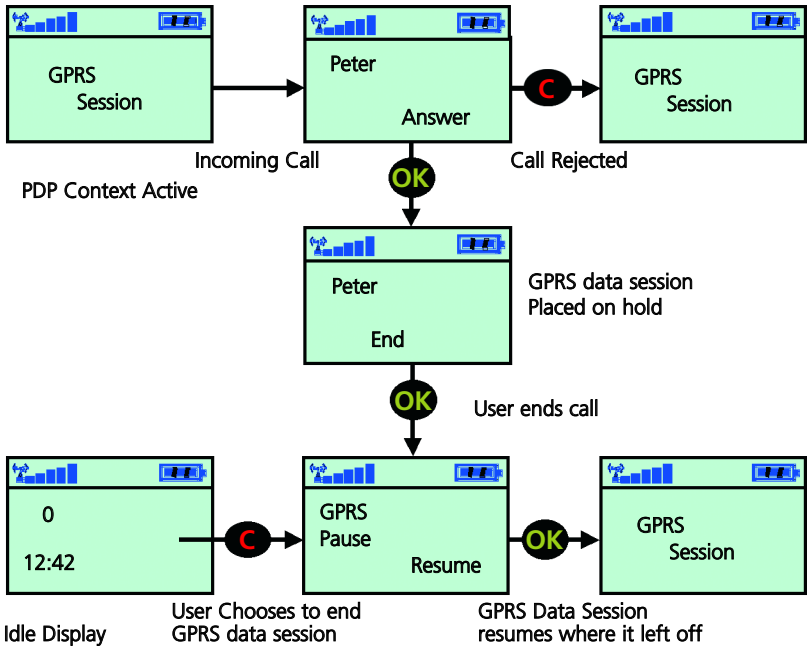


Figure 3:
Voice Call is Received whilst a GPRS Data Call is in Progress.

4. The importance of the access point name

Each data network connected to O2's GPRS network is an 'access point', identified by a unique Access Point Name (APN). The access point may be classed as either private or public. This determines whether O2 carries out a preliminary validation of the GPRS user's subscription record before forwarding their access request to that data network.

- Private access points provide companies with 'closed user group' facilities. Any request for connection to a private access point will be validated by checking the GPRS user's subscription record includes the Access Point Name (APN) requested. If the user's subscription record does not hold the APN, the request will be immediately rejected by O2, and not forwarded to the external data network. Companies still retain responsibility for the security of their network and authentication of GPRS users by means of user names, passwords, etc.
- Public access points: O2 does not validate the subscription records of the GPRS user requesting access to a public access point, and may therefore forward requests for access from GPRS users unknown to the customer. The customer is responsible for the security of their network and authentication of GPRS users if required.
- The APN must be in the form of a registered internet domain name (e.g. anycompany.co.uk or anycompany.com). In many instances organisations will already have a registered Internet domain name, which is used as the basis for that customer's APN. An APN may be formed by adding a prefix to the registered domain name (e.g. gprs.anycompany.com).
- The APN consists of one or more labels, each separated by a dot. Labels should consist only of alphabetic characters (A-Z and a-z), digits (0-9) and the dash (-). The case of alphabetic characters is not significant.
- Each label must start with an alphabetical character, but not with the strings "rac", "lac" or "sgsn".
- Each label must end with an alphabetical character or a digit.
- The APN cannot end with the label ".gprs".
- O2 recommend that APNs should not exceed 22 characters. The customer must ensure that any mobile devices they may use are capable of accepting the length of their APN.
- Where multiple APNs are used, each must be unique and comply with the above rules.

5. Connecting to the corporate LAN via GPRS

Currently, O2's GPRS/3G portfolio consists of three service offerings:

- O2 Bearer Service: O2 provides private circuit(s) to connect the customer network to O2's network. The customer can select between 2 Bearer Service products:
  a. DataLink – consists of a single leased line and a router installed on the Customer Premises.
  b. Resilient DataLink – resilience is provided via the use of two leased lines and two routers.
- O2 Mobile Web service: full internet access is provided.
- O2 Mobile Web VPN service: this service was specifically introduced to allow customers to access their LAN environment via VPN technology.

5.1. Overview

O2's Bearer Service offers business customers a high quality private mobile data connection to their own private domain.

O2's Bearer Service can be used to support both GPRS and 3G data traffic (e.g. the same infrastructure supports both 3G and GPRS users).

The key aspects of O2's Bearer Service are as follows:

- Each connection is defined by a unique, private Access Point Name (APN).
- Connectivity is provided via a physical leased line that connects the O2 network with the customer's LAN.
- Customers can define which Subscriber Identification Module (SIM) cards are able to access their APN.
- The service does not provide any direct access to the Internet.
- All private Bearer Services connect to resilient GPRS Gateway Support Nodes (GGSN's) in the O2 network.

The installation of this service offers customers the opportunity to design the mobile data connectivity service of their choice. Almost every aspect of the service can be configured to the customer's requirements as this is a private service that connects customers to the O2 GPRS and 3G networks directly, using physical leased line infrastructure.

Customer configuration choices include:

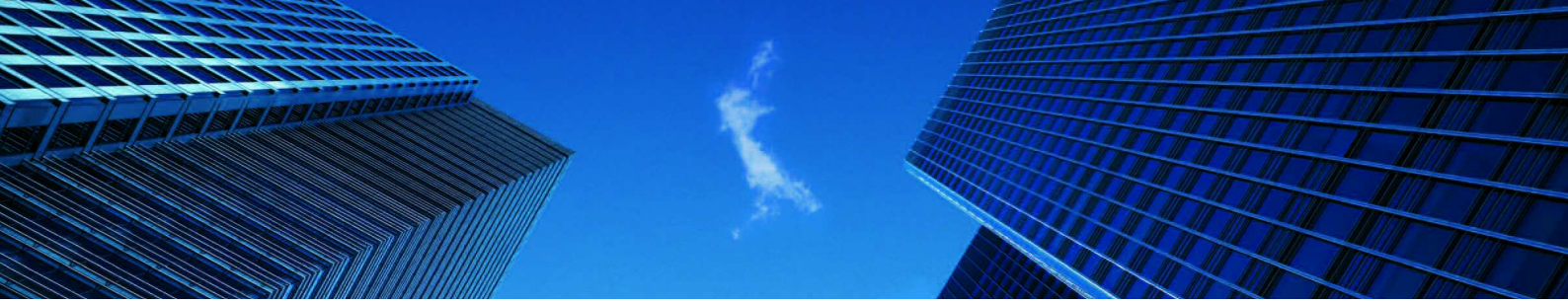
- APN name (normally the same as their Internet registered Domain Name).
- Private (restricted) or Public (open) APN access.
- O2 or customer hosted RADIUS authentication.
- Dynamic or static mobile device IP allocation.
- Private or Public IP Addresses for the mobile devices.

This service is designed for customers that require a private connection to their company LAN, which will offer them the highest quality of service and most consistent data communications performance.

O2's Bearer Service is delivered and managed end-to-end by O2 to ensure the smoothest service delivery and shortest problem resolution timescales. O2 proactively monitor the status of the service and produce detailed usage reports to ensure suitable service levels are maintained at all times.

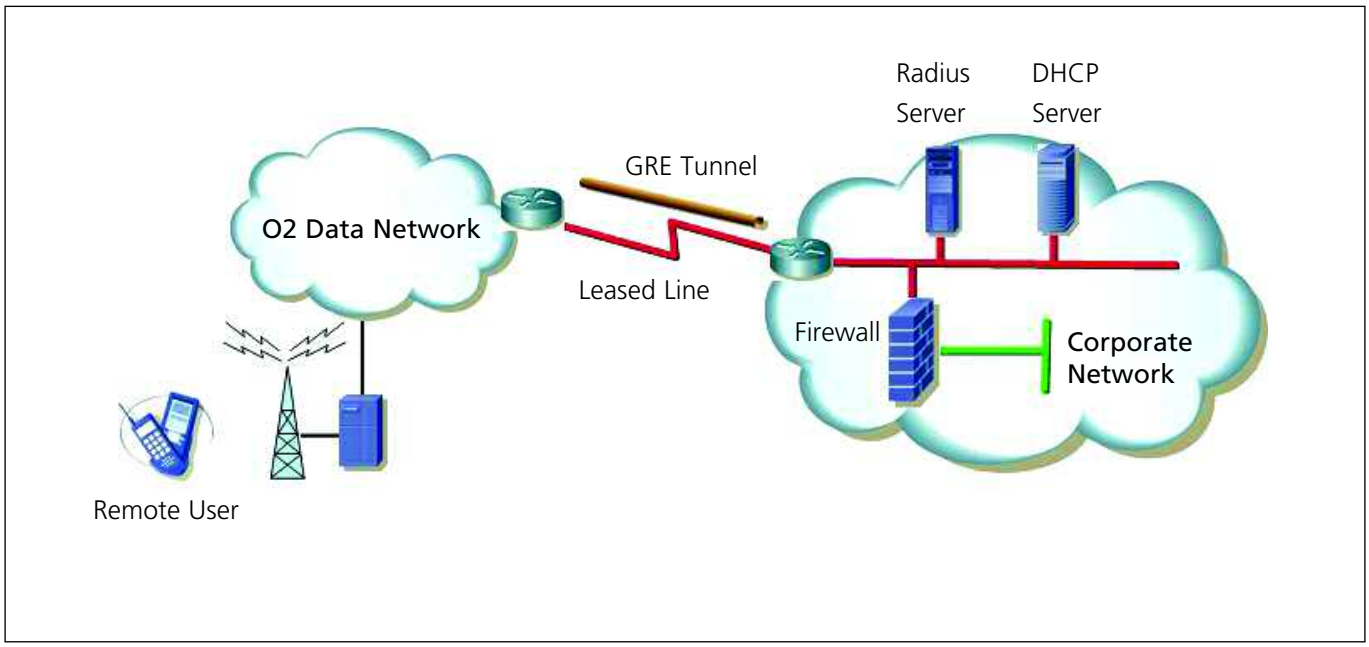
The leased line infrastructure offers the highest level of availability via two basic types of physical connection: DataLink (refer to section 5.2) and Resilient DataLink (refer to section 5.3).

Customers wishing to order O2 Bearer Services should discuss their options with their O2 Account Manager in the first instance. A detailed, "Application For Service", form is used to capture customer requirements and service can be provided in 43 working days after this form has been processed.



5.2. DataLink

Standard connectivity for Bearer Service customers is delivered via a single leased line (128 Kbit/s, 256 Kbit/s, 512 Kbit/s and 2 Mbit/s bandwidths are available), terminating on a single router that is installed, at the customer's premises. Once installed, the router presents a single Ethernet or Token Ring connection to the customers LAN.



Each DataLink can support multiple APNs, each with its own Bearer Service definition. This is useful where customers wish to provide separacy of service to different internal departments, external customers or application user bases.

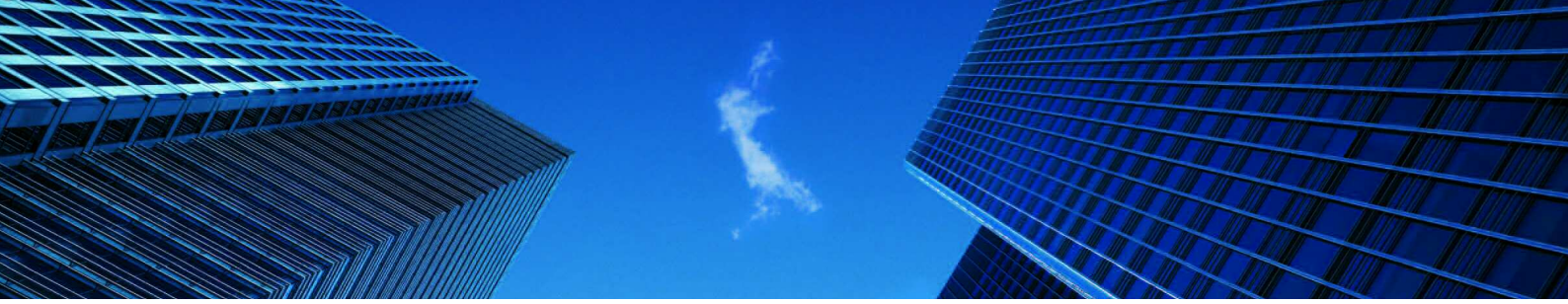
Figure 4:
At a top level, a typical GPRS/3G Bearer Service connection.

5.3. Resilient DataLink

For those customers requiring the very highest levels of availability, O2 offers a Resilient DataLink leased line option to Bearer Service customers. Two links and routers are provided as part of this solution.

The two links and routers can be terminated at the same site, or preferably, at a completely different customer site.

LAN connectivity is required between the two O2 routers and Hot Standby Routing Protocol (HSRP) provides resilience against router failure by allowing two or more routers to share the same virtual IP address (and MAC address) on the same Ethernet LAN segment.



5.4. O2 Mobile Web service

O2's Mobile Web service is designed to enable O2's customers to access Internet content via the GPRS and 3G bearers (refer to Figure 5).

The key aspects of the service are as follows:

- This is a public service and can be used by any O2 post-pay customer.
- The APN associated with the service is "mobile.o2.co.uk"
- Users are allocated a dynamic, private unregistered IP address. However, it should be noted that users of O2's Mobile Web service will be allocated a public IP address, via an O2 Internet facing firewall, when they access Internet resources. The public IP addresses will be allocated in the range 193.113.235.161 to 193.113.235.190.
- Users can surf the Internet, access FTP servers, access email and generally utilise Internet resources.
- The service incorporates an optimisation capability which improves the performance of Internet applications.

This service is similar to broadband services offered by many Internet Service Providers to residential and business customers but does have some important differences:

- The throughput performance available to users is not fixed and will depend on a number of factors including the GPRS/3G device being used, how many other people are using 3G/GPRS in the same area and the capabilities of the O2 network in a given geographic location – refer to section 7 for further information.
- The O2 Mobile Web service uses private IP addressing and Port Address Translation (PAT) when users access Internet resources. PAT was defined by the Internet Engineering Task Force (IETF) as a way to convert private IP addresses to public routable Internet addresses and enables organisations to minimise the number of Internet IP addresses they require (e.g. by using PAT companies can connect thousands of systems/users to the Internet via a few public IP addresses). The use of PAT has implications as although PAT provides many benefits, some applications, including IPSec VPNs, can experience issues when PAT is being used.
- Devices are issued a dynamic, private unregistered IP address, which is not directly visible from the Internet. This means that user's devices are hidden from hackers and other undesirables and affords users some protection when accessing the Internet.
- By default Mobile Web users enjoy an optimised experience when accessing Internet content at no extra cost. This network hosted optimisation can speed up the delivery of Web pages by optimising graphic images and compressing text content. It can however degrade the image quality in Web pages and interfere with some other Internet applications. If this is experienced, the optimisation platform can be bypassed by changing the user name in the Mobile Web settings of the handset/device, as follows:

  – Default settings – includes optimisation:
    - User name: faster
    - Password: password
  – No optimisation required:
    - User name: bypass
    - Password: password

The Mobile Web APN is associated with all new O2 post pay SIM cards. If customers do not wish this APN to be available to users they should specify this requirement prior to SIMs being provisioned.

O2 plan to introduce an anti-spam filtering capability in the near future.

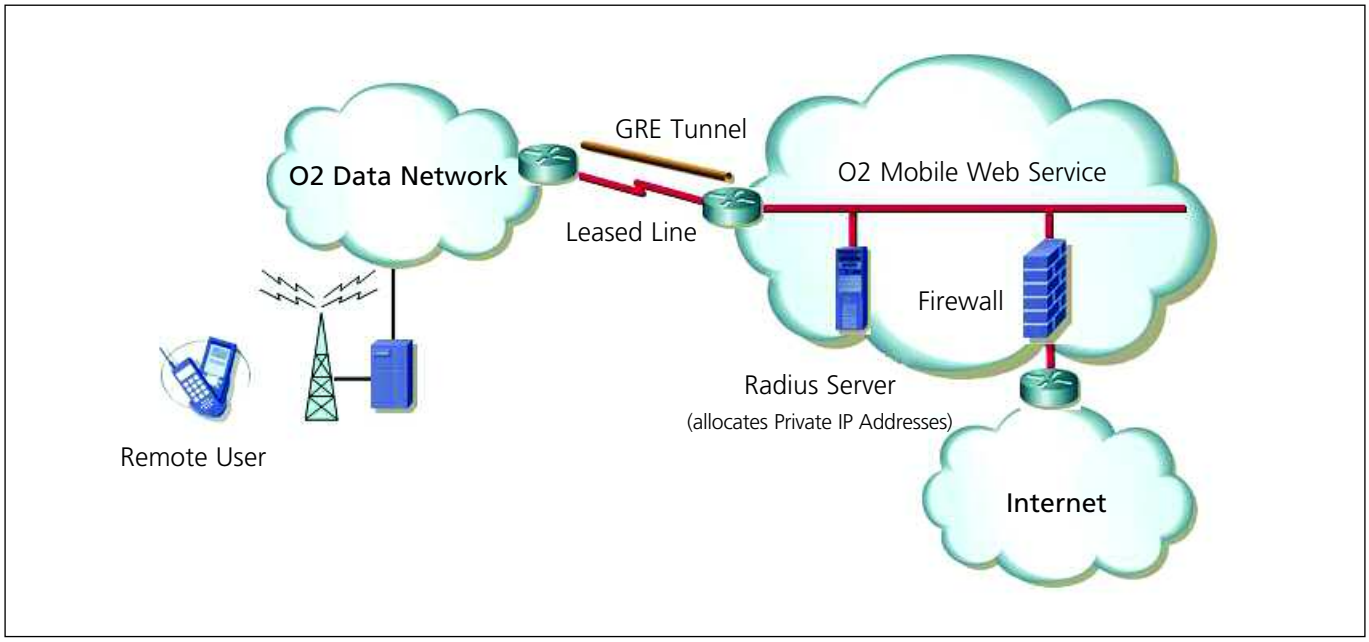
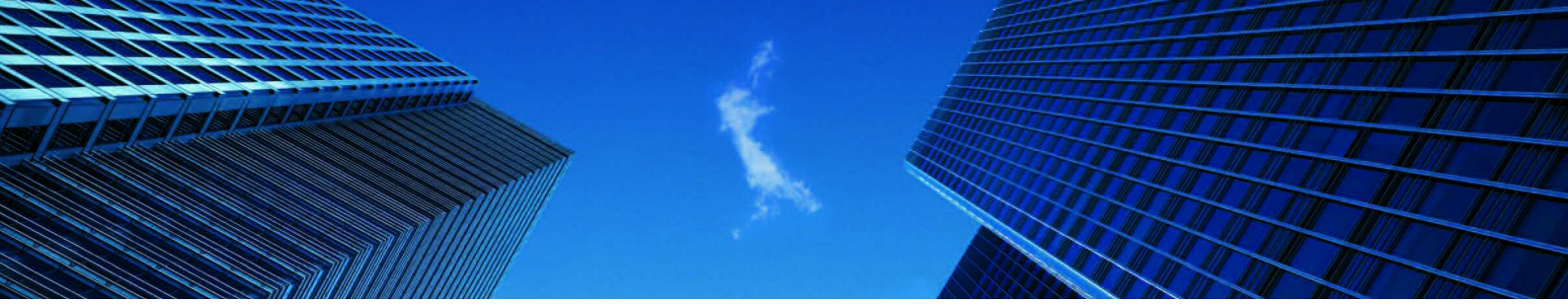


Figure 5:
Top Level Overview of O2's Mobile Web Service.



5.5. O2 Mobile Web VPN service

O2's Mobile Web VPN service was specifically developed to allow customers to use their VPN solutions with GPRS and 3G – assuming the customers VPN solution can be utilised via people connected to the Internet (refer to Figure 6).

The key aspects of the service are as follows:

- This is a public service and can be used by any O2 post-pay customer.
- The APN associated with the service is "vpn.o2.co.uk"
- Users are allocated a dynamic, public registered IP address that is drawn from the following ranges:
  - 82.132.160.1 to 82.132.163.254.
  - 82.132.168.1 to 82.132.171.254.

- Users cannot directly "surf" the Internet, access FTP servers, access email or utilise Internet resources:
  - At the request of customers the service was set-up so only VPN protocols can be used when users first establish their GPRS or 3G connection e.g. the firewall associated with the service will block all other traffic.
  - Once the VPN session is in place users will be able to browse the Intranet/Internet and access other corporate resources – assuming the corporate security policy allows such transactions to take place.
  - Split tunnelling will not work as users are not able to access Internet resources directly.

The O2 Mobile Web VPN service does not include any optimisation capability, and end user devices are allocated publicly registered IP addresses. The service offers businesses the ability to provide secure LAN access to their users via the Internet and control their usage through the application of their internal IT policy.

Access to Mobile Web VPN can be requested via O2 Customer Services and is usually provisioned within 24 hours.

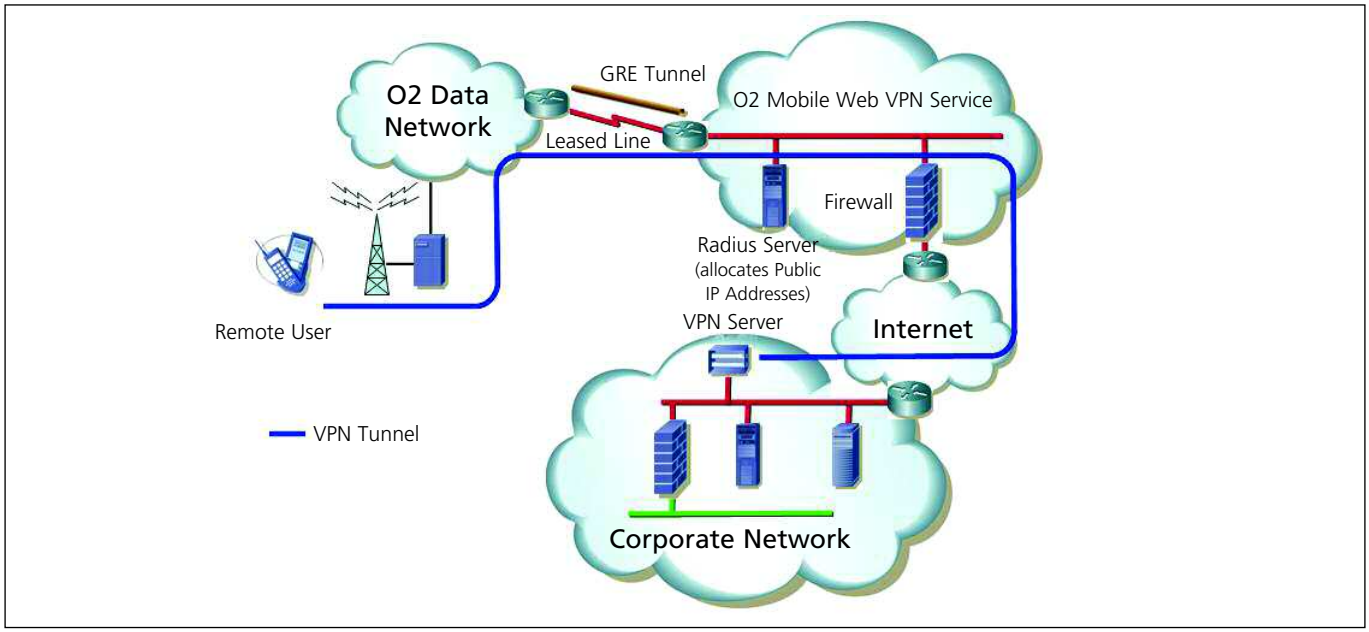


Figure 6:
A VPN Tunnel Established between a Remote User and the Corporate LAN.

6. How secure is GPRS?

A separate paper titled, "GPRS/3G Services: Security", written by O2 and Information Risk Management (IRM) considers security in detail.

IRM[2] were selected by O2 to assess, over a period of several months, all the potential attack vectors associated with the GPRS and 3G infrastructure and developed scenarios whereby attacks could be mounted.

During the project IRM developed new tools and techniques in order to test for vulnerabilities in protocols and products for which there are no publicly available testing methodologies.

All areas of the infrastructure were evaluated, from the mobile user, through the air interface, core network, to the customer's corporate network. At each stage scenario-based attacks were mounted with the intention of gaining unauthorised access to any of the infrastructure components.

Throughout the entire investigation none of the discoveries by IRM were classified as 'high risk' and all findings were swiftly addressed and mitigated by O2. The GPRS and 3G services provided by O2 were considered to be extremely well configured and managed.

[2]IRM were selected by O2 because they were in a unique position to provide expertise not only in IP based networks, but also in cellular networks. IRM are acknowledged as industry leaders in the vulnerability and penetration testing space.

7. Throughput performance of the GPRS Bearer

7.1. Capabilities of the O2 GPRS network

GPRS is classed as being a packet switched network whereby radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user for a fixed period of time, the available radio resource can be concurrently shared between several users. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell. The actual number of users supported depends on the applications being used and how much data is being transferred.

The throughput performance is the rate at which IP packets are transferred and is dependent on a number of factors including the following:

- The capabilities of the O2 GPRS network in a given geographic location.
- How many other people are using GPRS in the same area and what applications they are utilising.
- The GPRS device being used.
- The coding scheme being used.

As a 'rule of thumb', in the majority of O2's network, the data rate available to applications will be approximately 8 to 10 Kbit/s per timeslot. This assumes coding scheme 2 is being used, refer to section 7.3, and that the O2 network is able to provide the maximum radio resources supported by the GPRS device.

O2 (UK) has deployed many thousands of cellular base stations around the UK. Base stations serve a particular geographic location and have a number of timeslots available that can be used to support voice or GPRS data calls. The timeslots on the base-station are configured as follows:

- At least one timeslot is dedicated for use by GPRS devices.
- Timeslots that are not dedicated to GPRS are classed as being switchable.
- Switchable timeslots can be used to support voice or GPRS data calls. However, voice calls will take precedence.

It should be noted that O2's radio planners are constantly reviewing O2's network to ensure that sufficient radio resources are available (e.g. timeslots) for both voice and GPRS data calls in a given location.

7.2. Multislot class of GPRS devices

GPRS devices have a multislot class which defines the maximum achievable data rates that can be supported by the device in both the uplink (e.g. out of the device) and downlink (e.g. into the device) directions.

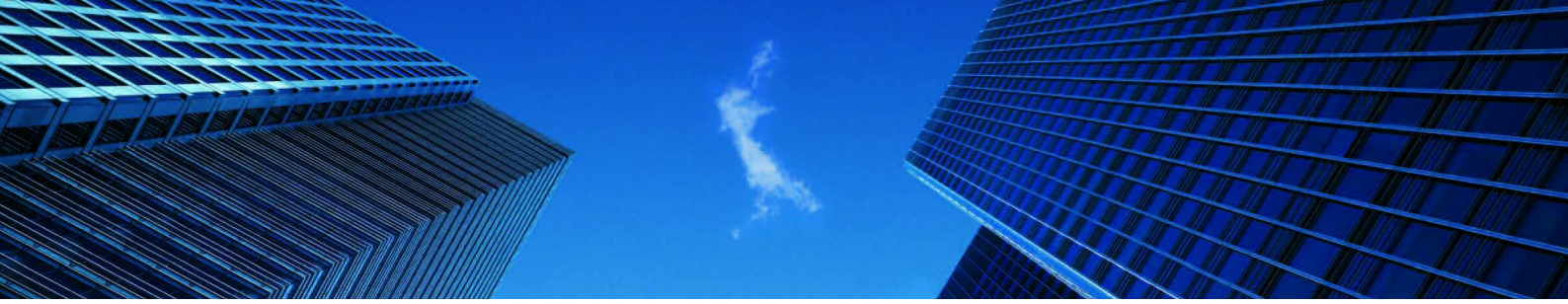
Often equipment manufacturers will indicate the capabilities of their devices in the form of two numbers, 3+1 or 2+2 for instance. The first number indicates the amount of downlink timeslots that the mobile device can support for data transfer and the second number indicates the amount of uplink timeslots the device can utilise to transmit data.

The GPRS network will always try to provide the maximum number of timeslots the device can support regardless of how much data is to be transferred.

Table 1 details the number of downlink and uplink slots associated with the most common multislot classes. The active slots parameter details the total number of slots the GPRS device can use simultaneously for both uplink and downlink communications.

Multislot class	Downlink slots	Uplink slots	Active slots
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5

Table 1:
Attributes of a number of different GPRS multislot classes.



7.3. GPRS coding schemes

Four coding schemes are defined for GPRS – although only Coding Scheme 1 (CS-1) and Coding Scheme 2 (CS-2) are currently widely supported. Table 2 details the data rates achievable for a given number of timeslots. However, the following should be noted:

- The figures presented include some overhead (e.g. the actual data rate available to applications will be less than shown in the Table 2).
- The higher coding schemes offer the potential of increased data rates. However, these rates are at the expense of some degree of data robustness, making these schemes more susceptible to interference and poor signal strength.
- The cell radius for the higher coding schemes (CS3 and CS4) is smaller than that for CS1 and CS2 thereby reducing the effective area of coverage.
- As detailed in the previous section the multislot class of the GPRS device will define how many timeslots can be used by a device.

Coding Scheme Data Rates (Kbit/s)				
Timeslots	**CS-1**	**CS-2**	**CS-3**	**CS-4**
1	9.05	13.4	15.6	21.4
2	18.1	26.8	31.2	42.8
3	27.15	40.2	46.8	64.2
4	36.2	53.6	62.4	85.6

Table 2:
GPRS Coding Scheme Data Rates.

Glossary of Terms

8. Glossary of terms

APN	Access Point Name
BSC	Base Station Controller
BSS	Base Station System
CG	Charging Gateway
CLI	Call Line Identifier
CS	Coding Scheme
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Service Digital Network
LAN	Local Area Network
MS	Mobile Station
MSC	Mobile Switching Centre
NAT	Network Address Translation
PAT	Port Address Translation
PCU	Packet Control Unit
PDP	Packet Data Protocol
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SIM	Subscriber Identity Module
SGSN	Serving GPRS Support Node
URL	Uniform Resource Locator
VLR	Visitor Location Register
VPN	Virtual Private Network
WAN	Wide Area Network