GPRS and 3G Services: Connectivity Options

An O2 White Paper

Contents

1. Executive Summary

O2's General Packet Radio Service (GPRS) and Third Generation (3G) services offer high speed wireless packet data capabilities to mobile devices connected to the network. These services enable devices to attach to the network and then establish data connections via both public and private domains. These domains are defined by use of an Access Point Name (APN), which is similar in structure and function to an Internet domain name.

In the context of this paper O2's GPRS and 3G connectivity 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 Virtual Private Network (VPN) service: this service was specifically introduced to allow customers to access their Local Area Network (LAN) environment via VPN technology.

When determining which service is most appropriate to a particular customers needs it is envisaged a number of factors will be considered including the following:

- Cost of the service:
  - The Bearer Service options require that a leased line(s) and router(s) be provided by O2 and there is a yearly rental cost associated with the link(s) and router(s).
  - If a company does not already have a method for allowing people to access the corporate LAN via the Internet, via a VPN gateway for instance, they may find it preferable to use O2's Bearer Service and choose an authentication approach which meets their requirements. This approach may prove a cheaper option than deploying new Internet facing gateways and using O2's Mobile Web or Mobile Web VPN services.
  - End users are only charged for the data they send and receive and O2's standard charges are the same regardless of which service is utilised (i.e. Bearer Service, Mobile Web or Mobile Web VPN).

- What applications and services are going to be used?
  - Is there a requirement to limit what Internet resources people can access via GPRS/3G? Users can access any Internet server via O2's Mobile Web service – although it is noted that personal firewalls can be used as a way of "policing" what Internet resources people can use.
  - Is there a requirement to interact with the mobile device from a server – perhaps to poll the remote client for instance? This may not be possible if O2's Mobile Web and Mobile Web VPN services are used.
  - Do the applications work if Port Address Translation (PAT) is being used – O2's Mobile Web service utilises PAT.

- O2's Mobile Web service includes optimisation which allows Web pages to be downloaded more quickly.
- Are the mobile applications that are going to be deployed mission critical to an organisation? If they are, customers are recommended to use O2's Bearer Service, preferably with a Resilient DataLink, as O2 are responsible for all aspects of the Bearer Service.

- What level of service and support is required?
  - Although O2 endeavour to provide the highest level of service on all its GPRS/3G services, if problems are experienced with the public services (i.e. Mobile Web or Mobile Web VPN services) it is far more difficult to ascertain what is happening and where the problem lies – for instance a number of ISPs may lie between O2 and the customer.
  - O2 pro-actively monitor the status of the Bearer Service and have established Service Level Agreements (SLAs) with the telecoms organisations that provide the leased line connections.
  - If customers procure the Bearer Service, O2's technical consultancy teams will work with them to ensure they derive the required business benefit.

Information on each of O2's GPRS/3G services is provided in the following sections of this report.

2. Bearer Service

2.1. 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 2.2) and Resilient DataLink (refer to section 2.3).

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.

2.2. 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.

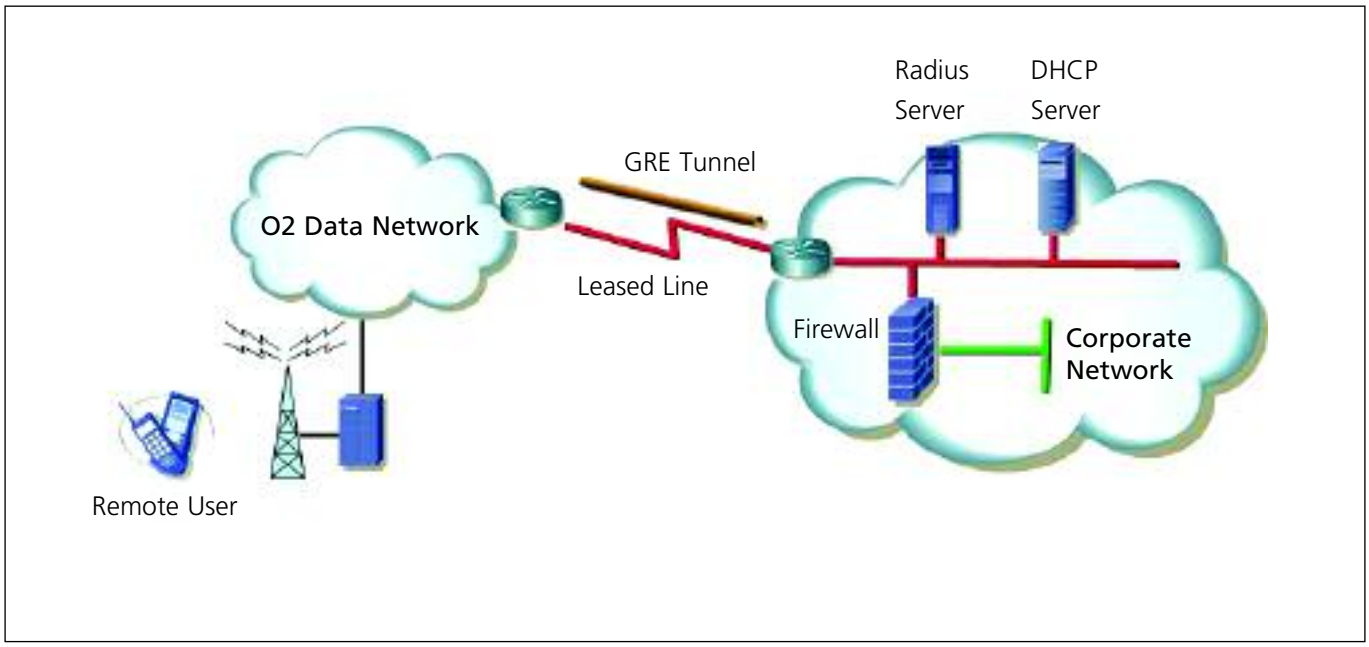

Figure 1:
Typical GPRS/3G Bearer Service Connection.

2.3. 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. However, it is strongly recommended that they are deployed in different computer rooms which are served by different exchanges and duct routes.

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.

2.4. Application Support

O2 does not impose any restrictions on the type of data or ports that can be used for data transfer between the mobile devices and the corporate network. Consequently, all applications can be used in conjunction with O2's Bearer Service.

3. Mobile Web

3.1. Overview

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 2).

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. An O2 White Paper, "GPRS – How It Works", considers in detail what affects the throughput of the GPRS bearer.
- 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.

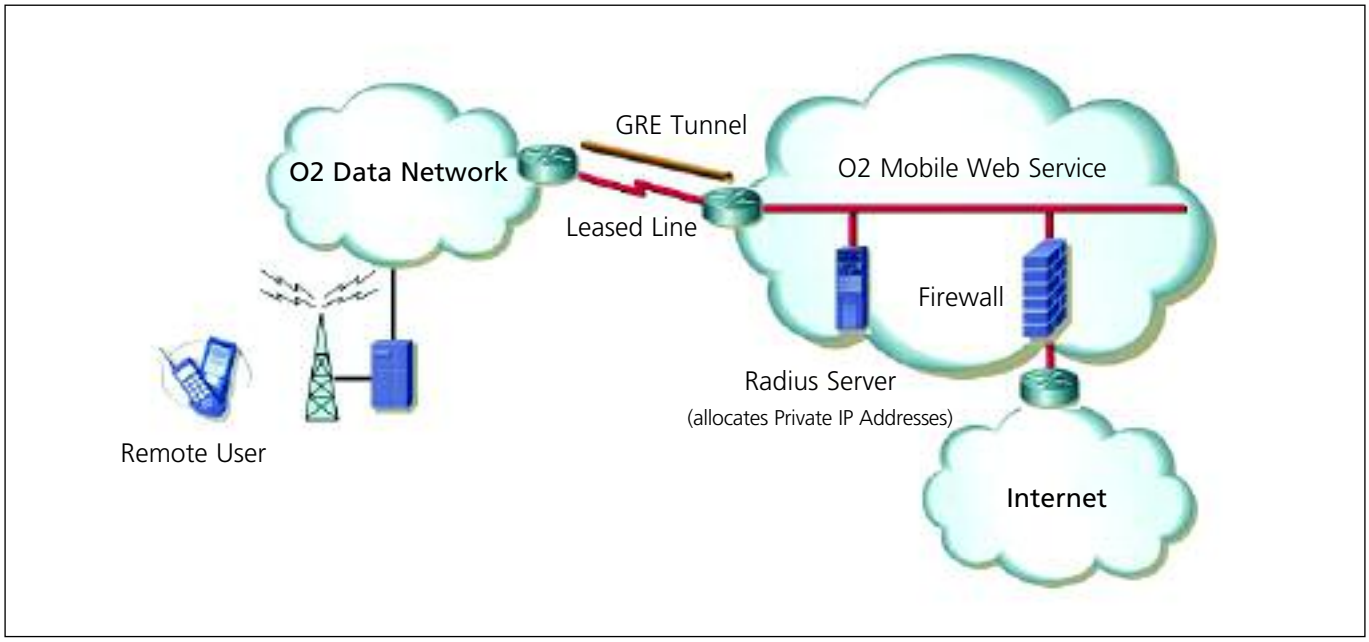

Figure 2:
Top Level Overview of O2's Mobile Web Service.

3.2. Application Support

Most applications will work in conjunction with O2's Mobile Web service without any problems being experienced. However, as detailed in section 3.1 O2's Mobile Web service does incorporate an optimisation cluster and this can have an undesirable impact on some applications. If problems are experienced the user name bypass should be used to remove the optimisation functionality.

If there is a requirement to interact with the mobile device from a server (i.e. perhaps to poll the remote client for instance) then the following must be taken into account:

- If a Transmission Control Protocol (TCP) based application is being used it will not be possible to poll the mobile device from the server. The firewall that underpins the O2 Mobile Web service will only allow TCP sessions to the mobile device if it is a continuation of an existing TCP session that was started by the mobile device.
- If a User Datagram Protocol (UDP) based application is being used it is possible to poll the mobile device from the server. However, as O2's Mobile Web service uses Port Address Translation (PAT) to conserve IP addresses the IP address, source port and destination port being used by the mobile device application must be captured at the server. In order to send UDP data back to the mobile device the source port of the server sent data must be the same as the destination port of the received data from the mobile – similarly the destination port of the server sent data needs to be the same as the source port of the received data from the mobile. The following example illustrates what must be done at the server:

  The UDP packets received at a server from a mobile device have the following parameters – ports chosen at random:
  - IP address: 193.113.235.167.
  - Source port: 8000.
  - Destination port: 3000.

  In order to send UDP packets back from the server to the mobile device the following parameters would need to be used:
  - IP address: 193.113.235.167.
  - Source port: 3000
  - Destination port: 8000

It should also be noted that the UDP session will be terminated if there is inactivity for 15 minutes or more i.e. if no data has been sent from the mobile for 15 minutes or longer the UDP session will be "torn down" by the firewall.

Unless customers wish to support split tunnelling they are recommended to use O2's Mobile Web VPN service in conjunction with their IPSec based VPN solution (refer to section 4 for more information on O2's Mobile Web VPN Service).

Split tunnelling is the process of allowing a remote VPN user to access the Internet at the same time that the user is allowed to access resources on the corporate LAN via the VPN Service. This method of network access enables the user to access remote resources, such as corporate email, at the same time as accessing the public network. An advantage of using split tunnelling is that it alleviates bottlenecks and conserves bandwidth as Internet traffic does not have to pass through the VPN server. A disadvantage of this method is that the corporate LAN IP policy is not imposed on the user as they access the Internet directly.

Point-to-Point Tunnelling Protocol (PPTP) and Secure Sockets Layer (SSL) based VPN solutions can be used in conjunction with O2's Mobile Web service.

4. Mobile Web VPN

4.1. Overview

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 3).

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.

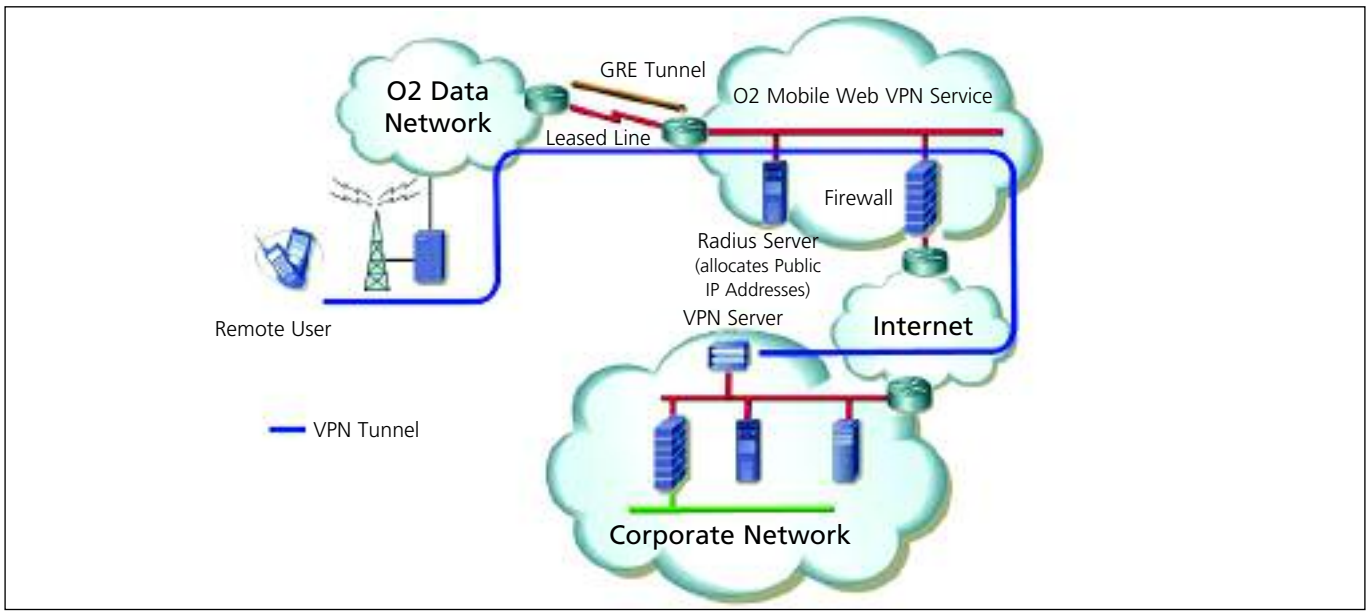

Figure 3:
A VPN Tunnel Established between a Remote User and the Corporate LAN.

4.2. Application Support

The VPN solutions supported can be summarised as follows:

- Only IP ports associated with VPN protocols can be used when users first establish their GPRS or 3G connection.
- The supported VPN protocols are IPSEC, L2TP, PPTP and SSL. O2's White Paper titled, "O2's GPRS/3G Services: VPN Solutions Supported", provides detailed information on the protocols and ports that are supported by the service.
- Tracert and ping are supported for connectivity testing.

5. Service Comparison

5. Service Comparison

Table 1 summarises the differences between the O2 GPRS/3G services.

Service Comparison Matrix			
Metric	**Bearer Service**	**Mobile Web**	**Mobile Web VPN**
APN	Customers Choice	mobile.o2.co.uk	vpn.o2.co.uk
Access Type	Public or Private	Public	Public
Number of devices supported	Unlimited	Unlimited	Unlimited
Direct Internet Connectivity	Internet Connectivity via corporate LAN – subject to IT policy	Yes	Internet Connectivity via corporate LAN – subject to IT policy
Mobile IP Addresses	Customers Choice	Private (PAT)[1]	Public
IP Address Allocation	Customers Choice	Dynamic	Dynamic
Supported Protocols	All	Most Internet	VPN Only
Bearer Optimisation	Customers Choice	Optional	No
Content Optimisation	Customers Choice	Optional	No
TCP Inactivity Timeout	Customer Choice	30 minute	30 minute
UDP Inactivity Timeout	Customer Choice	15 minute	15 minute
Access Lead Time	43 working days	Immediate	<24 hours
Service Reach	End to End	Gateway only	Gateway only
Service Performance[2]	O2 pro-actively monitors the status of the Bearer Service	Best endeavours	Best endeavours

Table 1:
Service Comparison Matrix.

1. 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.

2. Although O2 endeavour to provide the highest level of service on all its GPRS/3G Services if problems are experienced with the public services (i.e. Mobile Web or Mobile Web VPN services) it is far more difficult to ascertain what is happening and where the problem lies – for instance a number of ISPs may lie between O2 and the customer. Hence, the term, "best endeavours" is used in the table.

6. Appendix 1

6. IP Addresses used by the O2 services

Service	Public IP Address Range		Availability	
	Start	End	Start	End
Mobile Web	193.113.235.161	193.113.235.190	Current	N/A
Mobile Web VPN	82.132.160.1	82.132.163.254	Current	N/A
	82.132.168.1	82.132.171.254	Current	N/A

7. Private IP Addresses used by O2's Mobile Web Service

7.1. No Optimisation

If a user name of bypass is used (no optimisation) a private IP address from the following ranges will be allocated to the end device:

- 10.228.160.1-10.228.167.254
- 10.228.168.1-10.228.175.254
- 10.228.176.1-10.228.191.254
- 10.233.168.1-10.233.175.254
- 10.233.176.1-10.233.183.251
- 10.233.184.1-10.233.191.251

7.2. Full Optimisation

If a user name of faster is used (full optimisation) a private IP address from the following ranges will be allocated to the end device:

- 10.228.192.1-10.228.207.254
- 10.228.208.1-10.228.223.254
- 10.228.224.1-10.228.255.254
- 10.233.192.1-10.233.223.254
- 10.233.224.1-10.233.239.251
- 10.233.240.1-10.233.255.251

7.3. Web Optimisation

If a user name other than faster or bypass is used (Web optimisation) a private IP address from the following ranges will be allocated to the end device:

- 10.225.1.1-10.225.255.254
- 10.226.1.1-10.226.255.254
- 10.234.1.1-10.234.255.254
- 10.235.1.1-10.235.255.254
- 10.247.1.1-10.247.255.251
- 10.249.1.1-10.249.255.251

Glossary of Terms

8. Glossary of Terms

3G	Third Generation mobile phone service (AKA: UMTS)
APN	Access Point Name
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
GGSN	GPRS Gateway Support Nodes
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HSRP	Hot Standby Routing Protocol
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
L2TP	Layer 2 Tunnelling Protocol
MMS	Multimedia Messaging Service
PAT	Port Address Translation
PPTP	Point-to-Point Tunnelling Protocol
RADIUS	Remote Access Dial In User Service
SIM	Subscriber Identification Module
SMS	Short Message Service
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telephone Service
VPN	Virtual Private Network
WAP	Wireless Application Protocol