GLOSSARY OF TERMS

ADM - Add-Drop Multiplexer
An add-drop multiplexer has the capability to add one or more lower-bandwidth signals to an existing high-bandwidth data stream, and at the same time can extract or drop other low-bandwidth signals, removing them from the stream and redirecting them to some other network path. This is used as a local “on-ramp” and “off-ramp” to the high-speed network.

Air Cooling
Computer equipment generates heat, and is sensitive to humidity and dust. Maintaining a stable temperature and humidity within tight tolerances is critical to IT systems reliability. In most server rooms “close control air conditioning” systems, also known as PAC (precision air conditioning) systems, are installed. These systems control temperature, humidity and particle filtration within tight tolerances 24 hours a day and can be remotely monitored. They can have built in automatic alerts when conditions within the server room move outside defined tolerances.

Apache
One of the world’s most popular Web server programs, Apache was built by a group of open-source programmers and is often used because of its outstanding performance, strong security features and the fact that it is free.

Application Infrastructure
The software components that custom applications rely on for their functionality. Examples include web servers, application servers and database servers.

Bandwidth
The amount of data that can be transmitted at a given moment to a server. The higher your bandwidth, the larger the amount of traffic your site can handle at one time.

BIOS - Basic Input / Output System
The BIOS in a PC is the code that runs when the computer is first turned on. It is stored in a form of memory on the motherboard, and when run will initialise and configure the hardware, load boot code for the operating system (usually from a hard disk), then transfer control to the operating system.

Blade Server
A blade server is a stripped down server computer with a modular design optimised to minimize the use of physical space and energy. Blade servers have many components removed to save space, minimize power consumption and other considerations, while still having all the functional components to be considered a computer. Unlike a rackmount server, a blade server needs a blade enclosure, which can hold multiple blade servers, provides services such as power, cooling, networking, various interconnects and management.

Bridging
Combining two network segments as if they were one network. An Ethernet bridge does not use routing, but rather relies on broadcasting to communicate between the two segments.
GLOSSARY OF TERMS

Broadcasting
Sending packets that are designed to be received by all devices on a subnet. Broadcasting is limited to the broadcast domain, which includes only those computers able to talk to one another on a network directly, without going through a router.

CGI - Common Gateway Interface
A small script the processes data taken from the user, such as from a form application.

CGI - Bin
The directory on a web server where CGI scripts are stored.

Circuit Switching
In a circuit switching network, a dedicated circuit must be opened between users before they can communicate and while the circuit is open no other users may use that circuit or parts of it. A circuit may remain open without any information transmission and still be unusable by others; it must be closed before its components are available to different users.

Cloud
A pool of highly available servers and computing services made available for general use by web and other network based applications.

Cloud Bursting
Using cloud resources as a pressure valve when an increased amount of computer resources are required for a burst in traffic, or short term demand spikes in activity or load.

Cloud Computing
The sharing of compute resources and related infrastructure components to facilitate the deployment and operation of web and network based applications. Cloud computing environments provide developers and their customers direct, on-demand access to large scale and scalable computing capabilities, at a lower cost level, resilience and data security of dedicated options such as managed data centres, colocation facilities, or private data centres.

Codec
An algorithm that encodes audio, video or pictures into a digital format for transmission over the network and can then decode it back for listening or viewing. Different codecs make different trade-offs between high quality, bandwidth usage, and CPU cycles.

Colocation (Colo)
Use of a third parties data centre to install and run your own IT equipment. The provider maintains the environment, power, cooling, protection systems, security etc. The customer provides servers and storage. Space in the facility is leased by the rack, cabinet, cage or room. Many Colos have extended their offerings to include managed services that support their customers business initiatives.

CPE - Customer Premises Equipment
Any device at a customer’s premises connected to a telecommunications network on the customer side of a demarcation point.
GLOSSARY OF TERMS

Dark Fibre
An unused optical fibre available to be lit for use in fibre-optic communication. The term can refer to an unused cable already installed in the ground or to a new cable to be dug in.

DDoS - Distributed Denial of Service
The most common form of attack on network devices. It overwhelms a network by monopolising its bandwidth by flooding it with information from multiple hosts thereby preventing legitimate network traffic.

Demarc - Demarcation Point
The point at which the wiring on a customer’s premises meets that of telecommunications providers. A demarc can be as simple as a connection between internal and external telephone wires, or a box allowing connection of all forms of telecommunications, from telephone and cable, to fibre optic connections.

Device
Refers to the individual hardware components that make up a unique hosted configuration. This includes servers, firewalls and load balancers.

Diversity
Network diversity is having two or more separate connections from two different providers running in separate ducts along different physical paths. This ensures that no single point of failure exists.

DHCP - Dynamic Host Configuration Protocol
A protocol used between clients (network devices such a computers) and a DHCP server so that the client can obtain a valid IP address and other information such as default gateway, subnet mask, and DNS servers for the client to connect to the network.

DNS - Domain Name System
The system that provides information about domain names to users of the internet. A widespread distributed directory of information about the internet. Publically available domain names must be globally unique and are managed via central registries. Domain names are matched to the IP address of specific hosts; these addresses of specific hosts; these addresses must also be globally unique. The domain name system can take a domain name and return information about how to reach it (IP address); how to send mail to a user on it (mail exchange servers); and digging further, even information about the owner of the domain, when it was registered and when it might expire.

DWDM - Dense Wavelength Division Multiplexing
A technology that puts data from different sources together on an optical fibre with each signal carried at the same time on its own separate wavelength. Using DWDM, up to 80 (and theoretically more) separate wavelengths or channels of data can be multiplexed into a light stream transmitted on a single optical fibre.

EAD - Ethernet Access Direct
Ethernet Access Direct provides point-to-point data connectivity between sites. It can be used to build and extend customer networks, develop new infrastructure and meet low-capacity backhaul requirements.
GLOSSARY OF TERMS

Encryption
A process by which information is changed from a meaningful usable form (called plaintext) into an encrypted form (called ciphertext) which is undecipherable except to those with the key to decrypt it. Encryption may apply to a single file on disk, to all data in packets over a network connection or to an entire stream of data.

Ethernet, Fast Ethernet, Gigabit Ethernet
A family of related protocols for sending data up to and including the data link layer, as per the OSI model. Ethernet generally refers to the entire family or sometimes just 10 megabit per second connections. Fast Ethernet is 100 megabits per second and Gigabit Ethernet is 1,000 megabits (or one gigabit) per second.

Fibre Optic
Optical fibre or “fibre optic” refers to the medium and technology associated with the transmission of information as light pulses along a glass or plastic strand or fibre. Optical fibre carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to re-transmit signals but does require repeaters at distance intervals. Glass fibre requires more protection within an outer cable than conventional copper wire.

Firewall
A piece of security software or hardware designed to protect web servers. They are typically used to protect sites from hacker attacks and unauthorised access.

FQDN - Fully Qualified Domain Name
A complete domain name that unambiguously refers to an address in DNS. As an example, a host named next connex at example.com will have the FQDN of nextconnex.example.com

FTP
Short for File Transfer Protocol, a method of allowing remote users and web servers to exchange files.

GRE - Generic Routing Encapsulation
A tunnelling protocol that provides encapsulation of OSI layer 3 packets inside IP packets. GRE provides a virtual point-to-point link between machines at remote points on an IP network like the internet. GRE is completely insecure, but it provides a fast and simple way to access a remote network.

Grid Computing
An architecture for server networking whereby processing cycles of all computers in a grid network can be allocated to a particular application. This differs from other architectures in that the integration is accomplished at the hardware level, thereby making the grid appear as a single large resource, rather than a pool of shared autonomous resources.

Hosting
The hosting provider usually provides the servers used to run your applications. Typically a website, remote software solution, or maybe an email service.
An ethernet hub is a networking device with multiple ports that connect many networking devices in a star topology. When a packet arrives in one of the hub’s ports, the hub simply repeats that packet to all of its other ports so it is received by all computers connected to the hub, in the hope that the correct destination machine will receive the packet. Because every packet on every port in the hub is repeated back out its other ports, collisions occur frequently and slow down the network.

**Hub**

An ethernet hub is a networking device with multiple ports that connect many networking devices in a star topology. When a packet arrives in one of the hub’s ports, the hub simply repeats that packet to all of its other ports so it is received by all computers connected to the hub, in the hope that the correct destination machine will receive the packet. Because every packet on every port in the hub is repeated back out its other ports, collisions occur frequently and slow down the network.

**HTML - Hyper-Text Mark-up Language**

The language by which web servers and client browsers communicate. All server-side functions (such as database processing), although they may be performed in another language, must eventually be output back to the user in HTML.

**HTTP - Hyper-Text Transfer Protocol**

The protocol by which HTML files move across the internet. HTTP requires a client browser and HTTP server, typically a web server.

**IDS - Intrusion Detection System**

Recognises all types of hostile network traffic and computer usage that can’t be detected by a conventional firewall.

**IIS - Internet Information Server**

Short for internet information server, Microsoft’s server software for Windows NT/2000

**Interface**

A name used in Linux operating systems to describe a network connection. The connection may directly correlate to a physical device such as eth0 (describing a specific ethernet port), or a virtual connection through another connection, such as tun0 tunneled over another connection.

**IOS - Internet Operating System**

Used in most Cisco routers. IOS is a specific purpose operating system designed for handling network tasks on Cisco networking hardware.

**IP - Internet Protocol**

Designates the format of data packets that are used to exchange information over the internet. IP is the protocol involved in transporting a packet of information from one computer on a network to a remote machine potentially on the other side of the world. Routers pay attention to the IP address carried in an IP packet, and perform the magic required to shift the packet hop-by-hop to its final destination. IP provides no guarantees of reliability so if packets are lost in transit, accidentally duplicated, arrive in the wrong order, or arrive corrupted, no effort is made to address the problem on the IP level - that is left to protocols a layer above, such as TCP.

**IP Transit**

The service of allowing network traffic to cross or “transit” a computer network, usually used to connect a smaller internet service provider (ISP) to the larger internet.
**GLOSSARY OF TERMS**

**IPsec - IP security**
A set of protocols for encrypting, authenticating, and integrity checking packets at the level of IP streams. IPsec also includes protocols for cryptographic key establishment and is widely used in some implementations of Virtual Private Networking (VPN). IPsec operates at the network layer below that of other internet security systems (such as SSL), which can give extra flexibility with the trade off of more complexity. IPsec has two modes of operation: transport mode and tunnel mode. Transport mode is performed by each machine at the end of a connection, and only encrypts the payload of the IP packet, leaving the IP header as the plaintext so it can be routed (although not by using NAT, which re-writes part of the packet, causing it to fail integrity checking). In tunnel mode, the entire packet is encrypted and then encapsulated into a new IP packet to allow routing to function - using the method, secure traffic flow between two LANs can be provided by two nodes, one in each LAN.

**ISDN - Integrated Services Digital Network**
A digital network technology using ordinary telephone wires. ISDN is capable of delivering multiple channels of data, voice, video or fax over a single physical line. Channels on ISDN are either B (for bearer, usually 64Kbps channels that most data is transmitted on) or D (for the channel used to transmit control signals). Different ISDN services can provide varying numbers of channels from a basic two B and one D, up to services with 30 B channels. In much of the world, ISDN has been supplanted by DSL.

**J2EE - Java 2 Platform, Enterprise Edition**
A programming platform for developing and running distributed multi-tier architecture applications based largely on modular components running on an application server.

**LAMP**
An acronym for a set of free software programs commonly used together to run dynamic web sites:
- **Linux** - the operating system.
- **Apache** - the web server.
- **MySQL** - the database management system (or database server); Perl, PHP and Python scripting languages.

**LAN - Local Area Network**
Networks based on a small physical area such as a residence, building or college campus. They tend to consist of fast connections between systems (Gigabit Ethernet and Wi-Fi are common) and don’t involve a paid network connection to the internet as part of their structure, although one may be used to connect the LAN to the rest of the world.

**LDAP - Lightweight Directory Access Protocol**
A protocol for accessing information in and writing information to an LDAP directory. The directory itself is a database designed for very fast consistent reads used for relatively static information like user data, passwords, security keys, customer data, etc. LDAP clients connect to an LDAP server and send requests, generally a client can send multiple requests to the server and does not need to wait for responses in between and the LDAP server can return responses in any order.
GLOSSARY OF TERMS

Latency
Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. In some environments (for example, AT&T) latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the latency.

Layer - Open Systems Interconnection Model (OSI Model)
7. Application Layer
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data-Link Layer
1. Physical layer
Some services do not fit neatly into the model, MPLS for example is somewhere between layers 2 and 3.

Load Balancing
Distributing data across a network of servers in order to ensure that a single web server does not get overloaded with work, thereby affecting performance.

Managed Backup
Refers to the copying of data for the purpose of having an additional copy of an original source, specifically storing data on separate tape media not located on the server. If the original data is damaged or lost, the data may be copied from that source.

Managed Services
A Managed Services Provider will typically own and maintain the servers and will normally look after the entire environment including, in some cases your applications. They will effectively become your IT team.

Name Server
A server responsible for translating domain names and IP addresses.

Modem
A device that encodes (by modulation of a carrier signal) digital data for transmission over an analogue phone connection and decodes a received analogue signal back into a digital stream. Modems are best known for connecting two computers over the telephone system, but different forms of modems using other analogue transmission mediums (such as radio) exist.

MPLS - Multiprotocol Label Switching
A standards-approved technology for a speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the - Asynchronous Transport Mode, and frame relay network protocols. With reference to the standard OSI model for a network, MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS).
GLOSSARY OF TERMS

MPPE - Microsoft Point-to-Point Encryption
A protocol used to encrypt PPP and VPN connections. MPPE uses RSA's RC4 encryption using up to 128-bit session keys. Session keys are changed frequently for extra security, but due to keys being derived from information originally sent as plaintext MPPE is not a particularly robust encryption.

Multicast
IP Multicast is the process of sending a packet to multiple machines on a network. Multicast only requires the source to send a packet once, no matter the number of receivers; the nodes within a network replicate the packet as many times as needed. Movement and replication of the packet within the network to the correct hosts depends on the source sending to a group address and having multiple receivers who have already announced to the network that they are part of that group. Nodes within the network (knowing who has joined the multicast group) can then intelligently forward the packet on, replicating it only when needed.

Multi-Mode Fibre
Optical fibre that is designed to carry multiple light rays or modes concurrently, each at a slightly different reflection angle within the optical fibre core. Multimode fibre transmission is used for relatively short distances because the modes tend to disperse over longer lengths.

Multiplexer (MUX)
A device that sends multiple signals on a carrier channel at the same time in a form of a single complex signal to another device that recovers the separate signals at the receiving end. The receiver is sometimes called a demux (or “Demux”).

Multiplexing
Sending multiple signals or streams of information on a carrier at the same time in the form of a single complex signal and then recovering the separate signals at the receiving end.

NAS - Network Access Server
A point of access to a network that guards access to that network. The NAS takes credentials from a client wishing to connect to the network, passes them to an authentication service of some kind and then grants or denies the client access depending on the response from the authentication service. To perform as a NAS, a server does not require information about which clients are allowed to access, although the authentication service used by the NAS may run on the same physical device. All the NAS must be able to do is prevent or allow a client access to the resources behind it.

NAT - Network Address Translation
A method used to allow a single public IP address to represent an entire private subnet, and to run public servers with private non-routable addresses.
GLOSSARY OF TERMS

NIC - Network Interface Card or Controller
The hardware that allows a computer to connect to a network. It may consist of a card that plugs into a computer motherboard, it could connect via a USB port, or it could be integrated into the motherboard itself. It provides the physical connection that allows the computer to talk to the rest of the network. Most common is a connection to a TCP/IP network that may use cat5, wireless, or coax connections. NICs exist for other network types, including token ring and optical fibre.

NNI - Network to Network Interface
An interface that specifies signalling and management functions between two networks. An NNI circuit can be used for interconnection of signalling, Internet Protocol, or ATM networks.

NOC - Network Operations Centre
Usually where most of a company’s administration, technical support and physical storage takes place.

NSS - Name Server Switch
A part of many Unix and related systems that defines how lookups for information relating to the environment of the machine are made.

NTP - Network Time Protocol
A protocol designed to allow computers on a network to synchronize their clocks, and taking into account the variable latency on a packet switched network. By using NTP it’s possible for all computers on a network (like the internet) to have clocks synchronized to within hundredths of a second.

On-demand software
Software applications provided through networks such as the internet or as network based services. On demand software delivery for local installation use is sometimes referred to as software-on-demand.

OSA - Optical Spectrum Access
A highly flexible and cost-effective way of moving very large amounts of data between two locations. Provided over dedicated optical fibre links. It offers secure, always-on point-to-point connections using dense wavelength division multiplexing (DWDM) technology.

Packet
A formatted unit of data carried by a packet-switched network. Packets consist of two kinds of data: control information and user data (also known as payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically control informations found in packet headers and trailers, with payload data in between.

Packet Filtering
Filtering by the attributes of a packet entering a device or network. Attributes may include the service or destination address for the device, the port, connection type, elements of the data payload, or any other number of detectable attributes of the packet.
GLOSSARY OF TERMS

Packet Switching
A packet switched network breaks information to be transmitted into discrete packets, each of which is sent over a shared network used by multiple machines or users. Each individual packet contains information pertaining to its source and destination, and does not require a dedicated path to reach its destination. Of course, packets may travel between the same source and destination using different paths. Multiple users may transmit packets over the same connection at the same time, independently of one another.

PBX - Private Branch eXchange
Originally a private telephone exchange that handled a business's own internal telephone requirements so that an entire building's internal phone calls wouldn't need to use the costly public phone network. A PBX is any system that handles in-house telephony, from manual exchanges to VOIP systems that route telephony over IP networks.

PDU - Power Distribution Unit
A power distribution unit (PDU) or mains distribution unit (MDU) is a device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment located within a data centre.

PKI - Public Key Infrastructure
A system that handles the work of creating public-key certificates containing identities tied to public keys and signed by a certificate authority (CA). The PKI can publish the public-key certificates to those who wish to communicate with the key's owners, and verify that a certificate containing some public key and identity is genuine, so that the public key can be trusted to belong to the owner described.

Platform as a Service (PaaS)
A variation of SaaS (Software-as-a-Service) delivering integrated development as a turnkey service.

PoP - Point of Presence
An artificial demarcation point or interface point between communicating entities. It may include a meet-me-room. It is a physical location that houses servers, routers and switches. It may be either part of the facilities of a telecommunications provider that the Internet Service Provider (ISP) rents or a location separate from the telecommunications provider. ISPs typically have multiple PoPs, which are also located at the Internet exchange points and colocation data centres.

PPP - Point-to-Point Protocol
Used to provide a layer 2 (data link) between two nodes over a serial modem connection to allow TCP/IP to function and give a computer internet access. Defined within PPPs specification is Link Control Protocol (LCP), which automatically configures the interfaces at each end of the PPP connection.

PPTP - Point-to-Point Tunnelling Protocol
A protocol used to create VPN over an IP based network such as the Internet. Network protocols on the original networks are sent over a regular PPP session using a Generic Routing Encapsulation (GRE) tunnel.
GLOSSARY OF TERMS

PUE - Power Usage Effectiveness
The measure of how efficiently a computer data centre uses energy; specifically, how much energy is used by the computing equipment (in contrast to cooling and other overheads). PUE is the ratio of total amount of energy used by a computer data centre facility to the energy delivered to computing equipment.

QoS - Quality of Service
Any system whereby packets moving around a network are handled in different ways according to their importance and need. Applications sending and receiving data don’t all require the same performance from the network; VOIP may have strict requirements for low delay, high quality video may need consistent high throughput.

Rack Unit - U
Racks are divided into regions, 1.75 inches (44.45 mm) in height, within which there are three complete hole pairs in a vertically symmetric pattern with the holes being centred 0.25 inches (6.35 mm), 0.875 inches (22.23 mm), and 1.5 inches (38.10 mm) from the top or bottom of the region. Such a region is commonly known as a U for “unit”, and heights within racks are measured by this unit. Rack-mountable equipment is usually designed to occupy some integer number of U. Rack-mountable computers are mostly between 1U and 4U high. A blade server enclosure might require 10U.

RAID - Redundant Array of Independent Disks
A method of data protection and backup. Data is stored over a number of servers so that information will still be accessible if a piece of hardware or software crashes.

Resilience
The ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation. Threats and challenges for services can range from simple misconfiguration over large scale natural disasters to targeted attacks. As such, network resilience touches a very wide range of topics. In order to increase the resilience of a given communication network, the probable challenges and risks have to be identified and appropriate resilience metrics have to be defined for the service to be protected.

RIP - Routing Information Protocol
A method by which routers within a network are able to adapt changing network conditions (such as a downed router or suddenly congested links) by communicating to other routers. About every 30 seconds a RIP-enabled router multi-casts its routing table to any other connected routers, and can be triggered to do the same on certain events for quicker response to sudden changes.

ROADM - Reconfigurable Optical Add-Drop Multiplexer
A device that can add, block, pass or redirect modulated infrared (IR) and visible light beams of various wavelengths in a fibre optic network. ROADMs are used in systems that employ wavelength division multiplexing.
GLOSSARY OF TERMS

Routing
IP Routing is the process of path selection for packets travelling through an IP-based network. Compared to bridging, which automatically discovers the route that network traffic takes between multiple network segments and does so via OSI Layer 2 (the data link layer), routing relies upon a coordinated OSI Layer 3 (network layer) network, and uses the IP addresses of packets to decide where to forward them. Routing is usually controlled by pre-constructed routing tables that define where a packet should go. Each router only needs to know where a packet should be sent on its next hop and doesn’t know or care what happens afterward; the next hop plus one is the responsibility of the next router, and so on through the network until a packet reaches its destination.

SAN - Short for Storage Area Network
A network designed to attach computer storage devices such as disk array controllers and tape libraries to servers. In a storage network a server issues a request for specific blocks or data segments, from specific disk drives. This method is known as “block storage”. The device acts in a similar fashion to an internal drive, accessing the specified block ad sending the response across the network.

Scalability
The ability to adapt to rapid changes in demand by dynamically adding or removing resources based upon changes to requirements.

Server Stack/Solution Stack
A set of software subsystems or components needed to create a complete platform such that no additional software is needed to support applications. Applications are said to “run on” or “run on top of” the resulting platform.

SFP - Small Form-Factor Pluggable
A compact, hot-pluggable transceiver used for both telecommunication and data communications applications. It interfaces a network device motherboard (for a switch, router, media converter or similar device) to a fibre optic or copper networking cable. It is a popular industry format jointly developed and supported by many network component vendors. SFP transceivers are designed to support SONET, gigabit Ethernet, Fibre Channel, and other communications standards.

Single Mode Fibre
Optical fibre that is designed for the transmission of a single ray or mode of light as a carrier and is used for long-distance signal transmission. For short distances multi-mode is used. Single mode fibre has a much smaller core than multi-mode fibre.

SIP - Session Initiation Protocol
A popular VOIP protocol. Commercial VOIP providers like Vonage use SIP. SIP is not a multimedia protocol itself but rather carries any type of audio or video stream, it creates, modifies and terminates sessions between at least two endpoints.
GLOSSARY OF TERMS

SLA - Service Level Agreement
A formal agreement that defines the level of service to be expected from a provider of those services. The SLA itself defines the basis of understanding between the two parties for delivery of the service itself. The document can be quite complex and sometimes underpins a formal contract. Generally and SLA should contain clauses that define a specified level of service, support options, incentive awards for service levels exceeded and penalty provisions for services not provided.

SOHO - Small Office / Home Office
A term applying to a small business with up to about 10 users. Computing equipment labelled SOHO may be designed with some features typically for business use, but not necessarily capable of handling the requirements of large organisations with hundreds of users.

SaaS - Software-as-a-Service
Provisioning of software and applications over the public internet or private networks on a shared basis. SaaS applications typically provide equivalent functionality to dedicated single-purchase applications, however they are delivered and used on a month-by-month service contract or subscription basis. Some components may be required to operate locally.

SQL - Standard Query Language
A standard protocol used to request information from databases. Servers that can handle SQL are known as SQL servers.

SSH - Secure Shell
A protocol that allow the opening of a secure encrypted channel between two computers with secure authentication. SSH is most often used to provide a secure shell to log in to a remote machine, but also supports file transfers, TCP, and X11 tunnelling.

SSL - Secure Sockets Layer
A protocol developed by Netscape to handle and protect confidential / sensitive information required for e-commerce transactions like credit card numbers. SSL addresses usually begin with “https”.

State
Filtering on the known state of a packet, identified by previous network activity. For example, a machine behind a firewall may request a web page from a web server. The web server then sends a response back, and the firewall allows the response because it knows a machine requested information from that server. The same response from the web server would be denied if there had been no original request passing through the firewall. It’s state was derived by the firewall through previous activity between the two hosts.

Static Address
A “Static Address” is one meant to be matched to a particular computer so that it always has the same address. This is necessary when you have a server on a network, and must know a permanent IP address in order to use it.
GLOSSARY OF TERMS

Subnet
In the context of an IP-based network, a subnet is a group of related IP addresses all beginning with the same binary network part and ending in a unique binary sequence identifying the host within the subnet. An example might be the IP address 192.168.100.12 with subnet mask of 255.255.255.0. The first 24 bits of the address, shown by bits in the subnet mask, reveal which part is the network address (192.168.100.0) with the last 8 bits corresponding to the host (12 in the example). The entire subnet thus spans the address range 192.168.100.0 to 192.168.100.255. Dividing a network into subnets in this hierarchical fashion keeps the routing easy, as the IP address within a subnet can all be derived from the network address.

Switch
Switches take note of the address of connected computers in order to send data only to the correct machine. For example, a packet arrives in a port on a switch, and is destined for one particular machine connected via another port. The switch has previously paid attention to which machines are connected to which port and forwards the packet out only to the correct machine. An unmanaged switch can be configured for various network fine tuning such as limiting speed on certain ports, QoS, SNMP reporting and control, link aggregation and so on.

SYN/ACK - Synchronization/Acknowledgement
Part of opening a new TCP connection. When a client wishes to connect to a server on the internet, it first sends a SYN packet to the server. The server responds back with a SYN-ACK (an acknowledgement) and the client returns a SYN-ACK-ACK (a return acknowledgement). Both acknowledgements together indicate that the server can talk to the client, the client can talk to the server, and a TCP connection is now open for use between the two hosts.

Tier System
There are a number of international bodies that award tier ratings for facilities based on resilience, security, redundancy of infrastructure, and data security. Most credible data centres claim to, and are expected to have sufficient infrastructure to allow them to remove any single element of their power or cooling equipment and still be fully operational. Coupled with robust security controls and procedures, these would qualify a data centre to claim to operate to “tier 3” standard.

TCP - Transmission Control Protocol
Allows applications to create connections that, once established, the applications can stream data across. TCP stacks in an operating system to the hard work of splitting the stream of data into segments with a sequence number and sending them out over an IP-based network. At the remote end, the TCP stack acknowledges packets that have been received (so that missing packets can be resent) and reassembles received packets in the correct order to provide an in-order data stream to the remote application.
GLOSSARY OF TERMS

VLAN - Virtual Local Area Network
A logically separate IP sub-network which allows multiple IP networks and subnets to exist on the same switched network. VLAN is a logical broadcast domain that can span multiple physical LAN segments. It is a way administrators configure switches into virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones.

VNC - Virtual Network Computing
A remote display system where by a user can view or control the desktop environment of a remote computer that may be across the room, or on the other side of the world over the internet. When controlling, communication goes both ways - keyboard and mouse events are sent from the viewer (the client) to the remote machine and the remote server provides updates of the screen display back to the client. A user may connect to a server, use its desktop for a time, then disconnect and move to another location. Upon reconnecting to the server, the user will see the exact desktop, down to the mouse pointer being in the same place.

VPN - Virtual Private Network
A private communications network usually used within a company or by several companies to communicate over a public network.

WAN - Wide Area Network
A network that spans a large geographic area relative to a LAN. It will likely contain a paid network connection by a telecommunications provider. A school campus may consider it’s entire on-campus network to be a LAN (even if that supplies hundreds of buildings on the one site) and the connection to other campuses in different cities to be part of the WAN. The internet can be considered the largest of all WANs.

WAP - Wireless Access Point
The device that connects a wired LAN to a wireless network and acts to move data between wireless devices and the wired LAN, or directly to the internet. The WAP contains the antenna that transmits/receives wireless signals to/from any wireless-connected devices such as laptops, and is the device that implements the encryption required for good wireless security.

Wi-Fi
Refers to the standards (the 802.11 family) that define wireless networking most commonly used on LANs. While IEEE formally defines the 802.11 standards, testing and certification of products following the standard is performed by the Wi-Fi alliance, and industry group formed to push the adoption of standard wireless networking. Only products tested by the Wi-Fi alliance may carry the Wi-Fi trademark. Wi-Fi certification is a moving target that involves not just the wireless connection itself, but relevant technologies such as encryption, QoS, and power saving. As new wireless developments are ratified, the requirements for Wi-Fi certification change too. One example is security; WPA2 certifications compulsory in order to obtain certification as of 2006.
GLOSSARY OF TERMS

Web Hosting
A service that allows users to post web pages to the internet. A web-host, or hosting service provider (HSP), is a business that provides the technologies and services needed for websites to be viewed on the web.

WPA/WPA2 - Wi-Fi Protected Access
Encryption schemes used to secure wireless networks. There are two types of WPA; WPA and WPA2. WPA is an upgrade of WEP; both use RC4 stream encryption. It was designed to be a transitional protocol between WEP and WPA2. WPA is stronger than WEP but not as strong as WPA2. WPA2 uses a stronger encryption protocol called Counter Mode with CBC-MAC Protocol (CCMP), which is based on Advanced Encryption Standards (AES).

XML
Short for Extensible Mark-up Language. XML is a language allowing developers to create their own mark-up tags. All XML tags are defined by the programmer and can be interpreted differently in different applications. For example, the <i> tag in HTML means italics but could mean anything in XML, depending on the function the developer assigns to it.