Glossary

0 - 9

802.11. While 802.11 is a wireless protocol in its own right, 802.11 is often used to refer to a family of wireless networking protocols used mainly for local area networking. Three popular variants include 802.11b, 802.11g, and 802.11a. See also ***Wi-Fi.***

95th percentile. A billing method used by calculating the highest traffic rate for a given period, discarding the highest 5%. Compare with ***flat rate*** and ***actual usage***.

A

ACCEPT. The netfilter target that permits packets to pass. Packet matching stops immediately once the ACCEPT target is met. Compare with ***DROP***, ***LOG***, and ***REJECT***.

Acceptable Use Policy see ***AUP.***

ACL (***Access Control List***). A set of rules that must be matched before access is granted to a system. IP addresses, user names, and port numbers are frequently used in ACLs.

ACL elements. In Squid, ACL elements define a list of attributes (such as source IP, MAC address, user name, or browser type) to be later matched by rules. Together, elements and rules define the resources that are permitted by the Squid cache.

ACL rules. In Squid, ACL rules take some action (usually to permit or deny access) by comparing the request with various ACL elements.

actual usage. A billing method used by calculating the total number of bytes transferred in a given time period (usually one month). Compare with ***flat rate*** and ***95th percentile***.

Address Resolution Protocol see ***ARP.***

address space. A group of IP addresses that all reside within the same logical subnet.

ADSL (***Asymmetric Digital Subscriber Line***) see ***DSL***.

advertised window. The portion of a TCP header that specifies how many additional bytes of data the receiver is prepared to accept.

adzapper. A Squid redirector that intercepts advertisements and replaces them with smaller static graphic files. Available from *http://adzapper.sourceforge.net/.*

ALTQ (***Alternate Queuing***). ALTQ is a packet scheduler used to shape network traffic on BSD systems.

Analog (*http://www.analog.cx/*). A popular web and cache server log reporting tool.

AND logic. A logical operation that only evaluates as true if all of the items being compared also evaluate as true. See also ***OR logic***.

Application firewalls. A special kind of network firewall that can approve or deny traffic based on a high level analysis of the application protocol being used. For example, a web application firewall can inspect the contents of HTTP packets to determine whether a particular connection should be permitted.

Application Layer. The topmost layer in the OSI and TCP/IP network models, where applications can exchange data without regard for underlying network layers.

Argus. An open source network monitoring tool used for tracking flows between hosts. Argus is short for ***Audit Record Generation and Utilization System***. Available from *http://www.qosient.com/argus* .

ARP (***Address Resolution Protocol***). ARP is a protocol widely used on Ethernet networks to translate IP addresses into MAC addresses.

ARQ (***Automatic Repeat Request***). ARQ provides radio link layer error recovery on HF networks by managing retransmission requests.

Asymmetric Digital Subscriber Line (***ADSL***) see ***DSL***.

AT command set. A common set of commands used by modems to select operating parameters and control a data connection. Originally developed by the Hayes corporation in the early 1980s.

Audit Record Generation and Utilization System see ***Argus.***

AUP (***Acceptable Use Policy***). A formal set of rules that defines how a network connection may be used. ISPs often provide service contingent upon adherence to an AUP.

authenticating cache servers. A caching web proxy that requires credentials (such as a user name and password) is an authenticating cache server. Authentication enables the ability to implement quotas, billing,

and other services based on the usage patterns of individuals.

automatic proxy configuration. A technique used to automatically configure web browsers to detect and make use of a web proxy.

Automatic Repeat Request see ***ARQ.***

AWStats. A popular web and cache server log reporting tool available from *http://awstats.sourceforge.net/*

B

bands. A queue used for prioritised delivery of network traffic. In the QoS implementation in Linux, a packet's TOS bits determine the band that is used for delivery. See also ***PRIO***, ***QoS***, and ***TOS***.

Bandwidth. A measure of frequency ranges, typically used for digital communications. The word bandwidth is also commonly used interchangeably with ***capacity*** to refer to the theoretical maximum data rate of a digital communications line.

benchmarking. Testing the maximum performance of a service or device. Benchmarking a network connection typically involves flooding the link with traffic and measuring the actual observed throughput, both on transmit and receive.

Berkeley Internet Name Domain see ***BIND***.

BGAN (***Broadband Global Access Network***). One of several standards used for satellite Internet access. See also ***DVB-S*** and ***VSAT***.

BIND (***Berkeley Internet Name Domain***). BIND is probably the most common implementation of DNS used on the Internet. It is published by the Internet Systems Consortium, and is available from *http://www.isc.org/sw/bind/.*

bits per second see ***bps***.

Bonding. A method used for combining the throughput of two or more network connections.

bps (***bits per second***). A measure of capacity of a digital communications line. Often, bps is used in conjunction with the common prefixes K (kilo), M (mega), or G (giga). For example, a T1 line may be said to provide a 1.544 Mbps connection.

branch node. When using HTB, a branch node refers to a class that contains other child nodes. See also ***leaf node***.

bridge. A network device that connects two networks together at the Data Link layer. Bridges do not route packets at the Network Layer. They simply repeat packets between two link-local networks. See also ***router*** and ***transparent bridging firewall***.

Broadband Global Access Network see ***BGAN***.

broadcast address. On IP networks, the broadcast IP address is used to send data to all hosts in the

local subnet. On Ethernet networks, the broadcast MAC address is used to send data to all machines in the same collision domain.

BSD Compression (***bsdcomp***). A common data compression algorithm used for compressing PPP headers. See also ***deflate*** and ***VJ***.

burst. To temporarily use a data rate above the agreed rate. In VSAT systems using shared bandwidth, bursting allows for a temporary increase in the maximum available throughput by "borrowing" from customers whose lines are idle.

by-the-bit see ***actual usage***.

C

Cable modem. A device that implements DOCSIS, allowing two-way network communications over consumer cable television lines.

Cache. A local copy of data that takes a long time to compute or retrieve. Network operations can be sped up by keeping a local cache of network data, such as web pages or DNS requests, and serving the local copy on subsequent requests.

cache digests. A very compact summary of the objects available in a cache. By using cache digests, inter-cache communications can be significantly reduced, increasing performance.

cachemgr. A command-line diagnostic interface that displays the status of a running Squid cache.

caching web proxy. A server that makes web requests on behalf of clients, and saves a local copy of the retrieved data to increase performance and decrease Internet utilisation.

Cacti (*http://www.cacti.net/*). A popular web-based monitoring tool written in PHP.

Calamaris. A very powerful web cache log analyser. Available from *http://cord.de/tools/squid/calamaris*

capacity. The theoretical maximum amount of traffic provided by a digital communications line. Often used interchangeably with ***bandwidth***.

captive portal. A mechanism used to transparently redirect web browsers to a new location. Captive portals are often used for authentication or for interrupting a user's online session (for example, to display an AUP).

CBQ (***Class Based Queueing***). A very popular and complex queuing discipline used for traffic shaping.

chains. One of the many phases of packet evaluation used by the Linux netfilter firewall system. Chains contain rules that determine the fate of every packet passing through the system. See also ***netfilter***, ***rules***, and ***tables***.

CIDR (***Classless Inter-Domain Routing***). CIDR was developed to

improve routing efficiency on the Internet backbone by enabling route aggregation and network masks of arbitrary size. CIDR replaces the old class-based addressing scheme. See also ***Class A, B, and C networks***.

CIDR notation. A method used to define a network mask by specifying the number of bits present. For example, the netmask 255.255.255.0 can be specified as /24 in CIDR notation.

Class A, B, and C networks. For some time, IP address space was allocated in blocks of three different sizes. These were Class A (about 16 million addresses), Class B (about 65 thousand addresses), and Class C (255 addresses). While CIDR has replaced class-based allocation, these classes are often still referred to and used internally in organisations using private address space. See also ***CIDR***.

Class Based Queueing see ***CBQ***.

Classless Inter-Domain Routing see ***CIDR***.

collision. On an Ethernet network, a collision occurs when two devices connected to the same physical segment attempt to transmit at the same time. When collisions are detected, devices delay retransmission for a brief, randomly selected period.

colocation facility (***colo***). A service that provides hosting close to the Internet backbone. This may be provided as virtual space on a shared server, or as physical room for server equipment. ISPs often offer colo services to their customers.

connectionless. A network protocol (such as UDP) that requires no session initiation or maintenance. Connectionless protocols typically require less overhead than session oriented protocols, but do not usually offer data protection or packet reassembly. See also ***session oriented***.

connection tracking see ***stateful inspection***.

content filtering. Selectively allowing information to flow through a network based on the actual contents of the data. This may include virus scanners, spam filters, advertising blockers, or web proxy filters.

contention ratio. The ratio of customers to the available bandwidth. If an ISP provides a 1 megabit service and sells access to twenty customers, the contention ratio is 20:1.

cron job. A Unix facility that allows timed and repeated execution of programs.

curl (*http://curl.haxx.se/*). A command line tool for downloading web pages.

D

DansGuardian . A Squid redirector that provides web content filtering. Available at *http://dansguardian.org/*

Data Link Layer. The second layer in both the OSI and TCP/IP network models. Communications at this layer happen directly between nodes. On Ethernet networks, this is also sometimes called the MAC layer.

Data Over Cable Service Interface Specification see ***DOCSIS***.

default gateway. When a router receives a packet destined for a network for which it has no explicit route, the packet is forwarded to the default gateway. The default gateway then repeats the process, possibly sending the packet to its own default gateway, until the packet reaches its ultimate destination.

default route. A network route that points to the default gateway.

deflate. A compression algorithm used by PPP to reduce the size of packet headers. See also ***bsdcomp*** and ***VJ***.

delay pools. A packet shaping method used by Squid to prioritise data delivery.

Denial of Service see ***DoS***.

deny by default. A firewall policy that only allows traffic that is explicitly permitted. This is widely considered to be more secure than filtering only undesirable traffic.

DHCP (***Dynamic Host Configuration Protocol***). A protocol used by hosts to automatically determine their IP address.

dial on demand. A network connection that is only made when required. Dial on demand is often used with dial-up connections.

Digital Subscriber Line see ***DSL***.

Digital Video Broadcast see ***DVB-S***.

DNS Black List see ***DNSBL***.

DNS caching. By installing a DNS server on your local LAN, DNS requests for an entire network may be cached locally, improving response times. This technique is called DNS caching.

DNSBL (***DNS Black List***). A spam prevention technique that rejects inbound mail based on the originating IP address.

Dnsmasq. An open source caching DNS and DHCP server, available from *http://thekelleys.org.uk/*

DOCSIS (***Data Over Cable Service Interface Specification***). DOCSIS is the protocol spoken on cable modem networks that provides two-way data communications.

DomainKeys. A spam fighting technique developed by Yahoo! designed to verify the authenticity of the sender, as well as the integrity of the message.

DoS (***Denial of Service***). An attack on network resources, usually achieved by flooding a network with traffic or exploiting a bug in an application or network protocol. When the source of these attacks is distributed across a large number of machines, it

is called a ***Distributed Denial of Service attack*** (***DDoS***).

download manager. A program that keeps track of downloaded files, often claiming to improve download speeds as well. Many download managers implement a peer-to-peer protocol to improve performance, which can cause significant impact on network utilisation. See also ***peer-to-peer***.

DROP. This netfilter target immediately discards the packet in question and stops any further processing. Compare with ***ACCEPT***, ***LOG***, and ***REJECT***.

DSL (***Digital Subscriber Line***). A family of related high speed network technologies implemented using standard telephone lines. The most common form is ADSL (Asymmetric Digital Subscriber Line), which provides faster download speeds than upload speeds. Another version is SDSL (Symmetric Digital Subscriber Line), which provides matching upload and download speeds, but usually at significantly greater cost. DSL can provide much greater capacity than dial-up, but has a limited installation range.

DSL modem. A device used to provide DSL service over traditional telephone lines.

DVB-S (***Digital Video Broadcast***). One of several standards used for satellite Internet access. See also ***BGAN*** and ***VSAT***.

Dynamic Host Configuration Protocol see ***DHCP***.

E

edge. The place where one organisation's network meets another. Edges are defined by the location of the external router, which often acts as a firewall.

equal cost routing. A technique used for aggregating network links in a round-robin fashion.

EtherApe. An open source network visualisation tool. Available at *http://etherape.sourceforge.net/*

Ethereal see ***Wireshark***.

EuroDOCSIS. The European version of the DOCSIS cable modem specification.

Exim (*http://www.exim.org/*). Exim is a popular email server (MTA) designed for flexibility and ease of administration.

external traffic. Network traffic that originates from, or is destined for, an IP address outside your internal network, such as Internet traffic.

F

far-side scrubbing. An optimisation technique where content filtering takes place at your ISP before it is sent across your Internet connection.

fibre optic see ***optical fibre***.

Fibre To The Home (***FTTH***) and ***Fibre To The Premises*** (***FTTP***). Very high speed Internet service provided via optical fibre. FTTH and FTTP are currently available in limited areas in only a few countries.

filter. The default table used in the Linux netfilter firewall system is the filter table. This table is used for determining traffic that should be accepted or denied.

firewall. A router that accepts or denies traffic based on some criteria. Firewalls are one basic tool used to protect entire networks from undesirable traffic. See also ***personal firewall***.

Flat rate billing. A billing method where a predetermined rate is charged for service, regardless of the amount of bandwidth used. Compare with ***95th percentile*** and ***actual usage***.

FLUFF. A distributed download system developed by the University of Bristol. More information is available at *http://www.bristol.ac.uk/fluff/*

flush. To remove all entries in a routing table or netfilter chain.

forwarding. When routers receive packets that are destined for a different host or network, they send the packet to the next router closest to its ultimate destination. This process is called forwarding.

forwarding loops. A routing misconfiguration where packets are forwarded cyclically between two or more routers. Catastrophic network failure is prevented by using the TTL value on every packet, but forwarding loops need to be resolved for proper network operations.

frame relay. A digital communications technology used for wide-area networks in cases where leased lines, DSL, or other wired network connections are impractical.

FTTH see ***Fibre To The Home***.

FTTP see ***Fibre To The Premises***.

G

Globally routable IP addresses. An address issued by an ISP or RIR that is reachable from any point on the Internet. In IPv4, there are approximately four billion possible IP addresses, although not all of these are globally routable.

greylists. A spam fighting technique where incoming emails are automatically deferred for a short amount of time. Greylists get their name from the combined use of whitelists and blacklists.

H

Hayes AT command set see ***AT command set***.

HF (***High-Frequency***). Radio waves from 3 to 30 MHz are referred to as

HF. Data networks can be built on HF that operate at very long range, but with very low data capacity.

Hierarchical Token Buckets see ***HTB***.

High-Frequency see ***HF***.

hop. Data that crosses one network connection. A web server may be several hops away from your local computer, as packets are forwarded from router to router, eventually reaching their ultimate destination.

HTB (***Hierarchical Token Buckets***). A class-based queuing discipline used for traffic shaping.

HTTrack (*http://www.httrack.com*). An open source offline browser utility used to make a local copy of websites.

hub. An Ethernet networking device that repeats received data on all connected ports. See also ***switch***.

I

IANA (***Internet Assigned Numbers Authority***). The organisation that administers various critical parts of Internet infrastructure, including IP address allocation, DNS root nameservers, and protocol service numbers.

ICMP (***Internet Control Message Protocol***). A Network Layer protocol used to inform nodes about the state of the network. ICMP is part of the Internet protocol suite. See also ***TCP/IP***.

ICP (***Internet Cache Protocol***). A high performance protocol used to communicate between web caches.

inbound traffic. Network packets that originate from outside the local network (typically the Internet) and are bound for a destination inside the local network. See also ***outbound traffic***.

infecting. The process where a network virus spreads from machine to machine. Viruses can sometimes be stopped by firewalls, and should be eliminated from your network using anti-virus software.

Integrated Services Digital Network see ***ISDN***.

interception caching see ***transparent caching***.

Internet Cache Protocol see ***ICP***.

Internet Control Message Protocol see ***ICMP***.

Internet Protocol see ***IP***.

Internet protocol suite. The family of communication protocols that make up the Internet. Some of these protocols include TCP, IP, ICMP, and UDP. Also called the ***TCP/IP protocol suite***, or simply ***TCP/IP***.

Intrusion Detection System (***IDS***). A program that watches network traffic, looking for suspicious data or behaviour patterns. An IDS may make a log entry, notify a network adminis-

trator, or take direct action in response to undesirable traffic.

IP (***Internet Protocol***). The most common network layer protocol in use. IP defines the hosts and networks that make up the global Internet.

IPF and ***IPFW***. Two of the three popular firewall implementations used in BSD. See also ***PF***.

iproute2. The advanced routing tools package for Linux, used for traffic shaping and other advanced techniques. Available from *http://linux-net.osdl.org/*

iptables. The primary command used to manipulate netfilter firewall rules.

ISDN (***Integrated Services Digital Network***). A network connection using digital signaling over the traditional telephone network.

ISM band. ISM is short for Industrial, Scientific, and Medical. The ISM band is a set of radio frequencies set aside by the ITU for unlicensed use.

Isoqlog. An open source MTA log processing and reporting tool. (*http://www.enderunix.org/isoqlog/*)

K

known good. In troubleshooting, a known good is any component that can be replaced to verify that its counterpart is in good, working condition.

L

l7-filter. An open source application layer firewall application. L7-filter can catch traffic based on the high level protocol being used, regardless of the source or destination port numbers used. This processing usually requires significant CPU resources. *http:///l7-filter.sourceforge.net/*

LAN (***Local Area Network***). A network (typically Ethernet) used within an organisation. The part of a network that exists just behind an ISP's router is generally considered to be part of the LAN. See also ***WAN***.

Latency. The amount of time it takes for a packet to cross a network connection. It is often (somewhat incorrectly) used interchangeably with Round Trip Time (RTT), since measuring the RTT of a wide-area connection is trivial compared to measuring the actual latency. See also ***RTT***.

leaf node. When using HTB, a leaf node refers to a class that contains no child nodes. See also ***branch node***.

lease time. In DHCP, IP addresses are assigned for a limited period of time, known as the lease time. After this time period expires, clients must request a new IP address from the DHCP server.

leased line. A dedicated physical connection between two locations, usually leased from the local telephone company.

link-local. Network devices that are connected to the same physical segment communicate with each other directly, and are said to be link-local. A link-local connection cannot cross a router boundary without using some kind of encapsulation, such as tunneling or a VPN.

listen. Programs that accept connections on a TCP port are said to listen on that port.

Local Area Network see ***LAN***.

LOG. This netfilter target writes the packet to the system log and continues processing rules. See also ***ACCEPT***, ***DROP***, and ***REJECT***.

Log analysis. Computer logs can be read by humans, but are often more useful when processed by a log analyser. These tools can distill a large number of events into aggregated reports and trends, and can notify a human immediately when emergency conditions occur.

long fat pipe. A network connection (such as VSAT) that has high capacity and high latency. In order to achieve the best possible performance, TCP/IP must be tuned to traffic on such links.

M

MAC (***Media Access Control***) ***layer***. See ***Data Link Layer***.

MAC table. A network switch must keep track of the MAC addresses used on each physical port, in order to efficiently distribute packets. This information is kept in a table called the MAC table.

Mail Delivery Agent see ***MDA***.

Mail Transfer Agent see ***MTA***.

Mail User Agent see ***MUA***.

malware. Software such as a virus or keylogger that performs undesirable actions on a computer, often without the user's knowledge. See also ***trojan horse***, ***virus***, and ***worm***.

managed. Networking hardware that provides an administrative interface, port counters, SNMP, or other interactive features is said to be managed.

masquerading. A form of Network Address Translation used by Linux routers.

master browser. On Windows networks, the master browser is the computer that keeps a list of all the computers, shares and printers that are available in **Network Neighborhood** or **My Network Places**.

match condition. In netfilter, a match condition specifies the criteria that determine the ultimate target for a given packet. Packets may be matched on MAC address, source or destination IP address, port number, data contents, or just about any other property.

MDA (***Mail Delivery Agent***). A program that delivers an email to a storage device (usually a hard disk on an email server). This may be implemented in the MTA itself, or using an external program such as procmail. See also ***MTA*** and ***MUA***.

Media Access Control see ***MAC***

message types. Rather that port numbers, ICMP traffic uses message types to define the type of information being sent. See also ***ICMP***.

Microsoft Windows Server Update Services see ***WSUS***.

milter. An email filter specification supported by Sendmail and Postfix.

Mirroring. Making a complete local copy of a web site or other online resource. Bandwidth can be saved by directing users to the local copy, rather than allowing them to access the original site directly.

modem. Short for modulator / demodulator, the term modem was once used to refer to any interface between a computer and an analog network connection (such as a telephone line). In recent years, it has come to represent any device that bridges a network to Ethernet.

monitor port. On a managed switch, one or more monitor ports may be defined that receive traffic sent to all of the other ports. This allows you to connect a traffic monitor server to the port to observe and analyse traffic patterns.

MRTG (***Multi Router Traffic Grapher***). An open source tool used for graphing traffic statistics. Available from *http:///oss.oetiker.ch/mrtg/*

MTA (***Mail Transfer Agent***). A program that transports email between networks. Servers run an MTA such as Sendmail or Postfix to accept mail for a domain. See also ***MDA*** and ***MUA***.

mtr (***My TraceRoute***). A network diagnostic tool used as an alternative to the traditional traceroute program. *http://www.bitwizard.nl/mtr/.* See also ***traceroute*** / ***tracert***.

MUA (***Mail User Agent***). A program that retrieves and displays email message. Thunderbird and Outlook are examples of MUAs. See also ***MDA*** and ***MTA***.

Multi Router Traffic Grapher see ***MRTG***.

My TraceRoute see ***mtr***.

N

Nagios (*http://nagios.org/*) A real-time monitoring tool that logs and notifies a system administrator about service and network outages.

NAT (***Network Address Translation***). NAT is a networking technology that allows many computers to share a single, globally routable IP address. While NAT can help to solve the problem of limited IP ad-

dress space, it creates a technical challenge for two-way services, such as Voice over IP.

nat. The table used in the Linux netfilter firewall system to configure Network Address Translation.

negative-cached. In addition to normal responses, network failures can also be cached for increased performance. Squid will cache failures (such as **404 Not Found** responses) to client requests to prevent redundant retrieval of nonexistent pages. Caching DNS servers will also cache negative responses (replies to nonexistent host names) for the amount of time defined in the domain's zone file.

NetBIOS. A session layer protocol used by Windows networking for file and printer sharing. See also ***SMB***.

netfilter. The packet filtering framework in modern Linux kernels is known as netfilter. It uses the iptables command to manipulate filter rules. *http://netfilter.org/*

netmask (***network mask***). A netmask is a 32-bit number that divides the 16 million available IP addresses into smaller chunks, called subnets. All IP networks use IP addresses in combination with netmasks to logically group hosts and networks.

NeTraMet. An open source network flow analysis tool available from *http://www.auckland.ac.nz/net/*

network address. The lowest IP number in a subnet. The network address is used in routing tables to specify the destination to be used when sending packets to a logical group of IP addresses.

Network Address Translation see ***NAT***.

network etiquette. Generally accepted guidelines of behaviour that are considered to be polite to other network users. Conserving bandwidth, making sure your computer is virus-free, and refraining from sending spam email are considered good network etiquette.

Network Layer. The third layer of the OSI and TCP/IP network models, where IP operates and Internet routing takes place.

network mask see ***netmask***.

ngrep. An open source network security utility used to find patterns in data flows. Available from *http://ngrep.sourceforge.net/*

nmap. An open source network security utility used to scan networks and hosts to probe available services. *http://insecure.org/nmap/*

Norton Personal Firewall. A commercial personal firewall program published by Symantec. See also ***firewall***, ***personal firewall***, and ***Zone Alarm***.

ntop. A network monitoring tool that provides extensive detail about connections and protocol use on a local area network. *http://www.ntop.org/*

O

open relay. An email server that accepts mail delivery to any domain when sent from any location is called an open relay. Spammers make extensive use of open relays to hide the origin of their traffic. See also ***spam***.

Optical fibre. Communication cables made from glass that provide very high bandwidth and very low latency across very long distances. See also ***FTTH***, ***FTTP***, and ***SDH***.

OR logic. A logical operation that evaluates as true if any of the items being compared also evaluate as true. See also ***AND logic***.

OSI network model. A popular model of network communications defined by the ISO/IEC 7498-1 standard. The OSI model consists of seven interdependent layers, from the physical through the application. See also ***TCP/IP network model***.

outbound traffic. Network packets that originate from the local network and are bound for a destination outside the local network (typically somewhere on the Internet). See also ***inbound traffic***.

P

pac see ***Proxy Auto Configuration (.pac) file***

Packet filter. A firewall that operates at the Internet layer by inspecting source and destination IP addresses, port numbers, and protocols. Packets are either permitted or discarded depending on the packet filter rules.

packets. On IP networks, messages sent between computers are broken into small pieces called packets. Each packet includes a source, destination, and other routing information that is used to route it to its ultimate destination. Packets are reassembled again at the remote end by TCP (or another protocol) before being passed to the application.

partition. A technique used by network hubs to limit the impact of computers that transmit excessively. Hubs will temporarily remove the abusive computer (partition it) from the rest of the network, and reconnect it again after some time. Excessive partitioning indicates the presence of an excessive bandwidth consumer, such as a peer-to-peer client or network virus.

peer-to-peer. Any of several popular programs (such as BitTorrent, Gnutella, KaZaA, or eDonkey2000) used for file sharing. A peer-to-peer program turns a user's computer into both a client and a server, where information is exchanged directly with everyone else who is also running the program. Peer-to-peer programs consume considerable bandwidth, both inbound and outbound. See also ***download manager***.

PEPsal. An open source performance enhancing proxy used for improving TCP performance on links

with different characteristics (such as VSAT and VPNs). Available from *http://sourceforge.net/projects/pepsal/*

personal firewall. An application used on client computers to provide a small measure of protection from network attacks.

PF. One of three firewall implementations used in BSD (along with IPF and IPFW). See also ***IPF*** and ***IPFW***.

pfifo_fast. The default queuing discipline used on Linux network interfaces. It defines three bands of priority that are used according to the Type Of Service (TOS) bits present in a given packet. See also ***qdisc***, ***QoS***, and ***TOS***.

Physical Layer. The lowest layer in both the OSI and TCP/IP network models. The physical layer is the actual medium used for communications, such as copper cable, optic fibre, or radio waves.

ping. A ubiquitous network diagnostic utility that uses ICMP echo request and reply messages to determine the round trip time to a network host. Ping can be used to determine the location of network problems by "pinging" computers in the path between the local machine and the ultimate destination.

Point-to-Point Protocol see ***PPP***.

policy. In netfilter, the policy is the default action to be taken when no other filtering rules apply. For example, the default policy for any chain may be set to ACCEPT or DROP.

port counters. Managed switches and routers provide statistics for each network port called port counters. These statistics may include inbound and outbound packet and byte counts, as well as errors and retransmissions.

Postfix (***http://www.postfix.org/***). A popular email server (MTA) designed as a more secure alternative to Sendmail.

PPP (***Point-to-Point Protocol***). A network protocol typically used on serial lines (such as a dial-up connection) to provide IP connectivity.

Presentation Layer. The sixth layer of the OSI networking model. This layer deals with data representation, such as MIME encoding or data compression.

PRIO. A queuing discipline used with Linux QoS to prioritise traffic according to Type Of Service (TOS) bits present in the packet. See also ***qdisc***, ***QoS***, and ***TOS***.

PRIQ (***Priority Queueing***). A queuing discipline used to implement QoS on BSD systems. See also ***CBQ***, ***qdisc***, and ***QoS***.

private address space. A set of reserved IP addresses outlined in RFC1918. Private address space is frequently used within an organisation, in conjunction with Network Address Translation (NAT). The reserved private address space ranges include 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. See also ***NAT***.

protocol analyser. A diagnostic program used to observe and disassemble network packets. Protocol analysers provide the greatest possible detail about individual packets.

protocol stack. A set of network protocols that provide interdependent layers of functionality. See also ***OSI network model*** and ***TCP/IP network model***.

Proxy Auto Configuration (.pac) file. A file used in conjunction with a web server to automatically provide proxy information to a web browser.

proxy server. A network server that makes requests on behalf of client computers. Requests may or may not be cached locally, and the server may require authentication credentials. The Squid web cache is one example of a proxy server.

public good. A resource that can be consumed by an individual in arbitrarily large amounts, irrespective of the contribution made by that individual to conserving or renewing that resource.

Q

qdisc (***queuing discipline***). An algorithm that controls when and how the interface is allowed to send packets. See also ***ALTQ***, ***CBQ***, ***HTB***, ***pfifo_fast***, ***PRIO***, and ***PRIQ***.

qmail (*http://www.qmail.org/*). A popular email server (MTA) designed for security and speed.

QoS (***Quality of Service***). QoS allows you to prioritise the delivery of traffic based on some criteria, such as the type of service or originating network. Since packets are already sent as quickly as possible, QoS techniques only help when a communications line approaches saturation. See also ***TOS***.

queuing discipline see ***qdisc***.

R

Really Simple Syndication see ***RSS***.

Realtime monitoring. A network monitoring tool that performs unattended monitoring over long periods, and notifies administrators immediately when problems arise.

Redirector. A feature of the Squid web proxy that allows an administrator to intercept a user's browser and redirect them to different web content. This feature is used to implement captive portals, bandwidth enforcement pages, advertisement blocking, etc.

regex (***Regular Expression***). A pattern matching language used to determine if a given string matches a particular pattern. Many programs use a form of regular expressions to match various kinds of input. For example, Squid can use regex matches to determine if a requested URL fits a particular pattern (such as your organisation's domain name).

Regional Internet Registrar see ***RIR***.

Regular Expression see ***regex***.

REJECT. The netfilter target that returns an ICMP error message on matched packets. This is considered more polite, but less secure, than using the DROP target. Packet matching stops immediately once the REJECT target is met. Compare with ***ACCEPT***, ***DROP***, and ***LOG***.

RFC (***Request For Comments***). RFCs are a numbered series of documents published by the Internet Society that document ideas and concepts related to Internet technologies. Not all RFCs are actual standards, but many are either approved explicitly by the IETF, or eventually become de facto standards. RFCs can be viewed online at *http://rfc.net/.*

RIR (***Regional Internet Registrar***). The 4 billion available IP addresses are administered by the IANA. The space has been divided into large subnets, which are delegated to one of the five regional Internet registries, each with authority over a large geographic area.

robot exclusion standard (***robots.txt***). A convention used to limit the impact of automatic web crawlers (spiders) on a web server. Well-behaved web page retrieval software will only visit pages permitted by the robots.txt file. This can significantly reduce the load on your web server and Internet connection.

Round Robin Database see ***RRD***.

Round Trip Time see ***RTT***.

router. A device that forwards packets between different networks. The process of forwarding packets to the next hop is called ***routing.***

routing table. A list of networks and IP addresses kept by a router to determine how packets should be forwarded. If a router receives a packet for a network that is not in the routing table, the router uses its default gateway. Routers operate at the Network Layer. See also ***bridge*** and ***default gateway***.

RRD (***Round Robin Database***). A database that stores information in a very compact way that does not expand over time. This is the data format used by RRDtool and other network monitoring tools.

RRDtool. A suite of tools that allow you to create and modify RRD databases, as well as generate useful graphs to present the data. RRDtool is used to keep track of time-series data (such as network bandwidth, machine room temperature, or server load average) and can display that data as an average over time. RRDtool is available from *http://oss.oetiker.ch/rrdtool/*

RSS (***Really Simple Syndication***). A format used for providing news feeds. Anything that can be broken down into discrete items (such as news stories, wiki posts, or blog entries) can be syndicated with RSS. Rather than using a web browser, users collect RSS feeds using an RSS browser.

rsync (*http://rsync.samba.org/*). An open source incremental file transfer utility used for maintaining mirrors.

RTT (***round trip time***). The amount of time it takes for a packet to be acknowledged from the remote end of a connection. Frequently confused with ***latency***.

rules. Entries used in netfilter chains to match, manipulate, and determine the ultimate fate of a packet. See also ***chains***, ***netfilter***, and ***tables***.

S

SACK (***Selective acknowledgment***). A mechanism used to overcome TCP inefficiencies on high latency networks, such as VSAT.

Sawmill. A commercial log processing and reporting tool. Available from *http://www.sawmill.net/*

SDH (***Synchronous Digital Hierarchy***). A popular Data Link Layer protocol used on fibre optic networks.

SDSL (***Symmetric Digital Subscriber Line***) see ***DSL***.

Selective acknowledgment see ***SACK***.

Sender Policy Framework see ***SPF***.

Sendmail. The oldest open source email server still in wide use. Available from *http://www.sendmail.org/*

Server Message Block see ***SMB***.

Service Level Agreement see ***SLA***.

Session Layer. Layer five of the OSI model, the Session Layer manages logical connections between applications.

session oriented. A network protocol (such as TCP) that requires initialisation before data can be exchanged, as well as some clean-up after data exchange has completed. Session oriented protocols typically offer error correction and packet reassembly, while connectionless protocols do not. See also ***connectionless***.

SFQ (***Stochastic Fairness Queuing***). A fair queueing algorithm designed to require fewer calculations than other algorithms while being almost perfectly fair. Rather than allocate a separate queue for each session, it uses an algorithm that divides traffic over a limited number of queues using a hashing algorithm. This assignment is nearly random, hence the name "stochastic." See also ***ALTQ***, ***CBQ***, and ***HTB***.

Shorewall (*http://shorewall.net/*). A configuration tool used for setting up netfilter firewalls without the need to learn iptables syntax.

Simple Mail Transfer Protocol see ***SMTP***.

Simple Network Management Protocol see ***SNMP***.

site-wide web cache. While all modern web browsers provide a local

data cache, large organisations can improve efficiency by installing a site-wide web cache, such as Squid. A site-wide web cache keeps a copy of all requests made from within an organisation, and serves the local copy on subsequent requests. See also ***Squid***.

SLA (***Service Level Agreement***). A document that describes the precise level of network service that will be provided, including technical support, minimum uptime statistics, emergency contact procedures, and liability for unforeseen service outages. ISPs typically provide SLAs to customers at different rates depending on the level of service requested.

SMB (***Server Message Block***). A network protocol used in Windows networks to provide file sharing services. See also ***NetBIOS***.

SmokePing. A latency measurement tool that measures, stores and displays latency, latency distribution and packet loss all on a single graph. SmokePing is available from *http://oss.oetiker.ch/smokeping/*

SMTP (***Simple Mail Transfer Protocol***). The protocol used to exchange email between MTAs.

SNMP (***Simple Network Management Protocol***). A protocol designed to facilitate the exchange of management information between network devices. SNMP is typically used to poll network switches and routers to gather operating statistics.

Snort (*http://www.snort.org/*). A very popular open source intrusion detection system. See also ***IDS***.

SOCKS proxy. A generic application proxy server used for improving site security. There are many free and commercial SOCKS servers and clients available. Most web browsers have support for SOCKS proxies. See RFC1928.

spam. Unsolicited and undesirable communications, usually in the form of email messages, news group postings, or blog comments. Spam messages often include advertising or attempt to involve the recipient some kind of fraudulent activity. Spam wastes bandwidth, causes frustration in users, and the sending of it has been made illegal in many parts of the world.

spammers. People who engage in sending spam in an effort to attack, annoy, enrage, exploit, extort, swindle, or steal. Keep them out of your networks.

Speed. A generic term used to refer to the responsiveness of a network connection. A "high-speed" network should have low latency and more than enough capacity to carry the traffic of its users. See also ***bandwidth***, ***capacity***, and ***latency***.

SPF (***Sender Policy Framework***). A technique used to fight email forgery, which is often used in scam emails. SPF allows you to verify that mail apparently from a particular domain (say, a financial institution or government office) was sent from an authorised mail server. SPF verifies the

path that email took to arrive at your MTA, and can discard email that originated at unauthorised MTAs before the message is transmitted, thus saving bandwidth and reducing spam.

split horizon DNS. A technique used to serve different answers to DNS requests based on the source of the request. Split horizon is used to direct internal users to a different set of servers than Internet users.

Spot check tools. Network monitoring tools that are run only when needed to diagnose a problem. Ping and traceroute are examples of spot check tools.

Squid. A very popular open source web proxy cache. It is flexible, robust, full-featured, and scales to support networks of nearly any size. *http://www.squid-cache.org/*

Squidguard. A Squid redirector that provides web content filtering. *http://www.squidguard.org/*

stateful inspection. Firewall rules that are aware of the the state associated with a given packet. The state is not part of the packet as transmitted over the Internet, but is determined by the firewall itself. New, established, and related connections may all be taken into consideration when filtering packets. Stateful inspection is sometimes called connection tracking.

Stochastic Fairness Queueing see ***SFQ***.

subnet. An IP network that is broken down into smaller groups of hosts through the use of netmasks.

subnet mask see ***netmask***.

swarming. Another name for peer-to-peer activity. See ***peer-to-peer***.

switch. A network device that provides a temporary, dedicated connection between communicating devices. See also ***hub***.

Symmetric Digital Subscriber Line see ***DSL***.

Synchronous Digital Hierarchy see ***SDH***.

T

tables. Groups of netfilter chains that define the type of operation to be done (such as filter or nat). See also ***chains, netfilter***, and ***rules***.

target. In netfilter, the action to be taken once a packet matches a rule. Some possible netfilter targets include ***ACCEPT***, ***DROP***, ***LOG***, and ***REJECT***.

TBF (***Token Bucket Filter***). An algorithm used to throttle traffic to a particular rate. It is the algorithm used by delay pools in Squid, and can be used as a queuing discipline. See also ***ALTQ***, ***CBQ***, ***HTB***, ***pfifo_fast***, ***PRIO***, and ***PRIQ***.

TCP (***Transmission Control Protocol***). A session oriented protocol that operates at the Transport Layer, providing packet reassembly, congestion avoidance, and reliable delivery. TCP is an integral protocol used by many Internet applications, including HTTP and SMTP. See also ***UDP***.

TCP window size. The TCP parameter that defines how much data that may be sent before an ACK packet is returned from the receiving side. For instance, a window size of 3000 would mean that two packets of 1500 bytes each will be sent, after which the receiving end will either ACK the chunk or request retransmission.

TCP/IP. See ***Internet protocol suite***.

TCP/IP network model. A popular simplification of the OSI network model that is used with Internet networks. The TCP/IP model consists of five interdependent layers, from the physical through the application. See also ***OSI network model***.

tcpdump. A popular open source packet capture and analysis tool available at *http://www.tcpdump.org/.* See also ***WinDump*** and ***Wireshark***.

thrashing. Excessive hard disk use that occurs when a system has insufficient RAM, and must continually swap processes out to disk.

Throughput. The actual amount of information flowing through a network connection, disregarding protocol overhead.

Time To Live see ***TTL***.

Token Bucket Filter see ***TBF***.

TOS (***Type Of Service***). TOS bits may be assigned to a packet to determine QoS characteristics. The TOS bits determine whether a packet should be prioritised to minimise delay, maximise throughput, maximise reliability, minimise monetary cost, or some combination of these. Applications request the appropriate TOS bits when transmitting packets. See also ***QoS***.

traceroute / tracert. A ubiquitous network diagnostic utility often used in conjunction with ping to determine the location of network problems. The Unix version is called traceroute, while the Windows version is tracert. Both use ICMP echo requests with increasing TTL values to determine which routers are used to connect to a remote host, and also display latency statistics. Another variant is tracepath, which uses a similar technique with UDP packets. See also ***mtr***.

Transmission Control Protocol see ***TCP***.

transparent bridging firewall. A firewall technique that introduces a bridge that selectively forwards packets based on firewall rules. One benefit of a transparent bridging firewall is that it does not require an IP address. See also ***bridge***.

transparent cache. A method of implementing a site-wide web cache that requires no configuration on the web clients. Web requests are silently redirected to the cache, which makes the request on behalf of the

client. Transparent caches cannot use authentication, which makes it impossible to implement traffic accounting at the user level. See also ***site-wide web cache***, ***Squid***.

Transport Layer. The third layer of the OSI and TCP/IP network models, which provides a method of reaching a particular service on a given network node. Examples of protocols that operate at this layer are ***TCP*** and ***UDP***.

Trending. A type of network monitoring tool that performs unattended monitoring over long periods, and plots the results on a graph. Trending tools allow you to predict future behaviour of your network, which helps you plan for upgrades and changes.

trojan horse. A type of malware that claims to perform some useful function while secretly performing some other task (such as sending spam email or infecting a system with a virus). See also ***malware***, ***virus***, and ***worm***.

trunking. A feature of network switches that support VLAN tagging. A trunked connection can carry traffic from multiple VLANs on a single physical cable, and extend the reach of a VLAN to other network devices. See also ***VLAN***.

TTL (***Time To Live***). A TTL value acts as a deadline or emergency brake to signal a time when the data should be discarded. In TCP/IP networks, the TTL is a counter that starts at some value (such as 64) and is decremented at each router hop. If the TTL reaches zero, the packet is discarded. This mechanism helps reduce damage caused by routing loops. In DNS, the TTL defines the amount of time that a particular zone record should be kept before it must be refreshed. In Squid, the TTL defines how long a cached object may be kept before it must be again retrieved from the original website.

tunnel. A form of data encapsulation that wraps one protocol stack within another. This is often used in conjunction with encryption to protect communications from potential eavesdroppers, while eliminating the need to support encryption within the application itself. Tunnels are often used conjunction with VPNs. See also ***VPN***.

Type Of Service see ***TOS***.

U

UBE (***Unsolicited Bulk Email***). Another term for ***spam***.

UDP (***User Datagram Protocol***). A connectionless protocol that operates at the Transport Layer. UDP does not provide error correction or packet reassembly, but it requires less overhead than TCP connections. UDP is an integral protocol used by many Internet applications, including DNS, VoIP, streaming media, and gaming. See also ***TCP***.

Unsolicited Bulk Email see ***UBE***.

User Datagram Protocol see ***UDP***.

V

Van Jacobson see ***VJ***.

vector. A place where malware enters a computer or network. Vectors are security holes that should be fixed whenever they are found.

versionitis. The chaos that often ensues when multiple people attempt to make changes to the same document. Unless the changes are managed intelligently, the result may be several different copies of the same document, each with incompatible changes.

Very Small Aperture Terminal see ***VSAT***.

Virtual LAN see ***VLAN***.

Virtual Private Network see ***VPN***.

virus. A type of malware that exploits security holes to cause a computer to perform an undesirable task (such as sending spam email, deleting files, or infecting other systems). See also ***malware***, ***trojan horse***, and ***worm***.

VJ (***Van Jacobson***). A type of PPP header compression defined in RFC1144. See also ***bsdcomp*** and ***deflate***.

VLAN (***Virtual LAN***). A logical network that can coexist with, and be isolated from, other VLANs on the same physical medium. VLANs are normally implemented by network switching hardware, and so it makes no difference to a computer whether it is connected to a LAN or a VLAN. See also ***trunking***.

VoIP (***Voice over IP***). A technology that provides telephone-like features over an Internet connection. Examples of popular VoIP clients include Skype, Gizmo Project, MSN Messenger, and iChat.

VPN (***Virtual Private Network***). A tool used to join two networks together over an untrusted network (such as the Internet). VPNs are often used to connect remote users to an organisation's network when travelling or working from home. VPNs use a combination of encryption and tunneling to secure all network traffic, regardless of the application being used. See also ***tunnel***.

VSAT (***Very Small Aperture Terminal***). One of several standards used for satellite Internet access. VSAT is the most widely deployed satellite technology used in Africa. See also ***BGAN*** and ***DVB-S***.

W

WAN (***Wide Area Network***). Any long distance networking technology. Leased lines, frame relay, DSL, fixed wireless, and satellite all typically implement wide area networks. See also ***LAN***.

web application firewall. A firewall that understands HTTP data, and can make packet delivery decisions based on that data. For example, a web application firewall may refuse to

allow requests that post spam or virus data to a public forum.

Web Proxy Auto Discovery see ***WPAD***.

Webalizer. A popular open source web and cache server log reporting tool. *http://www.mrunix.net/webalizer/*

webmail. An MUA implemented as a web application. Hotmail, Gmail, and Yahoo! mail are examples of webmail applications. Webmail uses considerably more bandwidth than traditional email services.

wget. An open source command line tool for downloading web pages. *http://www.gnu.org/software/wget/*

Wi-Fi. A marketing brand owned by the Wi-Fi Alliance that is used to refer to various wireless networking technologies (including 802.11a, 802.11b, and 802.11g).

Wide Area Network see ***WAN***.

wiki. A web site that allows any user to edit the contents of any page. One of the most popular public wikis is *http://www.wikipedia.org/*

window scale. A TCP enhancement defined by RFC1323 that allows TCP window sizes larger than 64KB.

WinDump. The Windows version of tcpdump. It is available from *http://www.winpcap.org/windump/*

Wireless Fidelity see ***Wi-Fi***.

wireshark. A free network protocol analyser for Unix and Windows. *http://www.wireshark.org/*

worm. A type of malware similar to a virus that attempts to spread copies of itself to as many hosts as possible. Worms differ from viruses in that they do not contain an intentionally malicious payload, but their presence can consume bandwidth and cause other problems. See also ***malware***, ***trojan horse***, and ***virus***.

WPAD (***Web Proxy Auto Discovery***). A protocol that provides a number of methods for generating a URL that refers to a Proxy Auto Configuration file. See also ***Proxy Auto Configuration (.pac) file***.

WSUS (***Microsoft Windows Server Update Services***). A server used to replace the standard Microsoft update site. By directing clients to a local WSUS mirror, tremendous amounts of bandwidth can be saved as the clients automatically update their Windows components.

Z

ZoneAlarm. A commercial personal firewall program available from *http://www.zonelabs.com/*. See also ***Norton Personal Firewall***, ***personal firewall***.

Colophon

Lead copy editor: **Lisa Chan**, *http://www.cowinanorange.com/*
Supporting copy edit: **Kimberly Thomas**, kimthomas73@earthlink.net
Illustrations and cover: **Jessie Heaven Lotz**, *http://jessieheavenlotz.com/*
Technical review: **Roger Weeks** (*http://www.oreillynet.com/pub/au/1280*)
and **Richard Lotz** (*rlotz@seattlewireless.net*)

Produced by Hacker Friendly LLC, Seattle, WA, USA.
http://hackerfriendly.com/