

Glossary

ACMA: Australian Communications and Media Authority

ACMA blacklist: A list of web pages prohibited by ACMA. These URLs are typically reported to ACMA by ISPs for consideration for inclusion on the list.

Availability: This refers to the proportion of time which a device or service is actively doing its duty. For example, 99 percent availability means a service is active 99 percent of the time, with the remaining one percent being downtime due to unexpected faults or scheduled servicing.

Deep Packet Inspection (DPI): The analysis of every packet of data (traffic) passing a given point. DPI technology is not only used for content filtering but also to detect network attacks, malware and other security functions.

Download: This is the process of drawing data from the internet to a computer or other device.

eMetric: eMetric is a network performance toolset created by Enex TestLab that measures various broadband performance attributes and includes:

- Download & Upload Speed Measurement Test
- Web page download Test
- Latency Test

F-test: This is a statistical test used to determine if the difference between two sets of numbers is big enough to be considered important and not simply due to random chance. A result of 99 percent indicates that we are very sure that two sets of results are different enough to warrant paying attention to, but a result of 50 percent would suggest that the difference is equally likely to be caused by sheer chance. Typically, anything less than 90 percent surety is considered unworthy of special attention.

Failover: This is the capacity of a device or application to smoothly and automatically transfer control or data to another system in the event of failure.

Fail to wire: This refers to a device's ability to allow data to pass freely in the event that the device malfunctions and is unable to correctly process the incoming information. In the context of content filters, this would mean that failure of a filter would allow unfiltered internet access as opposed to simply cutting off all internet access.

Hybrid filter: (see Pass-by filter)

IP address: (Internet Protocol address) This kind of addressing takes the form of four numbers separated by dots (e.g.: 192.168.0.24). These numbers are the actual internet addresses of computers and servers connected to the internet or a local network and may include additional information defining a particular directory or file on the computer being addressed (e.g.: 202.101.7.23/directory/file.txt.). For convenience, a more human friendly *URL* is commonly used as an alias for such addresses.

ISP: Internet Service Provider

Latency: This is a delay resulting from the time taken for a request for information to be relayed to a data source and the time taken for the first portion of the requested data to travel back to the origin of request. Latency varies according to the number of steps in the path taken by the data and the total distance travelled.

Load generator: This is a device which simulates activity on a network. This allows testers to assess how a system will respond to different workloads in a real life situation.

Over-blocking: This refers to a situation where innocuous material, expected to be ignored by a content filter, is blocked from being accessed by internet users. For example a filter might block web-pages containing words which can have distasteful or obscene meanings in another context.

Pass-by filter: A pass-by filter does not require all traffic to pass through the filter. Pass-by filters comprise two types: hybrid and port mirroring. Only hybrid pass-by technology was used in this trial.

Hybrid pass-by filters consist of two-stages. The most common first stage populates routers with IP addresses relating to the URLs to be blocked (generally using Border Gateway Protocol). The routers then divert any traffic to those IP addresses to a second stage. The second stage examines the diverted traffic to see if the actual URL request matches that on the block list. Most commonly the action by a filter is a block-page being returned to the end-user, otherwise the traffic is allowed to pass on and the site returned to the user.

If the request is for a site with an IP address that is not on the filter's translated list, then the request is processed as a normal transaction with no further involvement by the filter. The premise of hybrid technology is that the majority of traffic on a network is not to sites sharing an IP address with a site to be blocked, and therefore most traffic can pass-by without examination (except for a cursory check against an IP list on the router).

Pass-through filter: A pass-through filter operates in-line with the traffic, essentially examining every address passing through. There are a number of pass-through technologies available, most of these are Deep Packet Inspection (DPI). DPI technology is not only used in content filtering devices but also to detect network attacks, malware and other security functions.

Proxy server: This is a server that caches, or stores, requests from users for a variety of purposes—traditionally to increase network performance to downstream end-users if the upstream connection is limited. Today, proxy servers can also be used for content filtering by comparing a list of blocked URLs against the incoming requests and, where necessary, re-directing to a block page. Proxy servers are commonly used as the second stage in conjunction with pass-by filters.

Redundancy: In a server or other device, this refers to the extent to which parts are duplicated in order to ensure that the device can continue to operate in the event that something should fail.

SOHO: Small Office / Home Office

Streaming: This is the process of transferring data across a network in an ordered state for smooth presentation. Data is presented as a single steady stream as would be required for viewing a video file or listening to a music file. Realtime/Live video/voice is considered to be streaming.

Stateful: Indicates that something can retain its state. In particular, when an application or device is shut down, it keeps track of all settings and other information so that it can be restored properly when restarted.

Under-blocking: This refers to a situation where some of the undesirable material expected to be blocked by a content filter is allowed through to internet users. For example a filter might claim to block racist websites, but, in fact, will almost certainly fail to block some racist sites.

Upload: This is the process of sending data from a computer or other device to the internet.

URL: (Uniform Resource Locator) This is a human friendly internet address in a form such as: www.somecompany.com.au/section. This kind of addressing is normally provided to people in order to allow them to find websites or individual web-pages. The portion after the slash indicates that a particular sub-section or page of the website is being addressed. URLs are properly prefixed with 'http://' or 'https://', but browsers usually forgive this omission. (See also: IP address)

Enex TestLab

Enex TestLab, founded in 1989 as the RMIT University IT test lab, is now wholly owned by Enex Pty Limited. Enex has eight business divisions all involved in separate areas of independent testing services and reporting, hardware, software, systems, security, gaming/wagering, media/communications, physical/materials and usability/accessibility.

As a leading provider of independent testing services for hardware, systems, software and user experience, Enex TestLab is ISO 9001 certified and an ISO17025 accredited test facility. The company has offices in, Sydney, Melbourne, Shanghai and London and laboratories in Melbourne, Shanghai, and Cwmbran (UK).

Regularly published in magazines and titles of note, including CBS interactive media properties; ZDNet and CNET, Enex TestLab has authored product tests and reviews for over 18 years.

Enex TestLab provides a wide range of services designed to assist clients with risk reduction. These services include:

- **Manage procurement risk.** Technology procurement can be extremely expensive if you don't get it right. Enex TestLab can reduce the risk of product choice with our comprehensive quality assurance services and systems testing.
- **Independent product evaluation.** Scientific, Objective, Independent testing and reporting services enabling clients peace of mind when gaining a balanced impartial understanding of technologies available in the market. Claims testing of vendors products and systems, comparative testing between vendors/technologies, testing for capital raising, and testing for Government policy consideration are just some examples.
- **Improve product development.** Enex TestLab can support your new application, website or ICT hardware product throughout the development lifecycle. We help ensure the final product meets user needs, fulfils business requirements, is easy to use and technically robust.
- **Increase return on investment.** Enex TestLab's quality assurance services take the gamble out of product selection and development. Our customers can be confident their technology investments will provide value for money and tangible benefits to the organisation and end users.

Enex TestLab provides a number of services that help improve the user experience with technology-based projects. These services include user centred design, user needs analysis, usability testing and accessibility consulting and testing.

Enex is a member of the Australian Internet Industry Association (www.iaa.net.au), the International Information Systems Security Certification Consortium (www.isc2.org) the Information Systems Audit and Control Association (www.isaca.org) the Australian Information Security Association (AISA) and the Information Systems Security Association (www.issa.org). Enex adheres to and endorses the professional codes of conduct required by those organisations.

Enex TestLab's broad range of skills, combined with the latest tools and techniques, are the proven equation for success. Enex TestLab gives you peace of mind when evaluating or designing technology systems.