REVIEWED: LIGHTTPD a small lightweight web server

O3:

The Open Source Enterprise Data Networking Magazine

Issue 1 / November 2005

http://www.o3magazine.com

Control Voice Infrastructure Costs with Open Source Telephony

Linux Multi-Layer Switching with LISA

AppOS a next generation Linux distribution with a focus on SECURITY

Opening the jar on Google Honeypots

Monitoring the Network Intrusion Detection with SNORT

Leveraging Open Source for business

Reclaim lost time

Levanta Intrepid™

The world's first Linux management appliance

Plug the Levanta Intrepid™ into your network and perform the most important Linux management tasks in a fraction of the time you spend now. And gain power and flexibility that you've never had before:

- **Fast & Portable:** Provision servers or workstations practically anywhere, anytime – in minutes. Swap them around, mix it up.
- **Flexible:** Supports commodity hardware, blades, virtual machines, and even mainframes.
- **Out of the Box:** Includes pre-defined templates for servers, workstations, & software stacks. Or create your own.
- **Total Control:** Track any file changes, by any means, at any time. And undo them at will.
- **Disaster Recovery:** Bring dead machines quickly back to life, even if they're unbootable.

Based upon technology that's already been proven in Fortune 500 enterprise data centers. Now available in a box, priced for smaller environments. **Just plug it in and go.**

30-Day
Money-Back Guarantee

Order online by 11/30/05
Get $500 Off
Enter PROMO CODE: 03M0905

LEVANTA®
www.levanta.com
1.877.LEVANTA

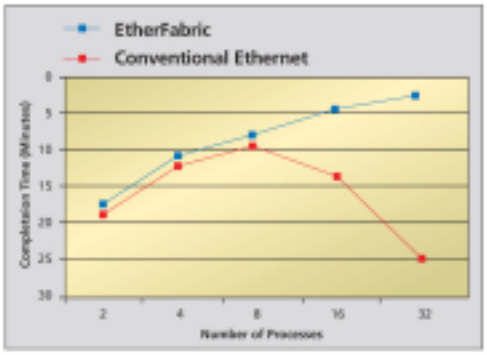
WINNER
LINUXWORLD
Most Innovative Hardware Solution

ACCELERATE APPLICATION PERFORMANCE!

>> HALF THE LATENCY

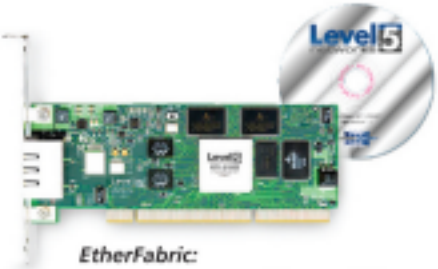
>> TWICE THE BANDWIDTH

>> 4X THE PERFORMANCE



Take EtherFabric for a ride today and experience the accelerated performance for yourself.

Visit **www.level5networks.com/landing/3.php** and take advantage of our limited time offer to ship you one extra EtherFabric NIC with your initial order.



EtherFabric:
High Performance Ethernet NIC

Level 5 networks

Level 5 Networks Inc. • 840 West California Avenue, Suite 240 • Sunnyvale, California 94086 • 408.245.9300

CONTENTS

@O3

INTERNET

Abul Asim M. R. Qarshi looks at Google Hack Honeypots, and how Google can reveal problems with unsecure servers.

BUSINESS

James Hollingshead provides a detailed introduction to Open Source, and tips for having a positive impact on the community

VOIP (Voice over IP)

The first part in a series on Open Source Telephony, starting with an introduction to Asterisk, the benefits and more...

NEXT MONTH

Rapid Web Development
Developing AJAX Applications
A look at mod_security
PostgreSQL and much more..

SECURITY

AppOS a new upcoming Enterprise Linux distribution, get a first look at its advanced security features.

WEB TECH

Mathew Burford looks at Lighttpd 1.4.7, a lightweight web server with a focus on speed, compliance, security and more..

NETWORKING

A look at LISA and multilayer switching frameworks for Linux.

The Linksys WRT54G captive portal

Introduction to Snort and IDS.

(IN)SECURE

Open. Informative. To the point. (IN)SECURE Magazine is a free digital security magazine discussing some of the hottest information security topics.

// www.insecuremag.com //

and so it begins...

RIGHT NOW YOUR COMPETITORS ARE PITCHING LINUX TO YOUR CUSTOMERS, WHY AREN'T YOU?

BY JOHN BUSWELL

Thank you for taking the time to read through our first issue of O3 Magazine. O3 is an electronic publication dedicated to open source Enterprise Data Networking solutions. Each month O3 will look at all aspects of enterprise data networking from network level solutions such as firewalls, routers, switching to server side applications such as FreeRadius, OpenLDAP and Apache.

Our goal at O3 is to introduce Enterprise Data Networking technologies to small and medium sized businesses, discuss open source solutions for providing those technologies and to provide the technical information on how to deploy and maintain those solutions. O3 however is not just targeted at small and medium sized business, the solutions we discuss are already deployed in most large businesses, government agencies and educational institutions, not necessarily open source solutions though. CIOs, CTOs, IT management and staff at larger entities will benefit from exposure to lower cost open source alternatives.

I don't personally see the point of promoting open source solutions if you do not use them yourself, as such O3 is designed, developed and published using open source technology exclusively. Every article in O3, including this editorial is written in Open Office (*www.openoffice.org*) under Linux, those articles are then imported into Scribus (*www.scribus.org.uk*), while graphics artwork is created with the Gimp. Scribus is used to export the completed publication in PDF format.

Each month O3 provides a round up of open source events, as well as an upcoming event calender, we have done our best to track down as many major events as possible, but if you have an event, whether its a local LUG meeting or a full scale trade show we would like to hear about it. O3 also provides an "Open Source Report", this is a short round up of interesting open source software that has been released over the past month.

Each issue of O3 features Security, Internet, Web Tech, Business, Networking, VoIP, Network Applications and Network Security columns. This first issue of O3 is more of an introductory issue, starting next month (December) each issue will have a particular theme. For December it is rapid web application development.

We have an exciting line up for 2006, in the first quarter we will be looking at Linux on the zSeries mainframe, including a first look at some new innovative Linux solutions for the zSeries. A detailed look at networking technologies in Linux including OSPF, RIP and BGP, as well as a look at providing end to end QoS solutions with Linux. We will wrap up Q1 2006 with a detailed look at Open Source Telephony.

Finally, I would like to take a moment to thank our advertisers who very graciously put their names on a brand new magazine. Enjoy the issue and feel free to send feedback.

O3 Magazine
November 2005
Issue 1

EDITOR IN CHIEF
JOHN BUSWELL
EDITOR@O3MAGAZINE.COM

EXECUTIVE EDITOR
JAMES HOLLINGSHEAD
JAMES@O3MAGAZINE.COM

ARTWORK
JOHN BUSWELL

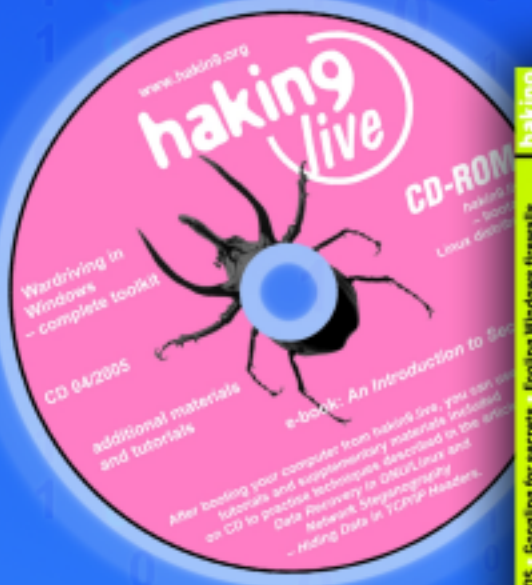
PROOF READERS
GREG JORDAN
SHAWN WILSON
FRANK BOYD
STEW BENEDICT

SALES AND MARKETING
GREG JORDAN
SALES@O3MAGAZINE.COM

SUBSCRIPTIONS
O3 MAGAZINE IS DISTRIBUTED ELECTRONICALLY FREE OF CHARGE BY SPLICED NETWORKS LLC. TO SUBSCRIBE VISIT WWW.O3MAGAZINE.COM.

SOFTWARE
SCRIBUS 1.3.1
GIMP 2.0.5
OPENOFFICE 1.1.2

We have knowledge. Want some?



www.haking.org/en

If you want to buy a magazine, please visit us at www.shop.software.com.

available at the beginning of July

EVENTS

NOVEMBER EVENTS

Open Source Database Conference

november 8, 9 2005

frankfurt, germany

http://www.opendbcon.net

LinuxWorld Expo

november 9, 10 2005 (utrecht, netherlands)

november 15 - 17 2005 (frankfurt, germany)

april 3 - 6 2006 (boston, united states)

http://www.linuxworldexpo.com

SC|05 (Supercomputing Conference)

november 12 - 18 2005

seattle, washington, usa

http://sc05.supercomputing.org

IP.4.IT

november 14 - 16 2005

las vegas, nevada, usa

http://www.ip4it.com

GULEV

november 17 - 19 2005

veracruz, mexico

http://www.gulev.org.mx

FOSS.IN (india's premier open source event)

november 29 - december 2nd

bangalore palace, bangalore, india

http://www.foss.in

UPCOMING EVENTS (DECEMBER)

Open Source Developers Conference 2005

december 5 - 7 2005

melbourne, australia

http://www.osdc.com.au

ApacheCon 2005

december 10 - 14 2005

san diega, california, usa

http://www.apachecon.com

Interop

december 12 - 16

new york, usa

http://www.interop.com

have an upcoming event? tell us about it, send email to events@o3magazine.com with details.

FEATURED PAST EVENT

OHIO LINUXFEST 2005

october 1st 2005

columbus, ohio, usa

http://www.ohiolinux.org

Ohio LinuxFest is a community focused free event that is run by a volunteers and funded by sponsors. This year key sponsors of the event were Novell and Digium, additional sponsors included IBM, Spliced Networks, RocketCalc, Sybase, Pantek, Imagestream and many others.

The event overall was great for both the visitors and the sponsors. Every sponsor we spoke with indicated they were happy with the event and would return again next year. Over 700 visitors attended the third annual event which ran all day and into the evening.

The quality of the speakers was good, with keynotes from Chris Hicks of IBM, and Novell's Jerry Mayfield. Some of the slides are available from the event's website.

NOVEMBER OPEN SOURCE REPORT

Welcome to the Open Source Report. This is the section of O3 where we give a brief run-down of the major applications which made releases during the month.

LINUX KERNEL

http://www.kernel.org/
Release: **2.6.14**

The latest release of the Linux kernel has many new features including HostAP support to act as a wireless access point, a Linux port of the plan9 9P protocol, FUSE (which allows fully functional filesystems in a userspace program), lock-free file descriptor lookup, and several new drivers.

APACHE

http://www.apache.org/
Release: **2.0.55**

The latest release of Apache includes several security fixes, corrects a few instances of possible memory leaks and bad program behavior and adds extra logging capabilities.

MANDRIVA

http://www.mandrivalinux.com/
Release: **Mandriva 2006**

The 2006 release of Mandriva includes a desktop search tool (Kat) which allows searching for both file names and file content, and interactive firewall, official support for Intel Centrino mobile technology, integration of Skype, and an auto-installation server.

SNORT

http://www.snort.org/
Release: **2.4.3**

The 2.4.3 release of Snort fixes a buffer overflow vulnerability which existed in the Back Orifice preprocessor.

ASTERISK

http://www.asterisk.org/
Release: **1.2**

The 1.2 release for Asterisk includes improved voicemail features, easier configuration, improved SIP support, new features for the IAX protocol, use of sound files for native-on-hold music, and improvements to the dialplan.

PROFTPD

http://www.proftpd.org/
Release: **1.3.0**

A “timing attack” protection module has been released to help solve the timing leak described by Leon Juranic.

LIGHTTPD

http://www.lighttpd.net/
Release: **1.4.7**

Lighttpd is covered by Mathew Burford on page 18 of this issue.

SCAPY

http://www.secdev.org/projects/scapy/
Release: **1.0.2**

Scapy is a powerful interactive packet manipulation program capable of forging or decoding packets from a wide range of protocols. Scapy is an excellent tool for testing and reproduce complex network / network device problems.

NATSTAT

http://svearike.sytes.net/natstat/
Release **0.0.11**

Network monitoring tool providing real time information based on the iptables configuration.

Behind AppOS Security

DISCOVER THE MULTI-TIER SECURITY APPROACH BEHIND THIS UPCOMING LINUX DISTRIBUTION FOCUSED ON RESHAPING THE DATACENTER

BY JOHN BUSWELL

AppOS is a highly secure Linux based appliance framework that is designed to limit the damage that can occur in the event that a service or appliance is compromised by a third party due to an un-patched or a previously unknown vulnerability. In most enterprise environments, some of the network security techniques employed by AppOS are already in production, so migrating to or adding AppOS into the data center is often a trivial task. For smaller businesses there may be some network changes required in order to conform to the AppOS framework, particularly those related to out of band management and network storage.

OUT OF BAND MANAGEMENT

AppOS utilizes out of band management and storage networks to provide an extra layer of security. Out of band means that the management and storage networks are not on the same network as regular application traffic (such as http "web" traffic). AppOS supports out of band management in several forms including physically separate Ethernet segments, VPN based management and the use of 802.1q VLANS. Physically separate Ethernet segments are the preferred method of out of band management. In the event an Internet facing interface is DoS (Denial of Service) attacked, there may not be sufficient bandwidth to reliably manage the device remotely. Here a separate physical Ethernet interface on its own private segment will remain fully accessible unless the server itself has crashed. A separate physical interface enables an administrator to disable the Internet facing interface without losing connectivity to the system. Management traffic can include traffic such as syslog, snmp, ssh, https, and even DNS. Aside from limiting the access to this information for security purposes, out of band management enables syslog and snmp trap traffic to continue to work reliably even if the Internet facing Ethernet ports are congested.

Another advantage to out of band management is that it frees up traffic on production networks, especially if you offload DNS traffic to the management network to be handled by secure / trusted caching name servers. It is for this reason that out of band management can assist in improving the scalability of even small networks.

An important part of the AppOS network security framework is to place user data in out of band storage networks. Storage networks can be as simple as a gigabit switched Ethernet segment running a network file server using NFS or GFS between the file servers and the application servers on the network. Placing user data on an out of band network has many advantages including reducing the load on your production "Internet facing" network, thus improving scalability and enabling a finer access control over the user data. In a web hosting environment for example, a small number of restricted access servers may have write access to user data, making it possible for security policies to limit access to that infrastructure, while allowing for a large number of publicly accessible web servers to serve data with only read-only access. In the event of a zero-day security vulnerability existing in your web server software, the publicly accessible web servers only have read-only access to the data, preventing potential malicious users from uploading code to execute on the server. Advanced access control lists, mount options and other measures can be used to prevent execution of unapproved executables on the publicly accessible web servers.

While this approach offers an extra degree of security it can cause problems with legitimate web applications that need to have the capability to write to user data. Typically, user data is written via database transactions, such as information for e-Commerce transactions, creating accounts or often

even uploading files, the AppOS approach to this problem is to take database transactions out of band and to pass file uploads through an out of band inspection system before making the files accessible. While the approach can cause problems for existing web applications where security may not have been taken into account, the effort involved to migrate such applications often involves just putting a good security and best practices policy into place.

QOS

The final piece of the network security framework in AppOS is to rate-limit application traffic, employ Quality of Service (QoS), packet queuing techniques and provide high availability solutions through industry standard protocols such as VRRP (Virtual Router Redundancy Protocol). These techniques aid in protecting the network against a variety of network based attacks while providing high availability.

LINUX IMAGE MANAGEMENT / BOOT SYSTEM (LIMBS)

AppOS provides a highly secure Linux based operating system that utilizes the Linux Image Management / Boot System (LIMBS). LIMBS, essentially runs a Linux based OS from a single image file mounted via loop back on a ram disk. The security comes in the type of file system used in the image file, using something such as ext3 is only going to provide you with the same degree of security as a normal Linux system, but using an "unwritable" file system such as SquashFS means that in order to "write" to the file system, the entire image file has to be regenerated and replaced. AppOS works by placing the right files on the SquashFS file system and the right files on the ram disk to insure proper operation of the Linux system.

LIMBS, currently at release 1.1.9, is available under the GPL. LIMBS performs some error detection and essentially sets up the system for booting by loading the appropriate OS image. The framework that AppOS and LIMBS provide has great potential for booting different kernels (Linux, BSD, OpenSolaris) while retaining the same application images.

LIMBS hands over control to init, which in an AppOS based system will hand over control to ExMS, the management system.

APPLICATION IMAGES

AppOS places a specific application such as a DNS server into separate application specific image called an ASI. The ASI is used to generate separate file system images, one for configuration files, and one for executables. These two files along with user data are mounted into three directories within a chroot environment while files themselves exist outside of the chroot environment. The end result is that if your DNS server has a vulnerability, even if it's exploited and the attack gains root access within the chroot, they cannot "break out" of the chroot due to Grsecurity. They cannot modify the configuration due to the fact they are sitting on an unwritable SquashFS file system, and for the same reason they cannot overwrite or replace the executables, the Linux kernel has no means of writing to the file system and the attacker does not have access to the image files or the tools to regenerate them. If the user data is secured through a read-only network storage framework as discussed earlier in this article, then the attacker cannot do anything; they cannot even disrupt the service.

GRSECURITY, PAX, STACK SMASH PROTECTION AND PIE

AppOS is Glibc based, and utilizes Grsecurity, PaX, Position Independent Executables (PIE), enhanced random number generators, privilege separation for daemons, Stack Smashing Protector, non-lazy binding and relocation read-only linking. The latter two are now standard in binutils.

Grsecurity is an innovative open source project licensed under the GNU Public License (GPL). It takes a multi-layer detection, prevention and containment approach to security. Grsecurity provides chroot hardening, a robust Role-Based Access Control system, prevention of exploits related to address space bugs (through PaX), enhanced randomness in the Linux TCP/IP stack, restricted access to process lists, advanced auditing and many other features.

Stack smashing protector is an extension to the GNU Compiler Collection (GCC) for protecting applications from stack-smashing attacks. The protection is provided by buffer overflow detection and a variable reordering feature to avoid corruption

of pointers. The protection is applied when AppOS is built (at compile time).

Binary executables contain memory locations called virtual addresses, these addresses are often useful for debugging as the same functions are located at the same memory location on any system running the same binary. Unfortunately what makes for easier debugging also enables an attacker to load up the same executable locally to determine memory locations on a remote target system. So if you're running Apache from Red Hat 9, and an attacker determines this by querying your web server with a standard HEAD / HTTPD/1.1 request, and inspecting the server token. They can simply download the same Red Hat 9 apache binaries and determine what memory locations are being used by your server because it is running the same executable. Position Independent Executables essentially make each system different, randomizing those memory locations, making it much more difficult for an attacker to determine the address.

CONCLUSION

AppOS provides state of the art network and system security through a multi-layered approach. By taking simple steps such as implementing management and network storage out of band, strong network security policies and best practices it is possible to tighten control over your network while retaining functionality and improving scalability. AppOS utilizes state of the art open source security solutions such as Grsecurity/PaX, Stack smashing protector, Position Independent Executables, enhanced randomization and file system access control lists. AppOS takes these technologies a step further by implementing applications in a secure chroot environment within a system of unwritable loop back based file systems. Thus creating a safety net in the event a technique is developed to circumvent these great open source technologies designed to protect vulnerable software.

The bottom line is that AppOS provides the best available zero-day protection against applications which contain undiscovered vulnerabilities and exploits.

APPOS AVAILABILITY

The current release of AppOS is 1.0.0, which ships on AppOS based SN series appliances. AppOS 2.0.0 is scheduled for release on Jan 3rd 2006. A public beta of AppOS 2.0.0 shall be available from Spliced Networks LLC from November 28th 2005.

FURTHER READING

grsecurity
http://www.grsecurity.net

PaX
http://pax.grsecurity.net

Stack Smashing Protector
http://www.trl.ibm.com/projects/security/ssp/

Frandom
http://frandom.sourceforge.net

SquashFS
http://squashfs.sourceforge.net

Disk / Swap Encryption
http://www.sdc.org/~leila/usb-dongle/readme.html

John Buswell is co-founder and Chief Technology Officer of Spliced Networks LLC. He can be reached by email (johnb@splicednetworks.com).

Special thanks to Shawn Wilson (Time Warner Cable / Road Runner Business Cincinnati), Stew Benedict (Mandriva), Frank Boyd (Spliced Networks), Raja Hammad (Spliced Networks) and Mat Burford (Spliced Networks) for providing technical review of this article.

Opening the Jar on Google Honeypots

GOOGLE PROVIDES A POWERFUL SEARCH ENGINE HOWEVER AN UNINTENDED

USE HAS BEEN THE ABILITY FOR MALICIOUS USERS TO SEARCH FOR VULNERABLE SERVERS

BY ABUL ASIM M.R. QARSHI

The Internet's horizons have increased massively over the last 10 years. Now there are billions of web pages containing content related to nearly every aspect of personal and business information. With this growth in the Internet, a problem arose: finding the page with the information you are actually looking for. This is where search engines come into play, allowing Internet users to find the page that they want. However, Alltheweb, AltaVista, Yahoo, MSN, etc were all giving limited search functionality and none of them took it as challenge and business opportunity until Google came along.

Every search engine vendor wants to become more effective, efficient, and to find accurate results in the least time possible. Most search engines index the pages to search and rank them to maintain accuracy. To do this, most search engines' bots or crawlers start traversing the web by using links that appear on the pages.

Information collected by the search engine is mostly comprised of the name, file type, url, etc. These search engines also index the dynamic pages based on php, shtml, etc. for example *http://www.domain.com/?id=myd*

FILE SEARCH

Most search engines provide the functionality to search files on the Internet. That means the search bot indexes the different types of "readable" files. Most search engine vendors claim that this will increase the performance of their system. For example, Google claims the benefit of searching non-html files is "a wider view of the contents available on the World Wide Web".

While Search Engines index non-html file types such as PDF, doc, txt etc., they also index other file types, so be aware that your pwd, htaccess, or any other very critical file that could make your system vulnerable could also be found via Google.

According to Matt Kesner, chief technology officer

at Mountain View, Calif.-based law firm Fenwick & West LLP, "The ability of search engines to discover a lot of information that was not necessarily hidden but was a lot less available previously is scary."

SEARCHING POWER

Search engine vendors, specifically Google, have given us keywords such as "info" "link", and "related" to include in the search query which rectify and give us more accurate results. The complete list of keywords can be found at *http://www.googleguide.com/advanced_operators.html*

Now we will analyze some well crafted queries to find appropriate results. First of all we are going to search people's CVs. Place the following query in the Google search box, and look at the result:

(filetype:pdf OR filetype:doc OR filetype:rtf) (intitle:resume OR inurl:resume OR "my resume")(-apply OR -submit OR -benefits OR -recruiter OR -Openings)

Next, let's try to browse to a particular URL that we know is password protected. The server immediately prompts you for a username and password, but depending on the URL, you might be able to plug it into Google, select the Cache link and read the password protected page. A good example is searching for content with inurl:webstats or inurl:accesswatch, or the default url of any other popular web stats program. Many of these are protected by .htaccess files but plugging them into Google reveals the page when following the cache option. Google is able to do this because the administrators of these servers unwittingly have the servers misconfigured, but with Google, a clever malicious user now has access to information that the administrator believes is hidden.

VULNERABLE SYSTEM DETECTION

To get into any system, a malicious user needs to know information about that system, and search engines provide an easy tool to help them detect vulnerabilities to exploit. For example, Apache can be configured to hide version information using the ServerTokens directive, but if an administrator hasn't removed the manuals installed in the htdocs directory, a quick search can reveal the release version the administrator is using. The same search could be used to locate unconfigured default installations of Apache on the Internet:

inurl:"/manual/" +Apache 1.3

These types of queries are easy to search for default files, making it easy for malicious users to detect systems where the administrator may have left files they've assumed are hidden from the public. If an administrator has left the default files, it might be an indication they are inexperienced and thus an easier target. The above query can easily become more specific by using site: operator which will restrict it to any specific domain.

Similarly a malicious user can also find default installations of particular applications such as WebMail by simply crafting the query with **intitle:"Welcome to Mailtraq WebMail"** (Mailtraq is a Web based Email Client). Such queries can often find test systems on live networks that administrators are using to test out new and unsecured applications.

SEARCHING PASSWORDS

If you have any readable files that contain passwords uploaded on the server, then it's time for some bad news: hackers can use queries on search engines to find passwords. For example, inurl:passlist.txt can be used for this purpose.

PREVENTION

To prevent search engine based attacks, a web site administrator can indicate which parts of the site should not be visited by a robot by providing a specially formatted file on their site in robots.txt. In addition, a web author can indicate if a page may or may not be indexed or analyzed for links through the use of a special HTML META tag. For example, a <META NAME="Googlebot" CONTENT="nofollow"> tag in the header can stop Googlebot from indexing the pages.

To Prevent Googlebot from following any particular link on the page that might link to your critical page or any secret web server you can add rel=”nofollow” in the hyperlink. I can't vouch for this link.

Note that these methods rely on cooperation from the robot, and are by no means guaranteed to work for every robot. If you need stronger protection from robots and other agents, you should use alternative methods such as password protection.

GOOGLE HACK HONEYPOTS

The methods discussed so far in this article are called Google Hacks. The "Google Hack" Honeypot project *http://ghh.sourceforge.net* provides a means to observe search engine hackers using Google against your resources by emulating a vulnerable web application, allowing itself to be indexed by search engines. The transparent link method used will reduce false positives and avoid malicious users detecting the honeypot.

The honeypot then logs to a file information about the attempted attacks, the source IP, referral information and user agent. Using this information, the administrator can detect and monitor attackers performing reconnaissance against their resources and get a detailed view of specific attackers.

ABUL ASIM M.R QARSHI IS A NETWORK SECURITY SPECIALIST FOR SPLICED NETWORKS LLC BASED OUT OF PAKISTAN.

Mandriva

Businesses need rock-solid IT solutions

**Mandriva Linux Corporate Server & Corporate Desktop offer outstanding robustness, scalabilty, and reliability.
All with the ease of use specific to Mandriva products.**

- Full IT solution for server and desktop deployments
- Open standards
- Both x86-32 and x86-64 architectures are supported
- 5-year product maintenance
- 24/7 support
- Mandriva Online update service - Professional Level
- Incredible price

http://www.mandriva.com/business/corporate-server

http://www.mandriva.com/business/corporate-desktop

www.mandriva.com

Lighttpd 1.4.7 Review

LIGHTTPD IS A LIGHTWEIGHT WEB SERVER WITH A FOCUS ON PERFORMANCE, SECURITY AND FLEXIBILITY WORTHY OF CONSIDERATION IN THE DATACENTER

BY MATHEW J. BURFORD

If your web server's performance is suffering due to high load then your solution may be here. There is interest brewing in Lighttpd, a relatively new web server developed by Jan Kneschke et al. In addition to claims of a low memory footprint, its main website *www.lighttpd.net* boasts that Lighttpd has security, speed, compliance, flexibility and an advanced feature set. Lighttpd is a "high load performance optimized" web server that is intended to be used for web servers which must serve lots of small files rapidly and php servers which are placed under high load. Despite this, Lighttpd seems to be useful in many other areas, such as an embedded system which have limited resources. This article will look into Lighttpd's claims and features and discuss them.

I installed Lighttpd on a 1.7Ghz Pentium 4 with 775636Kbytes DDR SDRAM running Gentoo Linux (kernel version 2.6.11). For testing purposes, Siege (described below) was installed on a 15” Powerbook (1.5Ghz PowerPC G4 with 512Mbytes DDR SDRAM) running MacOSX, version 10.4.2. Both machines were connected to a Netgear 54Mbps wireless router (WGR614 v4).

BASIC TESTING

At first glance of Lighttpd, the source download file of version 1.3.16 consisted of 690 kbytes, very light indeed. Compilation and installation used the typical 'configure/make/make install' system. I was pleased to find there was minimal complexity getting the webserver up. The usual example configuration file is shipped with Lighttpd, which follows the "include only if you need" philosophy. Hence it was very small, well commented and easy to follow. Surprisingly, in 10 minutes Lighttpd was up and running and serving static files with a basic configuration. The installation directory was 2688kb in size. This included various unused modules and random docs. The Lighttpd executable file size is 925Kbytes.When running, the memory usage for Lighttpd was 418Kbytes. Overall, it appears to be quite a very compact program. For Gentoo users, the install can be simplified to 'emerge www-servers/Lighttpd'. You might have to set an unstable flag to download the latest version. This automates the installation, but also sets up a Lighttpd account for the server to run within and various other things to get it working fast.

I was eager to test the base install of Lighttpd. I downloaded the latest version (2.63) of Siege, an http web server benchmarking tool, (freshmeat.net/projects/siege/) from freshmeat and installed it. I had to be careful with siege, as it seemed to use a lot of resources. On my MacOSX Powerbook, I used Siege to simulate 15 users, and I recommend you do this for yourself through your own network so that you can compare it with your current web server's performance. Choose a document to serve which will use the features that your web server typically serves.

After testing with 1000+ concurrent simulated users, I was flooded with errors which indicated that I had run out of file descriptors and as a result requests to the server were being denied. The Lighttpd website documentation (www.lighttpd.net/documentation/performance.html) has a fix for this if you find you are having trouble here. The solution involves lowering the defaults of HTTP Keep Alive so that file descriptors aren't held on to as long. Otherwise you can simply increase the file descriptors with a quick

% echo 76680 > /proc/sys/fs/file-max

PERFORMANCE ENHANCEMENTS

While the Lighttpd website provides a good amount of documentation, in my opinion the documentation is still underdeveloped and much of what is there needs revision. This is most likely due to the project still being in its early stages, so this will certainly improve.

One interesting section is performance (www.lighttpd.net/documentation/performance.html), which states that Lighttpd can be configured so that it uses the native 'event handler' provided by the the operating system. For Linux kernel 2.6.* this should be 'epoll' and would require a line like this to be added to the Lighttpd config file:

```
server.event-handler = "linux-sysepoll"
```

The advantage of using 'epoll' over the default 'select' is that select is limited to FD_SETSIZE handles. This is hard coded in, and not easily changed, using 'epoll' however overcomes this problem. I would recommend you set this especially if your server tends to serve a large number of clients. For more information on this topic see www.kegal.com/c10k.html.

EVENT HANDLER TESTING RESULTS

These tests are not ideal, but show a general analysis of the server when the 'epoll' system is used. It does not effectively test the features of 'epoll'. Below are the results when simulating 15 users abnormally flooding the server with requests. Note: 3 tests were run with the first test was considered a server 'warm-up' so is not listed. This command was used to start siege:

```
% ./siege www.myserver.net -b -t1M > /dev/null
```

This instructs siege to connect to www.myserver.net and ready 15 users. The -b option enables benchmarking of throughput and -t1M instructs the simulation to run for 1 minute. The last section (> /dev/null) will forward unnecessary output (which slows the test) to /dev/null. During all the tests below I monitored the CPU usage using the 'top' utility. CPU usage averaged about 35% and varied about 10%.

The test results opposite suggest that there is little performance difference in using epoll over select, so why use it? Well, as I mentioned before, epoll overcomes certain restrictions of select. Interestingly, the results of 'epoll' deviated much less than those of 'select' which suggests more reliability.

	Test 2 'select'	Test 3 'select'	Test 2 'epoll'	Test 3 'epoll'
Transactions (hits)	*71210*	*77950*	*73074*	*73399*
Availability (%)	*100.00%*	*100.00%*	*100.00%*	*100.00%*
Elapsed Time (seconds)	*60.36*	*59.91*	*59.67*	*60.44*
Data Transferred (MB)	*176.16*	*192.84*	*180.77*	*181.58*
Response Time (seconds)	*0.00*	*0.01*	*0.01*	*0.01*
Transaction Rate (transactions per second)	*1179.75*	*1301.12*	*1224.62*	*1214.41*
Throughput (MB/sec)	*2.92*	*3.22*	*3.03*	*3.00*
Concurrency	*5.83*	*12.84*	*7.47*	*7.05*
Successful transactions	*71210*	*77950*	*73074*	*73399*
Failed transactions	*0*	*0*	*0*	*0*
Longest transaction (seconds)	*0.51*	*0.52*	*0.51*	*0.51*
Shorest transaction (seconds)	*0.00*	*0.00*	*0.00*	*0.00*
Lighttpd version tested	*1.4.7*	*1.4.7*	*1.4.7*	*1.4.7*

SECURITY SUPPORT

The aim here is to prevent Lighttpd being used as a point of attack against the system. One method which limits the damage an intruder can perform is to run the Lighttpd daemon in a chroot jail. Chrooting will limit Lighttpd to a sub directory of the filesystem, which Lighttpd will see as root. Lighttpd supports being run in a chroot jail and it is highly recommended to do so as it is also not overly complex to set one up. The Lighttpd website has a link which will guide you through much of the process (*http://www.lighttpd.net/documentation*).

In general it is a bad idea to run Lighttpd with root privileges, as before the aim is to limit any damage an intruder can perform. Another supported method is to drop root-privileges and run Lighttpd as a low-privilege user. This is trivial and effective. First create a user called 'Lighttpd' by adding a line similar to the line below to your /etc/passwd file.

lighttpd:x:100:400:lighttpd:/www/pages/:/bin/false

Next, you should add a line similar to the line below to your /etc/group file while making sure that the numbers 100 and 400 are not taken by any other entries in these files.

lighttpd:x:400:

To set Lighttpd to run as this non-privilege user/group simply modify the configuration file to contain these settings:

change uid to <uid> (default: don't care)

server.username = "lighttpd"

change uid to <uid> (default: don't care)

server.groupname = "lighttpd"

It is also important that your server does not easily give itself away to users. One method attackers may use to gain information about a system is to simply read the html header. This is trivial to counter in Lighttpd, as described below.

First you might like to see what information the web server is giving out. Assuming you have telnet installed this can be done by entering the command:

% telnet localhost 80

You should receive a prompt as below:

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

You should now enter the below HTTP command, followed by two enter keystrokes:

HEAD / HTTP/1.0
(hit enter twice)

You should receive something similar to this:

HTTP/1.0 200 OK
Connection: close
Content-Length: 80
Date: Thu, 11 Aug 2005 20:47:04 GMT
Last-Modified: Wed, 10 Aug 2005 12:14:49 GMT
ETag: "-1257421618"
Accept-Ranges: bytes
Content-Type: text/html
Server: lighttpd/1.3.16

As you can see, the server by default sends out its name and version number. This provides an attacker with enough information to look up weaknesses in your particular software and version. I recommend for these security reasons that you set this to something non-helpful. To change this tag, again modify the configuration file to contain a line similar to this:

server.tag = "httpd"

After restarting your server, you may retrieve the header from the server and you should have modified that tag:

HTTP/1.0 200 OK
Connection: close
Content-Length: 80
Date: Thu, 11 Aug 2005 20:49:30 GMT
Last-Modified: Wed, 10 Aug 2005 12:14:49 GMT
ETag: "-1257421618"
Accept-Ranges: bytes
Content-Type: text/html
Server: httpd

Here you have been introduced to some basic aspects of Lighttpd's high configurablility. For more options, see the documentation provided with Lighttpd or look at the copies available on their website: (*http://www.lighttpd.net/documentation/*).

FEATURES

One of the biggest selling points of Lighttpd is its rich list of features. Below I look at FastCGI and MySQL based Virtual Hosting, two of the more popular features. Lighttpd however has a very clear cut state engine and plugin interface, which makes Lighttpd very easy to modify should you need to insert specialized capabilities into this small httpd.

FASTCGI

The aim of FastCGI is to remove a lot of the performance issues posed by CGI programs. Support for this is provided by the module mod_fastcgi and can be enabled by uncommenting the appropriate line in your configuration file, found under server.modules. FastCGI allows fast and extensive php support for Lighttpd, For more information see (*www.lighttpd.net/documentation/fastcgi.html*).

MYSQL BASED VIRTUAL HOSTING

There are a two vhost modules available for Lighttpd. An interesting one is mod_mysql_vhost, which allows you to provide virtual hosts using a MySQL table. Lighttpd recommends not to mix vhost modules as only one is supposed to be active at any given point in time. MySQL vhost allows you to place docroot and domain pairs in a table, then lighttpd will query the MySQL server to locate the docroot.

OTHER FEATURES

I felt that it was important to mention some of the other features in Lighttpd. SSL support is integrated into Lighttpd, and basic rate limiting support either on a per connection or server (all connections) basis. Like Apache it supports compression, the standard gzip compression which is supported on the majority of web browsers can decrease web server bandwidth utilization, Lighttpd also supports deflate and bzip2. Other interesting features include an rrdtool module for outputing bandwidth and load utilization, SCGI which is based heavily on FastCGI and is primarily used for Python + WSGI. Some anti-hotlinking features including trigger b4 download round out some of Lighttpds unique feature set.

EXPANDING LIGHTTPD

Lighttpd has been documented very clearly and in great detail by the Lighttpd development team. The documentation link off their main web page has full state machine information for both FastCGI and the httpd state machine. The documentation even includes the function names where the processing occurs. This makes Lighttpd, along with its size a very tempting solution for developers who need unique features or processing. It wouldn't take much to modify the Lighttpd code by inserting your own additional processing to perform custom URL or other modifications beyond those supported in mod_rewrite. Lighttpd also includes very useful plugin documentation.

CONCLUSION

Lighttpd is an exciting project which raises the expectations of small footprint web servers. As its userbase increases, much more documentation will be available. This server is highly configurable in a non-complicated way, which enables new users to quickly get their web server running with little trouble. Lighttpd is a competitive option to other popular web servers, and may be run alongside other webservers, such as tomcat or apache, to take advantage of the benefits offered by each. It will be interesting to see the direction Lighttpd takes on the Internet as it matures.

Mathew Burford is an Application Developer for Spliced Networks LLC based out of Wollongong, Australia.

Performance Hosting
quality service

Whether you are promoting a new business venture or expanding your existing one, you need a solid and secure hosting partner.

Why settle for less?

BLACKNIGHT SOLUTIONS

www.blacknight.ie sales@blacknight.ie +353 (0)59 9137101

An Introduction to Linux and Open Source for Business

LINUX AND OPEN SOURCE MIGHT BE TERMS YOU HAVE HEARD BUT ARE NOT QUITE FAMILIAR WITH

LINUX AND OPEN SOURCE CAN BENEFIT BUSINESSES OF ANY SIZE... AND NO IT IS NOT JUST FOR BANKS...

BY JAMES HOLLINGSHEAD

Open source. It's amazing how much confusion and mixed feelings those two little words can cause. What is it? How does it work? Is it for our business?

This article is an attempt to answer your questions and give a brief overview of what open source is, how it can help you and your business, and what you can do to help. Since it is a huge subject and answering everyone's questions would take entire books, this is really just a fairly high level look at open source arranged as a sort of question and answer session.

WHAT IS THIS "OPEN SOURCE" THING I KEEP HEARING ABOUT?

That's a very simple question to which there are a number of answers. At the most basic level, open source is the software development community and businesses working together in order to make quality software that anyone can use. It's a way for groups and individuals to contribute according to their skill sets on projects that they find interesting so that everyone can come out ahead.

It's real defining points are the license that the software is released under and the fact that the program is distributed free of charge. There are quite a few licenses that are considered to be open source by the Open Source Initiative (*www.opensource.org*), the non-profit organization which keeps track of and promotes open source licenses.

What most of the accepted licenses boil down to is that the source code for the software is open for the world to see, modify, contribute to, and use. Certain licenses require that you release all changes you make while others just require you to give them credit for having code in your project.

I HEARD THAT LINUX IS HARD TO SETUP AND USE IS THAT TRUE?

If you had asked me that question in 1998 when I first tried to install Linux on a new desktop that I bought, I would have said it was a nightmare to get running. Now, however, it's a great deal better and is actually ready for a lot of home and business uses.

Many of the applications now have graphic interfaces that are just as good as what you are used to now and have the functionality that you've come to expect from your business apps. That's not to say that there isn't a little bit of a learning curve, but it really is a pretty slight one.

On top of this, Linux is now a breeze to install on most hardware. To give you an idea, I recently installed Linux on my laptop. Anyone who has installed Windows on a laptop will tell you about the fun that you're in for. It takes a stack of cds, most of the day, and constantly babysitting the laptop to answer questions and switch out disks. On top of that, you have to provide the right video, audio, and network drivers and then you have to run security updates and install service packs.

With Linux, it took four cds, a network connection, and about three hours to install the operating system, most of the software that I use, and to update the entire system. Ethernet worked out of the box; so did the video. To install the last two programs that I wanted to use required two very short commands and updating the entire laptop required one more. Most of the time that was spent installing Linux was used to do other things while my laptop worked quietly in the other room without needing me to babysit it.

It's come that far.

IF I WANT TO USE OPEN SOURCE SOFTWARE, DO I HAVE TO RUN LINUX?

While most software released for Linux is open source, not all open source software is Linux-only (or even runs on Linux). It is possible to have open source projects on other platforms, such as Windows and OSX, and indeed many popular projects, such as the Firefox web browser and the Eclipse programming environment for Java, are released on a wide variety of platforms.

The developers and companies behind the projects realize that not everyone can standardize on a single platform, so they often do their best to provide solutions where they make sense.

WHAT SORT OF OPEN SOURCE SOFTWARE IS THERE?

Open source software exists across the spectrum of applications.

- For operating systems, you have various forms of Linux and BSD, which are all Unix-like operating systems. While they allow fine control of practically everything that you could want to do with your computer from a functionality and security standpoint, they also have rather nice graphic interfaces, allowing both casual users and the more experienced to use them with ease.

- The popular web browser, Firefox, is a piece of open source software that grew out of the old Netscape browser. It also has sibling programs Thunderbird for email and Bugzilla, a bug tracking software package used by many developers. All of these programs may be found at www.mozilla.org

- Open Office (*www.openoffice.org*) is a popular open source suite that includes word processor, spreadsheet, and presentation software and is available on both Linux and Windows.

- GIMP (*www.gimp.org*) is an open source graphics program which is available both on Linux and Windows and is used by this magazine.

- Many programming environments such as Eclipse (*www.eclipse.org*) are open source as are the source control tools Subversion (*http://subversion.tigris.org*) and CVS (*www.nongnu.org/cvs*).

- There are even several very good open source databases out there such as MySQL (*www.mysql.com*) and PostgreSQL (*www.postgresql.org*).

There are many other open source offerings out there. If you're interested in looking for open source applications, a good place to start is The Open CD project (*www.theopencd.org*), which lists applications for Windows, but also links back to websites for the projects so you can get versions for different platforms.

BUT IF IT'S FREE, HOW DO WE MAKE MONEY ON IT?

That's a very good question. The answer is that, just like everything else in business, making your project open source isn't for everyone. However, there are several fairly standard ways that companies are making money with open source projects.

- **Support** – companies like Redhat (*www.redhat.com*), maintainers of a popular Linux distribution, charge money for providing professional technical support.

- **Sell hardware** – companies like Digium (*www.digium.com*), the makers of Asterisk, an open source PBX software, make a great deal of their money selling pre-made PBX solutions while also providing the software to the general public for those who feel adventurous.

- **Training** – many pieces of software, whether open or closed, really benefit from people being able to go to classes in order to learn how to get the most use out of them. Who better to provide the training than the company who makes the product?

- **Custom builds** – no software will do everything that everyone wants it to do, because there are so many things that its creators never thought of. In some cases, businesses may want functionality added to the programs that you make which they are willing to pay for.

There are many other ways that companies are making money on open source software, but what it all comes down to is where you expect to make your money. If you just plan to sell your software, then open sourcing your project probably isn't for you. There are exceptions to this. MySQL, a popular open source database, offers its software for free if it is used in-house and asks that you pay a modest fee

if you include it in a commercial product. However, if your real money comes from somewhere else, then you have a decent chance of making a successful business.

WHAT DO I GET OUT OF MAKING MY SOFTWARE OPEN SOURCE?

By making your software project open source, you gain potential access to the professional development community at large. As I said before, many major open source projects are staffed partially by developers being paid by technical companies in order to add the features and functionality that their employers want. However, many professional developers work on open source projects on their own time as well for a number of reasons including to keep their skills sharp, to add new skills, and even just because the project interests them.

This means several things to anyone who wants to have a successful software project:

- **Access to outside skills** - Everyone who starts a piece of software wants the people working on it to be the best. Unfortunately, your budget often doesn't allow to you hire them and keep them full time. With open source, you can have access to people (either on a contract basis or, in some cases, just because they're interested in your project) that you otherwise wouldn't be able to hire.

- **Reduced development time** - With the possibility of more people working on your project than you could otherwise afford, there is a good chance that it will take less time to complete your project. For example, Windows Vista (formerly codenamed Longhorn) was announced years ago and isn't supposed to be delivered until sometime in 2006. By contrast, Fedora, Redhat's non-business Linux distribution, has gone from version 1 to version 4 since I first started using it in 2003, and each new version has been a marked improvement over the previous one.

- **Different points of view** - There are always useful features or uses for your software that you didn't originally think of. With members of the software developer community at-large looking at (and working on) your project, you may end up with functionality that you never considered before.

- **Many eyes looking at your project** - The more people who review the source code of your project, the greater the chance that bugs and security flaws will be caught, allowing them to be fixed sooner.

- **Community goodwill** - Never underestimate the power of free advertising. If your project becomes popular within the technical community, like Linux has, that popularity can spill over into the business arena.

WHY WOULD PEOPLE WANT TO VOLUNTEER TO WORK ON MY PROJECT?

We developers (yes, I am one of them) are strange people. We like to work on projects that we find interesting or that challenge us. It's a chance to gain experience that we can point to when looking for a new job. It's also a way to get recognized by the community as a capable developer. On top of all of those things, it's a chance for us to give something back to the people who have helped us out along the way and to help others who may not be so fortunate. Some of us think of it as a form of voluntary community service.

IF EVERYONE CAN LOOK AT MY SOFTWARE, WHAT'S TO STOP THEM FROM JUST TAKING IT?

That's a very good question, and one that I hear quite often. The answer is it all comes down to the license that you choose to release your work under. There are a lot of accepted open source licenses, so I am only going to give a brief description of a few of the more popular ones.

- **BSD** – The person who modifies the project may choose whether or not to open source their derivative, but the copyright notice for the original project must be included with the documentation (if the derivative work is closed) or in the code (if the derivative work is open). Basically, under this license, anyone can do anything with the code that they want as long as they say that the code is in there.

- **Apache** – If a software development project contains code released under the Apache license, their copyright notice and disclaimer must be included in the documentation and the source is allowed to be either open or closed.

- **GPLv2** – If the project that contains code licensed under the GPLv2 is released, all changes to the code must also be released under the GPL. This is the license used by many open source projects including the Linux kernel.

LET ME GET THIS STRAIGHT. IF I USE CODE LICENSED UNDER THE GPL, I HAVE TO RELEASE WHAT I MAKE WITH IT THE SAME WAY?

If you release the project that you incorporate the GPL'ed code in, then yes, you have to open source your project as well. If, on the other hand, you just use the software you make in-house, you don't have to publish your code. However, even if it is just in-house, you should think about whether there is actually anything to be gained by keeping people from seeing it. If the answer is not really, then consider opening it up anyway.

I LIKE THE IDEA OF THE GPL, BUT DO I HAVE TO ACCEPT EVERYTHING THAT SOMEONE OFFERS MY PROJECT?

While the GPL has a great deal of benefits that come from accepting contributions to your project (functionality and bug fixes among the big ones), at the end of the day, you're the one in control of the project and can decide who you want to be able to contribute things to it. You don't have to accept anything suspect or that you don't want to if you're in control of the project.

HOW DO I JOIN THE COMMUNITY?

The easiest way is to contribute. Start a project or work on an existing one by adding functionality or submitting patches. Sourceforge (www.sourceforge.net) is an excellent place to find or start projects. You can also join the mailing list for the project that interests you in order to communicate with the other people who are working on the project. As time goes on, you will be able to take on more responsibility on that project, and thus in the community, if you want.

I hope this article helped answer most of the questions that you had concerning open source for your business. As I said at the beginning, this was just a brief overview of what open source is and how it can work for you. If you have more questions, there are a great deal of places that you can turn to. One of the best of these is your local Linux User's Group, many of which can be found via Linux.org's list of user's groups located at *www.linux.org/groups/*.

JAMES HOLLINGSHEAD IS THE EXECUTIVE EDITOR FOR O3 MAGAZINE. JAMES IS BASED OUT OF CHILLICOTHE, OHIO. JAMES CAN BE REACHED VIA EMAIL AT JAMES@O3MAGAZINE.COM.

"... LINUX, ISN'T THAT FOR BANKS? I DON'T NEED THAT KIND OF SECURITY!" -- INTERNET CAFE OWNER

Several years ago I was asked to put together a quote for an Internet cafe on the west coast of Ireland. Several local and national computer retailers had already quoted but were too high for this very small startup run by a business lady who had no computer experience at all.

The owner was concerned about Windows and connecting Windows to the Internet because of security. I put together two quotes, one for Linux desktops and one for just securing the Windows desktops with a Linux based firewall / router.

What was interesting about this particular experience was that the business owner didn't want anything to do with Linux, not because it "looks different" but because it was "too secure". She felt that she didn't need that level of security and that Linux solutions were really for banks.

Five years later, this particular individual got in contact with me through one of my previous employers. Her network of Windows desktops were being constantly compromised by both local students and remote users.

Turns out that a national computer company sales rep told her Linux was for banks, this type of sales rep FUD resulted in a solution thats cost more and in the long run failed. **-- Comments from the Editor**

Is your data center cramping your style?

Growth always seems like a good idea. An extra processor here—one more server there. Until, all the sudden your data center feels as crowded as a center seat in coach. Let **the Penguin** upgrade you. Penguin Computing introduces BladeRunner™ 4140 the industry's densest Linux blade server. It comes with the AMD Opteron™ HE processor, which offers simultaneous 32- and 64- bit computing. So now you can pack 48 cores into a miniscule 4U of rack space, and optimize your data center. And put that 8GB of PC3200 RAM per blade to work and run your 64-bit apps in a fraction of the space. So go ahead. Stretch your legs. Tilt your seat back. **Love what you do.**

Visit www.penguincomputing.com

Join us at the Supercomputing Conference 2005 in Seattle, Washington State and Convention Trade Center, Booth #6222

AMD 64 Opteron

MultiLayer Switching in Linux

LINUX HAS HAD SOME FORM OF BRIDGING AND VLAN SUPPORT IN IT FOR AWHILE

MULTILAYER SWITCHING, SPANNING TREE AND OTHER ADVANCED SWITCHING FEATURES ARE NOW POSSIBLE

BY JOHN BUSWELL

At first glance LISA, the Linux Switching Appliance project looks like a very interesting project, providing Layer 2/3 packet switching support to Linux. Originally we planned to write an article specifically on LISA, unfortunately, we quickly discovered that LISA is still very much in a developmental stage, so this article has been expanded to cover the wider range of switching solutions for Linux. This is an introductory article, over the coming months the NETWORKING segment of O3 will go into detail on implementing various networking solutions in Linux and using open source projects to test and extend the security of traditional network protocols.

We tested LISA under Linux 2.6.10, it consists of a kernel patch providing the “Ethernet Switch” module under Networking Options and a couple of userspace tools. The project provides a mini-distribution, however all you really need is the patched kernel and the swctl userspace tool that is provided by the project.

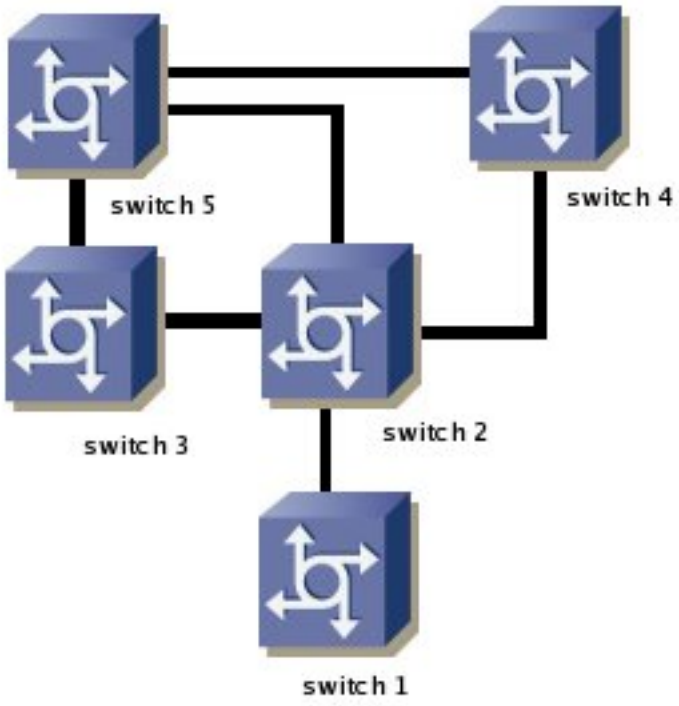
The swctl tool allows you to add/remove interfaces from the switch, add/remove vlans from the vlan database, create trunks and create virtual interfaces for a given vlan. We tested its layer 2/3 switching capabilities, performance was pretty good and the switches forwarding database worked as expected. Interoperability with other VLAN speaking devices seemed to work well, we tested LISA connected to Cisco Catalyst 5505 and Nortel 3408 Application Switches, layer 2 and layer 3 connectivity over the VLANs, and VLAN routing worked.

The downside to this project is clearly its future, the last release was back in June 2005, and it looks like a final year project for two Romanian students. If you plan to seriously consider using LISA, despite the sponsors, I would wait and see if the project continues development unless you plan to maintain the code yourself. At the time this article was written the latest release of LISA requires some patching to work with Linux 2.6.14. The userspace tools are hard-coded, so you have to modify the path to the Linux header files in each Makefile, and with changes to the skb code in 2.6.14, you will need to modify the calls to deliver_skb() and other possibly other skb routines that the switching code uses.

Overall, LISA has a good deal of potential, whether its current developers plan to continue development beyond University remains to be seen. LISA can be obtained from *http://lisa.ines.ro/*.

SPANNING TREE PROTOCOL (802.1D)

Most enterprise layer 2 switches support IEEE 802.1d “Spanning Tree Protocol”, while LISA itself doesn't provide STP, the Linux bridging suite (*http://bridge.sourceforge.net*) does provide good STP support. STP allows multiple bridges to work



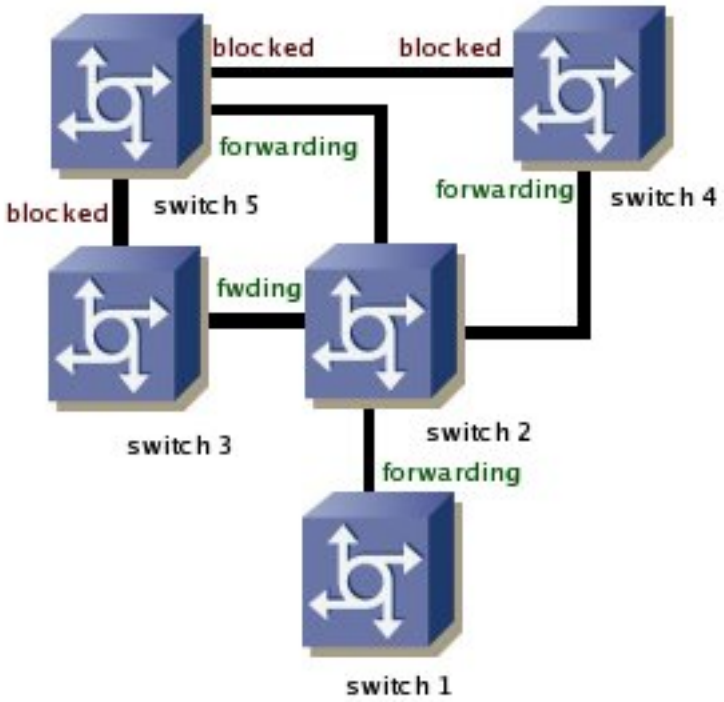
STP.1 EXAMPLE SPANNING TREE NETWORK

together by providing path redundancy while eliminating loops in the network, it is a Layer 2 protocol. STP works by sending out a special packet called a BPDU (bridge packet data unit) communicating with other bridges to discover how each is interconnected. The exchange of BPDUs results in the election of a root bridge. This is called spanning tree convergence. Once an STP has converged, each bridge sets a link to either a FORWARDING or a BLOCKED state. It is this determination of BLOCKED or FORWARDING when multiple active paths exist between bridges that prevents loops in the network. Spanning tree loops are not a good thing, they can flood the network, and more often than not lead to network failure. The best way to describe the BLOCKED state is that it is an active link sitting in standby

In diagram stp.1 we have 5 switches, during convergence a "root bridge" is elected through the exchange of BPDUs as mentioned above. Once the root bridge is selected, all links not required to reach the root bridge are placed into a BLOCKED state. In our diagram, switch 2 is best candidate for becoming the root switch. You can see how convergence plays out in that situation in the second diagram stp.2.

Spanning tree does not have any authentication, and a degree of trust must be assumed for each bridge/switch participating in the spanning tree. While this is typically a non-issue for switched environments, when considering the use of STP support on a Linux system through the bridging suite, you need to make sure that you don't create the capability of a remote attacker injecting STP BPDUs into your network either by compromising the bridge or the bridge simply forwarding packets received, this is especially important when bridging between a private network and the Internet or public WiFi network. STP filtering is possible with ebtables (*http://ebtables.sourceforge.net*) as part of the bridging suite.

There are two "extensions" to Spanning Tree that are typically of interest these are 802.1w and 802.1s. 802.1s is multiple spanning trees and implements spanning tree groups. A number of companies offer Layer 2 / Layer 3 switching solutions as proprietary solutions that work under Linux, one such company is ipinfusion (*www.ipinfusion.com*). At the time of this article, no open source 802.1s project was found. 802.1w is the rapid reconfiguration of spanning tree,



STP.2 SWITCH 2 AS ROOT BRIDGE / CONVERGENCE COMPLETED

often called rapid spanning tree, fast spanning tree or fast convergence. 802.1w becomes important in larger more complex switched environments where traditional spanning tree convergence can take a longer period of time due to the complexity of the network. 802.1w support is planned for the Linux bridging suite, and an RSTP library and simulator exist over at *http://rstplib.sourceforge.net*.

LAYER 2 FILTERING, EBTABLES, VLANS AND VMPS

An important part of the bridge suite is ebtables, ebtables is essentially the iptables for the layer 2 world. ebtables can filter ethernet protocols, mac addresses, simple IP headers, arp headers, 802.1q, interfaces. It can also perform MAC address translation, logging, frame counters, mark and match frames.

Another important part to Ethernet switching is VLAN support. Linux has decent 802.1Q support. VLAN (Virtual LAN) creates a logical Ethernet broadcast domain, this enables a switch for example to have multiple devices in different networks plugged into the same switch, and behave as if you had a separate switch for each network.VLANs in Linux are relatively easy to setup, you just mark the interface (eg. eth0) as up, then use the vconfig utility to add the interface to a particular vlan. Linux sees

the vlan as a typical network interface, you can assign an IP to it and so forth. Some network drivers in Linux need specific patches to make them work with 802.1Q.

VLAN Management Policy Server (VMPS) uses a special protocol called VQP (VLAN Query Protocol) to automatically determine VLAN membership based on the MAC address of the device connecting to the network. VMPS is supported on Cisco Catalyst switches, and the OpenVMPS project (*http://vmps.sourceforge.net*) provides an open source implementation.

MULTIPROTOCOL LABEL SWITCHING (MPLS)

Another type of switching is MPLS, Multiprotocol Label Switching. MPLS works by having a "label edge router" assign a label to incoming packets. Packets are forwarded along a "label switch path (LSP)" where each label switch router (LSR) makes forwarding decisions based solely on the contents of the label. At each hop, the LSR removes the existing label and applies a new label which tells the next hop how to forward the packet. LSPs provide a variety of solutions such as performance guarantees, routing around network congestion or to create IP tunnels for network based VPNs.

Linux has excellent MPLS support, there is an MPLS forwarding plane for the 2.6.x kernel, and an implemention of LDP (RFC3036). The MPLS project can be found at *http://mpls-linux.sourceforge.net* and *http://www.mplsrc.com* is an excellent source of information on MPLS if you are interested in learning more about MPLS.

TESTING LAYER 2 NETWORK SECURITY

Yersinia is a network security tool designed to take advantage of weaknesses in several protocols including Spanning Tree Protocol, Cisco Discovery Protocol, Dynamic Trunking Protocol, DHCP, HSRP, 802.1q, Inter-Switch Link Protocol (ISL) and VLAN Trunking Protocol. Yersinia is an open source project and can be found at *http://yersinia.sourceforge.net*. Next issue, we will take an in-depth look at Yersinia, and the attacks used against network protocols most enterprises have deployed in their production networks.

Yersinia provides an important tool, especially for larger companies that maintain lab duplicate environments of their production network. for testing and understanding how your network will respond to a particular attack, as well as to test new features provided by vendors designed to prevent or reduce the impact of specific attacks.

LAYER 4 SWITCHING WITH LINUX VIRTUAL SERVER

Layer 4 switching, more commonly referred to as IP load balancing, is the process of intelligently switching packets destined for a specific IP and port (TCP/UDP) to a different IP and/or ports. Essentially it is a fancy form of NAT and address translation where the destination is selected dynamically based on specific criteria, such as load balancing metrics, QoS or the health of the proposed destination. The device between the source and the target maintains state. The Linux Virtual Server project (*http://www.linuxvirtualserver.org*) provides an Open Source solution for Layer 4 switching.

For high capacity, port density or mission critical applications where higher session capability, advanced features and performance are a key factor, then proprietary solutions such as Nortel Application Switches (formerly Alteon), Cisco, F5, Foundry Networks and Radware all offer Layer 4 - Layer 7 solutions.

FURTHER READING

Linux has a good selection of projects for implementing multilayer switching. Below are a couple of useful links that were valid at the time this article was written, if you are interested in learning more about some of the concepts discussed in this article.

DYNAMIC VLANS

http://www.netcraftsmen.net/welcher/papers/switchvmps.html

UNDERSTANDING SPANNING TREE PROTOCOL

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm

LAYER 4-7 SWITCHING PRIMER

http://www.nortel.com/solutions/enterprise/enabling_tech/layer4-7/

>THIS IS **THE WAY**

TO ENSURE 99.999% RELIABILITY.

Hundreds of millions of wireless calls, billions of stock exchange transactions, 80% of the top 100 banks in the U.S., even the U.S. Department of Defense depend on Nortel.™

You'll find us wherever secure, reliable data and voice communications are critical.

>THIS IS NORTEL™

www.nortel.com/enhance

Reported customer availability metrics across Nortel Networks popular products exceeds 99.999%, August 2004.

Open Source Telephony

OPEN SOURCE TELEPHONY IS RELATIVELY EASY TO SETUP AND CAN SAVE YOUR BUSINESS THOUSANDS

SMALL BUSINESSES CAN NOW DEPLOY ADVANCED VOICE SOLUTIONS WHEN THEY WERE PREVIOUSLY COST PROHIBITIVE

BY JOHN BUSWELL

The Private Branch Exchange (PBX) is a critical component for any business regardless of size. The PBX provides a private, company owned telephone exchange which can drastically reduce the cost of services required from the telephone company. Traditionally, PBX systems have been expensive and required specialized technicians to deploy. However, that has changed with the dawn of Open Source Telephony and the digital PBX. The PBX takes a limited number of trunk lines from the business to the phone company's central office (local exchange), and enables them to be shared among the phone equipment within the company. Through the use of IP telephony and Virtual Private Networks (VPN) it is possible to connect and share PBX solutions at different company offices. This article will introduce you briefly to some of the terms, discuss a solution, the cost saving benefits and various open source projects.

T1, E1, J1, FXO AND FXS

Connecting your PBX to the public phone system will either involve a regular RJ11/PSTN (phone jack) connected to an FXO port, or some form of channelized trunk from the phone company. In North America these trunks are called T1, the equivalent of 24 phone lines (channels). In Europe they are called E1 (32 channels) and in Japan J1 (24 channels). An FXS port is a port on your PBX that you would connect a regular analog phone to. The FXS port generates the voltage on the wire to operate the analog phone.

VoIP

Voice over IP is analog audio (phone) converted to a digital format and distributed over an IP network to a destination. There are a number of different protocols that can be used to achieve VoIP; for the most part we will focus on SIP (Session Initiation Protocol) and IAX (Inter Asterisk Exchange) in our VoIP series.

Cisco has a proprietary protocol called SCCP (Skinny) and there is also H.323. Most Cisco IP phones support SIP, however they are typically shipped with SCCP software loaded.

HARDWARE

Digium (*http://www.digium.com*), the company behind the most popular open source PBX software, Asterisk (*http://www.asterisk.org*), provides a number of hardware options for connecting your open source PBX to the phone company. If you are a small business without the need for too many lines, then the TDM400 is a nice modular card that allows you to mix and match up to four modules (FXS or FXO) per card to meet your needs. They also supply T1/E1/J1 cards, single, dual and quad port cards. In addition to Digium, Sangoma Technologies (*http://www.sangoma.com*) also sells several Asterisk compatible channelized cards. Using the TDM400 cards you can also connect regular analog telephones to your PBX. Alternatively, you can use many of the available VoIP phones or ATA units on the market today. ATA (Analog Telephone Adapter) is essentially a small embedded device that converts VoIP to analog, similar to having a small system running asterisk and a TDM400 with FXS ports to drive your analog phones from a VoIP network. You will also need a server to act as your PBX with the appropriate hardware (discussed above) to connect to the phone company, as well as the appropriate hardware to connect either to your VoIP network or your analog phones.

ASTERISK

At the heart of the Open Source PBX, we have Asterisk. Asterisk is a fully featured PBX, providing all the features of traditional PBX systems, such as call queuing, conference bridging, voice mail and much more. There is a full list of features available on the Asterisk site (*http://www.asterisk.org/features/*). If you are using the Digium hardware you need to download the

zaptel suite as well as asterisk. The zaptel suite provides kernel drivers for the Digium hardware. Compiling asterisk is relative easy. Once uncompressed, it only requires a simple make; make install. It is important to read through the security material on Asterisk. Not only do you have to focus on the security of the server on which Asterisk resides, but you must also consider the security of Asterisk itself, and to make sure that inbound dialers (or restricted outbound dialers) don't have the capability to make toll calls or otherwise access parts of Asterisk via the phone system that would be undesirable. Configuring Asterisk is an involved process, well beyond the scope of this article. O3 will look at configuring Asterisk in depth in few issues.

EXAMPLE DEPLOYMENT

In the figure opposite, we have a sample deployment consisting of two office locations and a remote telecommuter. The first site is based in Cincinnati, Ohio in the United States, while the second site is located in Dublin, Ireland. The first site is connected via a T1 trunk (24 channels) to the local 513 area code, while the second site is connected via four standard PSTN lines to the local exchange in Dublin. Both sites are using Linux servers running Asterisk and are connected to the Internet via a high speed broadband connection.

For the sake of this example, lets say that the Dublin office is a sales office, while the Cincinnati office contains technical support staff. The company wishes to provide technical support from the Cincinnati office to customers in the Dublin area. This would be an expensive project to complete using traditional technology, however with Asterisk and Open Source technologies it is possible to implement this with relatively low costs to the company.

The two offices can be connected together using OpenVPN (http://www.openvpn.net), providing a secure transport for the communication between the two PBX systems. Asterisk comes with its own exchange protocol called IAX; alternatively you can run SIP as well. While IAX2 does have PKI style authentication and trunking, it won't protect the contents of your calls from being sniffed off the wire, so utilizing a VPN technology when routing private calls between offices over the Internet is your best bet.

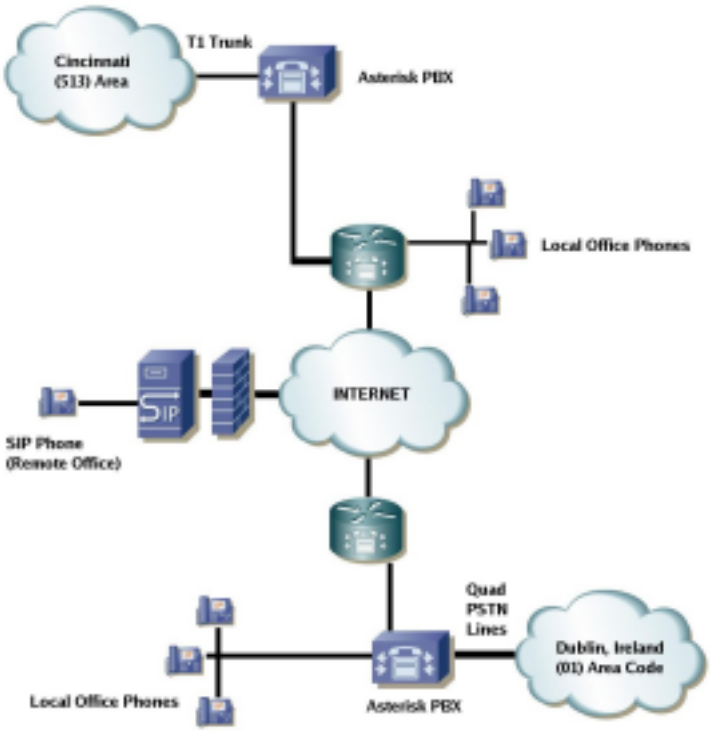
Once configured correctly, a client calling the local office in Dublin (local call), now has their call routed upon selecting the support option over the Internet to the Cincinnati support queue. Now the company can benefit from the expertise it has established locally in Cincinnati area to its Dublin customers, without requiring the customers to call long distance.

In addition, staff at the Dublin office can call, conference and perform a wide range of other tasks as if the Cincinnati location was local, and vice versa.

The example shows a remote worker. This might be an on call technical support engineer to cover the early morning business hours in Europe from their home. Here the engineer connects to the Cincinnati office via VPN, and has a firewall in place to protect their local network. The firewall is also running a SIP Proxy, which allows the SIP / soft phone to register with the Asterisk PBX while remaining behind its firewall.

SIP PROXY

Siproxd (http://siproxd.sourceforge.net) and PartySIP (http://www.nongnu.org/partysip/) are two open source SIP proxies. A SIP proxy handles registration of SIP clients on a private network and performs rewrites on the SIP messages to make



SIP connections possible through a firewall providing NAT (Network Address Translation). SIP (Session Initiation Protocol) is defined by RFC 3261 and is one of the protocols used by software and VoIP phones. The alternative approach is a method called STUN which enables a SIP client to determine the public IP address, but for this to work a wide range of ports must be opened on the firewall. Instead, projects such as siproxd actually perform layer 7 packet inspection and rewrite on the SIP packets sent through the proxy.

ASTLINUX

AstLinux (*http://www.astlinux.org*) is a custom Linux distribution centered around asterisk. AstLinux provides an out of the box solution with a wide range of features, making it a useful solution for a quick embedded or commercial Asterisk installation. With a little effort, it can be easily modified to fit almost any situation. The project provides a number of useful images, including a bootable ISO image. The project is geared towards using older Pentium-MMX, and embedded solutions such as the Soekris line of embedded devices. If you're looking to provide a large solution with multiple T1 lines, multiple IAX trunks and large amounts of space for IVR/Voice mail solutions, selecting your favorite enterprise Linux distribution and installing Asterisk from source might be a better approach.

ASTERISK@HOME

Asterisk @Home, which can be found online at *http://asteriskathome.sourceforge.net* is a fast and simple solution for getting Asterisk up and running quickly. Asterisk @Home is a Linux distribution that utilizes CentOS (*www.centos.org*) and provides a web based interface for configuring and managing Asterisk. The solution includes another project AMP (Asterisk Management Portal) which can be found at *http://coalescentsystems.ca/index.php.* AMP is web based with a flash operator panel. It provides a wide range of management tasks. If you want to get Asterisk running quickly without going in-depth, Asterisk @Home is a great solution.

ENUM, E.164 AND DUNDI

ENUM is essentially DNS for your telephone number. E.164 is an international telephone numbering plan administered by the ITU, which provides the format, structure and administrative hierarchy of telephone numbers. A fully qualified E.164 number contains the country code (eg. +353 for Ireland), area code and phone number for the destination. ENUM provides essentially reverse DNS mapping on the phone number, to convert that number to an IP address that would typically be able to handle call routing to that number (eg. a SIP proxy run by the phone company that provides PSTN service to the particular area code in that country).

DUNDi is a distributed peer to peer system for locating Internet gateways to phone services. DUNDi is a distributed solution with no centralized authority as with ENUM. DUNDi is a routing protocol so that services maybe routed and accessed using industry standard VoIP technologies such as IAX, SIP or H.323.

DUNDi provides a solution that enables the creation of highly available enterprise PBX solutions, where no one PBX creates a central point of failure. DUNDi also provides an Internet based E.164 peering system, for more details review the documentation and members at *http://www.dundi.com*.

SIPX

sipX (*http://www.sipfoundry.org/sipX/sipXuser/*) is an Open Source PBX solution based on SIP. sipX provides many of the PBX capabilities of asterisk such as DID, Hunt groups, Call forwarding, voice mail and so on. sipX doesn't provide any gateway capabilities with the PSTN, it is a pure SIP IP PBX solution. It has some interesting features such as XML based call routing and the ability to configure attached phones and gateways.

SIP EXPRESS ROUTER

The SIP Express Router, is a high performance configurable free SIP server which can act as a proxy, redirect or registrar server check it out at *http://www.iptel.org/ser/.* There is also the OpenSER project at *http://www.openser.org/***.**

RUBY ON RAILS INTEGRATION

Next issue a look at web integration with Asterisk using ragi (*http://ragi.sourceforge.net*).

DUNDi, IAX and Asterisk are trademarks of Digium Inc. (*http://www.digium.com*).

O3: The Open Source Enterprise Data Networking Magazine

Advertise in O3

"Right now your competitors are selling Open Source Solutions to YOUR customers.. why aren't you?"

O3 Magazine is a powerful means for promoting your business solutions and services. Due to its design, content and distribution, O3 can offer your business unique visibility to decision making enterprise customers.

O3 offers a flat fee, first come, first serve advertising solution. Discounts are available for long term commitments, small businesses, and free advertising is available to open source projects.

Full page rate is $1,000.00 (US Dollars, excludes OH sales tax)

Issue 2 Deadline: November 30th 2005

Contact sales@o3magazine.com

Deploying Wifidog -- The embedded Captive Portal

WIFIDOG IS A C BASED CAPTIVE PORTAL DESIGN FOR THE LINKSYS WRT54G BUT RUNS ON ANY LINUX PLATFORM. IT PROVIDES ACCESS CONTROL, BANDWIDTH ACCOUNTING AND MUCH MORE

BY JOHN BUSWELL

Wifidog is a lightweight captive portal solution designed to run on embedded devices such as the LinkSys WRT54G. The LinkSys WRT54G and WRT54GS are low cost wireless routers from LinkSys that run Linux. These devices can run alternative firmware, be careful because running such firmware will VOID YOUR WARRANTY. However most retail outlets have these routers for under $70, so it is not too much to risk.

OpenWRT is the alternative firmware choice for running open source applications on the WRT54G, from this point on I'll refer to the WRT54G/GS as AP (access point). Building OpenWRT is relatively easy, you simply download the latest release from www.openwrt.org, uncompress, run make menuconfig, run through the menu options to suit your needs, then run make. From that point on its pretty much automated, you will need an Internet connection, broadband is recommended due to some larger downloads such as the Linux kernel.

Why would you want to risk your warranty over some free software, surely Linksys has the best firmware? Well Linksys have the product designed for your average user, which works great, but the hardware platform is extremely flexible running OpenWRT. Once you have OpenWRT on there you are free to upload almost any open source application that will compile and fit on the hardware. You might want to run a SIP phone behind the wireless router, well with OpenWRT you can load siproxd onto the Linksys along with iptables and thats it. As you start to use OpenWRT more, you'll see exactly how flexible and how great it is to be able to add new capabilities to your network.

WHAT IS A CAPTIVE PORTAL

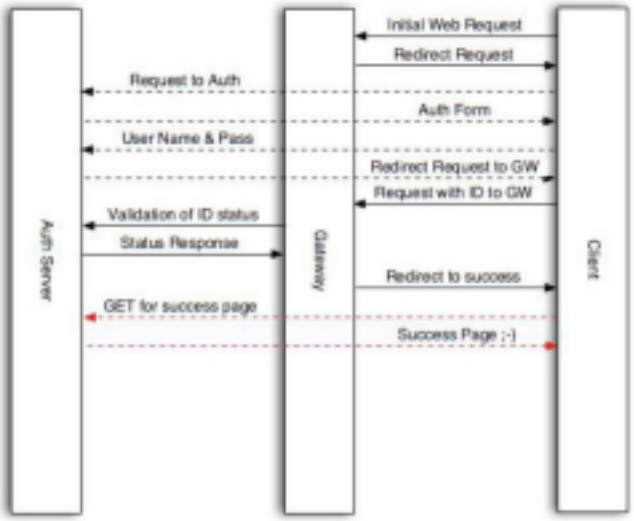
A captive portal is essentially a means to prevent a user from accessing network resources (mainly the Internet) until they have authenticated with a server. Typically a captive portal is used at wireless hotspots, allowing the user to log in, authenticate and use the network as their privileges allow. The user doesn't have to know a particular address, when they attempt to use their browser they are transparently redirected to the authentication page.

Wifidog is interesting in that it is lightweight enough to run directly on low cost wireless hardware such as the AP, and checks network activity rather than using a javascript window. Thus allowing PDA, Cellphones and Sony PSPs to utilize the resources.

HOW DOES WIFIDOG WORK?

The solution works by using firewall rules to control traffic through the router. When a new user attempts to access a web site, the wifidog component on the AP will transparently redirect the user to the auth server where they can either log in or sign up. The auth server and the wifidog component on the AP will negotiate how to handle the client, whether to permit or deny certain network access. The AP talks to the auth server periodically to update statistics such as uptime, load, traffic per client and to act as a heartbeat.

The flow diagram below illustrates the process that Wifidog utilizes (courtesy of ile sans fil (*www.wifidog.org*)).



The client does his initial request, as if he was already connected, (e.g.: *http://www.google.ca*)

- The Gateway's firewall rules mangle the request to redirect it to a local port on the Gateway. When that's the done, the Gateway provides an HTTP Redirect reply that contains the Gateway ID, Gateway FQDN and other informations
- The Client does his request to the Auth Server as specified by the Gateway
- The Gateway replies with a (potentially custom) splash (login) page
- The Client provides his identification informations (username and password)
- Upon succesful authentication, the client gets an HTTP Redirect to the Gateway's own web server with his authentication proof (a one-time token)
- The Client then connects to the Gateway and thus gives it his token
- The Gateway requests validation of the token from the Auth Server
- The Auth Server confirms the token
- The Gateway then sends a redirect to the Client to obtain the Success Page from the Auth Server
- The Auth Server notifies the Client that his request was successful

GETTING OPENWRT ON THE WRT54G/GS

OpenWRT takes some time to compile, once it is done, if you haven't run OpenWRT previously you need to do some work on your router first. The AP by default starts out on *192.168.1.1/24*. The easiest way to configure the router is if you have a second ethernet interface in your Linux workstation, connect the AP on port 1 to the second ethernet interface, and use **ip link set eth1 up ; ip addr add 192.168.1.10/24 dev eth1** to configure it. Next do a quick **ping 192.168.1.1** to make sure that you can see the AP. Now simply point a browser at *http://192.168.1.1* and use admin/admin as the username / password. This is the default for the AP. The first thing you need to do is check the firmware version, this is displayed in the upper right hand corner. For the AP we used the version was 3.37.7 but we needed 3.37.2 to enable the boot_wait option on the AP to install OpenWRT. A quick download from LinkSys, then follow the Administration -> Firmware upgrade option. Unzip the file from LinkSys, and in this case we used WRT54GS_3.37.2_US_code.bin to downgrade the router. Simply select browse, select the file and select upgrade.

Click continue once it completes, now you should see 3.37.2 (or 3.01.3 if you are using a WRT54G v3.0). Refer to the OpenWRT documentation for details and specific version numbers as they tend to change periodically.

In order for the OpenWRT installation to proceed we have to enable the boot_wait option in the firmware, this tells the AP to check for TFTP prior to loading the actual firmware, which gives us the opportunity to feed the AP, a OpenWRT image. The hack is relatively simple, just paste each line in turn below and select the ping button after each paste in the address part of the ping web tool in the LinkSys firmware. If you did it correctly, you'll see an output of NVRAM at the end of the last ping. You must configure a static IP address on the Internet interface before trying this, otherwise it won't work. You don't need link up, just a configured IP on the Internet (WAN) interface.

;cp${IFS}*/*/nvram${IFS}/tmp/n

;*/n${IFS}set${IFS}boot_wait=on

;*/n${IFS}commit

;*/n${IFS}show>tmp/ping.log

When OpenWRT completes its build, the images are stored in bin/. Simply figure out the correct one for your hardware, then use tftp to transfer it. Remove the power from the AP, then issue:

tftp 192.168.1.1
tftp> binary
tftp> rexmt 1
tftp> timeout 60

tftp> trace on
tftp> put openwrt-version.bin

[Now Power Up the LinkSys WRT54GS]

Give it a few minutes, as OpenWRT has to go through a few hoops before the AP will respond to pings. Now telnet to 192.168.1.1 once it responds to pings and you should see the OpenWRT banner. If you use the squashfs image, you need to follow the commands in the OpenWRT docs to remove the /etc/ipkg.conf symlink and copy the actual file from rom. You may also need to use the nvram command to set the wan_ipaddr and wan_gateway options in the firmware. Removing /etc/resolv.conf and creating the file manually will also be required.

GETTING WIFIDOG ON THE WRT54G/GS

Next to download and install wifidog simply:

cd /tmp
wget http://old.ilesansfil.org/dist/wifidog/wifidog_1.1.1_mipsel.ipk

ipkg install wifidog_1.1.1_mipsel.ipk -force-overwrite

The **-force-overwrite** is required if you are running a later version of OpenWRT with iptables as wifidog tries to install two ipt extensions that iptables has already installed.

Now the wifidog client is installed on the AP. Edit /etc/wifidog.conf, and run wifidog -f -d 7 (debug mode). The configuration file is well documented and self explanatory.

WIFIDOG QUICKSTART CONFIG

This is not intended to provide a production configuration, but a quick start guide on what to setup in the config, bare minimum to get wifidog running. Edit the GatewayID to match your Auth Server configuration

```
ExternalInterface vlan 1
GatewayInterface br0

AuthServer {
 Hostname auth.mydomain.com
 SSLAvailable yes
 Path /
}

CheckInterval 60
ClientTimeout 5

...
```

Leave the firewall rules to the default. Next configure the Auth Server, and then start wifidog on the AP.

AUTH SERVER

PostgreSQL, Apache and PHP 5 are required to get the Auth Server running. You install this on a local Linux box (not the AP). Simply download the auth server, make sure you have all the prerequisites listed in the INSTALL file available, copy the wifidog directory to your web server, plug the url into your browser (e.g. *http://wifidog.mycompany.com/wifidog/install.php*) and go through the steps.

TESTING

Now simply connect a WiFi device to the AP, try to browse somewhere and if you correctly configured wifidog you'll be presented with the captive portal sign-up / login page.

FURTHER READING

OpenWRT
http://www.openwrt.org

Wifidog
http://www.wifidog.org

NoCat
http://www.nocat.net

LinkSys
http://www.linksys.com

Spliced Networks LLC

The next stage in server evolution is coming ....

11.28.2005

are you ready ?

http://www.splicednetworks.com

Intrusion Detection

INTRUSION DETECTION SYSTEMS (IDS) MAKE UP AN IMPORTANT PART OF ANY NETWORK SECURITY POLICY

WHY DO YOU NEED IDS, WHERE DO YOU PUT IDS AND HOW DO YOU DEPLOY IT?

BY JOHN BUSWELL

An *Intrusion* is unauthorized network or system activity on your servers or networks. Intrusion Detection is the art of detecting this unauthorized activity amongst legitimate network traffic by sifting through the data flowing across your network. This article focuses on Network Intrusion Detection Systems (NIDS), another form of IDS is Host Intrusion Detection Systems (HIDS). The difference is primarily that the latter focuses on the protection of just one system. There are advanced solutions such as distributed IDS and IDS load balancing, these will be discussed in dedicated articles later in this series on IDS.

Some businesses feel that complex IDS solutions are overkill because they operate a small business that nobody is going to be concerned with. However, these days, it is the computing resources and your bandwidth to the Internet that attackers want, not necessarily your intellectual property or to disrupt your business. Think of attackers as network "car-jackers", they don't care who you are, they just want your "car". An IDS solution will help detect signs that someone is looking or trying specific exploits against your infrastructure in an attempt to gain further information or access.

There is one aspect of IDS that is often overlooked by technical staff and that is the legalities of performing Network IDS. In many countries there are strict wire-tapping laws and regulations, if you do not already have an IDS in place, especially for small and medium sized businesses it is always worth consulting with a legal expert to determine what laws and regulations you must abide by, as this may determine what you must disclose to employees, customers and how IDS information is reported.

Snort is the de facto standard for intrusion detection / prevention systems. Snort utilizes a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. Snort is the most widely deployed IDS technology in the world. If you want to do network IDS, then Snort is the way to go. Snort supports IP defragmentation, TCP stream reassembly and stateful protocol analysis. This article is going to briefly introduce Snort to you, how to attach it to your network and where to look next. As the series progresses, we will look at advanced techniques such as defragmentation, custom rules and much more.

ATTACHING SNORT TO YOUR NETWORKS

Before going into compiling and configuring snort, it is important to understand that Snort, like other Network IDS solutions must be attached to your network at the correct location, otherwise the effectiveness of the IDS solution is reduced. Typically the best location for small and medium sized businesses is to monitor links to/from the Internet. In a switched environment the router(s) to the Internet are connected to a switch port or VLAN, most enterprise grade switches support whats called port mirroring, or for Cisco users "SPAN". This allows you to configure the switch to take port or vlan traffic and duplicate it out a mirroring port. The downside to port mirroring is that on some switches under heavy load you can seriously impact the performance of the switch, also if the traffic you are trying to monitor exceeds the capabilities of the mirroring port, you will not be able to mirror all packets at high network utilization.

Another option is to insert a hub in-line, and attach the IDS to the hub, allowing normal traffic to flow across the hub. The downside to this method is that data loss occurs due to collisions at high bandwidth utilization, it creates an additional single point of failure and you will lose full-duplex capabilities. A more expensive option is to use network taps, taps are discussed in length at *http://www.snort.org/docs/#deploy.* Cost, multiple NICs and slightly more complex installation due to the addition of channel bonding in order to do stateful analysis are the downsides to using network taps.

For a typical small or medium business network, where LAN bandwidth utilization is low, and the IDS is focused on low-bandwidth Internet links, a switch capable of port mirroring should be sufficient. With larger networks the cost of a tap is less cost prohibitive.

GETTING SNORT

The latest version of snort at the time this article was written is 2.4.3. Before installing snort, you may have to install pcre (Perl Compatible Regular Expressions) required by snort. Both pcre and snort support the usual POSIX *./configure ; make && make install*. If you're not building from source, you'll need to check if snort is available for your Linux distribution.

Once built and installed, we can do a couple of check tests of snort in sniffer mode. Running *./snort -vde* should dump real time packet date out to the local terminal, hit ctrl+c to stop it, and scroll up to make sure its working. Snort will also log packet data for you, *./snort -l /tmp/testlog -b* (assuming you have created a /tmp/testlog directory) will log the packets, which can then be read back via Ethereal or snort itself using *./snort -dv -r packet.log*.

SNORT IN-LINE

Snort supports integrated intrusion prevention system capabilities with the snort_inline feature. This feature receives packets from iptables instead of libpcap and then applies rules to help iptables accept or drop packets based on Snort rules. We will look at Snort's IPS features in a future article.

CONFIGURING SNORT

Since the purpose of this article is to introduce snort. The config file for snort is located in /etc/snort.conf if you installed from source, you'll need to copy it from ./etc/snort.conf in the source tree. The configuration file is fairly straight forward, to get running simply configure the HOME_NET to match your local network, you may also want to tweak the rulesets depending on the rules you are using. Modify RULE_PATH to /etc/rules or your own customized path. In addition to snort.conf, you will need to copy classification.conf, reference.conf and unicode.map to /etc. These are all in the ./etc directory in the source tree.

RULES

At the heart of snort are the rules. Without the rules Snort becomes quickly outdated and is less effective. There are four different sets of rules distributed for Snort. The Community Rules are available for free and are distributed under the GPL. The other three sets are variations of the Sourcefire VRT Certified Rules – unregistered, registered and subscription. The unregistered rules are updated with each major release of Snort, maybe once a quarter. The registered rules require agreeing to a licensing agreement, and are released 5 days after they are made available to subscribers. Subscribers pay a modest fee for real-time access to new rules. Once you have your rules, copy the rules/ contents over to /etc/rules unless you changed the path in the snort.conf.

RUNTIME

Snort is now ready to go, to start it up simply execute:

```
mkdir -p /tmp/testlog
./snort -d -l /tmp/testlog/ -c /etc/snort.conf
```

The /tmp/testlog directory is where snort will store its log files, you will want to monitor the alert log. Now that you are up and running, you will need to go back over the configuration files in detail, look at the Snort documentation on how to write your own rules, and tweak the rulesets to best suit your needs.

FURTHER READING

The snort.org website has a considerable amount of documentation, papers and articles that go into many different aspects of snort and intrusion detection. If you are interested in a book, Snort 2.1 Intrusion Detection by Syngress is a good way to get started quickly with snort, but doesn't cover the Intrusion Prevention features in 2.3.0 and later.

The Prelude IDS framework for integrating different IDS sources is worth a look, the project site is available at *http://www.prelude-ids.org*.

NEXT

The next IDS article will look at testing the Snort installation, automated rule updates, barnyard and Snort frontends.

>THIS IS **THE WAY**

600 MILLION PEOPLE MOVE AROUND THE PLANET.

You'll find Nortel™ in every single one of the world's top twenty airlines. And wherever secure, reliable data and voice communications are most critical.

>THIS IS NORTEL™

www.nortel.com/commerce