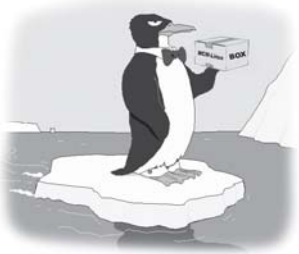
Die neue WCM Linux-Box

Der Linux Allround-Server

Wir haben weder Kosten noch Mühen noch Foreneinträge gescheut, um Ihnen beginnend mit dieser Ausgabe laufend Schritt für Schritt- Anleitungen zum und für den Linux Allround-Server bieten zu können. Stammlesern dürfte die WCM-Linux-Box noch in Erinnerung sein. Dabei handelt es sich um ein Referenzsystem, welches uns vom Einkauf über die Installation einer Distribution bis hin zur laufenden Wartung & Erweiterung begleitet und uns als Basis für alle folgenden Artikel zu diesem Thema dient. Einsteiger erhalten mit diesen Workshops eine schrittweise Einführung, Fortgeschrittene schnelle How-To's und Profis die eine oder andere Rosine zum Rauspicken. Fangen wir mit den Details zur Hardware unseres Referenzsystems an…

von Martin Müller & Ing. Christian Sudec



Vorweg noch eine Erklärung, was Sie sich, geschätzter Leser, von unserer neuen Serie erwarten können. Während Windows auf den Workstations quasi der Platzhirsch ist - was sich mittelfristig sicherlich nicht ändern wird – befindet sich Linux bei den Servern immer weiter auf dem Vormarsch. Ob nun der MP3-Server für daheim oder doch ein Datei- und Druck-Server für den Kleinbetrieb um die Ecke: mit Hilfe unserer Workshop-Serie ist jeder Computerinteressierte in der Lage, seine Anforderungen auf Basis von Linux in die Realität umzusetzen. Und da wären wir auch schon bei den zwei Möglichkeiten:

Variante A

Diese kann man in Betracht ziehen, wenn man vorhat, den zukünftigen Server für ein enges Tätigkeitsfeld zu verwenden. Beispiele sind hier Anwendungen als Router und/oder Firewall, Druck- oder sogar als CDDB-Server. Kurzum: als Kiste, die in der Ecke steht und um die man sich kaum kümmern muss.

Hierfür nimmt man am besten einen ausgedienten PC aus dem Keller bzw. eine abgesetzte Arbeitsstation aus dem Büro. Dabei erwarten wir allerdings schon einen halbwegs leistungsfähigen Prozessor, mindestens ein Pentium III oder AMD mit 800 MHz muss es sein. Weiters darf der Hauptspeicher, das RAM, nicht zu klein geraten: 256 MB, aber besser 512 MB setzen wir voraus, damit das System im Dauerbetrieb rund läuft. Und, was ganz wichtig ist: Bitte achten Sie darauf, dass so wenige Lüfter wie möglich im Rechner eingebaut sind. Außer dem Prozessorlüfter und dem Lüfter des Netzteiles sind keine weiteren Lüfter akzeptabel. Erstens damit sich der Geräuschpegel der WCM Linux-Box in Grenzen hält und zweitens bergen Lüfter immer die Gefahr dass sie ausfallen. Und wer denkt schon daran den Lüfter der Grafikkarte zu kontrollieren wenn die Box plötzlich instabil wird und alle 10 Minuten abstürzt?

Sollten Sie also einen alten PC verwenden wollen, schmeißen Sie alle unnötigen Komponenten aus der Box. Dazu gehört auch eine TV-Karte und falls vorhanden die Soundkarte. An die Grafikkarte wird so gut wie kein Anspruch gestellt, da kein ressourcenfressender Fenstermanager installiert wird und die Administration der WCM Linux-Box hauptsächlich über die lokale Kommandozeile oder über eine SSH-Sitzung von einem entfernten Rechner beziehungsweise mittels einem grafischen Webinterfaces stattfindet.

Je nach Netzwerktopologie entscheiden Sie ferner über die Verwendung von einer oder zwei Netzwerkkarten. Näheres erfahren Sie in den beiden Workshops zum Thema Netzwerk und Internet auf den folgenden Seiten. Bitte achten Sie in diesem Fall darauf dass Sie nur Netzwerkkarten mit gut unterstützten Chipsätzen verwenden, da diese bei einem Server nun mal das Um&Auf sind. Informationen dazu finden Sie z.B. unter *(www.scyld.com/network.html)*. Tipp: Netzwerkkarten um die 5,- EUR mit den kostengünstigen Chipsätzen von RealTek (z.B. 8139) sind problemlos und einfach einzubinden.

Variante B

Die zweite Möglichkeit für die Hardware ist natürlich ein kostengünstiges Neugerät. Für die jetzigen Workshops haben wir uns für diese Option entschieden, da sie einiges an Vorteilen mit sich bringt. Erstens, hält man mit einem neuen PC aktuelle und vor allem erweiterbare Technologie (inklusive Garantie) in Händen. Wenn z.B. in einem Jahr oder so die PATA-Festplatten vom Markt verschwinden oder zumindest nur noch zu Apothekerpreisen erhältlich sind, dann wünscht man sich beim wiederverwerteten PC sicherlich SATA-Anschlüsse. Gleiches gilt für Speichermodule (SD-RAM <-> DDR-RAM). Der zweite Vorteil wiegt unter Umständen noch schwerer: man kann sich sicher sein, dass die in den Workshops vorgestellten Konfigurationen 1:1 lauffähig sind. Damit wollen wir vor allem die Einsteiger unterstützen, die noch nicht in der Lage sind, einige Parameter so zu verändern, dass die WCM Linux-Box auch auf einer alternativen Basishardware problemlos funktioniert. Aber keine Sorge: Fortgeschrittene und Profis werden trotzdem in den Artikeln auf Tuning-Möglichkeiten und Unverträglichkeiten mit bestimmter Hardware hingewiesen.

Als Basis für unsere neuwertige WCM Linux-Box dient ein DI-Light 64 mit einem AMD Sempron 2600+-Prozessor der Firma DiTech Computer. Diese Maschine ist bereits um EUR 289.- erhältlich und bietet zusammen mit einer 80GB Festplatte genügend Leistungsreserven um alle zukünftigen Applikationen aufzunehmen und Dienste ausreichend schnell zur Verfügung zu stellen.

Da sich nahezu alle Komponenten (LAN, VGA, Sound) Onboard befinden, sind ebenfalls nur CPU- und Netzteil-Lüfter die einzigen Geräuschquellen. Mal sehen, ob unser Hardware-Guru Martin Schneider Ihnen in einer der nächsten Ausgaben ein paar Kniffe zu Lärmdämmung & Co präsentieren kann.

Bliebe als letzter Punkt noch das RAM zu erwähnen, wo leider ein wenig nachgebessert werden muss. Die verbauten 256MB sind nämlich eindeutig zu wenig. Ein zusätzliches 512MB-Modul verhilft in Summe zu 768MB und somit zur nötigen Performance. WCM wird auf jeden Fall noch bei DiTech nachfragen, ob hier nicht vielleicht ein günstiges Kombi-Paket geschnürt werden kann.

FAQ

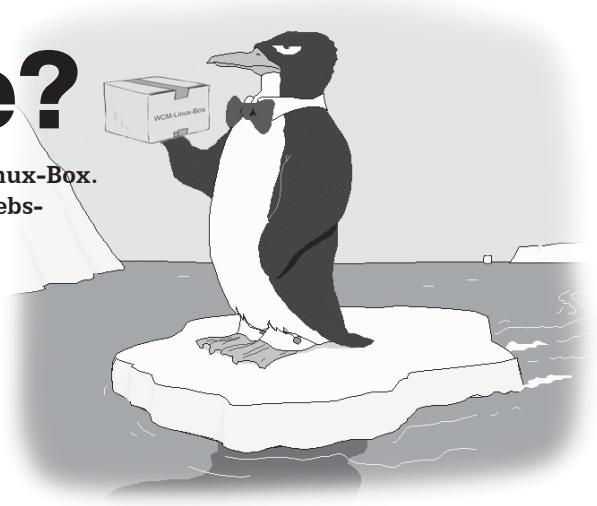
Einige Leser mögen sich jetzt unter Umständen fragen, warum wir nicht gleich einen 'gescheiten' Server ausgewählt haben. Also mit HotPlug-Fähigkeit, RAID, redundanten Netzteil und so weiter? Ganz einfach: zum einen wäre er in den Anschaffungskosten nicht mehr Privatanwender- und KMU-tauglich, zum anderen wird es eigene Workshops geben, die sich mit der Erweiterung unserer Linux-Box auseinandersetzen.

Gutes Gelingen

In diesem Sinne wünschen wir Ihnen viel Spaß mit den kommenden Workshops. ■

Die WCM-Linux-Box und Debian

Welche Software?



Die Hardware ist geklärt, jetzt geht´s an die Installation der WCM Linux-Box. Auf den nächsten Seiten erfahren Sie, wie Sie Schritt für Schritt das Betriebssystem aufsetzen und die grundlegenden Konfigurationen für Netzwerk, Festplatten, Benutzerkonto und Mailbox durchführen.

von Martin Müller

Doch zu Beginn gleich eine Warnung für all jene die von der Idee begeistert sind endlich eine riesige Mailbox zur Verfügung zu haben: Wer die Verantwortung für einen Web- und/oder Mailserver übernimmt, darf keineswegs leichtfertig agieren. Wird ein Dienst, oder gar der gesamte Rechner gehackt, könnten Ihnen durch den anfallenden Internet-Traffic Kosten entstehen, die im schlimmsten Fall auch tausende von Euro ausmachen können.

Außerdem sollten Sie sich nicht vor der Arbeit an der Linux-Kommandozeile zurück schrecken. Denn diese ist ein äußerst effektives und komfortables Werkzeug, wenn man sich erst einmal ein wenig eingearbeitet hat.

Distributions-Auswahl

Bei der Server-Software, der Linux-Distribution, fiel die Wahl auf Debian 3.1 – Sarge. Diese Distribution hat sich als äußerst stabil erwiesen, wird gut gepûegt und ist noch dazu relativ einfach zu bedienen. Alle Software-Pakete werden von den strengen Debian-Maintainern genau getestet bevor sie den Benutzern zum Download und zur Installation freigegeben werden.

Vorbereitungen

Debian Sarge können Sie direkt von der Projektseite *http://www.debian.de/CD/torrent-cd/* beziehen, eine starke Internetanbindung vorausgesetzt. Die CD-Grundinstallation hinterlässt immerhin 2.1 Gigabyte Transfervolumen. Unter dem angebenen Link finden Sie ISO-Images die Sie mittels BitTorent runter laden können. Sie benötigen nur die ersten drei Images. Sollte Ihnen BitTorent kein Begriff sein, so laden Sie bitte die CD-Images von *http://debian.inode.at:8080/debian-cd/3.1_r0a/i386/iso-cd/* oder die DVD-Images *http://debian.inode.at:8080/debian-cd/3.1_r0a/i386/iso-dvd/* herunter.

Die geladenen Images müssen Sie dann mit Hilfe von NeroExpress oder WinOnCD auf CD oder DVD brennen. Bei NeroExpress erledigen Sie dies unter dem Menüpunkt „Disk-Image oder gespeichertes Projekt“, bei WinOnCD im Menü Datei/Öffnen/ das ISO-Image auswählen und anschließend in das Feld „CD“ klicken und den Brenn-Button betätigen. Oder Sie kaufen unter www.linuxshop.de einen Satz CDs oder DVDs um wohlfeile 6.95 Euro.

Sind die Installationsmedien einsatzbereit, geht´s auch schon ans Installieren.

Die Installation

Sarge wird mit einem neuen Installer ausgeliefert. Dieser erkennt recht zuverlässig die eingesetzte Hardware, führt durch die Festplattenpartitionierung und hilft bei der Auswahl und Installation der richtigen Programmpakete. Der Installer besitzt allerdings keine grafische Oberûäche, zur Navigation wird die Tastatur benötigt, insbesondere die Pfeiltasten, die Leertaste und die Return-Taste.

Für die Box haben wir uns folgendes Partitionsschema zurecht gelegt.

Für das Basissystem soll mindestens 10 Gigabyte Festplattenspeicher reserviert werden. Davon wird sechs Gigabyte dem *root*-Filesytem zugeteilt, drei Gigabyte werden für die Partition *var* benötigt, sowie ein Gigybayte für die Speicherauslagerungsdatei *swap*.

Ran an den Rechner

Nun wirds ernst: Rechner einschalten, und im BIOS überprüfen ob das DVD-Laufwerk als erstes Boot-Device ausgewählt ist. Ins BIOS kommt man meist in dem man gleich nach dem der Rechner eingeschaltet wurde die ENTF-Taste Taste mehrmals hintereinander drückt. Je nach Bios oder Tastatur kann es auch die Taste DEL, ESC, F1, oder F2 sein. Bitte lesen Sie am Bildschirm die benötigte Taste ab. Im Bios müssen Sie dann mithilfe der Pfeiltasten zum je nach BIOS-Hersteller unterschiedlich lautenden Menüpunkt Boot Sequence, Bios Feature Setup, oder Advanced Bios Features gehen. Mit der Enter-Taste bestätigen Sie Ihre Auswahl und stellen dann die Bootreihenfolge so um, dass Ihr CD/DVD-Laufwerk an erster Stelle ist.

Ist dies erledigt verlassen Sie das Bios mit „Save & Exit Setup“.

Wenn Sie die empfohlene WCM-Linux-Box gekauft haben, entfällt dieser Schritt.

Der Rechner startet neu, nun vom Installationsmedium, und schon gibt´s die erste Auswahlmöglichkeit *„Press F1 for help, or ENTER to boot:“*. Wird hier einfach mit Return bestätigt, wird Debain mit dem alten Kernel der Versionsreihe 2.4 installiert. Wir setzen einen modernen Kernel der Reihe 2.6 ein, deshalb muss in der Befehlszeile *linux26* eingegeben und ebenfalls mit Return bestätigen werden.

Nach Auswahl der Sprache (German - Deutsch), des Landes (Österreich) sowie des Tastaturlayouts (Deutsch) wird die automatische Hardwareerkennung gestartet. Kommt es zu Problemen bei der Hardwareerkennung und der Rechner friert ein, sollte man im BIOS das *Memory Hole* 15 bis 16 MB deaktivieren und das *Advanced Power Management* auf *ACPI* stellen. Der Installer durchsucht anschließend das Installationsmedium und lädt weitere Komponenten nach.

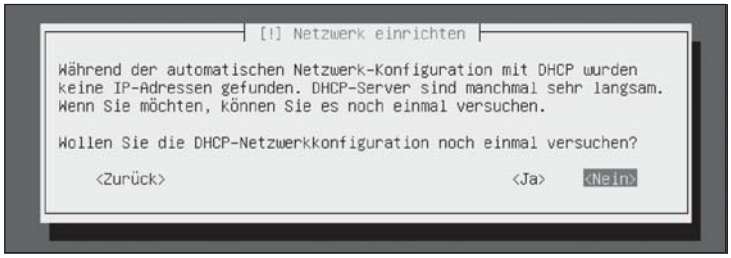
Nun folgt die Netzwerkerkennung. Wenn es schon einen existierenden DHCP-Server, etwa einen Hardware-Router mit entsprechender Funktion gibt, dann wird der Netzwerkkarte eine IP-Adresse zugewiesen. Um dies zu unterbinden, schließlich soll die WCM-Linux-Box erster Ansprechpartner für benötigte Services werden, ist der Rechner erst mal nicht mit dem bestehendem Netzwerk zu verbinden. Also Netzwerkkabel abgesteckt lassen!

Netzwerk einrichten

Wir wählen die Option „Netzwerk manuell einrichten“ und weisen der ersten Netzwerkkarte eine private IP-Adresse aus dem Bereich 192.168.x.x zu. Wir gehen davon aus, dass es noch kein bestehendes Netzwerk gibt, weshalb keine Rücksicht auf bereits vergebene Adressen genommen werden muss. Das interne Netzwerkinterface bekommt also die Adresse 192.168.123.1 zugewiesen, die Netzwerkmaske lautet 255.255.255.0. Die Frage der IP-Adresse des Routers zu beantworten ist je nach Internetprovider und Anbindung unterschiedlich. Wir lassen dies hier leer und auch der Gateway-Eintrag wird leer gelassen, es wird an anderer Stelle in dieser Ausgabe darauf eingegangen (Artikel „Die WCM-Linux-Box geht online“).

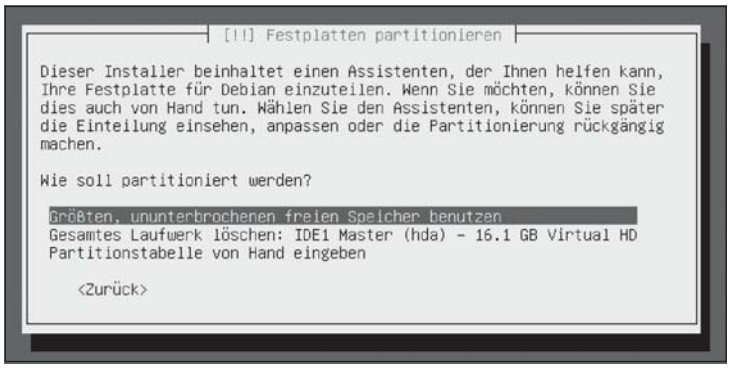
Anschließend müssen die IP-Adresse der Nameserver eingetragen (DNS-Server) eingetragen werden. Hier ist in den Unterlagen des Providers nachzulesen. Sind mehrere Nameserver verfügbar, so können diese nacheinander, getrennt durch ein Leerzeichen, eingetragen werden.

Nun wird noch ein Hostname abgefragt den man frei wählen kann, der Domainname muss schon jetzt gut überlegt und richtig eingetragen werden, soll der Rechner später als Web-Server im Internet dienen. Soll der Rechner nicht als Web-Server fungieren, dann bleibt der Domainname Geschmackssache. Sämtliche Informationen zum Netzwerk werden in den Dateien */etc/network/interfaces* und */etc/hostname* gespeichert und können gegebenenfalls nachträglich editiert werden.



Festplatten aufteilen

Als nächstes folgen die Eingaben zur Festplattenaufteilung. Wir wählen hier „Partitionstabelle von Hand eingeben“ weil dadurch Sicherheit gewonnen werden kann. Nun wählen wir die richtige Festplatte für das Basissystem aus. Diese ist unter dem Eintrag „IDE1 Master (hda)“ zu finden. „Eine neue Partition erstellen“ ist die richtige Wahl im nächsten Dialogfeld, die Größe der *root*-Partition ist mindestens *„6 GB“*. Haben Sie eine große Festplatte, können Sie hier auch ruhig etwas großzügiger sein, da auch temporäre Dateien wie sie auch beim Kernel kompilieren anfallen Platz benötigen. Diese erste *primäre* Partition sollte mit dem *ReiserFS*-Dateisystem formatiert werden. Wir wählen das ReiserFS-Filesystem da es bei der Verwaltung von vielen kleinen Dateien, wie Word- oder Excel-Dokumenten, Vorteile gegenüber anderen journalführenden Dateisystemen hat. Journalführende Dateisysteme müssen nach einem Absturz nicht mehr die gesamte Festplatte auf Fehler überprüfen, sondern nur die Bereiche die zum Zeitpunkt des Absturzes als „nicht abgeschlossen“ im Journal offen geblieben sind.



Das ReiserFS wird unter dem Punkt „Benutzen als“ angegeben. Angewendet wird die Einrichtung durch „Anlegen der Partition beenden“.

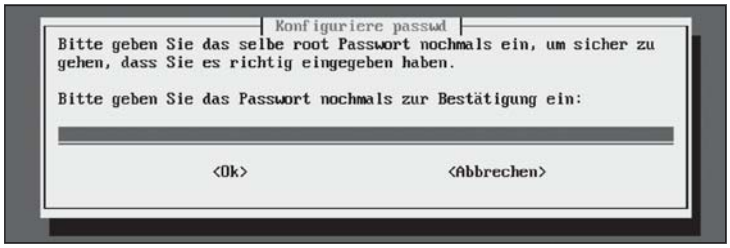
Danach zeigt sich wieder der erste Dialog „Festplatte partitionieren“ in dem nun der restliche verfügbare Plattenplatz unter „pri/log“ ausgewählt wird und nach dem selben Schema wie für die root-Partition vorgegangen wird. Die zweite Partition *var* benötigt *3 GB* und darf auch größer ausfallen, weil hier sämtliche Programmpakete die mit dem Paketmanager *apt* installiert werden, zwischengelagert werden. Wir trennen das Verzeichnis *var* absichtlich vom root-System, da im Falle eines Angriffs von außen viele Spuren aufgezeichnet werden. Dadurch wachsen die Log-Dateien im Verzeichnis an. Wenn diese nun den gesamten freien Speicherplatz auf der *var*-Partition benötigen, so ist das nicht mehr weiter schlimm, weil die root-Partition noch über ausreichend Platz verfügt und die Serverdienste weiter arbeiten können. Das Abtrennen erfolgt durch den richtigen Eintrag *var* unter *„Einhängepunkt (mount)“*. Als Dateisystem wählen wir wieder ReiserFS.

Virtueller Speicher

Die dritte Partition *swap* benötigt jedes Linux-System und bildet den virtuellen Speicher. Dieser Speicherbereich wird dann benötigt wenn der physikalische RAM nicht mehr ausreicht. Es werden dann Speicherbereiche auf die Festplatte geschrieben. Das dieses Verfahren zeitraubend ist versteht sich von selbst, weshalb ausreichend Hautpspeicher jedem System zu mehr Performance verhilft. Eine gute Größe ist hier 1 *GB*, bei *„Benutzen als“* muss *„Auslagerungsspeicher (Swap)“* angegeben werden.

Als vierte Partition empfiehlt sich ein ausreichend großer Bereich in dem alle Fileserver-Datein liegen sollen. Als Einhängepunkt kommt die Option *„von Hand angeben“* zu tragen in der nun */serverdaten* angegeben wird. Wir *„Benutzen als“* Dateisystem wieder ReiserFS. Die Parition */serverdaten* könnte auch gegen eine eigene Festplatte getauscht werden. Soll dies der Fall sein, dann kann die Einbindung gleich geschehen, oder es erfolgt die Einbindung ins Dateisystem zu einem späteren Zeitpunkt mit dem Befehl *fdisk* und dem Editieren der Datei */etc/fstab*.

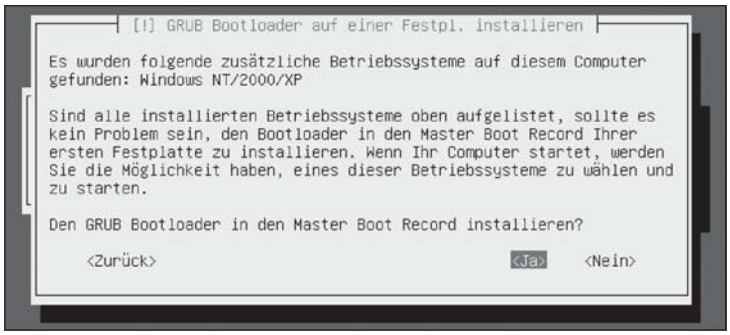
Wir schließen die Partionierung durch Anwahl von *„Partitionierung beenden und Änderungen übernehmen“* und bestätigen die Sicherheitsabfrage. Der Installer richtet nun die Bereiche ein und formatiert sie entsprechend. Anschließend wird das Grundsystem



auf die Platte geschrieben. Die Frage ob der Bootloader den Bootrecord schreiben soll beantworten wir mit *Ja* und nach erfolgtem Neustart beginnt die Konfiguration des Basissystems.

Beim root-Passwort ist Vorsicht geboten

Die Uhrzeit wird von der Hardware-Uhr übernommen (GMT auf *nein* stellen) und das root-Passwort eingeben. Das Passwort soll mit Bedacht gewählt werden, Groß- und Kleinbuchstaben sowie Ziffern enthalten und mindestens acht Zeichen lang sein. *root* ist jener Benutzer, der einfach alles darf. Fällt das root-Passwort in fremde Hände oder wird es geknackt, so ist das System in höchster Gefahr und bei einem Angriff verloren. In der Praxis hat sich bewährt die Anfangsbuchstaben eines Satzes zu nehmen den man sich leicht merkt. Zum Beispiel *„Meine Frau Gitte ist 24 Lenze jung“* woraus sich das Passwort *MFGi24Lj* ergibt. Achtung! Vergessen Sie das Passwort nicht, es gibt sonst keine Möglichkeit mehr dass Sie an dem System Änderungen vornehmen können!



Benutzerkonto erstellen

Danach wird ein Benutzerkonto erstellt mit dem die laufenden Arbeiten erledigt werden sollen. Wir raten ab als *root* zu arbeiten, da die meisten Befehle die abgesetzt werden, ohne Nachfrage ausgeführt werden. Ein Vertipper kann das ganze System außer Gefecht setzen oder sogar löschen. Also, zuerst den richtigen vollen Namen des Benutzers eingeben, danach einen Benutzernamen vergeben. Hinblickend auf weitere Serverdienste die ausgeführt werden, empfielt es sich eine Namenskonvention zu überlegen. Ein Beispiel wäre der erste Buchstabe des Vornames, gefolgt vom Nachnamen, beides getrennt durch einen Punkt (f.mustermax für den User Friedrich Mustermax). Bitte achten Sie darauf alles klein zu schreiben, da unixbasierende Betriebssysteme zwischen Groß- und Kleinschreibung unterscheiden. Wenn Sie sich angewöhnen, immer alles klein zu schreiben, fällt die tägliche Arbeit am Rechner wesentlich leichter. Abschließend vergeben Sie auch für diesen Benutzer ein sicheres Kennwort.

Nun fragt der Installer auf welchem Medium er zusätzliche Pakete finden kann. Hier wählen wir trotz des vorhanden DVD-Laufwerkes die Option *cdrom.*

Paketauswahl

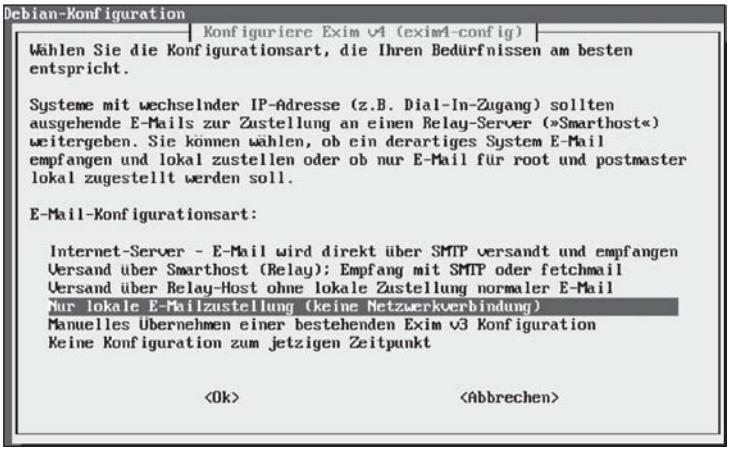
Jetzt geht es an die Auswahl der Pakete. Debian 3.1 bietet eine Auswahl an vorkonfigurierten Paketauswahlen an. Wir wählen mit Hilfe der Leertaste die Pakete *Web-Server, Druck-Server, Datei-Server* und *Mail-Server aus,* worauf die entsprechenden Pakete von der DVD installiert werden.

Firewall selbst hochgezogen

```
#! /bin/sh

# Flushen, Löschen, Neuerstellung - nicht vergessen im Script! #
#####################################################################
echo „Lösche Tabelle and initialisiere die Neuen...“
iptables -F
iptables -F -t nat

iptables -F sperre
iptables -X sperre
iptables -N sperre
iptables -F sperre

# Erster Kontakt #
##################
echo „Einige einfache Sperren...“
# Alles aus dem LAN ohne passende IP wegwerfen
iptables -A sperre -i eth0 -s ! 192.168.100.0/255.255.255.0 -j DROP
# Sonst alles vom internen Interface eth0 erlauben (Hier sollte man
# aufpassen,  was man den Usern gewähren will und sich vor
# Trojanern schützen.)
iptables -A sperre -i eth0 -j ACCEPT
# Für Loopback wird immer alles erlaubt ausser von nicht 127.0.0.1
iptables -A sperre -i lo -s 127.0.0.1/255.0.0.0 -j ACCEPT
# Alles aus dem Inet mit meinen IPs werwerfen
iptables -A sperre -i eth1 -s 192.168.100.0/255.255.255.0 -j DROP

# Akzeptieren von erlaubten Services #
##################################
echo „Jetzt erlaub ich gleich die Dienste...“
# SSH erlauben
iptables -A sperre -p tcp —dport 22 -j ACCEPT
# HTTP erlauben
iptables -A sperre -p tcp —dport 80 -j ACCEPT

# Antworten zulassen #
######################
iptables -A sperre -m state —state ESTABLISHED,RELATED -j
ACCEPT

# Alles andere abweisen (RFC-konform) #
#######################################
echo „Alles Andere abweisen...“
iptables -A sperre -p tcp -j REJECT —reject-with tcp-reset
iptables -A sperre -p udp -j REJECT —reject-with icmp-port-
unreachable

# Sperre aktivieren #
#####################
echo „Aktiviere Firewall...“
iptables -A INPUT -j sperre
iptables -A FORWARD -j sperre
iptables -P INPUT DROP
iptables -P FORWARD DROP

# Ausgehende Pakete vom Server immer akzeptieren
iptables -P OUTPUT ACCEPT
iptables -P OUTPUT ACCEPT -t nat

echo „Firewall gestartet!“
```

bitte umblättern

Der Installer will nun den Arbeitsgruppen-Namen der Windows-Netzwerkumgebung wissen. Weil hier von einem neuen Netzwerk ausgegangen wird legen wir diesen nach Lust und Laune fest. Für unsere WCM Linux-Box wird er ZENTRALE lauten. Muss sich der Server in ein bestehendes Netzwerk integrieren, muss der Arbeitsgruppenname aus den Netzwerkeinstellungen eines Windows-Rechners ausgelesen werden.



Als nächstes teilen wir der Installationsroutine mit, wie wir eMails empfangen wollen. Ungeachtet der späteren Verwendung als eMail-Server wählen wir hier *„nur lokale eMailzustellung“.* Anschließend wird der Benutzer der anstelle des Benutzers *root* Benachrichtungs-eMails des Systems emfpangen soll festgelegt. Das zuvor erstelle Arbeits-Konto ist hier die beste Wahl. - Fertig, die Grundeinrichtung ist abgeschlossen.

Das erste Mal

Nun loggt man sich mit dem Arbeitsbenutzer an der Konsole ein und schon treten wir das erste Mal mit der Paketverwaltung von Debian in Kontakt. *apt* besteht aus mehreren Teilen wie beispielsweise *apt-get, apt-cache und apt-config.* Dazu später mehr. Jetzt wollen wir das Paket *webmin,* das unserm Server eine grafische Konfigurationshilfe gibt, installieren. Wir versetzen uns mit dem Befehl *sudo* in die Lage einen Befehl als *root* auszuführen. Das Kommando *apt-get install* gefolgt vom Paketnamen stellt sämtliche Abhängigkeiten des Pakets fest und installiert diese mitsamt dem gewünschten Paket. In diesem Fall wird die Befehlsfolge *sudo apt-get install webmin* abgesetzt. Das Kommando *sudo* fragt nach dem *root*-Passwort, anschließend meldet sich *apt* ob diese Pakte mitsamt den Abhängigkeiten wirklich installiert werden sollen. Wer eine textmenübasierende Installation bevorzugt, sollte sich das Frontend *aptitude* ansehen. Nach erfolgter Installation editieren wir wieder als *root* mit dem Editor *nano* die Datei */etc/webmin/miniserv.conf (Befehl: su root nano /etc/webmin/miniserv.conf)*. In dieser setzten wir bei der Option *allow* unser internes Netzwerk *192.168.123.0/255.255.255.0* dazu.

Grundlegend muss hier noch erwähnt werden: Arbeiten Sie gerade wenn Sie mit Linux noch nicht so vertraut sind konzentriert und sehr genau! Oft ist ein falsch gesetzter Punkt oder ein Abstand an der falschen Stelle Grund, dass Dienste gar nicht oder nicht wie erwartet laufen. Also prüfen Sie Ihre Eingaben lieber ein zweites Mal nach, bevor Sie den Editor mit der Tastenkombination Strg-X und Beantwortung der Sicherheitsabfragen schließen.

Webmin muss nun die veränderte Konfigurationsdatei neu einlesen. Das erreicht man am besten durch Neustarten von *webmin* mit *sudo /etc/init.d/webmin restart.* Somit kann von jedem internen Rechner, der mit einem Browser wie Firefox oder InternetExlorer ausgestattet ist, durch Eingabe von *https://192.168.123.1:10000* unser Server grafisch administriert werden. Webmin wird uns in Zukunft oft hilfreich zur Seite stehen, doch nicht alle Aufgaben lassen sich über das grafische Frontend erledigen. Außerdem gibt es viele nicht so häufig benutzte Funktionen die grafisch nicht umgesetzt worden sind und deshalb über die Befehlszeile nachgereicht werden müssen.

Schotten dicht!

Als nächsten und letzten Schritt konfigurieren wir eine kleine restriktive Firewall die den Zugriff von außen komplett verbietet. Wenn die Firewall auch IP-Pakete ins Internet weiterleiten soll, beachten Sie bitte den Artikel „Die WCM-Linux-Box geht online“ in dieser Ausgabe. Die einzelnen Optionen zur Firewall werden in einer der nächsten Ausgaben ausführlich behandelt. Für die Errichtung der Firewall bedienen wir uns *itpables.* Mit *iptables* legen wir Regelketten an, die nacheinander abgearbeitet werden. Es ist also unbedingt erforderlich auf die richtige Reihenfolge der Regeln zu achten. Werden zum Beispiel in Zeile 1 Verbindungen auf Port 25 (smtp/eMail-Eingang) verboten, so nutzt es nichts wenn diese in Zeile 3 erlaubt werden, da die Ketten von oben nach unten abgearbeitet werden.

Der Regelsatz für die Maskierung und Abschottung nach außen findet sich in der Box *Kleine Firewall* wieder. Bei diesem Regelsatz wird davon ausgegangen, dass das externe Interface als eth1 eingebunden ist. Den Regelsatz speichern wir unter dem Name *firewall_script* in das Verzeichnis */etc/init.d/* und geben ihm die entsprechenden Rechte mit *chmod +x firewall_script.* Damit die Firewall bei jedem Systemstart automatisch geladen wird, muss man einen symbolischen Link durch *sudo ln -s /etc/init.d/firewall_script /etc/rc2.d/S90 firewall_script* in das Verzeichnis */etc/rc2.d/* legen.

Optional muss dem Kernel noch mitgeteilt werden, welches Netzwerkinterface er ansprechen muss wenn er Pakete abarbeitet die nicht zum internen Netz (LAN) gehören, sondern für das Internet (WAN) bestimmt sind. *route add default gw eth1* setzt die richtige Route.

Wer nun mit Hilfe des in diesem Heft zu findenden Artikels „Die WCM-Linux-Box geht online“ seinen Internetzugang erfolgreich konfiguriert hat, hat auch schon die Möglichkeit die installierten Pakete auf den neuesten Stand bringen.

Entweder startet man das Programm *apt-setup* und wählt dort die passende Installationsquelle, oder man fügt in der Datei */etc/apt/sources.list* folgende Einträge mit dem Editor *nano* dazu:

deb *http://ftp.at.debian.org/debian/ stable main non-free contrib*

deb-src *http://ftp.at.debian.org/*

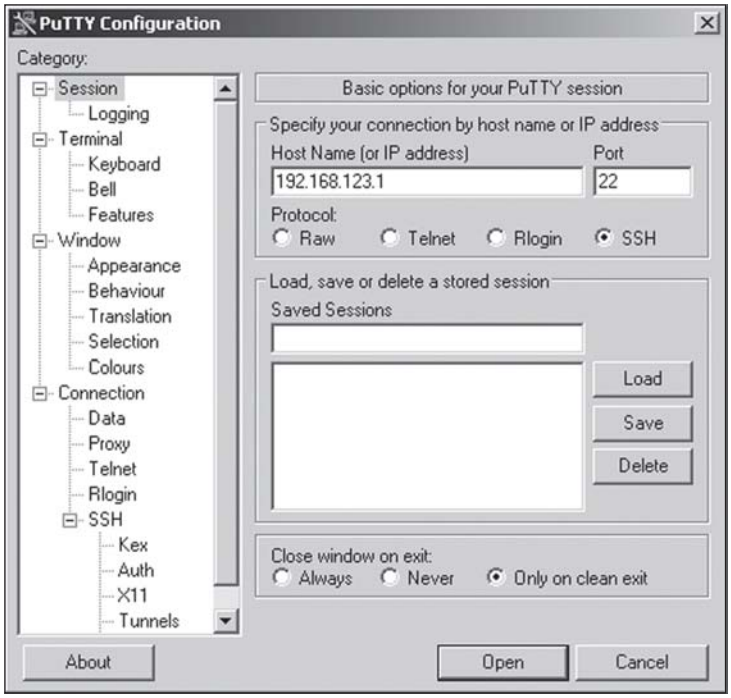
Befehlsreferenz Debian

cd Verzeichnis Verzeichniswechsel (Change Directory)
mv Datei1 Datei2 Datei bewegen oder umbennen (Move)
rm Datei Datei lšschen (Remove)
ln Quelldatei Linkdatei Verknüpfung anlegen (Link)
cp Quelldetei Zieldatei Datei kopieren (Copy)
mkdir Verzeichnis Verzeichnis anlegen (Make Directory)
chown Benutzer Dateiname Eigentümer eine Datei ändern (Change Owner)
chgrp Gruppe Dateiname Gruppenzugehšrigkeit einer Datei ändern
chmod Rechte Dateiname Zugriffsrechte auf eine Datei ändern

Für alle Befehle kšnnen Sie direkt von der Befehlszeile Beschreibungen aufrufen. *man Befehl* zeigt Ihnen die man-Page in der Sie den genauen Syntax und die Optionen des Befehls finden.

debian/ stable main non-free contrib
deb *http://security.debian.org/ stable/updates main contrib non-free*

Jetzt müssen noch die schon enthaltenen Zeilen auskommentiert werden, sonst will *apt* weiterhin von der CD/DVD installieren und updaten. Das Auskommentieren geschieht dadurch, dass man an den Anfang der Zeile eine Raute (#) stellt. Somit werden diese Zeilen nicht mehr durch die auslesenden Applikationen beachtet - sie sind Kommentare. Die Paketliste wird durch *sudo apt-get update* auf den neuesten Stand gebracht. Die Pakete selbst werden erst nach Eingabe von *sudo apt-get upgrade* geholt und eingerichtet.



Erreichbarkeit

Nachdem diese Schritte ausgeführt worden sind, ist die WCM Linux-Box von anderen Rechnern im Netzwerk per SSH erreichbar. Ein kostenloses Windows-Tool dass SSH-Sitzungen aufbauen kann, ist Putty. Sie können es von http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe auf Ihre Windows-Maschine laden. SSH-Sitzungen starten Sie, indem Sie im Programmfenster in der Zeile „Host Name" die IP-Adresse des Servers (192.168.123.1) eingeben, rechts unterhalb den Auswahlknopf SSH wählen und mit *Open* bestätigen. MacIntosh OSX-User verwenden einfach das mitgelieferte „Terminal", das sich unter *Programme/Dienstprogramme* befindet. Eine Sitzung öffnet man durch Eingabe von ssh benutzername@192.168.123.1.

Diese SSH-Verbindungen funktionieren aber nur, wenn sich die beteiligten Rechner im selben IP-Netzwerk befinden. Sie müssen also auf den Rechnern IP-Adressen im Bereich von 192.168.123.XXX vergeben.

Der Server läuft nun, ist über SSH erreichbar, kann sogar schon grafisch administriert werden und wird in den nächsten WCM-Ausgaben noch im Detail konfiguriert.

Zum Nachdenken...

Jetzt noch was zum Nachdenken, damit die zwei Wochen bis zur nächsten Ausgabe schneller vergehen: Wer sich entscheidet, selbst einen Server zu betreiben, steht immer in der Zwickmühle: Handle ich nach dem Motto „Never change a running system" oder aktualisiere ich von Zeit zu Zeit meine Softwarepakete um etwaige Sicherheitslücken zu schließen? Gerade bei Debian kommen in der Regel nur ausreichend getestete Pakete in Umlauf, ob sich das Risiko trotzdem lohnt?

Wie man nun seinen Server tatsächlich auf den letzten Stand hält erfahren Sie - im nächsten WCM. ■

Die Linux-Box im Netzwerk

Ein Pinguin verbindet...

Nach einer erfolgreichen Installation, kann unsere Linux-Box bereits im Netzwerk eingesetzt werden. Doch was tun, wenn Änderungen an der LAN-Konfiguration vorzunehmen sind bzw. das Netzwerk neu gestaltet wird? Spätestens dann nämlich ist Detailwissen gefragt, um ihre Box den neuen Umgebungsbedingungen anzupassen. Im Folgenden finden Sie daher eine Schritt-für-Schritt-Anleitung, damit die Kommunikation mit anderen Teilnehmern auch weiterhin reibungslos klappt.

von Ing. Christian Sudec

Wie bereits erwähnt, können Sie während der Installationsphase von Debian Sarge alle notwendigen Einstellungen in den dazugehörigen Dialogfenstern vorzunehmen, um die Linux-Box im LAN betreiben zu können, jedoch haben Sie diese Möglichkeit später im laufenden Betrieb nicht mehr. Hier wird von Sarge vorausgesetzt, dass sie sich in den Tiefen der Konfigurationsdateien zurechtfinden. Dass diese jedoch – wenn man es einmal weiß – eher seicht und relativ einfach zu ändern sind, werden Sie in den nächsten Abschnitten von selber feststellen. Also keine Angst :-)

Vorarbeit

Um die hier beschriebenen Änderungen durchzuführen, ist wieder mal eine Anmeldung als root fällig. Doch im Gegensatz zu den vielen anderen Verwaltungstätigkeiten sollten Sie die nachfolgenden Arbeitsschritte als eine der wenigen Ausnahmen nur lokal ausführen, da das editieren der Netzwerkkonfiguration über das Netzwerk (z.B. mit ssh) dem 'Sägen am eigenen Ast' gleichkommen würde. Nachdem diese Warnhinweise gesagt wurden, empfiehlt sich als erstes ein Blick auf die vom System erkannten Schnittstellen. Das dazu notwendige „ifconfig –a" liefert Ihnen eine vollständige Liste aller Gerätenamen, die bei der Installation erkannt wurden und jede Menge weiterer wertvoller Informationen.

Für spezielle bzw. nicht erkannte Netzwerkkarten ist im Normalfall eine Neukompilierung des Kernels die beste Wahl, da die Treiber dann gleich integriert werden können und man sich nicht mit Modulen und Abhängigkeiten herumschlagen muss. Wie dies funktioniert, wird noch in einem kommenden Workshop erläutert. Auf unserem Referenzsystem erscheint die NIC (Network Interface Card) jedenfalls als eth0 – Unix beginnt in der Regel immer mit '0' beim Zählen!

Schnittstelle

Ausgestattet mit dem Gerätenamen können wir uns im ersten Schritt an die Vergabe von IP-Adressen machen. Alle dazugehörigen Config-Dateien finden sich auf einem Haufen im Ordner /etc/network. Neben Skriptordnern (*.d), deren Inhalt beim Wechsel von NIC-Zuständen ausgeführt wird, finden sich dort die dazugehörigen Zustandsinformationen (ifstate*) und allgemeine Einstellungen (options), die wir hierfür allerdings nicht anpassen müssen.

Interessanter sind schon die Schnittstellendefinitionen, die wir mit „vi /etc/network/interfaces" zum Editieren öffnen. Am besten werfen Sie jetzt parallel einen Blick auf unsere Beispieldatei: zu Beginn (Schlüsselwort 'auto') werden alle erkannten Netzwerkgeräte aufgezählt. Ein „iface [Gerätename] inet [Typ]" leitet nun die einzelnen Konfigurationsabschnitte ein. Das Loopback-Device (lo) bedarf keiner weiteren Konfiguration, da es ja gar nicht wirklich da ist (siehe Textkasten) und sowieso immer vom System gleich konfiguriert wird.

Danach folgt jedoch der Abschnitt unserer eth0, wo die eingerückten Parameter zur Änderung bereitstehen.

Als erstes folgt hier die Adresse ('address'), welche die Schnittstelle erhalten soll und in der nächsten Zeile die Subnetmaske ('netmask') des Netzwerks. Nett, aber nicht unbedingt notwendig ist die Broadcastadresse ('broadcast'), da Linux sich diese aus obigen Daten bereits selbst generieren kann. Gleiches gilt für die Netzwerk-Adresse ('network'), wo als Faustregel nur alle auftretenden 255er in der vorangegangenen Zeile

DynDNS – Ein Konto wird erstellt

Viele Router bieten in Ihren Einstellungen die Möglichkeit an, DynDNS in Anspruch zu nehmen. Damit ist es Anwendern möglich, trotz dynamischer IP-Adressvergabe seitens des Providers, den Router trotzdem über einen Domainnamen permanent im Internet zu erreichen. Das Gerät kann nun mit der entsprechenden Konfiguration (z.B. mittels virtuellem Server) Anfragen an die Linux-Box weiterleiten. Die dazugehörigen Dienste werden in kommenden Workshops eingerichtet – jetzt folgt einmal die Grundinstallation im Router.

Der Hund liegt dort allerdings nicht in den komplizierten Einstellungen begraben, sondern in den benötigen Daten, die man sich vorher von der DynDNS-Homepage besorgen muss. Aus diesem Grund gibt es hier ein schnelles Kochrezept:

Schritt 1: Auf die Webseite www.dyndns.com gehen und unter ‚Account' à ‚Create Account' ein neues Benutzerkonto anlegen; Sinnvollerweise verschlüsselte Verbindung wählen!

Schritt 2: Vertragbedingungen akzeptieren (alle zwei Checkboxen abhaken), Username und Passwort wählen, sowie gültige e-Mail-Adresse eingeben und abschicken.

Schritt 3: Ihr e-Mail-Postfach zwecks Bestätigungsmail checken und den darin enthaltenen Link anklicken à das Konto ist jetzt aktiviert!

Schritt 4: Mit ihren Daten unter ‚Account' à ‚My Account' anmelden und nach ‚My Services' wechseln.

Schritt 5: Als Unterpunkt aus dem Menü links ‚My Hosts' wählen und darin ‚Dynamic DNS' anklicken. Nun kann mit ‚Add Host' ein neuer Eintrag erstellt werden.

Schritt 6a: Gewünschten Hostnamen eintragen und Domain auswählen (z.B. wcmbox.homelinux.org).

Schritt 6b: Die IP Adresse ist – sofern automatisch erkannt – bereits ausgefüllt; falls nicht, kann man sie aus den Anwahl-Logs des Routers raussuchen und manuell eintragen. Infos dazu finden sie in Ihrer Router-Dokumentation.

Schritt 6c: ‚Enable Wildcard' deaktiviert lassen – wir haben nur eine Linux-Box im LAN.

Schritt 6d: ‚Mail Exchanger (optional)' im Moment nicht ausfüllen – wir haben noch keinen Mail-Dienst auf der Box laufen.

Schritt 6e: Auf ‚Add Host' klicken à Fertig!

Im nun erscheinenden Fenster können Sie den (DNS-)Zustand ihres Routers kontrollieren. Die genutzten Kontodaten werden nun auch in Ihrem Router eingestellt, damit dieser veränderte Adressinformationen zu DynDNS schicken kann. Sofern das Gerät ping-bar ist (Sicherheitseinstellungen checken), könnten Sie nun einen Freund mit Internetzugang bitten, ein paar Testpakete an den oben eingestellten Namen zu schicken. Klappt alles, so können Sie sich auf der Homepage rechts oben über ‚Log Out' verabschieden. ■

Loop-Back-Ground

Unixsysteme waren ursprünglich die Platzhirsche, wenn es um die Dienstbereitstellung in Netzwerken ging. Aus diesem Grund waren viele der eingesetzten Programme vom Vorhandensein einer Netzwerkkarte abhängig und verabschiedeten sich sofort wieder, wenn keine solche eingebaut war. Um dies zu verhindern, schuf man das virtuelle Loopback-Device (Gerätename lo) welches fortan zwei wichtige Aufgaben erfüllte: zum einen garantiert es ein immer einsatzbereite NIC, an die sich Dienste binden können zum anderen verweist es mit der Adresse 127.0.0.1 immer auf den eigenen PC: alle Daten die man darüber rausschickt, landen gleich wieder in der Eingangsqueue. Wer einmal testen möchte, wie sich seine selbst programmierte Applikation im LAN verhalten würde, kann dies somit ohne Risiko über lo machen. ■

durch Nullen ersetzt werden. Wichtig ist allerdings wieder die Adresse des 'gateway'. Hier ist der Host im lokalen Netz einzutragen, über den eine Verbindung ins Internet hergestellt wird. In unserer Beispielkonfiguration wäre dies die IP-Adresse des Routers. Es hat sich etabliert, dass solche Gateways immer auf die letzte verfügbare Adresse im LAN (.254) eingestellt werden.

Haben Sie die Einträge entsprechend Ihrer Bedürfnisse angepasst und die Datei wieder abgespeichert, so ist der erste (große) Schritt getan. Noch eine Bemerkung zum Abschluss: zwar ließe sich hier auch DHCP aktivieren, jedoch ist dies für einen zukünftigen Server nicht sinnvoll, da einige Dienste eine fixe Adresszuweisung für den Start voraussetzen, was in diesem Fall jedoch nicht garantiert ist.

Namen statt Zahlen

Da sich Menschen ein aussagekräftiges 'www.derist.org' ungleich besser merken können als eine Adresse á la '10.239.178.47', führt uns der zweite Schritt direkt zur Einrichtung der so genannten Namensauflösung. Diese bedient sich auf Grund unterschiedlicher Konzepte mehrerer Config-Files, die miteinander zusammenspielen.

Den Beginn macht einmal /etc/hostname, wo in der einzig vorhandenen Zeile der aktuelle Name unserer Linux-Box geändert werden kann. Dieser taucht in Zukunft (nach einem Reboot) immer vor dem Eingabeprompt auf. Passt der Eintrag, so geht's als nächstes zur Datei /etc/hosts, wo eine lokale Auflösung eingerichtet werden kann. Das heißt, Linux sieht in dieser Datei nach, ob es zu einem FQDN (full-qualified-domainname) oder einfachen PC-Namen die dazugehörige IP-Adresse findet, ohne dabei auf DNS-Server zuzugreifen. Idealerweise trägt man sich in dieser Datei die lokalen Workstations im eigenen Netzwerk ein, um sie später schnell mit Namen ansprechen zu können.

resolv.conf

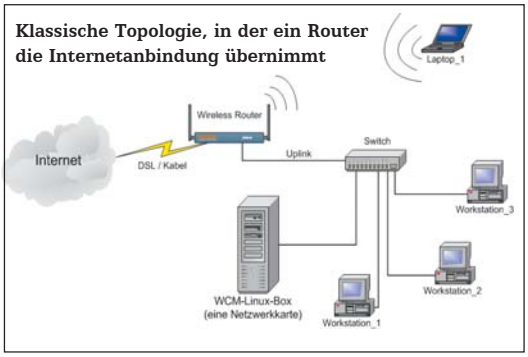
Damit eine Internetadresse (z.B. www.wcm.at) ebenfalls aufgelöst werden kann, ist spätestens jetzt der Kontakt mit einem professionellen Domain Name Service (DNS) erforderlich. Die dazugehörige Konfiguration findet sich in /etc/resolv.conf und hängt von der aktuellen Netzwerktopologie ab. In unserem Fall als ‚nameserver' die IP-Adresse des Routers eine gute Wahl, da dieser bei der Einwahl die aktuellen DNS-Server vom Provider erhält und eingehende Anfragen immer dorthin weiterleitet (=DNS-Forwarding). Sollte ferner jemand nur einen einfachen Rechnernamen angeben, so wird an diesen zur Auflösungs-Suche die angegebene 'domain' angehängt.

host.conf

Last but not least regelt die Datei /etc/host.conf die Reihenfolge des Zugriffs (z.B. „zuerst hosts konsultieren, danach Nameserver fragen!") auf obige Dateien neben ein paar weiteren Features. Diese braucht jedoch im Normalfall und auch bei uns nicht angepasst werden.

Damit alle gemachten Einstellungen (Schnittstellen und Namensauflösung) nun vom System eingelesen und angewandt werden, bedarf es zu guter Letzt noch des Neustarts des Netzwerk-Dienstes, was mit der Eingabe von „/etc/init.d/networking restart" sogleich erledigt wäre – Fertig!

Klassische Topologie, in der ein Router die Internetanbindung übernimmt



...Kontrolle ist besser

Da wir uns auch an das alte Sprichwort halten, testen wir mit Hilfe von „ping [IP-Adresse oder FQDN]" ob wir von einem anderen Rechner oder dem Router eine Antwort erhalten. Anders als das Windows-Pendant, welches nur drei Prüfpakete abschickt, sollte man das Tool hier mit Strg+C abbrechen, da es sonst endlos weiterläuft.

Bei etwaigen Problemen in/mit dem Netzwerk, gilt die Faustregel, sich immer von unten nach oben durch die OSI-Schichten durcharbeiten: also physische Verkabelung kontrollieren, Link(-LEDs) am Switch/Router/PC prüfen, Konfiguration checken und nach einem (Dienst-)Neustart erneut pingen. Auch ein häufiger Knackpunkt: manche (Desktop-)Firewalls machen so dicht, dass keine Antwortpakete (Echo-Reply) verschickt werden. Abgesehen, dass dies - entgegen anders lautender Meinungen - nicht optimal ist, sollten Filtertechniken erst implementiert werden, wenn das Netzwerk fertig konfiguriert ist und ohne Probleme läuft.

Ab hier

Mit den obigen Schritten sollten Sie jetzt in der Lage sein, die WCM-Linux-Box ins lokale Netzwerk einzubinden bzw. sie an Veränderungen in der LAN-Topologie anzupassen. Sollten Sie mehr als eine Ethernetkarte einbauen, so gilt es, die zusätzlichen Geräte analog zu obigen Beispielen mit IP-Adressen und eigenen, eindeutigen Domain-Namen zu versehen.

Der wichtigste Punkt ist hier: hängt die Box an zwei unterschiedlichen Netzwerken, so müssen dementsprechend auch unterschiedliche IP-Adressbereiche verwendet werden. Und um ferner Daten zwischen den Netzwerken auszutauschen, gehört zudem Routing/Masquerading implementiert. Doch dies ist Thema des Workshops zur Internetanbindung. *(Seite92)* ■

IPv4 in a nutshell

Das Internet Protokoll (IP) in der Version 4 hat sich Mitte der Neunziger als Standardprotokoll durchgesetzt und sorgt dafür, dass Autoren für Literatur zu diesem Thema nie Probleme mit zu geringer Seitenzahl haben. Nichts desto trotz folgt hier ein kurzer Schnellkurs: Eine IP-Adresse besteht immer aus vier Segmenten (w.x.y.z), die durch Punkte voneinander getrennt werden und die Werte im Bereich von 0-255 annehmen können.

Ebenso wie bei einer normalen Adresse ist nicht nur Name der Person (Host), sondern auch der Ort (Netzwerk) darin gespeichert. Den dazugehörigen Trick vollführt die Subnetmaske, die mit 255er-Einträgen den Netzwerteil und mit 0ern den Hostteil voneinander abgrenzt. Bei unserer Linux-Box wäre also 192.168.123(.0) die Adresse des Netzwerks und 1 die Nummer des Hosts in diesem. Neben 0 nimmt auch 255 eine Sonderstellung bei der Adressierung ein: sie bedeutet schlicht „alle Rechner im entsprechenden LAN" und wird ergo für Broadcasts (Rundruf-Pakete) eingesetzt. ■

Ab ins Internet

WCM-Linux-Box geht online

Ein Rechner ohne Internetzugang ist heute fast nicht mehr vorstellbar. Auch in Österreich ist schon in vielen Gebieten Breitbandinternet verfügbar, was wiederum zu einer rasanten Entwicklung in sämtlichen Lebensbereichen führt. Sei es bei der Informationsbeschaffung oder die neuen Möglichkeiten der Kommunikation durch Chat und eMail. Um nun diese Dienste für alle Familienmitglieder oder Mitarbeiter gleichzeitig zugänglich zu machen gibt es mittlerweile viele Hardwarehersteller die Router anbieten. Hardwarerouter haben heute viele Features die es früher nur bei „großen" Lösungen wie softwarebasierenden Routern gab. So können Sie die IP-Adressvergabe für die internen Geräte übernehmen und viele bieten sogar eine Firewall. Wir zeigen nun, wie man ohne Hilfe eines Hardwarerouters die WCM-Linux-Box online bringt.

von Martin Müller

Eines gleich vorweg: Nicht alles was Sie mit einem Router anstellen köönnen, ist auch legal! Einige Internetprovider verbieten in ihren Gechäftsbedingungen etwa, dass Sie mehrere Rechner an eine Leitung hängen dürfen. Chello erlaub dies zum Beispiel nur bei speziellen Produkten und dann nur für eine bestimmte Anzahl an Rechnern. Bei den günstigen Privattarifen ist laut AGBs meistens auch kein Serverbetrieb erlaubt. Also Achtung, bevor sie sich ans Werk machen, machen Sie sich in den AGBs Ihres Anbieters schlau ob Sie das auch dürfen.

Aufgrund der Vielzahl von Konfigurationsmöglichkeiten ist es uns hier leider nicht möglich, die Anleitung für die Hardwarerouter-Konfiguration nach außen zu beschreiben. Sie müssen so weit mit ihrem Gerät vertraut sein, dass Sie mit dem Gerät online gehen können und seine interne IP-Adresse auslesen bzw. konfigurieren können.

Wir gehen davon aus, dass der Hardware-Router mit der internen IP-Adresse 192.168.123.254 arbeitet, dass die DNS-Server richtig im Router konfiguriert sind und dass Sie eine Internetverbindung aufbauen können.

Weisen Sie also dem ersten Interface der WCM-Linux-Box *eth0* die IP-Adresse 192.168.123.1 und das Gateway 192.168.123.254 zu. Dies erledigen Sie durch Modifizierung der Einträge in */etc/network/interfaces*. Den genauen Syntax finden Sie in der Box „IP-Konfiguration". Nachdem Sie die Interfaces neu gestartet haben (*sudo /ect/init.d/network restart*) geht der Server über den Harwarerouter online.

Nun zur Einwahl: Grundsätzlich bedarf es bei der WCM-Linux-Box einer stabilen Internetanbindung, weshalb ausschließlich auf xDSL- und ADSL-Modems eingegangen wird, die über eine Ethernetverbindung verfügen. Modems die über ein USB-Kabel angeschlossen werden, scheiden aufgrund der Anbindung aus. Der USB-Bus ist uns nicht stabil genug, um im Servereinsatz Verwendung finden zu dürfen. Sollten Sie ein USB-Modem haben, wird dies in der Regel kostenlos gegen eines mit Ethernetanbindung vom Provider ausgestauscht. Sie müssen nur eine gute Begründung der technischen Notwendigkeit parat haben. Kreativität ist also angesagt :-) Da wäre zum Beispiel dass das Modem den Dienst versagt, sobald sie die neue externe USB-Video-Schnitt-Lösung von Pinnacle an den Bus bringen.

Bitte beachten Sie die AGBs Ihres Providers wenn Sie Ihr Problem vortragen! Sollte das alles nicht fruchten, müssen Sie sich selbst ein Modem kaufen. Viele Hardwarerouter haben ein xDSL-Modem eingebaut.

In einigen Fällen können Sie einfach am Modem die Anschluss-Art wechseln, denn aktuelle Modems haben USB und Ethernet an Bord. Schaffen Sie trotz Ethernetanschluss keine Verbindung (prüfen ob Statuslampe an Netzwerkkarte und Modem leuchtet), kann es auch am Ethernetkabel liegen. Möglicherweise benötigen Sie ein Crossover-Kabel bei dem die Datenleitungen ausgekreuzt sind. So ein Kabel haben Sie wahrscheinlich mit dem Modem mitgeliefert bekommen oder Sie beziehen es bei jedem Elektromarkt um die Ecke.

Wir gehen auf die drei größten Internetprovider in Österreich ein, nämlich Chello, iNode und Telekom Austria. Sollten Sie bei einem anderen Provider unter Vertrag stehen, so vergleichen Sie bitte die Windows-Beschreibung Ihre Anbieters mit den Lösungen die wir hier vorschlagen. Dort wo sie die meisten Parallelen entdecken, befinden Sie sich am richtigen Weg.

Chello-Produkte sind durch das Kabel-Modem noch am Einfachsten zu handhaben. Sie benötigen einfach nur die weltweit einzigartige Hardware-Adresse (MAC-Adresse) ihrer Linux-Box-Netzwerkkarte. Wenn Sie als *root* am Terminal angemeldet sind, geben Sie *ifconfig eth0* ein, in der zweiten Zeile der Ausgabe können Sie die Hardware-Adresse in der Form von 00:11:a4:41:3e:c2 lesen. Nun rufen Sie beim Chello-Support an und geben an, einen neuen Rechner an der Leitung betreiben zu wollen. Nachdem Sie die MAC-Adresse bekannt gegeben haben, ist die neue Netzwerkkarte nach circa einer halben Stunde bei Chello registriert. In der Zwischenzeit konfigurieren wir die erste Netzwerkkarte so, dass sich sich per DHCP die IP-Adresse holt. Dazu editiern wir die Datei /etc/network/interfaces mit dem Befehl *sudo nano /etc/network/interfaces*. Den richtigen Eintrag entnehmen Sie bitte dem Kasten IP-Konfiguration. Danach die Netzwerkinterfaces mit *sudo /etc/init.d/network restart* neu starten. Die WCM-Linux-Box ist automatisch online sobald Sie das Netzwerkkabel zwischen Chello-Modem und dem Netzwerk-Interface eth0 einstecken und die Registrieung bei Chello durch ist..

Nun zu den DSL-Verbindungen. Es werden zwei Protokolle in …sterreich verwendet. PPTP und PPPoE. Je nach Provider und Verbindungsart (ADSL/xDSL) müssen Sie die WCM-Linux-Box runterschiedlich konfigurieren. Sei benötigen jedenfalls Ihr Datenblatt des Providers auf dem Benutzername, Passwort und DNS-Server stehen.

Um für alle Fälle gerüstet zu sein, müssen Sie folgende Programme installieren: den DHCP-Client, den PpoE-Client und natürlich den PPP-Dämon. Sudo apt-get install dhcp-client pppoe ppp prüft ob die Pakte installiert sind und installiert diese gegebenenfalls nach.

Als erstes behandeln wir ADSL-Verbindungen. Bitte prüfen Sie die Datei /etc/resolv.conf ob die DNS-Server richtig eingetragen sind (sudo less /etc/resolv.conf). Vergleichen Sie die

```
#Optionales maskieren der Pakete wenn die Box #
#als Router verwendet werden soll              #
#Diese Zeilen einfach ans Ende der Datei
#/etc/init.d/firewall_script stellen           #
########################################

echo „Aktiviere NAT..."
echo „1" > /proc/sys/net/ipv4/ip_forward # Initialisierung des
Forwardings
iptables -A POSTROUTING -t nat -o eth1 -j MASQUERADE
echo „Maskierung gestartet!"
echo „Firewall-Script fertig."
```

Einträge mit dem Konfigurationsblatt Ihres Providers. Änderungen können Sie mit dem Editor *nano* vornehmen.

(sudo nano /etc/resolv.conf). Bitte achten Sie auf die korrekte Schreibweise Ð Debian ist sehr sehr heikel wenn es um die Auswertung der Konfigurationsdateien geht.

Als nächstes stellen wir für das erste Netzwerkinterface eth0 die richtige IP-Adresse ein. Sudo nano /etc/network/interfaces bringt uns die richtige Konfigurationsdatei. Der Kasten IP-Konfiguration zeigt die richtigen Einträge. Danach starten wir die Netzwerkdienste mit *sudo /sbin/init.d/network restart* neu.

Das ADSL-Modem sollte jetzt unter der Adresse 10.0.0.138 erreichbar sein. Wir schicken also mit ping -c 3 10.0.0.138 drei Pingpakete an das Modem und erhalten eine Ausgabe die aus mehrer Zeilen besteht, wovon 3 Zeilen in etwa so ausschauen: 64 bytes from 10.0.0.138: icmp_seq=1 ttl=64 time=0.254 ms

Das Modem ist nun erreichbar, als nächstes folgt der Verbindungsaufbau. Dazu müssen in der Datei /etc/ppp/options einge Einträge vorhanden sein. Welche das sind entnehmen Sie bitte der Box IP-Konfiguration. Einige stehen auch schon drinn, sie sind aber durch das Raute-Zeichen # auskommentiert. Es reicht also dieses Zeichen am Anfang der Zeile zu entfernen und schon wird der Eintrag bei der nächsten Auswerttung dieser Datei ausgelesen.

In /etc/ppp/pap-secrets sind Ihr Benutzername sowie Ihr Passwort, getrennt durch einen Abstand und dem Asterisk einzutragen (IhrBenutzername * IhrPasswort). Kommentieren Sie bitte die schon vorhanden Einträge durch das Raute-Symbol aus. Die selben Änderungen sind auch in der Datei /etc/ppp/chap-secrets nötig. Als Ausnahme der Regel stellt sich UTA/Tele2 dar. UTA/Tele2 authentifiziert ausschließlich über CHAP und sperrt Kunden die sich via PAP angemeldet haben. Benennen Sie daher die datei pap-secrets nach pap-secrets.bak um (*sudo mv /etc/ppp/pap-secrets /etc/ppp/pap-secrets.bak*). Sollte eine Sperre aufgetreten sein, müssen Sie beim UTA/Tele2-Support anrufen und die Sperre aufheben lassen.

Als nächstes installieren wir den PPTP-Client mit *sudo apt-get install pptp-linux* und starten den Client durch *sudo pptp 10.0.0.138* . In wenigen Fällen kann es sein dass der Client keine Verbindung zustande bringt, weil er nicht weiß mit welcher Netzwerkkarte er arbeiten muss. Versuchen Sie statt dessen *pptp 10.0.0.138 —localbind 10.0.0.140* .Ob die Verbindung tatsächlich zustande gekommen ist, sehen Sie in dem Sie *ifconfig* aufrufen. Sie bekommen eine Liste der aktiven Netzwerkinterfaces in der Sie die PPTP-Verbindung unter *ppp0* finden können. Ist kein Interface mit diesem Namen eingetragen, so hat was nicht geklappt. Prüfen Sie nochmals ob Sie das Modem anpingen können und halten Sie im Log-File mit *sudo less /var/log/syslog* nach Fehlermeldungen ausschau.

Ist die Verbindung erfolgreich, können Sie versuchen Ihre DNS-Server anzupingen (zB: *ping -c 3 195.3.96.67).* Jetzt müssen wir noch dafür sorgen, dass die Internetverbindung automatisch aufgebaut wird, sobald der Server hochfährt oder die Verbindung vom Provider getrennt wird. Die Provider trennen die Leitung alle paar Stunden, da Sie ja keine Standleitung bezahlt haben.

Das Script *AlwayOn* finden Sie im Kasten, legen Sie es durch *sudo nano /etc/init.d/alwayson* an.

Anschließend legen wir einen symbolischen Link in den Runlevel 2 sodass das Script automatisch gestartet wird wenn der Rechner bootet (*sudo ln -s /etc/init.d/alwayson /etc/rc2.d/S93alwayson).*

Wer über seinen Zugang über PPPoE (PointToPointProtocol over Ethernet) findet, zB diverse iNode xDSL-Produkte (nicht alle!), muss Folgendes beachten: Wir brauchen die PPPoE-Pakete installiert (*sudo apt-get install pppoe pppoeconf pppstatus*) und das Modem an der ersten Netzwerkkarte angeschlossen. Jetzt führen wir gleich *pppoeconf* aus. Das Script zeigt alle Netzwerkkarten an, wir verwenden die erste Karte (eth0). Anschließend versucht es eine Verbindung zum DSL-Modem aufzubauen. Die nächsten zwei Abfragen beantworten wir einfach mit JA, für den Benutzernamen ziehen wir das Datenblatt zu rate. Ebenso für die Passworteingabe im nächsten Schritt. Die Frage ob die DNS-Server übertragen werden sollen und die Frage nach dem automatischen Start beantworten wir auch mit JA. Nun wird die Konfiguration abgeschlossen und eine Verbindung gestartet. Verbindungen können auf der Befehlszeile mit *pon dsl-provider* hergestellt und mit *poff* abgebaut werden. Um die Verbindung nach einer Trennung wieder her zu stellen, modifziern wir die Datei */etc/ppp/ip-down*. Mit dem Befehl *nano* fügen wir ganz am Ende einfach *pon dsl-provider* an. Die Datei ip-down wird nämlich bei jedem Verbindungsabbau ausgeführt.

Wenn Sie sich im Artikel „Netzwerkkonfiguration“ so entschieden haben, dass die WCM-Linux-Box auch das Routen des Netzwerkverkehrs übernehmen soll, dann müssen wir nun das Gateway einrichten. Ein Gateway macht, salopp formuliert, nichts anderes als dass es die internen IP-Adressen (192.168.123.xxx) ins Internet übersetzt.

Dazu müssen zwei Netzwerkkarten vorhanden sein, eine zeigt nach innen (internes Netz), die andere nach außen (Internet). Damit die Box nun als Gateway fungieren kann, lesen Sie den Kasten „Gateway“ und ergänzen das Script *firewall_script* unter */etc/init.d/* mit diesen Einträgen.

Leider kochen viele Internet-Provider Ihr eigenes Süppchen, weshalb dieser Workshop nicht alle Konfigurationsmöglichkeiten abdecken kann. Dennoch sollte es kein Problem sein, mit diesem Workshop und ein bisschen Google eventuelle Fehlkonfiguration zu beseitigen. Die Linux-Box ist jedenfalls online und wartet auf die ersten richtigen Aufgaben im WorldWideWeb. ■

IP-Konfiguration in der Datei
/etc/network/interfaces

Der Abschnitt bei Nutzung eines Hardwarerouters

```
auto eth0
iface eth0 inet static
        address 192.168.123.1
        netmask 255.255.255.0
        network 192.168.123.0
        broadcast 192.168.123.255
        gateway 192.168.123.254
```

Der Abschnitt für das Kabelmodem

```
auto eth0
iface eth0 inet dhcp
```

Der Abschnitt für das erste Interface bei ADSL-Einwahl

```
auto eth0
iface eth0 inet static
        address 10.0.0.140
        netmask 255.255.255.0
        network 10.0.0.0
        broadcast 10.0.0.255
```

Die Einträge in /etc/ppp/options
bei ADSL-Einwahl

```
noipdefault
name „Ihr Benutzname“
noauth
defaultroute
replacedefaultroute
lcp-echo-interval 20
lcp-echo-failure 2
```

„Ihre Benutzername“ muss in Anführungszeichen angegeben werden, bei der Telekom ist der Benutzername die Teilnehmerkennung, bei andern Providern lautet er IhrBenutzername@IhrProvider.at