

Band

1

CHRISTIAN MÜHLBAUER

LINUX Server

Internet-Gateways mit SuSE Linux

LINUX SERVER

Internet-Gateways mit SuSE Linux

Dieses Dokument erhebt keinerlei Anspruch auf Richtigkeit oder Vollständigkeit. Für jegliche Fehler oder Schäden die aus der Nutzung des Dokuments entstehen wird keine Haftung übernommen.

Dieses Dokument ist Urheberrechtlich geschützt. Das Dokument darf nur unter der Voraussetzung weitergegeben werden, dass es vollständig und unverändert weitergegeben wird.

Sofern innerhalb dieses Dokuments Marken- oder Warenzeichen verwendet werden, berechtigt dies nicht zur Annahme, dass diese im Sinne der Marken- oder Warenzeichenschutzgesetze als frei zu betrachten sind. Die Marken- oder Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweils eingetragenen Eigentümer. Der Autor erkennt die Rechte dieser Eigentümer in vollem Umfang an.

© Christian Mühlbauer
Holunderweg 4 • 93494 Waffenbrunn.
Telefon 0 99 71 / 7 69 00 25 • Fax 0 99 71 / 7 69 00 26
e-mail: chris@cmuehlbauer.de
Internet: <http://www.cmuehlbauer.de>

Inhaltsverzeichnis

EINFÜHRUNG

Über dieses Dokument	1
Systemumgebung	1
Voraussetzungen	2
Legende	2

KAPITEL 1 • GATEWAY

Dialing	3
SMPPPD	3
Modem-Verbindung	3
ISDN-Verbindung	4
DSL-Verbindung	4
Problembehandlung	4
Router	5
Network Address Translation.....	5

KAPITEL 2 • FIREWALL

SuSE Firewall 2.....	6
“SuSE Personal-Firewall” deaktivieren	6

KAPITEL 3 • PROXY

Squid	7
Transparenter Proxy.....	8

KAPITEL 4 • DNS

BIND	9
Problembehandlung	10
WVDIAL-Anpassung	10
Firewall-Anpassung	10
IPTABLES-Anpassung.....	10
DNS-Zonen	12

KAPITEL 5 • WEB-SERVER

Apache	13
Startseite.....	14

KAPITEL 6 • STATISTIKEN

Webalizer.....	15
ISDN Connection Report	15

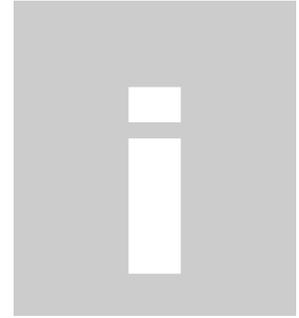
KAPITEL 7 • DHCP

DHCPD	16
--------------------	-----------

KAPITEL 8 • NET TIME PROTOCOL

XNTP	17
daytime	17
Aktualisierungs-Script	18

EINFÜHRUNG



Über dieses Dokument

Mit am verbreitetsten ist Linux derzeit in der Verwendung als Server. Eine der populärsten Funktion dabei ist der Einsatz als Internet-Gateway. Dabei ist nur der Linux-Server mit dem Internet verbunden und stellt seinerseits allen anderen Rechnern im Netz den Zugang zum Internet zur Verfügung.

In seiner kleinsten Form muss ein Gateway den Internetzugang (Dialing), die Weiterleitung der IP-Pakete (Routing) und die Umwandlung der Netzwerkadressen (NAT – Network Address Translation) realisieren. Weiterhin sinnvoll ist die Erweiterung um Firewall und Proxy. Darüber hinaus kann es evtl. noch sinnvoll sein andere Funktionen, wie z.B. DNS, DHCP, NTP, usw., auf dem Server zu integrieren.

Der Aufbau eines solchen Systems mit SuSE Linux ist in diesem Dokument beschrieben. Das Dokument beschränkt sich dabei auf die grundlegenden Notwendigkeiten. In erster Linie werden das Hinzufügen der notwendigen Dienste und die Anpassung der Konfigurationsdateien beschrieben.

Systemumgebung

Das Dokument wurde unter Annahme folgender Systemumgebung erstellt:

Linux-Installation

Distribution: SuSE

Version: 8.0

Provider

Name: T-Online

DNS-Server: 194.25.2.129

Netzwerk

Typ: Ethernet

Netz: 192.168.0.x

Netmask: 255.255.255.0

Domain: testnet.de

Gateway

Hostname: gateway

IP-Adresse: 192.168.0.254

EINFÜHRUNG

Voraussetzungen

Um mit diesem Dokument arbeiten zu können, werden grundsätzliche Linux-Kenntnisse vorausgesetzt. Der Anwender sollte wissen, wie Pakete installiert werden und wie man Dateien editieren kann.

Auf dem zukünftigen Server muss bereits ein SuSE Linux installiert und der Zugang zum internen Netzwerk möglich sein. Da das Gateway der einzige Rechner ist, der mit dem Internet verbunden wird, handelt es sich dabei um ein sicherheitskritisches System. Das SuSE Linux sollte daher als Minimalsystem installiert werden.

Für die Fehlersuche und Kontrolle ist es außerdem hilfreich das Paket „tcpdump“ zu installieren.

Legende



Dieses Symbol kennzeichnet Installationen die vorgenommen werden müssen.



Dieses Symbol kennzeichnet Konfigurationen die durchgeführt werden müssen.



Dieses Symbol kennzeichnet Befehle die ausgeführt werden müssen.



Dieses Symbol kennzeichnet Dateien welche angepasst oder verwendet werden müssen.



Dieses Symbol kennzeichnet Änderungen die in einer Datei vorgenommen werden müssen.

Hinweis:

In der Beschreibung zum Dialing wird die Vorgehensweise für Modem, ISDN und DSL beschrieben. In allen weiteren Beispielen wird jedoch von einer ISDN-Verbindung ausgegangen.

Dialing

Als erstes muss der zukünftige Gateway-Server mit dem Internet verbunden werden. Dies kann über Modem, ISDN oder DSL erfolgen. Das wichtigste dabei ist, den Internet-Zugang so zu konfigurieren, dass die Verbindung bei Bedarf automatisch aufgebaut wird. Dafür sorgt jeweils die Einstellung: „**Dial-On-Demand**“.

Verbindungen ins Internet laufen über PPP (Point-To-Point Protocol). Traditionell sorgt in Linux der PPPD für den Verbindungsaufbau. Für ISDN gibt es extra den . SuSE setzt nun diesen Dämonen noch den SMPPPD (SuSE Meta PPP Dämon) voran, der die komplette Steuerung der Elemente übernimmt.

SMPPPD



YAST2 – Paket „SMPPPD“ installieren.

Diese Installation bewirkt die Anlage folgender (wichtiger) Dateien:



/etc/smpppd.conf
/etc/ppp/options
/etc/ppp/peers/demand



YAST2 – System – Runlevel Editor:
SMPPPD in Runlevel 3 starten



Startbefehl:
rcsmpppd start

Modem-Verbindung



YAST2 – Network/Basic - Modem configuration

Diese Einstellung bewirkt die Änderung bzw. Anlage folgender Dateien:



/var/lib/smpppd/smpppd.var.conf
/etc/sysconfig/network/ifcfg-ppp0
/etc/sysconfig/network/providers/Tonline

GATEWAY

ISDN-Verbindung



YAST2 – Paket „i4L“ installieren.
+ Update von www.suse.de, da Fehlerhaft.



YAST2 – Network/Basic - ISDN configuration

Diese Einstellung bewirkt die Änderungen bzw. Anlage folgender Dateien:



`/var/lib/smpppd/smpppd.var.conf`
`/etc/sysconfig/network/ifcfg-ipp0`
`/etc/sysconfig/network/providers/Tonline`

DSL-Verbindung



YAST2 – Network/Basic - DSL configuration

Diese Einstellung bewirkt die Änderung bzw. Anlage folgender Dateien:



`/var/lib/smpppd/smpppd.var.conf`
`/etc/sysconfig/network/ifcfg-eth1`
`/etc/sysconfig/network/providers/Tonline`

Problembehandlung

Sollte die Verbindung nicht automatisch trennen, so kann dies daran liegen, dass der Server ständig überprüft ob der Provider noch verfügbar ist. In diesem Fall muss folgende Anpassung vorgenommen werden:



`/etc/ppp/options`
lcp-echo-interval 30 (auskommentieren)

GATEWAY

Router

Der Linux-Server selbst kann zwar jetzt eine Verbindung ins Internet herstellen, um aber auch anderen Rechnern im Netzwerk den Zugang zum Internet zu ermöglichen, muss der Server die ankommenden Pakete ins Internet weiterleiten, also als Router fungieren.



YAST2 - System - Sysconfig Editor - Network - Base - Ip - IP_FORWARD=yes



Aktivierung:
rcnetwork restart

Network Address Translation

Durch die letzte Einstellung werden zwar die Pakete der anderen Rechner an das Internet weitergeleitet, die Antworten aus dem Internet kommen jedoch nicht mehr an, weil sie an die vom Provider zugewiesene Adresse des Gateway-Servers gesendet werden und im internen Netzwerk andere, nicht registrierte, Adressen verwendet werden.

Es muss also für die Umsetzung der Adressen durch den Gateway-Server gesorgt werden. Dies erledigt das sogenannte NAT (Network Address Translation). NAT ist in Linux ein Teil der IPTABLES. Diese werden unter SuSE Linux am einfachsten über die „SuSE Personal Firewall“ angesprochen.



YAST2 – Paket „personal-firewall“ installieren.



/etc/sysconfig/personal-firewall



```
REJECT_ALL_INCOMING_CONNECTIONS = „ipp0 masq“
```



YAST2 – System – Runlevel Editor:
personal-firewall.initial in Runlevel 3 starten
personal-firewall.final in Runlevel 3 starten



Aktivierung:
rcnetwork restart

Damit ist das Gateway prinzipiell einsatzbereit. Die IP-Adresse des Gateway-Servers muss bei den anderen Rechnern als „Default Gateway“ eingestellt werden. Der DNS-Server des Providers muss ebenfalls am Client eingestellt werden.

SuSE Firewall 2

Um NAT zu ermöglichen ist bereits die „SuSE Personal-Firewall“ im Einsatz. Wesentlich mehr Steuerungsmöglichkeiten (welche für die Nachfolgenden Anwendungen auch benötigt werden) bietet aber die „SuSE Firewall 2“. Es ist daher sinnvoll auf diese Umzusteigen.



YAST2 – Paket „SuSE Firewall 2“ installieren.



/etc/sysconfig/SuSEfirewall2

```
FW_DEV_EXT = "ipp0"
FW_DEV_INT = "eth0"
FW_ROUTE = "yes"
FW_MASQUERADE = "yes"
FW_MASQ_NETS = "192.168.0.0/24"
FW_PROTECT_FROM_INTERNAL = "no"
FW_AUTOPROTECT_SERVICES = "yes"
```



YAST2 – System – Runlevel Editor:

SuSEfirewall2_final in Runlevel 3 starten

SuSEfirewall2_init in Runlevel 3 starten

SuSEfirewall2_setup in Runlevel 3 starten



Startbefehl:

/sbin/SuSEfirewall2 start

Die „SuSE Personal-Firewall“ muss jetzt natürlich deaktiviert werden.

“SuSE Personal-Firewall” deaktivieren



YAST2 – System – Runlevel Editor:

personal-firewall.initial aus Runlevel 3 entfernen

personal-firewall.final aus Runlevel 3 entfernen



/etc/sysconfig/personal-firewall

```
REJECT_ALL_INCOMING_CONNECTIONS = no
```



rcnetwork restart

Squid

Neben der Firewall kann der Einsatz eines Proxy-Servers zusätzliche Sicherheit bringen. Außerdem bringt bereits ein Cache in der Größe von ca. 2 GB einen spürbaren Geschwindigkeitsvorteil beim Zugriff auf Web-Seiten.



YAST2 – Paket „SQUID“ installieren.



/etc/squid.conf



```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
acl Netzwerk srcdomain .testnet.de
acl Sperrliste dstdomain "/usr/share/squid/blocklist.txt"
http_access allow Netzwerk
http_access deny Sperrliste

httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on

cache_dir ufs /proxy 1800 16 256
maximum_object_size 20480 KB
```

Die letzten beiden Zeilen legen den Cache des Proxy in einem besonderen Verzeichnis (**/PROXY**) an, welches sich auch auf einer anderen Festplatte befinden kann. Die Größe des Caches wird dabei auf 2 GB festgelegt.

Als Eigentümer des Verzeichnisses muss SQUID eingetragen werden:



chown squid /proxy



**YAST2 – System – Runlevel Editor:
squid in Runlevel 3 starten**



***Startbefehl:
rcsquid start***

Der Proxy-Server ist jetzt einsatzbereit. Allerdings muss die IP-Adresse und der Port (8080) des Proxies manuell auf dem Client in den Browser eingetragen werden.

PROXY

Transparenter Proxy

Die Verwendung des Proxies ist also von der Einstellung im Browser abhängig. Werden diese Einstellung nicht vorgenommen oder gelöscht, so wird der Proxy umgangen. Die Lösung hierfür ist ein sog. „transparenter“ Proxy. Das heißt alle IP-Anforderungen werden über den Proxy „gezwungen“. Die Umleitung der IP-Pakete erledigt die Firewall.

Die Firewall muß also noch angewiesen werden, alle Anforderungen für Webseiten über den Proxy zu leiten:



/etc/ sysconfig/SuSEfirewall2

```
FW_REDIRECT="192.168.0.0/24,0/0,tcp,80,3128
```

Jetzt braucht der Proxy nicht mehr im Browser eingestellt werden, sondern alle Anfragen laufen automatisch über den Proxy.

Hinweis:

Die Einrichtung des Gateways ist hiermit eigentlich abgeschlossen. Es werden aber noch andere Installationen auf den Rechner beschrieben, welche den Nutzen des Gateways erweitern können.

Es sei darauf hingewiesen, dass die jetzt folgenden Installationen die Sicherheit wieder herabsetzen.

Es ist also genau abzuwägen ob die folgenden Einrichtungen auf dem Gateway-Server oder evtl. auf eine andere Maschine bzw. gar nicht erfolgen sollten.

Die bisherige Einrichtung des Gateways ermöglicht Ihnen bereits den Zugriff auf das Internet über IP-Adressen. Um aber auch über Domain-Namen auf das Web zugreifen zu können muss der DNS-Server des Internet-Providers auf jedem Rechner im Netzwerk eingestellt werden.

An dieser Stelle bietet es sich an den Gateway-Server auch zum DNS-Server zu machen, so das dieser die Namensauflösung über den DNS-Server des Internet-Providers übernimmt. Die Rechner im Netzwerk stellen dabei Ihre Namens-Anfragen an den Gateway-Server. Sofern dieser die Adresse aufgrund seines Caches nicht selbst auflösen kann, stellt dieser seinerseits eine Anfrage an den DNS des Internet-Providers (in diesem Fall „Forwarder“ genannt).

BIND



YAST2 – Paket „BIND9“ installieren



/etc/named.conf

```
forwarders {194.25.2.129;};  
forward first;
```

Damit auch das Gateway sich selbst als DNS-Server benutzt, und nicht den vom Provider übermittelten, ist folgende Anpassung notwendig:



YAST2 - System - Sysconfig Editor - etc -
MODIFY_RESOLV_CONF_DYNAMICALLY = „no“

Natürlich muss jetzt auch die eigene IP-Adresse als DNS auf dem Gateway eingestellt werden:



YAST2 – Network/Advanced – Hostname and DNS



YAST2 – System – Runlevel Editor:
named in Runlevel 3 starten



Startbefehl:
rcnamed start

Damit ist der DNS-Server als sog. „Caching-Only-Server“ eingerichtet. Auf den Rechnern im Netzwerk muss jetzt die IP-Adresse des Gateways als DNS-Server eingetragen werden.

DNS

Problembehandlung

WVDIAL-Anpassung

Bei der Nutzung von Modem wird vom PPP-Dämon das Dienstprogramm WVDIAL zum Verbindungsaufbau genutzt. WVDIAL hat bei installiertem DNS-Server die Angewohnheit ständig zu Versuchen den Forwarder zu erreichen. Das führt dazu, dass eine Verbindung aufgebaut und aufgrund der ständigen Übertragungen nicht mehr getrennt wird.

Das Problem kann wie folgt gelöst werden:



```
/etc/wvdial.conf  
Auto DNS = off (default: on)  
Check DNS = off (default: on)
```

Firewall-Anpassung

Bei **SuSE 7.3** trat das Problem auf, dass die Namensauflösung von Internet-Adressen nicht funktionierte, weil die Antworten des Forwarders durch die „SuSE Firewall 2“ blockiert wurden.

Das Problem resultierte aus einem fehlerhaften IP-UP Script. Es gibt jedoch ein angepasstes IP-UP Script welches nur umkopiert werden muss:



```
cp /usr/share/doc/packages/SuSEfirewall2/ip-up /etc/ppp/ip-up
```

IPTABLES-Anpassung

Eine andere Lösung des Forwarding-Problems der „SuSE Firewall 2“ unter **SuSE 7.3** soll hier als Beispiel für die manuelle Anpassung der IPTABLES aufgeführt werden.



```
/etc/ppp/ip-up  
export LOCALIP (Zeile einfügen)
```

Dieser Befehl trägt die erhaltene IP-Adresse in eine Speichervariable ein.

DNS



/etc/ppp/ip-up.local



```
#!/bin/sh
# Firewall-Anpassung wg. Dialup-Verbindung
IPT=/usr/sbin/iptables
Echo „Die erhaltene IP-Adresse lautet: $LOCALIP
$IPT -D INPUT -j LOG --log-tcp-options --log-ip-options --log-level 4 --
log-prefix SuSE-FW-UNALLOWED-TARGET
$IPT -D INPUT -j DROP
$IPT -A INPUT -j ACCEPT -s 194.25.2.129 -d "$LOCALIP"
$IPT -A INPUT -j LOG --log-tcp-options --log-ip-options --log-level 4 --
log-prefix SuSE-FW-UNALLOWED-TARGET
$IPT -A INPUT -j DROP
```



chmod 744 /etc/ppp/ip-up.local



/etc/ppp/ip-down.local



```
#!/bin/sh
# Firewall-Anpassung wg. Dialup-Verbindung
IPT=/usr/sbin/iptables
Echo „Die erhaltene IP-Adresse lautet: $LOCALIP
$IPT -D INPUT -j ACCEPT -s 194.25.2.129 -d „$LOCALIP“
```



chmod 744 /etc/ppp/ip-down.local

Die letzten beiden Skripte sind neu zu erstellen und werden von IP-UP bzw. IP-DOWN automatisch aufgerufen.

DNS

DNS-Zonen

Werden zusätzliche Zonen definiert, so kann der DNS-Server auch zur Namensauflösung im internen Netzwerk verwendet werden.

```
 /etc/named.conf  
 # You can insert further zone records for your own domains below.  
  
zone "testnet.de" in {  
    type master;  
    file "testnet.de.zone";  
    notify no;  
};  
  
zone "0.168.192.in-addr.arpa" in {  
    type master;  
    file "0.168.192.in-addr.arpa.zone";  
    notify no;  
};
```

```
 /var/named/testnet.de.zone  
 $TTL      2D  
@          IN      SOA      testnet.de.      root.testnet.de. (  
    1          ;Seriennummer  
    1D        ;Refresh Intervall  
    2H        ;Retry  
    1000H     ;Expire  
    2D        ;Minimum TL  
)  
@          IN      NS       gateway.testnet.de  
client1   IN      A        192.168.0.1  
client2   IN      A        192.168.0.2  
client3   IN      A        192.168.0.3  
gateway   IN      A        192.168.0.254  
www       IN      CNAME    gateway
```

```
 /var/named/0.168.192.in-addr.arpa.zone  
 $TTL      2D  
@          IN      SOA      0.168.192.in-addr.arpa. root.testnet.de. (  
    1          ;Seriennummer  
    1D        ;Refresh Intervall  
    2H        ;Retry  
    1000H     ;Expire  
    2D        ;Minimum TL  
)  
@          IN      NS       gateway.testnet.de.  
1          IN      PTR      client1.testnet.de.  
2          IN      PTR      client2.testnet.de.  
3          IN      PTR      client3.testnet.de.  
254       IN      PTR      gateway. .testnet.de.
```

```
 rcnamed restart
```

Jetzt kann auf die Netzrechner auch über Hostnamen zugegriffen werden. Dabei wurde gleich ein Alias www für das Gateway angelegt, da dieses im nächsten Schritt um einen Web-Server erweitert wird.

Apache

Eine weitere gute Leistung des Gateways wäre jetzt die Bereitstellung einer Internet-Startseite auf der man verschiedene Links für den Einstieg ins Internet bereitstellen könnte. Dies kann über einen Webserver auf dem Gateway realisiert werden.

Außerdem wird der Webserver benötigt um später die Statistiken über die ISDN-Zugriffe, Proxy und natürlich auch des Webserver selbst, auf den Clienten abfragen zu können.



YAST2 – Paket „apache“ installieren.



/etc/httpd/httpd.conf

```
ServerRoot "/web" (statt /usr/local/httpd)
ServerName gateway.testnet.de
DocumentRoot "/web" (statt /usr/local/httpd/htdocs)

<Directory "/web"> (statt /usr/local/httpd/htdocs)
<Files /web/index.htm*> (statt /usr/local/httpd/htdocs/index.htm*)
```

Die letzten Einstellungen sorgen dafür, dass die zu veröffentlichen Seiten in einem eigenen Verzeichnis (/web) liegen.



**YAST2 – System – Runlevel Editor:
apache in Runlevel 3 starten**



**Startbefehl:
apache start**

Durch den Alias www der Bereits für die IP-Adresse des Gateways im DNS angelegt ist, kann jetzt im Browser direkt die Adresse <http://www.testweb.de> eingegeben werden, um auf die definierte Startseite zuzugreifen.

WEB-SERVER

Startseite

Anbei ein Beispiel für eine Startseite, welche auch gleich die Links zu den Statistiken enthält, welche im nächsten Kapitel eingerichtet werden.



/web/index.html



```
<html>
<head>
<title>TESTWEB Intranet</title>
</head>

<body bgcolor=#FFFFFF>

<table border=0 cellpadding=10 cellspacing=0>

<tr>
<td width=80 height=80 rowspan=2 bgcolor=green align=left valign=top>
</td>
<td width=560 height=80 bgcolor=green align=right valign=middle>
<font face=Courier New,Courier,mono size=5 color=white><b>+++ TESTWEB
Intranet +++ </b></font>
</td>
</tr>

<tr>
<td width=560 height=400 align=left valign=top>
<b><u>Links:</u></b><br>
<br>
<a href=http://www.google.de/>GOOGLE</a><br>
<br>
<b><u>Statistiken:</u></b><br>
<br>
<a href=http://www.testnet.de/squidstat/index.html>Auswertung der Proxy-
Zugriffe (SQUID)</a><br>
<br>
<a href=http://www.testnet.de/apachestat/index.html>Auswertung der
Webserver-Zugriffe (APACHE)</a><br>
<br>
<a href=http://www.testnet.de/cgi-bin/isdnrep.cgi>Auswertung der ISDN-
Verbindungen</a><br>
</td>
</tr>

</table>

</body>

</html>
```

SQUID und Apache protokollieren alle ihre Aktivitäten in LOG-Files. Genauso wird der Aufbau und die Dauer der ISDN-Verbindungen protokolliert.

Diese LOG-Files können mit verschiedenen Tools in gut lesbare Web-Seiten umgewandelt werden.

Webalizer



YAST2 – Paket „webalizer“ installieren.



crontab –e

```
*/15 * * * * webalizer -F squid /web/squidstat  
/var/log/squid/access.log -Q  
*/15 * * * * webalizer -F clr /web/apachestat  
/var/log/httpd/access_log -Q
```

Alle 15 Minuten erzeugt nun webalizer http-Dokumente. Diese Internet-Seiten werden praktischerweise gleich in Unterverzeichnissen zum Verzeichnis /web abgelegt, welches unser Web-Server veröffentlicht. Da auch unsere Startseite bereits die Links auf diese Dateien enthält, können von jedem Client aus die Statistiken eingesehen werden.

Jetzt fehlt noch die Statistik über die ISDN-Verbindungen.

ISDN Connection Report



cp /usr/bin/isdnrep /usr/local/httpd/cgi-bin/isdnrep.cgi

Die Web-Seiten werden in diesem Fall „Realtime“ beim Aufruf des Scripts generiert.

DHCPD

Um nicht auf jedem Clienten im Netzwerk das Default-Gateway und den DNS-Server einstellen zu müssen kann es weiterhin sinnvoll sein einen DHCP-Server zu integrieren.



YAST2 – Paket „dhcp-Server“ installieren.



/etc/dhcpd.conf



Allgemeine Definitionen

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;             # 2 hours
ddns-update-style none;
```

```
# Einstellungen
# Die eigentliche Aufgabe des DHCP-Servers
# besteht darin diese Angaben an die Clients zu übermitteln.
```

```
option domain-name "testnet.de";
option routers 192.168.0.254;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.0.254
```

```
# Addressbereich
```

```
subnet 192.168.0.0 netmask 255.255.255.0
{
  range 192.168.0.200 192.168.0.250;
}
```

```
# Feste IP-Adressen
```

```
host client1
{
  hardware ethernet 00:00:00:00:00:00;
  fixed-address 192.168.0.1;
}
```

Wenn die Feste IP-Adressen – Vergabe gewünscht wird, muss der letzte Eintrag „host“ für jeden Client der eine feste IP-Adresse bekommen soll wiederholt werden. Ansonsten kann er weggelassen werden.



**YAST2 – System – Runlevel Editor:
dhcpd in Runlevel 3 starten**



**Startbefehl:
*rcdhcpd start***

In einem Netzwerk mit vielen Diensten, so wie sie zwischenzeitlich auf dem Gateway implementiert sind, gestaltet sich die Fehlersuche teilweise sehr schwierig. Das wichtigste sind dabei die LOG-Dateien. Um aber LOG-Dateien auf verschiedenen Rechnern vergleichen zu können, ist es unerlässlich dass alle Rechner im Netzwerk exakt die gleiche Zeit aufweisen.

Ideal ist dazu die Erweiterung des Gateways zum NTP-Server. Das Gateway aktualisiert dabei seine Uhrzeit über Internet an einem Zeitserver. Die Rechner im Netzwerk synchronisieren sich dann mit dem Gateway.

XNTP



YAST2 – Paket „xntp“ installieren.



YAST2 – Sysconfig editor – Base-Administration- Time-Synchronisation – XNTPD_INITIAL_NTPDATE = ptbtime1.ptb.de



YAST2 – System – Runlevel Editor:
xntpd in Runlevel 3 starten



Startbefehl:
rcxntpd start

daytime



YAST2 – Paket „inetd“ installieren.



YAST2 – Network/Basic – Start/stop services (inetd) –
daytime (tcp + udp) aktivieren



YAST2 – System – Runlevel Editor:
xntpd in Runlevel 3 starten



Startbefehl:
rcinetd start

NET TIME PROTOCOL

Aktualisierungs-Script

Folgendes Script sorgt dafür, dass die Zeit am Gateway nicht nur beim Start des Gateways, sondern auch bei jedem Verbindungsaufbau ins Internet aktualisiert wird.

```
 /etc/ppp/ip-up.local  
#!/bin/sh  
  
 # Uhrzeit nach NTP-Server stellen  
echo "--- UHRZEIT NACH NTP-SERVER STELLEN ---"  
echo "Stoppen von XNTPD"  
/etc/init.d/xntpd stop  
echo "Start von XNTPD mit Initial-NTPDate"  
/etc/init.d/xntpd start  
echo "Anpassung der Hardware-Uhr"  
/sbin/hwclock --systemh  
/sbin/hwclock --show
```

```
 chmod 744 ip-up.local
```

Index

A

Alias	12
Apache	13

B

BIND	9
-------------------	---

C

Cache	7
Caching-Only-Server	9
crontab	15

D

daytime	17
Default Gateway	5
DHCPD	16
DHCP-Server	16
Dialing	3
Dial-On-Demand	3
Distribution	1
DNS-Server	9
DNS-Zonen	12
Domain	1
Domain-Namen	9
DSL	4

F

Firewall	6
Forwarder	9

G

Gateway	1
----------------------	---

H

Hostname	1
-----------------------	---

I

IPTABLES	10
IP-UP Script	10
ISDN	4
ISDN Connection Report	15

M

Modem	3
--------------------	---

N

NAT	5
Netmask	1
NTP-Server	17

P

Point-To-Point Protocol	3
Port	7
PPPD	3
Provider	1
Proxy	7

R

Router	5
---------------------	---

S

Sicherheit	8
SMPPPD	3
Squid	7
Startseite	14
Statistiken	15
Systemumgebung	1

T

tcpdump	2
Transparenter Proxy	8

V

Voraussetzungen	2
------------------------------	---

W

Webalizer	15
Webserver	13
WVDIAL	10

X

XNTP	17
-------------------	----

Z

Zeit	17
-------------------	----
