DNS Server (named) und Apache2 unter OS/2

www.anetgmbh.ch

Hinweis:

Auf der Website http://os2.a-net.ch finden sich REXX-Programme, welche die Installation von named und Apapche2 unter OS/2 und eCS erleichtern.

Am besten kopiert man alles auf eine CD (ins Root-Verzeichnis)
und behält die Verzeichnisstruktur bei. Dann ruft man auf der CD menu.cmd auf.

Benutzung wie immer auf eigene Gefahr!

DNS - Domain Name Service (Port 53)

- Setzt Namen in IP-Adressen um
  - z.B. www.anetgmbh.ch --> 195.141.97.123
- teilweise auch umgekehrt (Reverse Lookup)
  - z.B. 195186.1.110 --> dns1.bluewin.ch
- Server-Hierarchie:
  - Root-Server für ganzes Internet (ca. 15 Stück)
  - DNS-Server für eine/mehrere Domänen (z.B. vom Provider)
  - Registrierung
    - ICANN (weltweit: .com .org .edu .gov...)
    - SWITCH: Schweiz und Lichtenstein (.ch und .li)
- Name-Server unter OS/2
  - Bind (bind824.zip) herunterladen von hobbes.nmsu.edu
  - auspacken, konfigurieren und starten mit:
    - **named.EXE -c C:\MPTN\ETC\named.conf**

A-NET

Der DNS-Dienst basiert auf den Root-Servern im Internet A.ROOT-SERVERS.NET. In jedem Land gibt es eine Stelle, welche die lokalen Name-Server verwaltet.

Ein Name Server kann zu einer Adresse www.anetgmbh.ch die zugehörige IP-Adresse liefern, oft auch umgekehrt. Für jede Zone sind mindestens zwei DNS zuständig. Weiss ein DNS im Internet die Antwort nicht, fragt er, welche Server dafür zuständig sind (SOA Source of Authority) und fragt dann diese Server an.

Für kleine Netzwerke, in denen kein DNS betrieben werden soll, ist das neue MulticastDNS gedacht. Obwohl kein DNS im Netzwerk betrieben wird, kann mit DNS-Namen gearbeitet werden. Die Zone *muss* dann xxxxx.local heissen. Wenn nun eine Adresse mit .local gesucht wird, geht die Anfrage an die Multicast Adresse 224.0.0.251 an den Port 5353 und es wird keine DNS gefragt.

DNS - Domain Name Service

- Testen eine DNS:
  - nslookup (Win NT, 2000, XP, Linux bis SuSE 8.2, OS/2)
  - dig (Linux, OS/2) auch für IP V6 geeignet
  - Beispiel mit nslookup:

▸ nslookup [Enter]	Programm starten
▸ www.a-net.ch [Enter]	Abfrage einer Adresse (A-Record)
▸ set qt=**soa** [Enter]	Query Type = Source of Authority
▸ a-net.ch [Enter]	Domäne a-neti.ch abfragen
▸ set qt=**ns** [Enter]	Query Type = Name-Server
▸ a-net.ch [Enter]	Domäne a-net.ch abfragen
▸ set qt=**mx** [Enter]	Query Type = Mail Exchanger
▸ a-net.ch [Enter]	Domäne
▸ set qt=**a** [Enter]	Normale Adress-Records abfragen
▸ www.a-net.ch [Enter]	Names eines Hosts
▸ exit [Enter]	nslookup beenden

A-NET

Der Befehl nslookup beherrscht zwar nur IP V4, ist aber auf vielen Plattformen verfügbar und arbeitet überall mit der gleichen Syntax - einmal lernen - überall brauchen!

Erfragen kann man einfache A-Records (Adressen von Systemen), aber auch die authoritativen Server einer Domain (SOA) und den Mail Exchanger einer Domain (MX). Mit NS können die Name-Server erfragt werden.

Unter Linux und OS/2 (im bind824.zip) steht auch das Programm dig zum Testen eines DNS zur Verfügung. Dabei wird mit einem @-Zeichen der zu fragende DNS angegeben:

• dig	@195.186.1.110	www.anetgmbh.ch	(A-Record)
• dig	@195.186.1.110	anetgmbh.ch mx	(MX-Record)
• dig	@195.186.1.110	anetgmbh.ch soa	(SOA-Record)
• dig	@195.186.1.110	anetgmbh.ch ns	(NS-Record)

DNS-Files

- Files für den DNS (named = Name-Server)
  - **named.conf**
    - legt die Zonen fest, für die der DNS zuständig ist
    - Primary Zonen: für diese Zone ist dieser DNS bestimmend
    - Secondary: Backup DNS, kopiert das Zonen File vom Primary
    - Forward Lookup Zonen: Name --> IP-Adresse
    - Reverse Lookup Zonen: IP-Adresse --> Name
  - Zonen-Files (\var\lib\named\master)
    - **a-net.intern** : Daten für Domain a-net.intern
    - **112.168.192.in-addr.arpa** : Daten für Reverse Lookup Subnet 192.168.112.0
- Record-Typen in den Zonen-Files
  - SOA: Origin: bezeichnet den Namen der Zone und die Gültigkeitsdauer
  - A-Record: normaler Address-Record für einen Namen/IP
  - NS-Reocord: bezeichnet einen DNS für diese Zone
  - MX-Record: bezeichnet den Mail-Server für diese Domain
  - PTR-Record: Reverse Lookup Eintrag für eine IP-Adresse/Name
  - CNAME-Record: Alias für einen definierten Namen

Die Files der DNS-Server sind auf den meisten Systemen gleich, da sie ja alle auf dem gleichen RFC 1034 und 1035 basieren. Ältere DNS (z.B. WSeB) verwenden named.boot als Hautpkonfiguration, neuere haben eine named.conf. In beiden Fällen enthält die Datei eine Lister der Zonen und Reverse-Lookup-Zonen, für die dieser DNS Antwort geben kann.
Ausserdem werden je nachdem root.hints definiert. Darin sind die Namen der Root-Server des ganzen DNS-Systems aufgeführt. Diese werden für alle anderen Auskünfte hinzugezogen. Die aktuellen Namen dieser Server können mit nslookup angezeigt werden, wenn man den Abfragetyp auf NS setzt (set qt=ns) und als Domäne . (Punkt) angibt.
Pro Zone wird je ein Zonenfile erstellt, auch für die Reverse-Lookup Zonen gibt es je ein File.
Die Zonen-Files für die Slave-Zonen muss man *nicht* erstellen, diese werden bei der ersten Verbindung zum Master heruntergeladen (=Zonen Transfer).

Beispiel \mptn\etc\named.conf

```
options {                                   allgemeine Angaben
    directory "/var/lib/named";             hier sind die Zonen-Files gespeichert
    forwarders { 195.186.1.110; };          DNS des Providers, hier dns1.bluewin.ch
    forward first;                          (wird angefragt für alle anderen Domains)
    notify no;                              Slaves nicht benachrichtigen bei Änderungen
};
zone "a-net.ch"    {                        Zone  a-net.ch
    type slave;                             dieser DNS ist Secondary  (=Slave) dieser Zone
    file "slave/a-net.ch";                  Name des Zonen-Files
    masters  {
          81.6.49.206;                      von diesem DNS werden die Daten kopiert
          };
};
zone "anet.intern"  {                       Zone a-net.intern
    type master;                            dieser DNS ist der Master dieser Zone
    file "master/a-net.intern";             Name des Zonen-Files
};                                          (; nicht vergessen!)
zone "112.168.192.in-addr.arpa" in {        Reverse Lookup Zone für 192.168.112.0
    type master;                            dieser DNS ist Master
    file "master/112.168.192.in-addr.arpa"; Name des reverse lookup-Zonen-Files
};                                          (; nicht vergessen!)
```

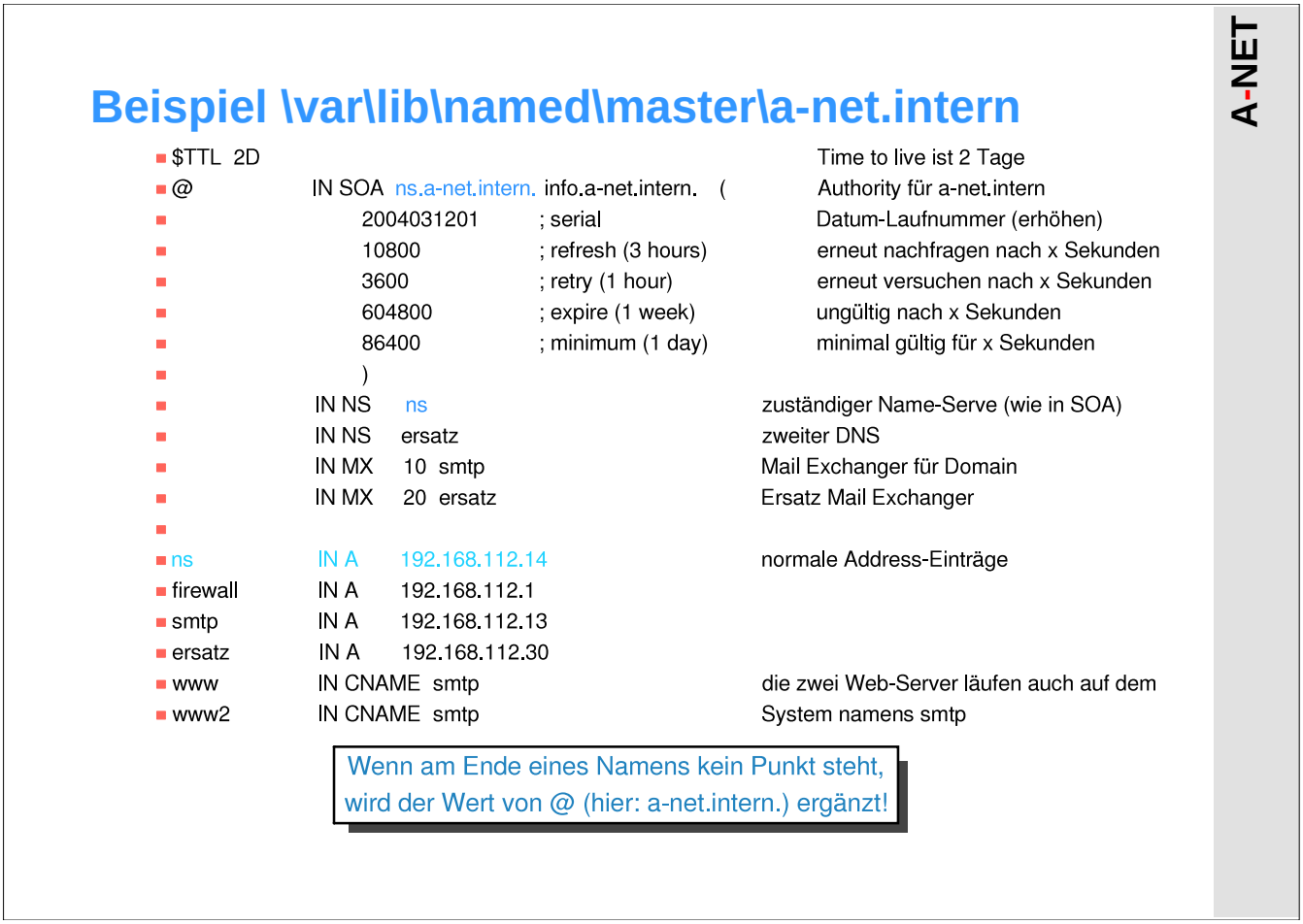
Der Eintrag directory "/var/lib/named" bezeichnet das Verezichnis, in dem die ZonenFiles liegen. Dort gibt es eine Verzeichnis master für die Zonen (=Domänen) für die dieser Server Master ist und slave für diejenigen Zonen, für die er Slave (oder secondary) ist.

Der Eintrag forwarders bewirkt, dass Anfragen, die der DNS nicht selber beantworten kann, an den/die hier aufgeführten DNS des Providers weitergeleitet werden. Ohne forwarder werden die Root-Sever gefragt (root.hint)

Wird eine Zone eingetragen, für die der DNS "slave" ist, wird das Zonenfile vom angegebenen "master" kopiert und in die angegebene Datei kopiert. Diesen Vorgang nennet man Zonen-Transfer.

Für jede Zone, für die dieser DNS "master" ist, sollte auch eine Reverse Lookup Zone erstellt werden. Diese liegt in der Pseudo-Domäne in-addr.arpa und hat die restliche IP-Adresse rückwärts eingetragen. Beachten Sie, dass es sich hier immer um ein Class C Netz handelt. Soll der Reverse Lookup für ein kleineres Subnet funktionieren, muss der zuständige Provider eine Zone Delegation konfigurieren. Fehlt diese, erhält eine Station, die nicht zufällig Ihren DNS abfrägt, einen Namen aus dem Bereich des Providers als Antwort.

Wichtiger Hinweis zu SuSE 9.1 und 9.2:
Die Domänen xxxx.local haben eine neue Bedeutung: .local sind Multicast Domains, die in kleinen Netzwerken ohne DNS-Server funktionieren. Das geschieht mit einem Multicast auf die Adresse 224.0.0.251 Port 5353. Wenn ein DNS-Server eingestzt wird, sollten die Zonen also anders heissen (z.B. .intern).
siehe: http://www.multicastdns.org



Beispiel eines kleinen Zonen-Files. Hier sind die Angaben für eine Forward Lookup Zone, nämlich a-net.intern.
@ bedeutet, dass der Name der Zone jeweils angehängt wird, falls am Ende eines Namens kein . (Punkt) steht. Er wird übernommen vom named.conf.
Folgende Zeilen bedeuten genau das selbe:

www	A	192.168.112.14	(ohne Punkt)
www.a-net.intern.	A	192.168.112.14	(mit Punkt)

Man könnte auch angeben $ORIGIN a-net.intern um den Wert von @ zu setzen.

IN SOA bestimmt die Source of Authority, also wer der Chef ist für diese Zone, es ist ns.a-net.intern. Falls Meldungen an den Verwalter des DNS zu machen sind, sollen diese an info.a-net.intern gesandt werden (das @ wird durch einen Punkt ersetzt, da das Zeichen hier etwas anderes bedeutet). Beachten sie den Punkt jeweils am Ende!
Eine Erhöhung der Serien-Nummer bewirkt, dass die Slaves die Datei neu kopieren. Man verwendet oft das Datum JJJJMMTTnn mit einer 2-stelligen Laufnummer.

NS-Einträge benennen die beiden Name-Server. Ihre IP steht in den beiden A-Records weiter unten. Mindesten eine solche NS- Zeile *muss* im Zonen-File vorkommen. Ein NS-Eintrag muss mit der Angabe auf der Zeile SOA übereinstimmen!

MX-Einträge legen die Mail-Server fest (allerdings ist diese Zone hier nur intern).

Mit CNAME wird ein Alias definiert. Oft ist nämlich die gleiche Maschine Web-Server, FTP-Server und so weiter.

Beispiel \var\lib\named\master\112.168.192.in-addr.arpa

```
$TTL 2D
@           IN  SOA     ns.a-net.intern. info.a-net.intern. (
                        2004030111      ; Serial
                        3H              ; Refresh (= 10800 Sekunden)
                        1H              ; Retry (= 3600 Sekunden)
                        1W              ; Expire
                        1D)             ; Minimum TTL
            IN NS       ns.a-net.intern.
14          PTR         ns.a-net.intern.
1           PTR         firewall.a-net.intern.
131         PTR         smtp.a-net.intern.
30          PTR         ersatz.a-net.intern.
```

Zonen-File für Reverse-Lookups. Wenn eine Station z.B. eine Abfrage macht:
nslookup 192.168.112.1
erhält sie den DNS-Namen firewall.a-net.intern als Antwort.

Beachten Sie: in-addr.arpa sind immer Class C Netzwerke. Soll die Abfrage auch für kleinere Subnetze und externe Stationen funktionieren, muss der Provider eine Zone Delegation einrichten.

Beispiel eines Reverse-Lookup Zonen-Files. Damit können mit IP-Aressen die zugehörigen DNS-Namen abgefragt werden.

Die ersten Zeilen entsprechen denjenigen im Zonen-File. Ein NS-Eintrag, der mit dem ns in der Zeile SOA übereinstimmt, muss vorhanden sein.

Dann folgen die PTR-Einträge für die einzelnen Stationen.

Das System 192.168.112.14 hat zum Beispiel den Namen ns.a-net.intern.

DNS Testen

- Die "beliebtesten" Fehler sind:
  - named.conf
    - jede { muss weiter unten mit einem }; geschlossen werden
    - ; am Ende der Zeile felt, besonders auch nach einem };
    - Zonenname oder Filename nicht zwischen " "
    - Zonenname für Reverselookup ist von hinten zu lesen 11.168.192.in-addr.arpa (und *nicht* 192.168.112.in-addr.arpa)
  - Zonenfiles
    - erste Zeile sollte $TTL 1D lauten (ausser WSeB)
    - @ am Anfang der SOA-Zeile fehlt
    - NS Zeile mit Nameserver (wie in SOA) fehlt
    - Nameserver ist ein Alias (CNAME)
    - Nameserver in SOA-Zeile muss unten definiert werden
    - **.** (Punkt) am Ender voller DNS-Namen vergessen (dns1.a-net.intern *wird so zu* dns1.a-net.intern.a-net.intern)
- Warp Server e-Business
  - \mptn\etc\named.boot (Funktion wie named.conf, format anders!)
  - \mptn\etc\namedb\ (Zonen-Files im gleichen Format)

A-NET

Der Befehl makefolder.cmd erstellt einen Ordner mit Icons zum Steuern des DNS. Wird named.exe von Hand gestartet, ist ein Beednen des Prozesses nur mit Mühe möglich. Die Menueinträge verwenden dazu emxkill. Das geht besser, allerdings nicht immer schnell und funktioniert auch nicht immer.

Apache2 - DER Websever

Der Apache-Server ist der am weitesten verbreitete Webserver und für fast alle Plattformen erhältlich.

HTTP-Server: WEB-Server (Port 80 und 443 https)

- HTTP (Hyper Text Transport Protokoll)
  - HTTPS als sicherere Version
  - viele Script-Sprachen:
    - Serverseitig:PHP, Perl, CGI, SSI, ASP..
    - Clientseitig: JavaScript, ActiveX, ..
- verschiedene Server
  - Apache V 2.x
    - für fast alle Plattformen (Linux, Unix, BSD, Windows, OS/2,MacOS,..)
  - IIS
    - nur Windows
  - Domino Server
    - iSeries, Windows, Linux
- noch mehr Clients
  - Mozilla (aus Netscape)
  - Opera (der sicherste)
  - IE (nur Windows)
  - Lynx (der sparsame)

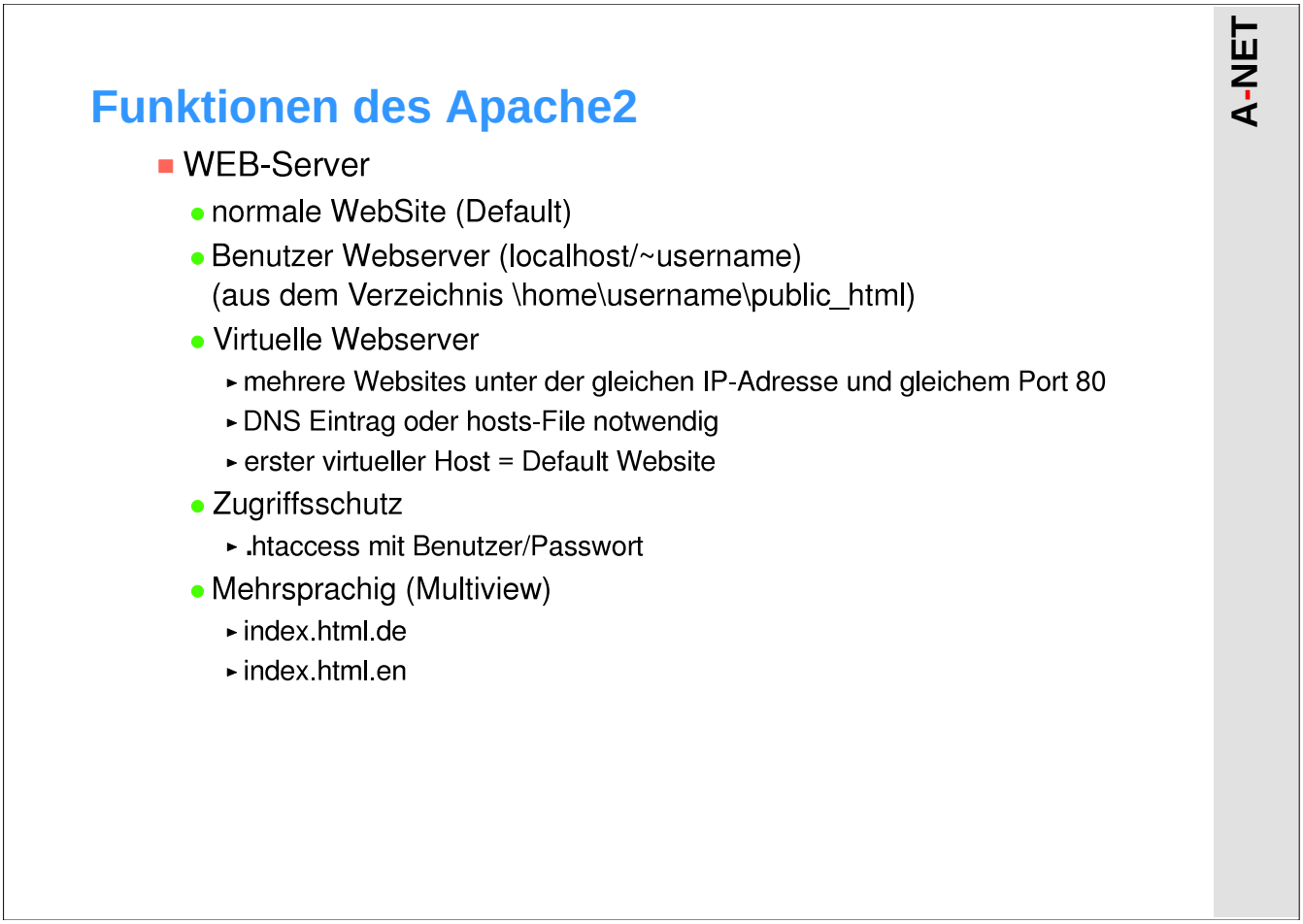
A-NET

Die HTTP-Server sind sehr bekannt und werden im ganzen Internet benutzt.

Der Apache WEB-Server ist auf fast allen Plattformen verfügbar und wird eingesetzt unter:
- Linux, FreeBSD, Unixe, OS/2, Windows, iSeries, IBM-Host etc.

Mit den Scriptsprachen lassen sich dynamische Elemente einbauen. Es gibt davon zwei Arten: Die einen laufen auf dem Server (und belasten damit diesen), die anderen laufen auf dem Client (und belasten somit den Client).

Unter den Browsern bieten vor allem Firefox, Mozilla und Opera eine guten Kompromiss zwischen reichen Funktionen und Sicherheit. ActiveX ist von der Sicherheit problematisch.



Der Apache2 ist in der Standard-Funktion ein Webserver für einen Namen/ Adresse. Ausserdem können Benutzer in ihrem home-Verzeichnis eine private Website erstellen. Die Daten dazu müssen im Verzeichnis c:\home\username\public_html stehen, also z.B. c:\home\fho\pulbic_html. Diese Daten werden gefunden unter 192.168.112.14/~fho (wenn dies die IP des Servers ist)

Ausserdem können Name Based Virtual Hosts eingerichtet werden. Dann können viele Namen unter einer eizigen IP erreichbar sein. Dazu ist ein DNS-Eintrag notwendig. (Zum Testen geht auch die hosts Datei).

Beispiel einer /etc/apache2/httpd.conf (gekürzt)

A-NET

```
### Section 1: Global Environment
ServerRoot "/os2httpd2"                    Programmverzeichnis
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15

Listen 80                                  Webserver hört auf Port 80 (Standard)
# fuer PHP4 Support A-Net GmbH
LoadModule php4_module  modules/modphp4.dll   PHP4 aktivieren

### Section 2: 'Main' server configuration
ServerAdmin info@anetgmbh.ch               Anregungen an diese Adresse senden
ServerName tp50.a-net.local:80             Name des Servers (Default-Server)
UseCanonicalName Off
DocumentRoot "/os2httpd2/htdocs"           Hier sind die HTML-Dokumente

<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>

<Directory "/os2httpd2/htdocs">
    Options Indexes FollowSymLinks
    AllowOverride AuthConfig               AuthConfig: Zugriffsschutz erlaubt (.htaccess)
    Order allow,deny
    Allow from all
</Directory>
```

Die Datei httpd.conf steuert den Apache WEB-Server. Zunächst erstaunt die Grösse, aber keine Angst, der grösste Teil ist Kommentar (# am Zeilenanfang) und vieles kann standardmässig belassen werden.

Wichtig sind:
ServerRoot: gibt das Basisverzeichnis der Programme an
Listen 80: auf diesem Port hört der Webserver
ServerAdmin: Mail-Adresse des Verantwortlichen dieses Servers
ServerName: DNS-Name des Default Servers:
DocumentRoot: hier sind die HTML-Dateien des Default-Servers
<Directory "/os2httpd2/htdocs">
  Options FollowSymlinks
  AllowOverride AuthConfig: Zugriffsschutz mit .htaccess ist erlaubt in diesem Verzeichnis und seinen Unterverzeichnissen (s. weiter hinten)

Wird der Server eingerichtet, ist ein Link auf die Dokumentation auf dem lokalen Disk vorhanden (http://localhost/manual)

Beispiel einer /etc/apache2/httpd.conf (gekürzt)

A-NET

UserDir public_html	Benutzer Website (tp5.a-net.intern/~username)
DirectoryIndex index.html index.html.var	mögliche Indexfiles, Standard: index.html

AccessFileName .htaccess
<Files ~ "^\.ht">
  Order allow,deny
  Deny from all
</Files>
	.ht - Files schützen (alle files, deren Name mit .ht beginnen, können vie WEB nicht eingesehen werden)

TypesConfig conf/mime.types DefaultType text/plain <IfModule mod_mime_magic.c> MIMEMagicFile conf/magic </IfModule> HostnameLookups On	Im Log stehen die Hostnamen der Clients (falls Verbindung zu einem DNS langsam ist oder fehlt: Off!)

DirectoryIndex legt den Namen der Default Index-Seiten fest. Standard ist index.html und die Sprachvarianten davon (s. Multiviews).

Hier wird der Zugiff auf alle Dateien, die mit .ht beginnen, verhindert, auch wenn sie in einem Dokumentenverzeichnis stehen. Diese Dateien enthalten die Zugriffsbeschränkungen (wenn AuthConfig aktiviert ist).

HostnameLookups On: bewirkt, dass mit Reverselookup die Namen der zugreifenden Clients ins Log-File geschrieben wird. Macht nur Sinn, wenn eine genügend schnelle Verbindung zum DNS besteht, sonst auf Off belassen.

Der Apache kann virtuelle Hosts bilden. Dabei können mehrere Web-Server unter der gleichen Adresse und Port-Nummer arbeiten, sie unterscheiden sich dann nur per DNS-Name.

NameVirtualHost *:80 Schaltet "name based virtual hosting" ein und zwar auf dem Port 80. Damit der Default-Server weiterhin funktioniert, muss nun mindestens ein erster virtual Host für den Default Server eingerichtet werden. Er enthält den gleichen Servenamen tp50.a-net.intern und das gleiche Dokumentverzeichnis /os2httpd2/htdocs, wie weiter oben bereits angegeben.

Nun können weitere Blöcke für virtuelle Hosts eingerichtet werden, jeweils mit unterschiedlichen Namen (hier www und www2.a-net.intern) und Dokumentenverzeichnissen (hier /ost2httpd2/vhosts/www und www2).

Dazu können auf verschiedenen IP-Adressen und/oder Ports auch merhrere Web-Server realisiert werden. Diese können dann via IP/Port angeprochen werden.(IP based virtual hosting).

Zugriff einschränken (.htaccess)

- Der Zugriff auf die Daten in einem Verzeichnis kann eingeschränkt werden. (Benutzer und Passwort)
- Sicherheit ist nicht sehr hoch, da Passwörter im Klartext über die Leitung gehen.
- Vorgehen:
  - zu Schützende Daten in ein Unterverzeichnis von htdocs legen
  - AllowOverride AuthConfig in httpd.conf aktivieren (s. 3 Seiten vorher)
  - .htaccess File im zu schützenden Verzeichnis erstellen
    - AuthType Basic
    - AuthName "Interner Bereich"
    - AuthUserFile /os2httpd2/htaccess/.htpasswd
    - AuthGroupFile /dev/null
    - require valid-user (oder: require user fho hans)
  - Datei \os2\httpd2\htaccess\.htpasswd erstellen:
    - xcopy \os2httpd2\htpasswd.exe \os2httpd2\htpasswd\ (Programm kopieren)
    - cd \os2httpd2\htpasswd (ins Verzeichnis gehen)
    - htpasswd -c .htpasswd fho (-c nur das *erste* Mal, 2x Passwort)
    - htpasswd .htpasswd hans (weiterer Benutzer, 2x Passwort)

Der Zugriff auf die Daten in einem Verzeichnis kann abhängig von einer Benutzerid und Passwort gemacht werden.Dazu erstellt man am besten ein Verzeichnis \os2httpd2\htaccess und kopiert das Programm \os2httpd2\bin\htpasswd.exe auch dorthin. Dann kann man eine Datei .htpasswd (mit Punkt) erstellen und einen oder mehrer Benutzer erfassen, jeweils mit Passwort. Das erste Mal erfolgt der Aufruf mit -c (für create), damit das Passwortfile erstellt wird.

htpasswd -c .htpasswd fho (dann 2x das Passowrt)
htpasswd .htpasswd hans (dann 2x das Passwort)

In das zu schützende Verzeichnis kommt dann eine Datei .htaccess mit diesem Inhalt:

```
AuthType Basic
AuthName "Interner Bereich"
AuthUserFile /os2httpd2/htaccess/.htpasswd
AuthGroupFile /dev/null
require valid-user
```

Nun wird beim Zugriff ein Passwort verlangt. Alle erfassten Benutzer erhalten Zugriff. Alternativ kann man die letze Zeile ändern auf "require user fho hans", dann haben nur fho und hans Zugriff.

Polyglott mit Multiviews

- MultiViews (mehrere Sprachen) ist standardmässig aktiv
- Folgende Dateien in ../htdocs erstellen:

  index.html.de (File mit deutschem Text)
  index.html.en (File mit englischem Text)
  index.html.html (Fallback Text, meist englisch)
- Der Browser zeigt für index.html folgendes an:
  - Browser hat de eingestellt: index.html.de
  - Browser hat en eingestellt: index.html.en
  - Browser hat eine andere Sprache: index.html.html
- Die Links in allen Sprachfiles lauten nur auf xxx.html (ohne .de etc!)

A-NET

Apache2 unterstützt mehrere Sprachen. Pro gewünschter Sprache erstellt man HTML-Seiten mit angehängtem Sprach-Code, z.B de und en. Der Benutzer erhält dann, abhängig von der Sprache, die er im Browser eingesellt hat, die Seite in seiner Sprache.

Alle anderen erhalten die Default-Sprache.