Network

LAN

- show all configured interfaces and it's status: `ifconfig`
- show information about an Ethernet interface: `ethtool eth0`

Files

- `/etc/sysconfig/network-scripts`: interface up/down scripts (CentOS/RHEL)
- `/etc/network/if-up.d`: interface up scripts (Ubuntu)
- `/sys/class/net`: network interfaces files (info)

WLAN

- WLAN configuration (und Signalpegel): `iwconfig wlan0`
- WLAN (detailed) info: `iwlist`
- List Wi-Fi networks (using *NetworkManager* CLI): `nmcli device wifi list`

DNS

- lookup a server per DNS: `nslookup fsf.org`
- lookup a host at DNS server: `dig +short @router.asus.com ralf-laptop`

Files

- `/etc/resolv.conf`: DNS configuration
- `/etc/hosts`: predefined hosts

Apache

Links

- How To Enable or Disable CGI Scripts in Apache 2.4

How to configure a user directory, for example ~/www

The main change is located in file `/etc/apache2/mods-enabled/userdir.conf`:

```
<IfModule mod_userdir.c>
```

```
    UserDir www
    UserDir disabled root

    <Directory /home/*/www>
        AllowOverride FileInfo AuthConfig Limit Indexes
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec \
            FollowSymLinks SymLinksIfOwnerMatch
        IndexOptions -FancyIndexing +SuppressHTMLPreamble
+SuppressDescription \
            +IgnoreClient +SuppressColumnSorting +FoldersFirst \
            +TrackModified +ScanHTMLTitles
        IndexHeadInsert "  <meta name=\"robots\"
content=\"noindex,follow\">"
        <Limit GET POST OPTIONS>
            Require all granted
        </Limit>
        <LimitExcept GET POST OPTIONS>
            Require all denied
        </LimitExcept>
    </Directory>
</IfModule>
```

How to redirect http automatically to https

Add this rule to the `.htaccess` file on server

```
<IfModule mod_rewrite.c>
  RewriteEngine on
  RewriteCond %{HTTP:X-Forwarded-Proto} =http [OR]
  RewriteCond %{HTTP:X-Forwarded-Proto} =""
  RewriteCond %{HTTPS} off
  RewriteRule (.*) __ BROKEN-
LINK:https://%{HTTP_HOST}%{REQUEST_URI}LINK-BROKEN__ [R=301,L]
</IfModule>
```

ht://Dig

Links

- ht://Dig Homepage
- Installing and Configuring the ht://Dig Search Engine

Installation (Ubuntu)

I use *ht://Dig* for local indexing my documents archive.

1. install packages: `htdig`, `htdig-doc`, `xpdf`, `catdoc`, `mailutils`
2. for indexing of Postscript, PDF, DVI decompress and copy *perl* script `conv_doc.pl` from `/usr/share/doc/htdig-doc/examples` to `/usr/local/bin`
3. add option -q to call of `pdftotext` in perl script `conv_doc.pl`, to get rid of a lot of warnings
4. edit `/etc/default/htdig` to enable daily/weekly/monthly indexing
5. create a *anacron* job in `/etc/cron.monthly` or simply move `/etc/cron.daily/htdig` to `/etc/cron.*`
6. change the *anacron* job to call `rundig` via `nice`, like this

```
nice -n 19 /usr/bin/rundig -s 2>&1 | tr -d '\000-\011\013-\037\177-
\377' | mail -s "ht://Dig archive rebuild" ralf@localhost
```

7. edit configuration file `/etc/htdig/htdig.conf`, add/change at least:

```
start_url:      __ BROKEN-LINK:http://localhost/...LINK-BROKEN__
limit_urls_to:      ${start_url}
remove_bad_urls:    true
maintainer:     yourname@localhost
max_doc_size:       10000000
no_excerpt_show_top:    true
maximum_pages:      20
matches_per_page:   50
external_parsers: application/msword->text/html
/usr/local/bin/conv_doc.pl \
               application/postscript->text/html
/usr/local/bin/conv_doc.pl \
               application/pdf->text/html /usr/local/bin/conv_doc.pl
```

Do not forget to setup Apache, including enable of `mod_userdir` (create symlink) and `mod_cgi` (execute `sudo a2enmod cgi`).

Samba

Commands

- show the *Samba* tree

```
smbtree
```

- shows a list of available shares at a server

```
smbclient -L <server> --no-pass
```

- *Smbclient* interactive shell

```
smbclient '\\<server>\<share>' -U <user>
```

- add a new user <user>

```
sudo smbpasswd -a <user>
```

Firewall

Add at least this rule (for example by use of the Uncomplicated Firewall)

```
sudo ufw allow proto udp from 192.168.178.0/24 to any port 137
```

to allow *NetBIOS* name service to see your host. In case you only want to access shares on **other** hosts (and not allow access to your own) this seems to be enough.

If you want to participate as a full SMB/CIFS host (exporting shares for public access) then you probably need:

```
sudo ufw allow from 192.168.178.0/24 to any app samba4
```

or a solution according to Ask Ubuntu.

Files

- `/etc/samba/smb.conf`: main *Samba* configuration file
- `/etc/samba/smbusers`: translation of *Samba* user names to *Linux* names

Howto automount a Windows share

Example: Automount a Windows share “Winshare” using CIFS[1] at `/mnt/samba/winroot` (read-only, as guest)

- edit file `/etc/auto.master` to make *Automount* responsible for mounts at directory `/mnt/samba`

```
/mnt/samba  auto.samba --ghost --timeout 120
```

- create the (so called) map file `/etc/auto.samba` with the following contents:[2]

```
winroot -fstype=cifs,guest,ro,noperm,nounix,domain=WORKGROUP
://Winhost/Winshare
```

- If your “Winhost” has a static IP address add it to `/etc/samba/lmhosts` (or use the IP address instead of the hostname “Winhost” in `/etc/auto.samba`).
- depending on your *Linux* distribution you might have to edit configuration file `/etc/sysconfig/autofs`

Spamassassin

Commands

- start *systemd* service: `systemctl enable spamassassin && systemctl start spamassassin`

Files

- `/etc/mail/spamassassin/local.cf`: main configuration file
- `~/.spamassassin/user_prefs`: user configuration file (see below)

```
# -*- mode: perl -*-
#
# Copyright (C) 2017 Ralf Hoppe <ralf.hoppe@ieee.org>
#
# SpamAssassin user preferences file.  See 'perldoc
Mail::SpamAssassin::Conf'
# for details of what can be tweaked.
###########################################################################

# How many points before a mail is considered spam (default at the moment).
required_score      5

# Whitelist and blacklist addresses are now file-glob-style patterns, so
# "friend@somewhere.com", "*@isp.com", or "*.domain.net" will all work.
# whitelist_from  someone@somewhere.com

# Speakers of any language that uses non-English, accented characters may
wish
# to uncomment the following lines.   They turn off rules that fire on
# misformatted messages generated by common mail apps in contravention of
the
# email RFCs.
score SUBJ_ILLEGAL_CHARS      0

# score BAYES_00 -4
# score BAYES_05 -2
# score BAYES_95 6
# score BAYES_99 9



#### main performance related settings

# By default, SpamAssassin queries max. 3 (of 13 default) servers to attempt
# to check if DNS is working or not.  This is the main performance killer,
# especially in case a connection fails.  But turning DNS off has side
effects
# of disabling of a lot of helpful network tests (only Bayes learning
remains).
# If your ISP performs such checks for you then this should not be a
problem.
dns_available no

# don't do DNS based RBL (Realtime blacklist) lookups
skip_rbl_checks 1

# By default, SpamAssassin checks the From: address for a valid MX two
times,
# waiting 5 seconds each time. This consumes a lot of time - so i want this
# check only once.
check_mx_attempts 1
check_mx_delay 2
```

[1] CIFS is the successor of SMBFS.

[2] “Winhost” is the hostname (resolvable by DNS or file `/etc/hosts`) or IP address of the Windows PC.

From:
https://wiki.rho62.de/ - **rho62 Wiki**

Permanent link:
https://wiki.rho62.de/doku.php?id=linux:administration:network

Last update: **2024/12/11 19:08**