Network applications

- Web browsers
  - Spoofing the User-Agent string
  - Browser extension
- The mail system
  - Email basics
  - Modern mail service limitation
  - Historic mail service expectation
  - Mail transport agent (MTA)
    - The configuration of exim4
    - The configuration of postfix with SASL
    - The mail address configuration
    - Basic MTA operations
- The remote access server and utilities (SSH)
  - Basics of SSH
  - User name on the remote host
  - Connecting without remote passwords
  - Dealing with alien SSH clients
  - Setting up ssh-agent
  - Sending a mail from a remote host
  - Port forwarding for SMTP/POP3 tunneling
  - How to shutdown the remote system on SSH
  - Troubleshooting SSH
- The print server and utilities
- Other network application servers
- Other network application clients
- The diagnosis of the system daemons

After establishing network connectivity (see ???), you can run various network applications.

> For modern Debian specific guide to the network infrastructure, read The Debian Administrator's Handbook — Network Infrastructure.
>
> If you enabled "2-Step Verification" with some ISP, you need to obtain an application password to access POP and SMTP services from your program. You may need to approve your host IP in advance.

Web browsers

There are many web browser packages to access remote contents with Hypertext Transfer Protocol (HTTP).

package	popcon	size	type	description of web browser
`chromium`	@-@popcon1@-@	@-@psize1@-@	X	Chromium, (open-source browser from Google)
`firefox`	@-@popcon1@-@	@-@psize1@-@	, ,	Firefox, (open-source browser from Mozilla, only available in Debian Unstable)
`firefox-esr`	@-@popcon1@-@	@-@psize1@-@	, ,	Firefox ESR, (Firefox Extended Support Release)
`epiphany-browser`	@-@popcon1@-@	@-@psize1@-@	, ,	GNOME, HIG compliant, Epiphany
`konqueror`	@-@popcon1@-@	@-@psize1@-@	, ,	KDE, Konqueror
`dillo`	@-@popcon1@-@	@-@psize1@-@	, ,	Dillo, (light weight browser, FLTK based)
`w3m`	@-@popcon1@-@	@-@psize1@-@	text	w3m
`lynx`	@-@popcon1@-@	@-@psize1@-@	, ,	Lynx
`elinks`	@-@popcon1@-@	@-@psize1@-@	, ,	ELinks
`links`	@-@popcon1@-@	@-@psize1@-@	, ,	Links (text only)

package	popcon	size	type	description of web browser
`links2`	@-@popcon1@-@	@-@psize1@-@	graphics	Links (console graphics without X)

List of web browsers

Spoofing the User-Agent string

In order to access some overly restrictive web sites, you may need to spoof the User-Agent string returned by the web browser program. See:

- MDN Web Docs: userAgent
- Chrome Developers: Override the user agent string
- How to change your user agent
- How to Change User-Agent in Chrome, Firefox, Safari, and more
- How to Change Your Browser’s User Agent Without Installing Any Extensions
- How to change the User Agent in Gnome Web (epiphany)

Browser extension

All modern GUI browsers support source code based browser extension and it is becoming standardized as web extensions.

The mail system

This section focuses on typical mobile workstations on consumer grade Internet connections.

> If you are to set up the mail server to exchange mail directly with the Internet, you should be better than reading this elementary document.

Email basics

An email message consists of three components, the message envelope, the message header, and the message body.

- The "To" and "From" information in the message envelope is used by the SMTP to deliver the email. (The "From" information in the message envelope is also called bounce address , From_, etc.).
- The "To" and "From" information in the message header is displayed by the email client. (While it is most common for these to be the same as ones in the message envelope, such is not always the case.)
- The email message format covering header and body data is extended by Multipurpose Internet Mail Extensions (MIME) from the plain ASCII text to other character encodings, as well as attachments of audio, video, images, and application programs.

Full featured GUI based email clients offer all the following functions using the GUI based intuitive configuration.

- It creates and interprets the message header and body data using Multipurpose Internet Mail Extensions (MIME) to deal the content data type and encoding.
- It authenticates itself to the ISP's SMTP and IMAP servers using the legacy basic access authentication or modern OAuth 2.0. (For OAuth 2.0, set it via Desktop environment settings. E.g., "Settings" -> "Online Accounts".)
- It sends the message to the ISP's smarthost SMTP server listening to the message submission port (587).
- It receives the stored message on the ISP's server from the TLS/IMAP4 port (993).
- It can filter mails by their attributes.
- It may offer additional functionalities: Contacts, Calendar, Tasks, Memos.

package	popcon	size	type
`evolution`	@-@popcon1@-@	@-@psize1@-@	X GUI program (GNOME, groupware suite)
`thunderbird`	@-@popcon1@-@	@-@psize1@-@	X GUI program (GTK, Mozilla Thunderbird)
`kmail`	@-@popcon1@-@	@-@psize1@-@	X GUI program (KDE)
`mutt`	@-@popcon1@-@	@-@psize1@-@	character terminal program probably used with `vim`
`mew`	@-@popcon1@-@	@-@psize1@-@	character terminal program under `(x)emacs`

List of mail user agent (MUA)

Modern mail service limitation

Modern mail service are under some limitations in order to minimize exposure to the spam (unwanted and unsolicited email) problems.

- It is not realistic to run SMTP server on the consumer grade network to send mail directly to the remote host reliably.
- A mail may be rejected by any host en route to the destination quietly unless it appears as authentic as possible.
- It is not realistic to expect a single smarthost to send mails of unrelated source mail addresses to the remote host reliably.

This is because:

- The SMTP port (25) connections from hosts serviced by the consumer grade network to the Internet are blocked.
- The SMTP port (25) connections to hosts serviced by the consumer grade network from the Internet are blocked.
- The outgoing messages from hosts serviced by the consumer grade network to the Internet can only be sent via the message submission port (587).
- Anti-spam techniques such as DomainKeys Identified Mail (DKIM), Sender_Policy_Framework (SPF), and Domain-based Message Authentication, Reporting and Conformance (DMARC) are widely used for the email filtering.
- The DomainKeys Identified Mail service may be provided for your mail sent through the smarthost.
- The smarthost may rewrite the source mail address in the message header to your mail account on the smarthost to prevent email address spoofing.

Historic mail service expectation

Some programs on Debian expect to access the `/usr/sbin/sendmail` command to send emails as their default or customized setting since the mail service on a UNIX system functioned historically as:

- An email is created as a text file.
- The email is handed to the `/usr/sbin/sendmail` command.
- For the destination address on the same host, the `/usr/sbin/sendmail` command makes local delivery of the email by appending it to the `/var/mail/$username` file.
  - Commands expecting this feature: `apt-listchanges`, `cron`, `at`, ...
- For the destination address on the remote host, the `/usr/sbin/sendmail` command makes remote transfer of the email to the destination host found by the DNS MX record using SMTP.
  - Commands expecting this feature: `popcon`, `reportbug`, `bts`, ...

Mail transport agent (MTA)

Debian mobile workstations can be configured just with full featured GUI based email clients without mail transfer agent (MTA) program after Debian 12 Bookworm.

Debian traditionally installed some MTA program to support programs expecting the `/usr/sbin/sendmail` command. Such MTA on mobile workstations must cope with Modern mail service limitation and Historic mail service expectation.

For mobile workstations, the typical choice of MTA is either `exim4-daemon-light` or `postfix` with its installation option such as "Mail sent by smarthost; received via SMTP or fetchmail" selected. These are light weight MTAs that respect "`/etc/aliases`".

> Configuring `exim4` to send the Internet mail via multiple corresponding smarthosts for multiple source email addresses is non-trivial. If you need such capability for some programs, set them up to use `msmtp` which is easy to set up for multiple source email addresses. Then leave main MTA only for a single email address.

package	popcon	size	description
`exim4-daemon-light`	@-@popcon1@-@	@-@psize1@-@	Exim4 mail transport agent (MTA: Debian default)
`exim4-daemon-heavy`	@-@popcon1@-@	@-@psize1@-@	Exim4 mail transport agent (MTA: flexible alternative)
`exim4-base`	@-@popcon1@-@	@-@psize1@-@	Exim4 documentation (text) and common files
`exim4-doc-html`	@-@popcon1@-@	@-@psize1@-@	Exim4 documentation (html)
`exim4-doc-info`	@-@popcon1@-@	@-@psize1@-@	Exim4 documentation (info)
`postfix`	@-@popcon1@-@	@-@psize1@-@	Postfix mail transport agent (MTA: secure alternative)
`postfix-doc`	@-@popcon1@-@	@-@psize1@-@	Postfix documentation (html+text)
`sasl2-bin`	@-@popcon1@-@	@-@psize1@-@	Cyrus SASL API implementation (supplement postfix for SMTP AUTH)
`cyrus-sasl2-doc`	@-@popcon1@-@	@-@psize1@-@	Cyrus SASL - documentation
`msmtp`	@-@popcon1@-@	@-@psize1@-@	Light weight MTA

package	popcon	size	description
`msmtp-mta`	@-@popcon1@-@	@-@psize1@-@	Light weight MTA (sendmail compatibility extension to `msmtp`)
`nullmailer`	@-@popcon1@-@	@-@psize1@-@	Strip down MTA, no local mail
`ssmtp`	@-@popcon1@-@	@-@psize1@-@	Strip down MTA, no local mail
`sendmail-bin`	@-@popcon1@-@	@-@psize1@-@	Full featured MTA (only if you are already familiar)
`git-email`	@-@popcon1@-@	@-@psize1@-@	`git-send-email`(1) program for sending series of patch emails

List of basic mail transport agent related packages

The configuration of exim4

For the Internet mail via smarthost, you (re)configure `exim4-*` packages as the following.

```
$ sudo systemctl stop exim4
$ sudo dpkg-reconfigure exim4-config
```

Select "mail sent by smarthost; received via SMTP or fetchmail" for "General type of mail configuration".

Set "System mail name:" to its default as the FQDN (see ???).

Set "IP-addresses to listen on for incoming SMTP connections:" to its default as "127.0.0.1 ; ::1".

Unset contents of "Other destinations for which mail is accepted:".

Unset contents of "Machines to relay mail for:".

Set "IP address or host name of the outgoing smarthost:" to "smtp.hostname.dom:587".

Select "No" for "Hide local mail name in outgoing mail?". (Use "`/etc/email-addresses`" as in The mail address configuration, instead.)

Reply to "Keep number of DNS-queries minimal (Dial-on-Demand)?" as one of the following.

- "No" if the system is connected to the Internet while booting.
- "Yes" if the system is **not** connected to the Internet while booting.

Set "Delivery method for local mail:" to "mbox format in /var/mail/".

Select "Yes" for "Split configuration into small files?:".

Create password entries for the smarthost by editing "`/etc/exim4/passwd.client`".

```
$ sudo vim /etc/exim4/passwd.client
 ...
$ cat /etc/exim4/passwd.client
^smtp.*\.hostname\.dom:username@hostname.dom:password
```

Configure `exim4`(8) with "`QUEUERUNNER='queueonly'`", "`QUEUERUNNER='nodaemon'`", etc. in "`/etc/default/exim4`" to minimize system resource usages. (optional)

Start `exim4` by the following.

```
$ sudo systemctl start exim4
```

The host name in "`/etc/exim4/passwd.client`" should not be the alias. You check the real host name with the following.

```
$ host smtp.hostname.dom
smtp.hostname.dom is an alias for smtp99.hostname.dom.
smtp99.hostname.dom has address 123.234.123.89
```

I use regex in "`/etc/exim4/passwd.client`" to work around the alias issue. SMTP AUTH probably works even if the ISP moves host pointed by the alias.

You can manually update `exim4` configuration by the following:

- Update `exim4` configuration files in "`/etc/exim4/`".
  - creating "`/etc/exim4/exim4.conf.localmacros`" to set MACROs and editing "`/etc/exim4/exim4.conf.template`". (non-split configuration)
  - creating new files or editing existing files in the "`/etc/exim4/exim4.conf.d`" subdirectories. (split configuration)
- Run "`systemctl reload exim4`".

> Starting `exim4` takes long time if "No" (default value) was chosen for the debconf query of "Keep number of DNS-queries minimal (Dial-on-Demand)?" and the system is **not** connected to the Internet while booting.

Please read the official guide at: "`/usr/share/doc/exim4-base/README.Debian.gz`" and `update-exim4.conf`(8).

> For all practical consideration, use SMTP with STARTTLS on port 587 or SMTPS (SMTP over SSL) on port 465, instead of plain SMTP on port 25.

The configuration of postfix with SASL

For the Internet mail via smarthost, you should first read postfix documentation and key manual pages.

command	function
`postfix`(1)	Postfix control program
`postconf`(1)	Postfix configuration utility
`postconf`(5)	Postfix configuration parameters
`postmap`(1)	Postfix lookup table maintenance
`postalias`(1)	Postfix alias database maintenance

List of important postfix manual pages

You (re)configure `postfix` and `sasl2-bin` packages as follows.

```
$ sudo systemctl stop postfix
$ sudo dpkg-reconfigure postfix
```

Chose "Internet with smarthost".

Set "SMTP relay host (blank for none):" to "`[smtp.hostname.dom]:587`" and configure it by the following.

```
$ sudo postconf -e 'smtp_sender_dependent_authentication = yes'
$ sudo postconf -e 'smtp_sasl_auth_enable = yes'
$ sudo postconf -e 'smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd'
$ sudo postconf -e 'smtp_sasl_type = cyrus'
$ sudo vim /etc/postfix/sasl_passwd
```

Create password entries for the smarthost.

```
$ cat /etc/postfix/sasl_passwd
[smtp.hostname.dom]:587     username:password
$ sudo postmap hush:/etc/postfix/sasl_passwd
```

Start the `postfix` by the following.

```
$ sudo systemctl start postfix
```

Here the use of "`[`" and "`]`" in the `dpkg-reconfigure` dialog and "`/etc/postfix/sasl_passwd`" ensures not to check MX record but directly use exact hostname specified. See "Enabling SASL authentication in the Postfix SMTP client" in "`/usr/share/doc/postfix/html/SASL_README.html`".

The mail address configuration

There are a few mail address configuration files for mail transport, delivery and user agents.

file	function	application
`/etc/mailname`	default host name for (outgoing) mail	Debian specific, `mailname`(5)
`/etc/email-addresses`	host name spoofing for outgoing mail	`exim`(8) specific, `exim4-config_files`(5)
`/etc/postfix/generic`	host name spoofing for outgoing mail	`postfix`(1) specific, activated after `postmap`(1) command execution.
`/etc/aliases`	account name alias for incoming mail	general, activated after `newaliases`(1) command execution.

List of mail address related configuration files

The **mailname** in the "`/etc/mailname`" file is usually a fully qualified domain name (FQDN) that resolves to one of the host's IP addresses. For the mobile workstation which does not have a hostname with resolvable IP address, set this **mailname** to the value of "`hostname -f`". (This is safe choice and works for both `exim4-*` and `postfix`.)

> The contents of "`/etc/mailname`" is used by many non-MTA programs for their default behavior. For `mutt`, set "`hostname`" and "`from`" variables in `~/muttrc` file to override the **mailname** value. For programs in the `devscripts` package, such as `bts`(1) and `dch`(1), export environment variables "`$DEBFULLNAME`" and "`$DEBEMAIL`" to override it.
>
> The `popularity-contest` package normally send mail from root account with FQDN. You need to set `MAILFROM` in `/etc/popularity-contest.conf` as described in the `/usr/share/popularity-contest/default.conf` file. Otherwise, your mail will be rejected by the smarthost SMTP server. Although this is tedious, this approach is safer than rewriting the source address for all mails from root by MTA and should be used for other daemons and cron scripts.

When setting the **mailname** to "`hostname -f`", the spoofing of the source mail address via MTA can be realized by the following.

- "`/etc/email-addresses`" file for `exim4`(8) as explained in the `exim4-config_files`(5)
- "`/etc/postfix/generic`" file for `postfix`(1) as explained in the `generic`(5)

For `postfix`, the following extra steps are needed.

```
# postmap hash:/etc/postfix/generic
# postconf -e 'smtp_generic_maps = hash:/etc/postfix/generic'
# postfix reload
```

You can test mail address configuration using the following.

- `exim`(8) with `-brw, -bf, -bF, -bV, …` options
- `postmap`(1) with `-q` option.

> Exim comes with several utility programs such as `exiqgrep`(8) and `exipick`(8). See "`dpkg -L exim4-base|grep man8/`" for available commands.

Basic MTA operations

There are several basic MTA operations. Some may be performed via `sendmail`(1) compatibility interface.

exim command	postfix command	description
`sendmail`	`sendmail`	read mails from standard input and arrange for delivery (`-bm`)
`mailq`	`mailq`	list the mail queue with status and queue ID (`-bp`)
`newaliases`	`newaliases`	initialize alias database (`-I`)
`exim4 -q`	`postqueue -f`	flush waiting mails (`-q`)
`exim4 -qf`	`postsuper -r ALL deferred; postqueue -f`	flush all mails
`exim4 -qff`	`postsuper -r ALL; postqueue -f`	flush even frozen mails
`exim4 -Mg queue_id`	`postsuper -h queue_id`	freeze one message by its queue ID
`exim4 -Mrm queue_id`	`postsuper -d queue_id`	remove one message by its queue ID
N/A	`postsuper -d ALL`	remove all messages

List of basic MTA operation

> It may be a good idea to flush all mails by a script in "`/etc/ppp/ip-up.d/*`".

The remote access server and utilities (SSH)

The Secure SHell (SSH) is the **secure** way to connect over the Internet. A free version of SSH called OpenSSH is available as `openssh-client` and `openssh-server` packages in Debian.

For the user, `ssh`(1) functions as a smarter and more secure `telnet`(1). Unlike `telnet` command, `ssh` command does not stop on the `telnet` escape character (initial default CTRL-]).

package	popcon	size	tool	description
`openssh-client`	@-@popcon1@-@	@-@psize1@-@	`ssh`(1)	Secure shell client
`openssh-server`	@-@popcon1@-@	@-@psize1@-@	`sshd`(8)	Secure shell server
`ssh-askpass`	@-@popcon1@-@	@-@psize1@-@	`ssh-askpass`(1)	asks user for a pass phrase for ssh-add (plain X)
`ssh-askpass-gnome`	@-@popcon1@-@	@-@psize1@-@	`ssh-askpass-gnome`(1)	asks user for a pass phrase for ssh-add (GNOME)
`ssh-askpass-fullscreen`	@-@popcon1@-@	@-@psize1@-@	`ssh-askpass-fullscreen`(1)	asks user for a pass phrase for ssh-add (GNOME) with extra eye candy
`shellinabox`	@-@popcon1@-@	@-@psize1@-@	`shellinaboxd`(1)	web server for browser accessible VT100 terminal emulator

List of remote access server and utilities

Although `shellinabox` is not a SSH program, it is listed here as an interesting alternative for the remote terminal access.

See also ??? for connecting to remote X client programs.

> See ??? if your SSH is accessible from the Internet.

> Please use the `screen`(1) program to enable remote shell process to survive the interrupted connection (see ???).

Basics of SSH

The OpenSSH SSH daemon supports SSH protocol 2 only.

Please read "`/usr/share/doc/openssh-client/README.Debian.gz`", `ssh`(1), `sshd`(8), `ssh-keygen`(1), `ssh-add`(1) and `ssh-agent`(1).

> "`/etc/ssh/sshd_not_to_be_run`" must not be present if one wishes to run the OpenSSH server.
>
> Don't enable rhost based authentication (`HostbasedAuthentication` in `/etc/ssh/sshd_config`).

configuration file	description of configuration file
`/etc/ssh/ssh_config`	SSH client defaults, see `ssh_config`(5)
`/etc/ssh/sshd_config`	SSH server defaults, see `sshd_config`(5)
`~/.ssh/authorized_keys`	default public SSH keys that clients use to connect to this account on this SSH server
`~/.ssh/id_rsa`	secret SSH-2 RSA key of the user
`~/.ssh/id_key-type-name`	secret SSH-2 *key-type-name* key such as `ecdsa`, `ed25519`, ... of the user

List of SSH configuration files

The following starts an `ssh`(1) connection from a client.

command	description
`ssh username@hostname.domain.ext`	connect with default mode
`ssh -v username@hostname.domain.ext`	connect with default mode with debugging messages
`ssh -o PreferredAuthentications=password username@hostname.domain.ext`	force to use password with SSH version 2
`ssh -t username@hostname.domain.ext passwd`	run `passwd` program to update password on a remote host

List of SSH client startup examples

User name on the remote host

If you use the same user name on the local and the remote host, you can eliminate typing "`username@`".

Even if you use different user name on the local and the remote host, you can eliminate it using "`~/.ssh/config`". For Debian Salsa service with account name "`foo-guest`", you set "`~/.ssh/config`" to contain the following.

```
Host salsa.debian.org people.debian.org
User foo-guest
```

Connecting without remote passwords

One can avoid having to remember passwords for remote systems by using "`PubkeyAuthentication`" (SSH-2 protocol).

On the remote system, set the respective entries, "`PubkeyAuthentication yes`", in "`/etc/ssh/sshd_config`".

Generate authentication keys locally and install the public key on the remote system by the following.

```
$ ssh-keygen -t rsa
$ cat .ssh/id_rsa.pub | ssh user1@remote "cat - >>.ssh/authorized_keys"
```

You can add options to the entries in "`~/.ssh/authorized_keys`" to limit hosts and to run specific commands. See `sshd`(8) "AUTHORIZED_KEYS FILE FORMAT".

Dealing with alien SSH clients

There are some free SSH clients available for other platforms.

environment	**free SSH program**
Windows	puTTY (PuTTY: a free SSH and Telnet client) (GPL)
Windows (cygwin)	SSH in cygwin (Cygwin: Get that Linux feeling - on Windows) (GPL)
Mac OS X	OpenSSH; use `ssh` in the Terminal application (GPL)

List of free SSH clients for other platforms

Setting up ssh-agent

It is safer to protect your SSH authentication secret keys with a pass phrase. If a pass phrase was not set, use "`ssh-keygen -p`" to set it.

Place your public SSH key (e.g. "`~/.ssh/id_rsa.pub`") into "`~/.ssh/authorized_keys`" on a remote host using a password-based connection to the remote host as described above.

```
$ ssh-agent bash
$ ssh-add ~/.ssh/id_rsa
Enter passphrase for /home/username/.ssh/id_rsa:
Identity added: /home/username/.ssh/id_rsa (/home/username/.ssh/id_rsa)
```

No remote password needed from here on for the next command.

```
$ scp foo username@remote.host:foo
```

Press ^D to terminating ssh-agent session.

For the X server, the normal Debian startup script executes `ssh-agent` as the parent process. So you only need to execute `ssh-add` once. For more, read `ssh-agent`(1) and `ssh-add`(1).

Sending a mail from a remote host

If you have an SSH shell account on a server with proper DNS settings, you can send a mail generated on your workstation as an email genuinely sent from the remote server.

```
$ ssh username@example.org /usr/sbin/sendmail -bm -ti -f "username@example.org" <
mail_data.txt
```

Port forwarding for SMTP/POP3 tunneling

To establish a pipe to connect to port 25 of `remote-server` from port 4025 of `localhost`, and to port 110 of `remote-server` from port 4110 of `localhost` through `ssh`, execute on the local host as the following.

```
# ssh -q -L 4025:remote-server:25 4110:remote-server:110 username@remote-server
```

This is a secure way to make connections to SMTP/POP3 servers over the Internet. Set the "`AllowTcpForwarding`" entry to "`yes`" in "`/etc/ssh/sshd_config`" of the remote host.

How to shutdown the remote system on SSH

You need to protect the process doing "`shutdown -h now`" (see ???) from the termination of SSH using the `at`(1) command (see ???) by the following.

```
# echo "shutdown -h now" | at now
```

Running "`shutdown -h now`" in `screen`(1) (see ???) session is another way to do the same.

Troubleshooting SSH

If you have problems, check the permissions of configuration files and run `ssh` with the "`-v`" option.

Use the "`-p`" option if you are root and have trouble with a firewall; this avoids the use of server ports 1 — 1023.

If `ssh` connections to a remote site suddenly stop working, it may be the result of tinkering by the sysadmin, most likely a change in "`host_key`" during system maintenance. After making sure this is the case and nobody is trying to fake the remote host by some clever hack, one can regain a connection by removing the "`host_key`" entry from "`~/.ssh/known_hosts`" on the local host.

The print server and utilities

In the old Unix-like system, the BSD Line printer daemon (lpd) was the standard and the standard print out format of the classic free software was PostScript (PS). Some filter system was used along with Ghostscript to enable printing to the non-PostScript printer. See ???.

In the modern Debian system, the Common UNIX Printing System (CUPS) is the de facto standard and the standard print out format of the modern free software is Portable Document Format (PDF).

The CUPS uses Internet Printing Protocol (IPP). The IPP is the cross-platform de facto standard for remote printing with bi-directional communication capability.

Thanks to the file format dependent auto-conversion feature of the CUPS system, simply feeding any data to the `lpr` command should generate the expected print output. (In CUPS, `lpr` can be

enabled by installing the `cups-bsd` package.)

The Debian system has some notable packages for the print servers and utilities.

package	popcon	size	port	description
`lpr`	@-@popcon1@-@	@-@psize1@-@	printer (515)	BSD lpr/lpd (Line printer daemon)
`cups`	@-@popcon1@-@	@-@psize1@-@	IPP (631)	Internet Printing CUPS server
`cups-client`	@-@popcon1@-@	@-@psize1@-@	, ,	System V printer commands for CUPS: `lp` (1), `lpstat` (1), `lpoptions` (1), `cancel` (1), `lpmove` (8), `lpinfo` (8), `lpadmin` (8), ...
`cups-bsd`	@-@popcon1@-@	@-@psize1@-@	, ,	BSD printer commands for CUPS: `lpr` (1), `lpq` (1), `lprm` (1), `lpc` (8)
`printer-driver-gutenprint`	@-@popcon1@-@	@-@psize1@-@	Not applicable	printer drivers for CUPS

List of print servers and utilities

> You can configure CUPS system by pointing your web browser to "http://localhost:631/" .

Other network application servers

Here are other network application servers.

package	popcon	size	protocol	description
`telnetd`	@-@popcon1@-@	@-@psize1@-@	TELNET	TELNET server
`nfs-kernel-server`	@-@popcon1@-@	@-@psize1@-@	NFS	Unix file sharing
`samba`	@-@popcon1@-@	@-@psize1@-@	SMB	Windows file and printer sharing

package	popcon	size	protocol	description
`netatalk`	@-@popcon1@-@	@-@psize1@-@	ATP	Apple/Mac file and printer sharing (AppleTalk)
`proftpd-basic`	@-@popcon1@-@	@-@psize1@-@	FTP	General file download
`apache2`	@-@popcon1@-@	@-@psize1@-@	HTTP	General web server
`squid`	@-@popcon1@-@	@-@psize1@-@	, ,	General web proxy server
`bind9`	@-@popcon1@-@	@-@psize1@-@	DNS	IP address for other hosts
`kea`	@-@popcon1@-@	@-@psize1@-@	DHCP	IP address of client itself

List of other network application servers

Common Internet File System Protocol (CIFS) is the same protocol as Server Message Block (SMB) and is used widely by Microsoft Windows.

> See ??? for integration of server systems.

> The hostname resolution is usually provided by the DNS server. For the host IP address dynamically assigned by DHCP, Dynamic DNS can be set up for the hostname resolution using `bind9` and `kea` as described in the DDNS page on the Debian wiki.

> Use of proxy server such as `squid` is much more efficient for saving bandwidth than use of local mirror server with the full Debian archive contents.

Other network application clients

Here are other network application clients.

package	popcon	size	protocol	description
`netcat-traditional`	@-@popcon1@-@	@-@psize1@-@	TCP/IP	TCP/IP swiss army knife

package	popcon	size	protocol	description
`netcat-openbsd`	@-@popcon1@-@	@-@psize1@-@	TCP/IP	TCP/IP swiss army knife with support for IPv6, proxies, and Unix sockets
`openssl`	@-@popcon1@-@	@-@psize1@-@	SSL	Secure Socket Layer (SSL) binary and related cryptographic tools
`stunnel4`	@-@popcon1@-@	@-@psize1@-@	, ,	universal SSL Wrapper
`telnet`	@-@popcon1@-@	@-@psize1@-@	TELNET	TELNET client
`nfs-common`	@-@popcon1@-@	@-@psize1@-@	NFS	Unix file sharing
`smbclient`	@-@popcon1@-@	@-@psize1@-@	SMB	MS Windows file and printer sharing client
`cifs-utils`	@-@popcon1@-@	@-@psize1@-@	, ,	mount and umount commands for remote MS Windows file
`wget`	@-@popcon1@-@	@-@psize1@-@	HTTP and FTP	web downloader
`curl`	@-@popcon1@-@	@-@psize1@-@	, ,	, ,
`transmission-gtk`	@-@popcon1@-@	@-@psize1@-@	BitTorrent	BitTorrent client (GTK)
`transmission-qt`	@-@popcon1@-@	@-@psize1@-@	, ,	BitTorrent client (Qt)
`ktorrent`	@-@popcon1@-@	@-@psize1@-@	, ,	BitTorrent client (Qt)
`qbittorrent`	@-@popcon1@-@	@-@psize1@-@	, ,	BitTorrent client (Qt)
`bind9-host`	@-@popcon1@-@	@-@psize1@-@	DNS	`host` (1) from bind9, "`Priority: standard`"
`dnsutils`	@-@popcon1@-@	@-@psize1@-@	, ,	`dig` (1) from bind, "`Priority: standard`"
`ldap-utils`	@-@popcon1@-@	@-@psize1@-@	LDAP	obtain data from LDAP server

List of network application clients

The diagnosis of the system daemons

The `telnet` program enables manual connection to the system daemons and its diagnosis.

For testing plain POP3 service, try the following

```
$ telnet mail.ispname.net pop3
```

For testing the TLS/SSL enabled POP3 service by some ISPs, you need TLS/SSL enabled `telnet` client by the `telnet-ssl` or `openssl` packages.

```
$ telnet -z ssl pop.gmail.com 995


$ openssl s_client -connect pop.gmail.com:995
```

The following RFCs provide required knowledge to each system daemon.

RFC	description
rfc1939 and rfc2449	POP3 service
rfc3501	IMAP4 service
rfc2821 (rfc821)	SMTP service
rfc2822 (rfc822)	Mail file format
rfc2045	Multipurpose Internet Mail Extensions (MIME)
rfc819	DNS service
rfc2616	HTTP service
rfc2396	URI definition

List of popular RFCs

The port usage is described in "`/etc/services`".

□□□ #2
□ □□□ □□□ 2026-10-31 13:07:47 UTC
□ □□□ □□□ 2026-10-31 13:07:49 UTC