Network tools

telnet

Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

https://en.wikipedia.org/wiki/Telnet

Telnet - port 80

```
hesa@schnittke:~$ telnet www.gnu.org 80
GET /index.html http/1.0
# type enter twice
```

Telnet - port 25

```
hesa@schnittke:~$ telnet
a.mailserver.com 25
EHLO client.yrgo.com
….
MAIL FROM: <you@yourdomain.com>
RCPT TO: <friend@mailserver.com>
DATA
Hejsan
.
```

network sniffers

tcpdump

wireshark

tcpdump

Sniffing http (over tcp)

$ sudo tcpdump -i enx0050b65c4375 tcp port http

```
14:26:29.516628 IP6 web-f2.sunet.se.http > 2001:6b0:2:2f02:b975:2d66:e641:b538.48014: Flags [P.], seq 1:552, ack 379, win 232, options [nop,nop,TS val 286628832 ecr 1925852], length 551: HTTP: HTTP/1.1 301 Moved Permanently

14:26:29.516638 IP6 2001:6b0:2:2f02:b975:2d66:e641:b538.48014 > web-f2.sunet.se.http: Flags [.], ack 552, win 234, options [nop,nop,TS val 1925855 ecr 286628832], length 0
```

Http tools

NAME

lwp-request, GET, POST, HEAD - Simple command line user agent

…

DESCRIPTION

This program can be used to send requests to WWW servers and your local file system. The request content for POST and PUT methods is read from stdin. The content of the response is printed on stdout. Error messages are printed on stderr. The program returns a status value indicating the number of URLs that failed.

Http tools

```
$ lwp-request -m HEAD aftonbladet.se
200 OK
Cache-Control: private,s-maxage=0
Connection: close
Date: Thu, 02 Feb 2017 13:38:02 GMT
Via: 1.1 varnish
Via: 1.1 varnish
Server: Apache-Coyote/1.1
Vary: Accept-Encoding,X-AB-Device-Type,X-AB-Aftonbladet-Service,X-AB-Test-Segment
Content-Type: text/html;charset=utf-8
Client-Date: Thu, 02 Feb 2017 13:36:53 GMT
Client-Peer: 144.63.250.10:80
Client-Response-Num: 1
Set-Cookie: X-AB-Segment=9; Expires=Wed, 01-Jan-2020 00:00:01 GMT; Path=/;
Domain=.aftonbladet.se
Set-Cookie: X-AB-Device-Type=desktop; Expires=Wed, 01-Jan-2020 00:00:01 GMT; Path=/;
Domain=.aftonbladet.se
X-UA-Compatible: IE=edge,chrome=1
```

Http tools

```
$ lwp-request -m HEAD www.forsvarsmakten.se
200 OK
Cache-Control: public
Connection: close
Date: Thu, 02 Feb 2017 13:36:12 GMT
Vary: *
Content-Type: text/html; charset=utf-8
Expires: Thu, 02 Feb 2017 14:12:43 GMT
Client-Date: Thu, 02 Feb 2017 13:34:56 GMT
Client-Peer: 159.72.137.10:80
Client-Response-Num: 1
```

HEAD

```
$ HEAD www.gp.se
200 OK
Cache-Control: public, max-age=120, s-maxage=120
Connection: close
Date: Thu, 04 Feb 2016 22:51:04 GMT
Via: 1.0 www.gp.se
Age: 29
Server: Apache/2.2.23
Vary: Accept-Encoding
# in Cygwin: $ lwp-request -m HEAD www.gp.se
Content-Language: sv
Content-Length: 191575
Content-Type: text/html; charset=utf-8
Expires: Thu, 04 Feb 2016 22:52:37 GMT
Last-Modified: Thu, 04 Feb 2016 22:50:37 GMT
Client-Date: Thu, 04 Feb 2016 22:51:04 GMT
Client-Peer: 80.76.155.148:80
Client-Response-Num: 1
```

GET

```
GET sunet.se/index.html
```

```
lwp-request -m GET sunet.se/index.html
```

wget / curl

Get sunet’s web page

```
wget  www.sunet.se
```

Get sunet’s web page - recursively

```
wget -r www.sunet.se
```

curl:a in data to a web server

```
curl --data '{ "name": "Alfons Åberg" }' --header "Content-Type: application/json" --request POST appserver.webserver.com/
```

netstat

Check how you OS routes your IP traffic

```
$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         129.16.1.4      0.0.0.0         UG        0 0          0 enx0050b65c4375
0.0.0.0         10.0.0.1        0.0.0.0         UG        0 0          0 wlp1s0
10.0.0.0        0.0.0.0         255.255.0.0     U         0 0          0 wlp1s0
129.16.0.0      0.0.0.0         255.255.0.0     U         0 0          0 enx0050b65c4375
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 docker0
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
```

netstat

Check how you OS routes your IP traffic

```
$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         129.16.1.4      0.0.0.0         UG    100    0        0 enx0050b65c4375
0.0.0.0         10.0.0.1        0.0.0.0         UG    600    0        0 wlp1s0
10.0.0.0        0.0.0.0         255.255.0.0     U     600    0        0 wlp1s0
129.16.0.0      0.0.0.0         255.255.0.0     U     100    0        0 enx0050b65c4375
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 docker0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
```

ping

```
ping sunet.se

ping -c1 www.google.com       # only one ping
ping -t 2 www.google.com      # timeout
ping -c1 -t 1 www.google.com # timeout, only one ping
```

traceroute

```
$ traceroute www.sunet.se
traceroute to www.sunet.se (192.36.171.231), 30 hops max, 60 byte packets
 1  gw-9-129.chl.chalmers.se (129.16.219.129)  0.397 ms  0.352 ms  0.411 ms
 2  core2-chl-gw.chalmers.se (129.16.2.89)  0.702 ms  0.779 ms  0.859 ms
 3  cth-r2.sunet.se (130.242.6.10)  0.562 ms  0.548 ms  0.569 ms
 4  goteborg-gbg7-r2.sunet.se (130.242.4.176)  0.700 ms  0.721 ms  0.705 ms
 5  trollhattan-trh-r1.sunet.se (130.242.4.41)  1.628 ms  1.614 ms  1.631 ms
 6  karlstad-kar1-r1.sunet.se (130.242.4.38)  3.842 ms  3.841 ms  3.764 ms
 7  orebro-lba-r1.sunet.se (130.242.4.29)  5.173 ms  5.121 ms  5.060 ms
 8  vasteras-fsn2-r1.sunet.se (130.242.4.30)  6.330 ms  6.304 ms  6.276 ms
 9  stockholm-tug-r1.sunet.se (130.242.4.35)  7.567 ms  7.546 ms  7.530 ms
10  stockholm-tug-r2.sunet.se (130.242.5.47)  7.551 ms  7.536 ms  7.522 ms
11  * * *
12  * * *
13  * * *
```

DNS - what IP?

whois

Who is sunet.se?

```
$ whois sunet.se
# Copyright (c) 1997- IIS (The Internet Foundation In Sweden).
# …….
#
state:            active
domain:           sunet.se
holder:           sunets0702-00001
admin-c:          -
tech-c:           -
billing-c:        vetens0911-00001
created:          1989-03-20
modified:         2016-11-10
expires:          2017-12-31
nserver:          server.nordu.net
nserver:          b.ns.kth.se
nserver:          sunic.sunet.se 192.36.125.2 2001:6b0:7::2
nserver:          ns1.sunet.se 2001:6b0:8:2::224
192.36.171.224
dnssec:           signed delegation
status:           ok
registrar:        SE Direkt
```

DNS

What IP has sunet.se?

host dig nslookup

DNS

```
$ dig www.forsvarsmakten.se

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.forsvarsmakten.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16864
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.forsvarsmakten.se.       IN   A

;; ANSWER SECTION:
www.forsvarsmakten.se.    1800 IN   A    159.72.137.10
www.forsvarsmakten.se.    1800 IN   A    159.72.137.11

;; Query time: 56 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Feb 02 15:33:47 CET 2017
;; MSG SIZE  rcvd: 82
```

DNS

```
$ nslookup www.forsvarsmakten.se
Server:      127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
Name:    www.forsvarsmakten.se
Address: 159.72.137.10
Name:    www.forsvarsmakten.se
Address: 159.72.137.11
```

DNS

```
$ host www.forsvarsmakten.se
www.forsvarsmakten.se has address 159.72.137.11
www.forsvarsmakten.se has address 159.72.137.10
```

DNS

What about redhat's email server?

```
$ dig -tMX redhat.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -tMX redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43506
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;redhat.com.                IN   MX

;; ANSWER SECTION:
redhat.com.         3600 IN   MX   10 mx2.redhat.com.
redhat.com.         3600 IN   MX   5 mx1.redhat.com.
```

nmap

“Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich)[1] used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.”

https://en.wikipedia.org/wiki/Nmap

nmap -sT - what ports are open?

```
hesa@schnittke:~$ nmap -sT 129.16.213.216
…..
Host is up (0.031s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
24/tcp  open   priv-mail
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 11.37 seconds
```

netcat

“Netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. Netcat is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool, since it can produce almost any kind of connection its user could need and has a number of built-in capabilities.”

https://en.wikipedia.org/wiki/Netcat

netcat as a web client

nc www.gnu.se 80

netcat as a web server

```
nc -l -p 80
```

Does not really answer anything useful .... kinda bad

Let’s echo some words to nc’s stdin

```
echo "<html><body><title>Simple web demo</title><h1>Hi
there</h1><BR>Date: $(date)</BODY></HTML>" |  nc -l -p 8080
```

Kinda bad to have to restart it??

netcat as a web server

```
$ nc -l -p 8080
GET / HTTP/1.1
User-Agent: Wget/1.17.1
(linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: localhost:8080
Connection: Keep-Alive
```

```
$ wget localhost:8080
--2017-02-02 14:47:03--  http://localhost:8080/
Resolving localhost (localhost)... 127.0.0.1
Connecting to localhost
(localhost)|127.0.0.1|:8080... connected.
HTTP request sent, awaiting response...
```

netcat as a web server

Kinda bad to have to restart it?? Let’s use a simple bash while loop

```
$ while (true); do echo "<html><body><title>Simple web demo</title><h1>Hi
there</h1><BR>Date: $(date)</BODY></HTML>" |  nc -l -p 8080 ; done
```

netcat as a web server

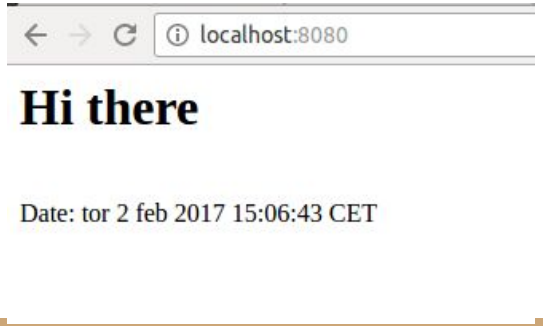
```
$ while (true); do echo
"<html><body><title>Simple web
demo</title><h1>Hi there</h1><BR>Date:
$(date)</BODY></HTML>" |  nc -l -p 8080
; done
```

```
GET / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: localhost:8080
Connection: Keep-Alive
```

```
$ curl localhost:8080
<html><body><title>Simple web
demo</title><h1>Hi there</h1><BR>Date:
tor  2 feb 2017 14:50:15
CET</BODY></HTML>
```

netcat as a web server - with header

```
$$ while (true); do echo -e "HTTP/1.0 200 OK\nConnection: close\nDate: $(date)\nContent-Type:
text/html; charset=utf-8\nContent-Length: 112\nServer: two idiots using
netcat\n\n<html><body><title>Simple web demo</title><h1>Hi there</h1><BR>Date:
$(date)</body></html>" |  nc -l -p 8080 ; done
GET / HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.76 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8,sv;q=0.6
Cookie: org.cups.sid=4e25cbe140b3582bacd243147abcf3a2
```



netcat as a web server - redirecting

```
$ $ while (true); do echo -e "HTTP/1.1 301 Moved Permanently\nLocation:
http://juneday.podbean.com" |  nc -l -p 8080 ; done
GET / HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.76 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8,sv;q=0.6
Cookie: org.cups.sid=4e25cbe140b3582bacd243147abcf3a2
```

ssh

“Secure Shell, or SSH, is a cryptographic (encrypted) network protocol to allow remote login and other network services to operate securely over an unsecured network.”

https://en.wikipedia.org/wiki/Secure_Shell

ssh login

```
ssh hostname            # log in to hostname

ssh -X hostname         # forward X protocol

ssh -l user hostname    # log in to hostname with user

ssh hostname ls         # log in to hostname and execute ls
```

ssh login

```
ssh -t host1 ssh -t host2 sudo /etc/init.d/networking restart # Login to host2
```

(via host1) and restart the network

```
ssh   -L9091:192.168.1.1:80 homehost
```

Open up a tunnel to router’s web interface

rsync

rsync is a utility for efficiently transferring and synchronizing files across computer systems

Backup to:

```
rsync -arv directory remotehost:backup/         # to the remote home folder

rsync -arv directory remotehost:/backup/ada/   # to /backup/ada
```

Sync from:

```
rsync -arv remotehost:backup directory/         # from the remote home folder
```