Network commands - summary

Tools and commands for networking in Bash

Checking if a host is up (responds) - ping

```
$ ping ftp.sunet.se # continuous ping
PING sunet.ftp.acc.umu.se (194.71.11.173): 56 data bytes
64 bytes from 194.71.11.173: icmp_seq=0 ttl=55 time=17,987 ms
64 bytes from 194.71.11.173: icmp_seq=1 ttl=55 time=18,055 ms
64 bytes from 194.71.11.173: icmp_seq=2 ttl=55 time=18,003 ms
64 bytes from 194.71.11.173: icmp_seq=3 ttl=55 time=18,004 ms
^C--- sunet.ftp.acc.umu.se ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 17,987/18,012/18,055/0,026 ms
$ ping -c 1 www.gu.se # send one ping
PING www.gu.se (130.241.151.114): 56 data bytes
64 bytes from 130.241.151.114: icmp_seq=0 ttl=62 time=0,776 ms
--- www.gu.se ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0,776/0,776/0,776/0,000 ms
```

Check the route to a computer - traceroute

```
$ traceroute www.su.se
traceroute to su.se (193.11.30.171), 64 hops max
  1   10.0.0.101  1,909ms  1,814ms  1,864ms
  2   129.16.4.177  1,989ms  1,933ms  2,608ms
  3   129.16.2.185  2,263ms  2,113ms  2,181ms
  4   130.242.6.10  2,172ms  2,626ms  2,073ms
  5   130.242.4.176  2,312ms  2,234ms  2,242ms
  6   130.242.4.41  3,400ms  3,207ms  3,207ms
  7   130.242.4.38  5,472ms  5,443ms  5,394ms
  8   130.242.4.29  6,773ms  6,638ms  6,605ms
  9   130.242.4.30  8,363ms  8,291ms  8,261ms
 10   130.242.4.35  10,089ms  9,299ms  9,248ms
 11   130.242.6.143  9,395ms  9,426ms  9,308ms
 12   130.237.154.26  9,571ms  9,535ms  9,578ms
 13   130.237.242.4  9,311ms  9,193ms  9,273ms
 14   193.11.30.171  9,668ms  9,747ms  9,654ms
$
```

Check the route to a computer - mtr

```
$ mtr -i 1 -r ftp.sunet.se # -i 1 (one sec betw. probes) -r (report - noninteractive)
Start: Sat Feb  4 16:12:44 2017
HOST: dellasoul                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 192.168.0.1                 0.0%    10    0.7   2.2   0.7  10.4   2.9
  2.|-- ???                       100.0     10    0.0   0.0   0.0   0.0   0.0
  3.|-- fa-bbr-1-be10-10.net.comh  0.0%    10    7.5  10.8   7.5  24.9   5.0
  4.|-- vrr-core-1-be104.net.comh  0.0%    10   15.6  15.9  13.8  17.9   1.1
  5.|-- mtc-core-1-be2.net.comhem  0.0%    10   16.3  21.5  14.1  72.8  18.1
  6.|-- 213.200.162.32             0.0%    10   15.6  20.8  13.0  53.8  12.2
  7.|-- netnod-ix-ge-a-sth-4470.s  0.0%    10   14.7  17.2  12.4  33.9   5.9
  8.|-- stockholm-fre-r1.sunet.se  0.0%    10   14.0  15.7  11.7  21.0   2.4
  9.|-- uppsala-upa-r1.sunet.se    0.0%    10   16.3  16.9  14.2  20.1   1.6
 10.|-- gavle-sbo-r1.sunet.se      0.0%    10   17.6  17.8  15.9  23.0   1.9
 11.|-- sundsvall-sva-r1.sunet.se  0.0%    10   24.8  20.9  19.1  24.8   1.7
 12.|-- umu2.sunet.se              0.0%    10   22.2  24.8  20.7  32.3   4.2
 13.|-- 130.239.0.29               0.0%    10   21.6  33.7  19.7 126.4  32.9
 14.|-- 130.239.0.86               0.0%    10   23.1  28.6  22.3  68.8  14.3
 15.|-- hammurabi.acc.umu.se       0.0%    10   23.4  24.1  21.4  30.4   2.6
```

DNS tools - host

```
$ host www.su.se # get IP from name
www.su.se is an alias for su.se.
su.se has address 193.11.30.171
su.se has IPv6 address 2001:6b0:5:50::171
su.se mail is handled by 10 v-mailfilter03.sunet.se.
su.se mail is handled by 10 e-mailfilter03.sunet.se.
su.se mail is handled by 20 e-mailfilter04.sunet.se.
$ host ait.gu.se
ait.gu.se has address 130.241.151.114
ait.gu.se mail is handled by 10 e-mailfilter03.sunet.se.
ait.gu.se mail is handled by 10 v-mailfilter03.sunet.se.
ait.gu.se mail is handled by 10 e-mailfilter04.sunet.se.
$ host 130.241.151.114 # get name from IP
114.151.241.130.in-addr.arpa domain name pointer www.gu.se.
```

DNS tools - host

```
$ host -t ns www.su.se # what DNS is responsible for www.su.se?
www.su.se is an alias for su.se.
su.se name server ns3.su.se.
su.se name server ns1.su.se.
su.se name server ns2.su.se.
$ host -t mx www.su.se # what mail server is responsible for su.se?
www.su.se is an alias for su.se.
su.se mail is handled by 10 v-mailfilter03.sunet.se.
su.se mail is handled by 10 e-mailfilter03.sunet.se.
su.se mail is handled by 20 e-mailfilter04.sunet.se.
```

DNS tools - nslookup

```
$ nslookup juneday.se
Server: 127.0.1.1
Address: 127.0.1.1#53
Non-authoritative answer:
Name: juneday.se
Address: 89.18.105.40
```

DNS tools - nslookup

```
$ nslookup -query=any juneday.se ns1.loopia.se # ← you can specify DNS server to use
;; Truncated, retrying in TCP mode.
Server: ns1.loopia.se
Address: 2a02:250:ffff::20#53
Name: juneday.se
Address: 89.18.105.40
juneday.se mail exchanger = 20 mail2.loopia.se.
juneday.se mail exchanger = 10 mailcluster.loopia.se.
juneday.se nameserver = ns2.loopia.se.
juneday.se nameserver = ns1.loopia.se.
juneday.se
origin = ns1.loopia.se
mail addr = registry.loopia.se
serial = 1561593600
refresh = 10800
retry = 3600
expire = 604800
minimum = 86400
```

DNS tools - dig

```
$ dig ituniv.se
; <<>> DiG 9.10.3-P4-Ubuntu <<>> ituniv.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21380
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ituniv.se. IN A
;; AUTHORITY SECTION:
ituniv.se. 496 IN SOA ns1.chalmers.se. cth-nic.chalmers.se. 2018051408 14400 3600 1209600
600
;; Query time: 5 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Jul 03 10:34:52 CEST 2019
;; MSG SIZE rcvd: 95
```

DNS tools - dig

```
$ dig ituniv.se NS # Type NS (name server)

; <<>> DiG 9.10.3-P4-Ubuntu <<>> ituniv.se NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22804
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ituniv.se.             IN    NS

;; ANSWER SECTION:
ituniv.se.        26751 IN    NS    ns2.chalmers.se.
ituniv.se.        26751 IN    NS    ns1.chalmers.se.
ituniv.se.        26751 IN    NS    ns3.chalmers.se.

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Aug 02 15:41:14 CEST 2019
;; MSG SIZE  rcvd: 101
```

DNS tools - dig

```
$ dig gu.se mx +short # Type MX (mail) and be brief about it)
11 e-mailfilter03.sunet.se.
10 v-mailfilter03.sunet.se.
11 e-mailfilter04.sunet.se.
```

DNS tools - Comparison of syntaces

```
$ dig gu.se mx +short
11 e-mailfilter03.sunet.se.
10 v-mailfilter03.sunet.se.
11 e-mailfilter04.sunet.se.
$ nslookup -query=mx chalmers.se
Server: 127.0.1.1
Address: 127.0.1.1#53
Non-authoritative answer:
chalmers.se mail exchanger = 10 e-mailfilter03.sunet.se.
chalmers.se mail exchanger = 10 e-mailfilter04.sunet.se.
chalmers.se mail exchanger = 10 v-mailfilter03.sunet.se.
$ host -t mx chalmers.se
chalmers.se mail is handled by 10 e-mailfilter03.sunet.se.
chalmers.se mail is handled by 10 e-mailfilter04.sunet.se.
chalmers.se mail is handled by 10 v-mailfilter03.sunet.se.
```

Domain tools - whois

```
$ whois -H utpressningskollen.se | grep -v \#   # -H (remove some headers)
state: active
domain: utpressningskollen.se
holder: hosbah6235-00001
admin-c: -
tech-c: -
billing-c: -
created: 2018-01-15
modified: 2019-02-13
expires: 2020-01-15
transferred: 2019-02-13
nserver: ns.bahnhof.se
nserver: ns2.bahnhof.se
dnssec: unsigned delegation
registry-lock: unlocked
status: ok
registrar: Loopia AB
```

Domain tools - whois reverse lookup

```
$ whois -B -H 94.254.0.94 | egrep -v \#          # -B show email etc, -H hide some text
% Information related to '94.254.0.0 - 94.254.0.255'
% Abuse contact for '94.254.0.0 - 94.254.0.255' is 'abuse@bahnhof.net'
inetnum: 94.254.0.0 - 94.254.0.255
country: SE
notify: ripe-kr@bahnhof.net
mnt-by: BAHNHOF-NCC
created: 2012-09-03T11:15:53Z
last-modified: 2012-09-03T11:15:53Z
source: RIPE
role: Bahnhof DBM
address: Bahnhof AB
address: Isafjordsgatan 32B
address: 164 40 Kista
address: Sweden
e-mail: ripe@bahnhof.se
% Information related to '94.254.0.0/18AS8473'
route: 94.254.0.0/18
descr: Bahnhof Internet, Sweden
```

Your computer network setup - ifconfig

```
$ ifconfig
lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:1042133 errors:0 dropped:0 overruns:0 frame:0
 TX packets:1042133 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1
 RX bytes:110036554 (110.0 MB) TX bytes:110036554 (110.0 MB)
wlp58s0 Link encap:Ethernet HWaddr 9c:b6:d0:f2:e1:f9
 inet addr:10.0.116.35 Bcast:10.0.255.255 Mask:255.255.0.0
 inet6 addr: 2001:6b0:2:2801:36bd:fb4f:417b:b503/64 Scope:Global
 inet6 addr: fe80::de1f:acad:148:d9b4/64 Scope:Link
 inet6 addr: 2001:6b0:2:2801:7c4a:f173:1eac:e775/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:11436971 errors:0 dropped:0 overruns:0 frame:0
 TX packets:7864743 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:6755283977 (6.7 GB) TX bytes:2080639936 (2.0 GB)
```

Your computer network setup - ip

```
$ ip address # address is an argument
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid_lft forever preferred_lft forever
 inet6 ::1/128 scope host
 valid_lft forever preferred_lft forever
2: wlp58s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
 link/ether 9c:b6:d0:f2:e1:f9 brd ff:ff:ff:ff:ff:ff
 inet 10.0.116.35/16 brd 10.0.255.255 scope global dynamic wlp58s0
 valid_lft 43146sec preferred_lft 43146sec
 inet6 2001:6b0:2:2801:7015:323b:6e9e:826c/64 scope global temporary dynamic
 valid_lft 604748sec preferred_lft 85748sec
 inet6 2001:6b0:2:2801:36bd:fb4f:417b:b503/64 scope global mngtmpaddr noprefixroute dynamic
 valid_lft 2591997sec preferred_lft 604797sec
 inet6 fe80::de1f:acad:148:d9b4/64 scope link
 valid_lft forever preferred_lft forever
```

Your computer network setup - hostname

```
$ hostname -I # -I ip numbers
10.0.116.35 2001:6b0:2:2801:7015:323b:6e9e:826c 2001:6b0:2:2801:36bd:fb4f:417b:b503

$ hostname # without argument, it gives you the computer name
newdelli
```

Your computer network - netstat

```
$ netstat -ta|grep -v tcp6 # → -ta means “tcp, all”
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 *:hostmon *:* LISTEN
tcp 0 0 newdelli:domain *:* LISTEN
tcp 0 0 localhost:ipp *:* LISTEN
tcp 0 0 10.0.116.35:52930 104.244.42.129:https ESTABLISHED
tcp 0 0 10.0.116.35:45548 ec2-52-207-41-59.:https ESTABLISHED
tcp 0 0 10.0.116.35:53612 104.17.9.41:https ESTABLISHED
tcp 0 0 10.0.116.35:42922 do-39.lastpass.co:https ESTABLISHED
tcp 0 0 10.0.116.35:53802 104.17.9.41:https ESTABLISHED
tcp 0 0 10.0.116.35:38052 a104-76-42-24.dep:https TIME_WAIT
tcp 0 0 localhost:35086 newdelli:42446 ESTABLISHED
tcp 0 0 10.0.116.35:54194 owa.gu.se:https ESTABLISHED
tcp 0 0 10.0.116.35:54188 owa.gu.se:https ESTABLISHED
tcp 0 0 10.0.116.35:42970 151.101.86.165:https ESTABLISHED
tcp 0 0 10.0.116.35:52934 169.236.13.217.in:https ESTABLISHED
tcp 0 0 10.0.116.35:39974 37.18.211.130.bc.:https ESTABLISHED
tcp 0 0 10.0.116.35:55796 151.101.85.209:https ESTABLISHED
tcp 0 0 10.0.116.35:54446 164.67.193.35.bc.:https ESTABLISHED
tcp 0 0 10.0.116.35:44736 104.244.42.195:https ESTABLISHED
tcp 0 0 10.0.116.35:33244 dhcp147.itit.gu.se:26 ESTABLISHED
tcp 0 0 10.0.116.35:40964 151.101.84.157:https ESTABLISHED
```

Your computer network - lastlog

```
$ lastlog |grep -v Never # who has logged into your system?
Username Port From Latest
latour pts/1 133.231.23.147 Wed Jun 26 10:16:53 +0200 2019
börje pts/8 212.193.1.157 Thu Mar 3 07:58:38 +0100 2016
ada pts/0 133.221.23.147 Wed Jul 3 14:57:09 +0200 2019
vatofa pts/2 10.230.8.53 Tue Dec 11 13:04:50 +0100 2018
malin pts/0 82.62.176.119 Sun Jun 24 17:22:36 +0200 2018
dumbom pts/11 129.16.134.81 Tue Jun 12 14:11:45 +0200 2018
```

Your computer network - what DNS am I using?

```
$ nmcli dev show | grep IP4.DNS
IP4.DNS[1]: 10.0.0.1
IP4.DNS[2]: 10.0.0.2
$ grep nameserver /etc/resolv.conf
nameserver 127.0.1.1 # ← Rikard is using dnsmasq
$ grep -Po ".*nameserver '\K[^']+" /var/log/kern.log | tail
-2
10.0.0.1
10.0.0.2
# -P use Perl regex
# -o print only the matching part of the line(s)
# \K[^']+  everything that is not a single quote (the IP numbers)
# Aug  2 16:06:17 newdelli NetworkManager[919]: <info>  [1564754777.1822]   nameserver '10.0.0.1'
```

Your computer network - what DNS am I using?

```
$ grep nameserver /var/log/kern.log | tail -2
Jul 4 08:57:55 newdelli NetworkManager[919]: <info> [1562223475.0392] nameserver '10.0.0.1'
Jul 4 08:57:55 newdelli NetworkManager[919]: <info> [1562223475.0393] nameserver '10.0.0.2'
```

Your computer network - what default gateway?

```
$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 10.0.0.1 0.0.0.0 UG 600 0 0 wlp58s0
10.0.0.0 * 255.255.0.0 U 600 0 0 wlp58s0
link-local * 255.255.0.0 U 1000 0 0 wlp58s0

$ ip r | grep default
default via 10.0.0.1 dev wlp58s0 proto static metric 600

$ netstat -r | grep default
default 10.0.0.1 0.0.0.0 UG 0 0 0 wlp58s0
```

Connecting to computers - lwp-request

```
$ lwp-request -m HEAD http://ait.gu.se
200 OK Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Connection: close Date: Thu, 04 Jul 2019 08:21:15 GMT
Pragma: no-cache Via: 1.1 varnish (Varnish/5.2)
Age: 0 Server: nginx/1.12.2
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Type: text/html;charset=utf-8
Last-Modified: Tue, 02 Jul 2019 09:14:20 CEST
Access-Control-Allow-Origin: http://cmssystem.gu.se:80
Client-Date: Thu, 04 Jul 2019 08:21:15 GMT
Client-Peer: 130.241.151.114:443
Client-Response-Num: 1
X-Backend: cmspres_vir_3: cms
```

Connecting to computers - curl

```
$ curl -s http://kursplaner.gu.se/pdf/kurs/sv/TIG015 -o TIG015.pdf
-s be silent about it (no status messages, progress)
-o save to the file...
```

Connecting to computers - ssh

```
[rikard@newdelli ~]$ ssh computer.domain-name.com
rikard@computer.domain-name.com's password: ← password is not echoed
[rikard@computer ~]$
```

Connecting to computers - ssh remote command

```
[rikard@newdelli ~]$ ssh computer.domain-name.com hostname
rikard@computer.domain-name.com's password: ← password is not echoed
computer ← the result of the command run on the other computer
[rikard@newdelli ~]$ ← rikard is still logged in at his own computer
```

Connecting to computers - scp, rsync download

```
[rikard@newdelli ~]$ scp computer.domain-name.com:WikiScreenshot.png .
rikard@computer.domain-name.com's password:
WikiScreenshot.png 100% 281KB 15.1MB/s 00:00
[rikard@newdelli ~]$ ← rikard is still logged in at his own computer

$ rsync -va computer.domain-name.com:WikiScreenshot.png .
# -v verbose -a archive
rikard@computer.domain-name.com's password:
receiving incremental file list
WikiScreenshot.png

sent 43 bytes received 287,635 bytes 191,785.33 bytes/sec total size is
287,455 speedup is 1.00
```

Connecting to computers - scp, rsync upload

Upload file using scp:

```
[rikard@newdelli ~]$ scp WikiScreenshot.png computer.domain-name.com: ← don’t forget
rikard@computer.domain-name.com's password:
WikiScreenshot.png 100% 281KB 15.1MB/s 00:00
[rikard@newdelli ~]$ ← rikard is still logged in at his own computer
```

Upload file using rsync:

```
[rikard@newdelli ~]$ rsync -va WikiScreenshot.png computer.domain-name.com:
rikard@computer.domain-name.com's password:
sending incremental file list
sent 73 bytes received 12 bytes 170.00 bytes/sec
total size is 287,455 speedup is 3,381.82
```

Summary part 1

- ping - see if host replies
- traceroute, mtr - see route to host
- host, nslookup, dig - translate between names and ip numbers
- whois - information about a domain name (who owns it etc)
- ip, ifconfig - information about your network cards etc
- hostname - information about your hostname and ip number
- netstat - information about your active connections
- you can find out what DNS your are using in various ways
- route, ip, netstat - you can find your default gateway
- lwp-request, curl, wget - tools for HTTP

Summary part 2

- ssh - connect to remote computer, run commands remote
- scp, rsync - copy files from and to computers