Linux_Networking

Linux Networking Course

History

*Arpanet
*switched network

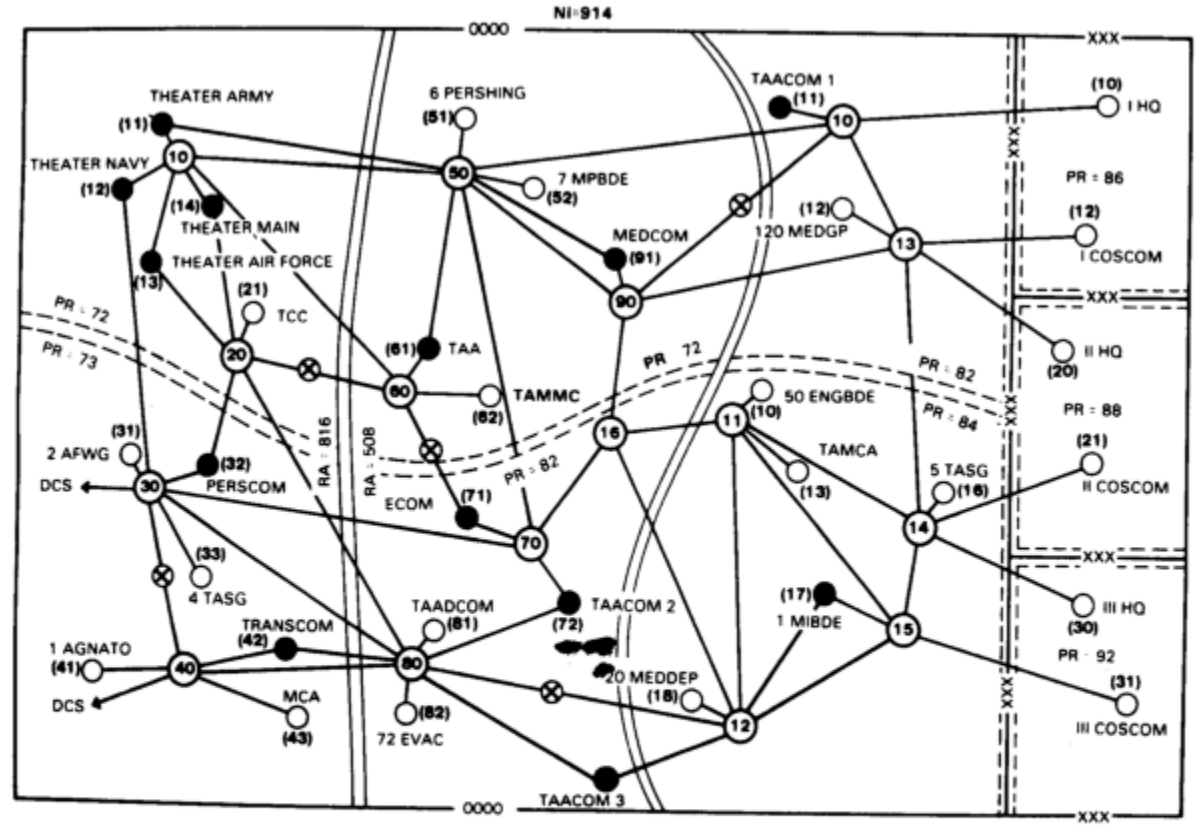


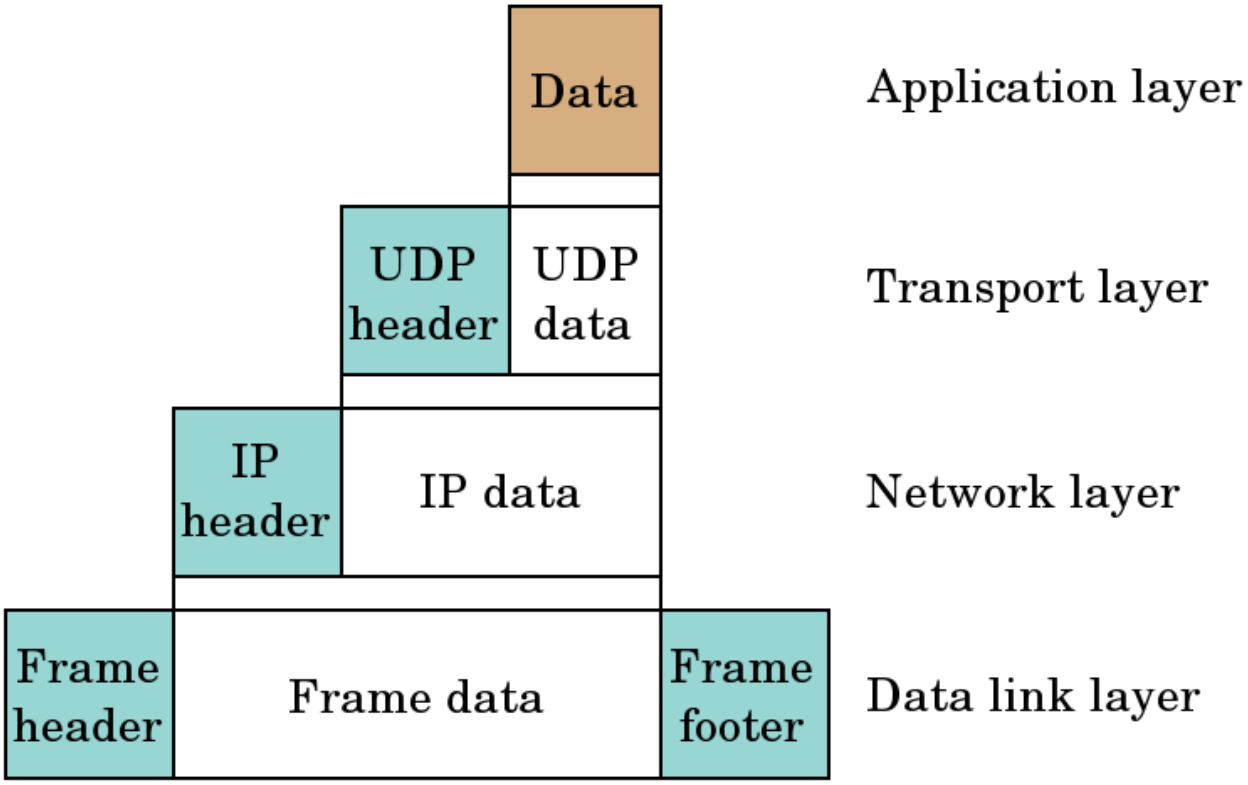
Figure B-1. Network numbering plan.

*TCP/IP
*spread in the 90's

TCP/IP

What is a protocol

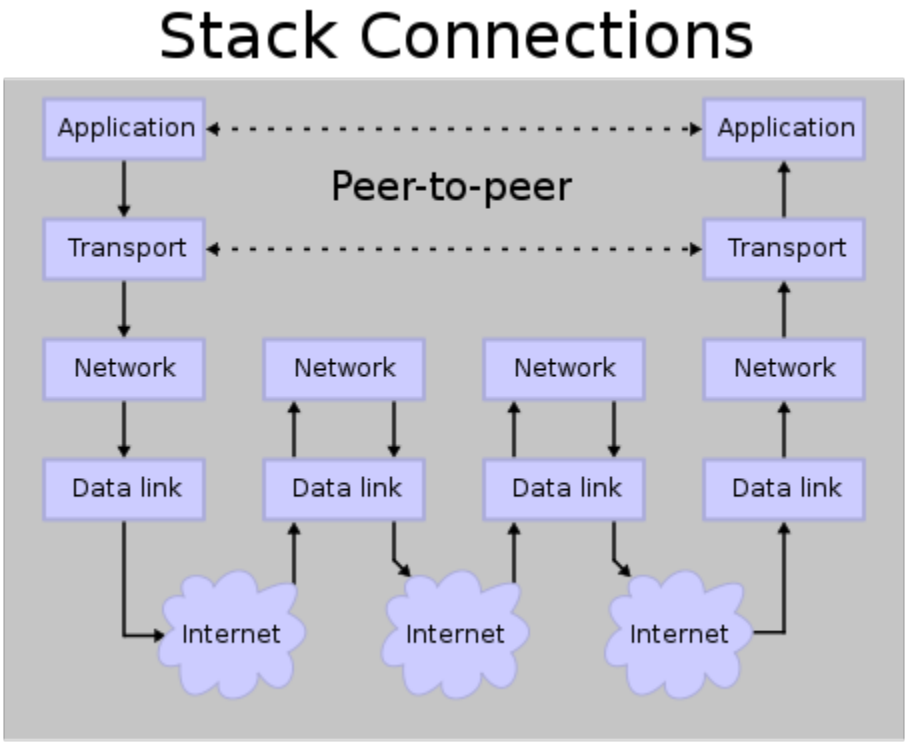
*strict procedure how things are done
*communication between layers
*clearly defined interfaces
*data encapsulation



*example

TCP/IP protocol

*Application
*Transport
*Network
*Physical / Data link



from wikipedia

Physical layer / Data link layer

*not much of a concern for us.
*different topologies (ethernet, wirless, DSL, modem etc)
*this is about the physical connection
*here the bits are shifted.
*how many Volt represent a 1, how many a 0
*ethernet address (HWaddr in Hex format)

Network layer

*IP ICMP
*IPv4 32bit written in dotted decimal notation
*65.212.180.178

*different classes

```
A starts with 0
B starts with 10
C starts with 110
D starts with 1110
```

*although outdated it roughly specifies the network and host part.
*Common now is the CIDR (Classless InterDomain Routing)

```
192.168.10.3/24
```

this actually stands for

```
11000000 10101000 00001010 00000011
11111111 11111111 11111111 00000000
```

private networks that are not routed

```
10.0.0.0        -   10.255.255.255  (10/8 prefix)
172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

localhost 127.0.0.0/8
"network addresses" ending with 0
"broadcast addresses" ending with 255
routing
nat
configuration

Transport Layer

UDP (User Datagram Protocol)

connectionless
media-streaming

TCP (Transmission Control Protocol)

makes sure every packet arrives
if it didn't arrive, it will request it again
ftp-data-transfer

*connections through ports
*well known ports can be found in /etc/services

```
~$ cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp
domain          53/tcp                          # name-domain server
domain          53/udp
mtp             57/tcp                          # deprecated
tacacs-ds       65/tcp                          # TACACS-Database Service
tacacs-ds       65/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
www             80/tcp          http            # WorldWideWeb HTTP
www             80/udp                          # HyperText Transfer Protocol
....snip....
```

Application Layer

DNS

HTTP

SSH

Tools

ifconfig

sample output of ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:19:D1:93:AE:EA
          inet addr:192.168.10.1  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::219:d1ff:fe93:aeea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:3345 (3.2 KB)
          Base address:0x30c0 Memory:90300000-90320000

eth1      Link encap:Ethernet  HWaddr 00:80:48:51:A5:31
          inet addr:192.168.0.100  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::280:48ff:fe51:a531/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3364 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2897 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3753263 (3.5 MB)  TX bytes:488792 (477.3 KB)
          Interrupt:21 Base address:0xe800

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:16436  Metric:1
          RX packets:74 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8537 (8.3 KB)  TX bytes:8537 (8.3 KB)
```

ip

output of ip route

```
192.168.0.0/24 dev eth1  proto kernel  scope link  src 192.168.0.100
192.168.10.0/24 dev eth0  proto kernel  scope link  src 192.168.10.1
default via 192.168.0.1 dev eth1  metric 100
```

ping

output of ping

```
ping 65.212.180.178
PING 65.212.180.178 (65.212.180.178) 56(84) bytes of data.
64 bytes from 65.212.180.178: icmp_seq=1 ttl=50 time=396 ms
64 bytes from 65.212.180.178: icmp_seq=2 ttl=50 time=420 ms
64 bytes from 65.212.180.178: icmp_seq=3 ttl=50 time=394 ms

--- 65.212.180.178 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3010ms
rtt min/avg/max/mdev = 394.577/403.996/420.659/11.838 ms
```

tracepath

output of tracepath

```
tracepath 65.212.180.178
 1:  192.168.0.100 (192.168.0.100)                          0.188ms pmtu 1492
 1:  192.168.1.2 (192.168.1.2)                            asymm 36   4.262ms
 2:  192.168.1.1 (192.168.1.1)                            asymm 102   5.671ms
 3:  59.92.64.1 (59.92.64.1)                              asymm  4 119.448ms
 4:  218.248.255.10 (218.248.255.10)                      141.537ms
 5:  218.248.255.10 (218.248.255.10)                      asymm  4 136.279ms
 6:  220.227.53.238 (220.227.53.238)                      160.888ms
 7:  62.216.145.81 (62.216.145.81)                        asymm 17 433.441ms
 8:  so-6-0-0.0.cjr01.ldn004.flagtel.com (62.216.128.145) asymm 16 432.633ms
 9:  82.195.188.21 (82.195.188.21)                        asymm 14 411.295ms
10:  sl-bb22-lon-8-0.sprintlink.net (213.206.128.60)      asymm 13 418.883ms
11:  sl-bb20-nyc-2-0.sprintlink.net (144.232.9.163)       asymm 13 433.378ms
12:  sl-bb26-nyc-6-0.sprintlink.net (144.232.13.9)        asymm 14 415.121ms
13:  144.232.8.194 (144.232.8.194)                        asymm 15 427.211ms
14:  tbr1.n54ny.ip.att.net (12.122.81.10)                 asymm 22 425.951ms
15:  cr1.n54ny.ip.att.net (12.122.16.161)                 asymm 21 442.912ms
16:  cr1.cgcil.ip.att.net (12.122.1.190)                  asymm 20 429.262ms
17:  cr1.st6wa.ip.att.net (12.122.31.162)                 asymm 19 439.363ms
18:  tbr1.st6wa.ip.att.net (12.122.23.154)                445.856ms
19:  gbr1.st6wa.ip.att.net (12.122.12.158)                asymm 17 440.989ms
20:  gar1.ptdor.ip.att.net (12.123.44.121)                asymm 15 422.986ms
21:  12.118.177.66 (12.118.177.66)                        asymm 13 421.216ms
22:  po1.ir1.cvo2.kattare.net (204.13.9.2)                asymm 14 420.901ms
23:  ground1.kattare.com (65.212.180.178)                 asymm 15 437.003ms reached
     Resume: pmtu 1492 hops 23 back 15
```

dig

dig bluelightav.org

```
; <<>> DiG 9.4.1-P1 <<>> bluelightav.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52347
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;bluelightav.org.               IN      A

;; ANSWER SECTION:
bluelightav.org.        2724    IN      A       65.212.180.178

;; AUTHORITY SECTION:
bluelightav.org.        2724    IN      NS      ns1.kattare.com.
bluelightav.org.        2724    IN      NS      ns2.kattare.com.

;; ADDITIONAL SECTION:
ns1.kattare.com.        170390  IN      A       69.59.195.60
ns2.kattare.com.        170390  IN      A       204.13.11.60

;; Query time: 0 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: Sat Apr 12 13:39:40 2008
;; MSG SIZE  rcvd: 128
```

content of /etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.10.1
        network 192.168.10.0
        netmask 255.255.255.0
        broadcast 192.168.10.255
        gateway 192.168.0.1

auto eth1
iface eth1 inet static
        address 192.168.0.100
        network 192.168.0.0
        netmask 255.255.255.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
```