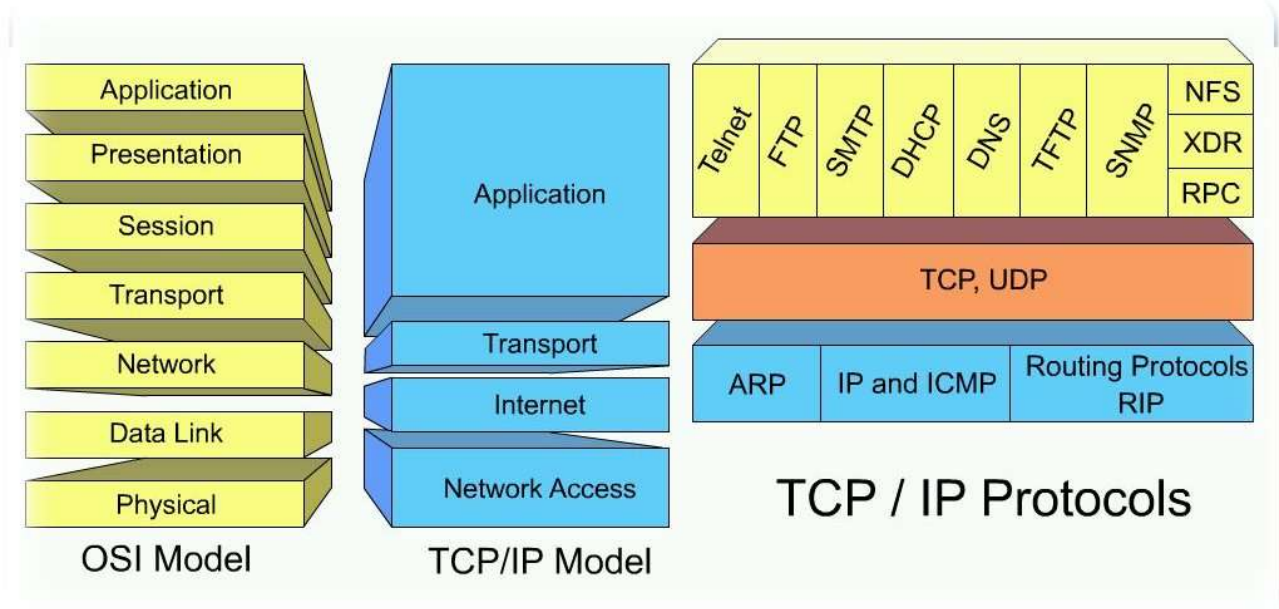


# H9 Elementair TCP/IP

## Historie van TCP/IP

Term TCP/IP komt van 2 van de 4 lagen uit communicatiemodel.



**TCP** regelt het samenstellen van een boodschap in kleinere pakketten die door de ontvanger weer worden samengesteld tot de oorspronkelijke boodschap.

TCP Header Information			
Source Port Number 16 bits (Number of calling port)		Destination Port Number 16 bits (Number of called port)	
Sequence Number 32 bits <b>(Number to ensure proper sequence of data.)</b>			
Acknowledgment Number 32-bits <b>(Identifies next segment expected)</b>			
Header Length 4 bits <b>(Number of 32 bit words in header)</b>	Reserved 6 bits <b>(Always 0)</b>	Code bits 6 bits <b>(Identifies type of segment, setup/termination of session)</b>	Window size 16 bits <b>(Number of octets the device is willing to accept)</b>
TCP Checksum 16 bits <b>(Used to ensure data integrity)</b>		Urgent Pointer 16 bits <b>(Indicates end of urgent data)</b>	
Options 0 or 32 bits <b>(Identifies maximum segment size)</b>			
Data			

**IP** regelt de adressering van ieder afzonderlijk pakketje opdat het bij de juiste bestemming uitkomt.

IP (Internet Protocol) versie 4(Ipv4)

TCP (Transmission Control Protocol) doet de foutcontrole aan de ontvangstkant en is een connection based protocol

UDP ( User Datagram Protocol) = connection less protocol

voorbeeld: audio-signaal over het netwerk. De controle op de juiste ontvangst dient door de applicatie zelf geregeld te worden.

ICMP (Internet Control Message Protocol) = boodschap- controle- en foutmeldingprotocol.

Het wordt eigenlijk alleen door het ping commando gebruikt.

PPP ( Point-to-Point Protocol) is een methode om een TCP/IP verbinding te realiseren.

Uitleg werking TCP/IP en routing in een film te zien en te downloaden bij warriorsofthe.net

### **Berekenen van netwerkid, broadcast, aantal hosts etc.**

Tip: Lees het eerst helemaal even door en probeer dan het geheel te vatten

Stel:

Je hebt een C-klasse adres (bv. 192.168.1.x)

De standaard subnet mask hiervoor is 255.255.255.0

Indien je gebruikt wilt maken van een subnet doe je als volgt:

Je neemt bijvoorbeeld: subnetmask 255.255.255.224

```
      255.255.255.255
-/-   255.255.255.224
      31
```

Ik heb hier dus de laatste 2 cijfers van elkaar af getrokken.

Dit geeft het broadcastadres dus: 192.168.1.31

het netwerkadres wordt dan: 192.168.1.0

De range van hosts wordt dan 192.168.1.1 t/m 30

Voor een subnetmask van 255.255.255.252 geldt:

Dit geeft het broadcastadres dus: 192.168.1.3

het netwerkadres wordt dan: 192.168.1.0

De range van hosts wordt dan 192.168.1.1 en 192.168.1.2

Voor een subnetmask van 255.255.240.0 geldt:

Dit geeft het broadcastadres dus: 192.168.15.255

het netwerkadres wordt dan: 192.168.1.0

De range van hosts wordt dan 192.168.1.1 t/m 192.168.15.254

subnetcalculator <http://www.warriorsofthe.net/utils/index.html>

professionele subnetcalculator [http://www.solarwinds.net/Tools/Free\\_tools/Subnet\\_Calc/index.htm](http://www.solarwinds.net/Tools/Free_tools/Subnet_Calc/index.htm)  
(windows executable)

## Interface:

Ook al heeft een netwerkkaart geen ip-nummer gekregen dan nog heeft deze een zogenaamd loopback adres t.w. 127.0.0.1 ofwel localhost.

Routes:

Gateways zijn systemen met 2 of meer netwerkkaarten welke subnetten middels een routetabel met elkaar verbinden.

## DNS:

Domain Name System heeft als doel om ip-nummers met "logische namen" te koppelen.

Het is opgebouwd vanuit Top Level domains ofwel TLD's zoals .nl, .edu, .org. Hieronder staan de domeinen zoals google, en hieronder weer subdomeinen.

WWW of FTP zijn dus ook subdomeinen !

## Applicatie-onderscheid

Om zaken eenvoudiger te maken hebben bepaalde services standaard poorten welke tot 1024 zijn vastgelegd. De poortnummers lopen tot 65535 en zijn vrij te gebruiken door overige applicaties danwel services.

De standaard poorten zijn beschreven in het bestand /etc/services (blz 206)

Belangrijke services/methodes:

<i>Naam:</i>	<i>Poort:</i>	<i>Doel/Toepassing:</i>	<i>Opmerking:</i>
FTP (File Transfer Protocol)	21	Controleren van verbinding	*1
	20	Overdracht van gegevens	
Telnet	23	Commandosessie	*2
SMTP(Simple Mail Transfer Prot.)	25	Mail overdracht	*3
DNS (Domain Name System)	53	Vertaling ip-nummer – domains	
HTTP(Hyper Text Transfer Prot.)	80	communicatie webserver-webclient	
POP3 (Post Office Protocol 3)	110	email ophalen	
NNTP(Network News Transfer Prot.)	119	uitwisseling nieuwsgroepen	
NETBIOS	137,138,139	Samba	
IMAP(Internet Message Access Prot)	143	mail blijft op server	*4
SNMP(Simple Network Management Prot)	161	korte berichten	*5

\*1 De verbinding is mogelijk op zowel active alsook passive. Gebruik altijd passive als je door een firewall heen moet.

\*2 Telnet kan geen bestanden over en weer zenden !

\*3 Er bestaan 3 soorten programma's t.a.v. Mail:

1. MUA (Mail User Agent) Dit is een programma waarmee je mail leest
2. MTA (Mail Transfer Agent) Dit is een programma waarmee email verstuurd wordt van de ene mailserver naar de andere.
3. MDA (Mail Delivery Agent) Dit is een programma waarmee het ontvangen van email geregeld wordt.

\*4 Met POP3 kun je alleen maar mail ophalen. Nadeel gedownload naar systeem A en dus de mail hebt verwijderd van de server is dit niet meer op systeem B te lezen. Bij IMAP worden de berichten altijd op de server beheerd. Bij het lezen zie je alleen de headers welke gedownload worden. Indien je een mail selecteerd wordt de inhoud gedownload. De locatie van de mailbox blijft te allen tijde de IMAP server.

\*5 SNMP wordt veel gebruikt om server danwel services info te vergaren. Denk aan of een systeem in de lucht is. Of de mailserver nog wel beschikbaar is van buitenaf etc.

## **Programma's:**

### **FTP**

op de commandline te gebruiken via: ftp <ftp.westwoud.net>

Enkele commando's:

ls	directory uitgelezen
get welcome.msg	welkomtekst opvragen
help <evt. commando>	extra info

Er zijn 2 manieren om files over te halen en de stelregel is:

Platte tekst als ASCII over halen en Binair/gecompileerde bestanden via BIN van binair.

### **Telnet**

op de commandline te gebruiken als:telnet localhost of telnet <ipnummer/hostname>

Let op ! Dit werkt prima maar is redelijk ouderwets en onveilig (wachtwoorden en overig verkeer gaat onversleuteld over de lijn) gebruik als het aanwezig is secure shell !!!

### **Host**

op de commandline te gebruiken om info over het systeem op te vragen.

Optie -a geeft heel veel meer info (DNS info).

### **Dig**

Leest meer uit de zonefile van de DNS server dan Host commando.

### **Whois**

Wordt gebruikt om administratieve gegevens te achterhalen van een bepaald domein.

- administrative contact
- domein servers
- email adres

standaard wordt het .com TLD geraadpleegd, indien je meer info wilt over .nl domein dan dien je de optie -h mee te geven: whois -h <TLD> <domein+extensie> bv. Whois -h nic.nl google.nl

### **Ping**

Middels een klein ICMP pakketje wordt getest of een server/computer beschikbaar is.

Let op! Op veel firewalls staat het toelaten van ICMP pakketjes op:

- Blocked waardoor de ip-pakketjes wel worden ontvangen maar niet worden teruggestuurd.
- Stealth waardoor de pakketjes lijken te verdwijnen in het niets ofwel host unreachable, net of deze dus niet bestaat

Extra opties voor ping zijn -c (hoeveel pings totaal te versturen) en -i (timeout in seconden)

### **Traceroute:**

Dit kan gebruikt worden om te achterhalen welke route een IP-pakket aflegt op weg van de afzender naar de bestemming. De routes zijn (zeker op internet) niet vaak gelijk. Dit wordt veroorzaakt door de gateways welke het pakketje onderweg tegenkomt.

# H10 TCP/IP configuratie en problemen oplossen

## Interfaces:

Om een netwerkkaart te configureren dient deze eerst door de kernel te worden ondersteund, hetzij als driver in de kernel, hetzij als een later geladen module.

## MAC adressen:

“unieke”identificatie van een netwerkkaart.

Eerste 4 cijfers bestaat uit een fabrikantnummer gevolgd door een volgnummer.

Elke netwerkkaart moet binnen het eigen netwerk qua MAC adres identiek zijn!

## NAT (Network Address Translation)

Dit wordt masquerading genoemd.

Het houdt een lijst bij van poortnummers en ip-adressen welke van het interne netwerk naar buiten en andersom gerouteerd moeten worden in de NAT tabel.

Reden: te kort aan ip-adressen

Op te lossen door in het interne netwerk publieke ranges te gebruiken.

## Adres instellen:

### Ifconfig:

Het commando om de netwerk interface te configureren.

Optie	Doel	Syntax	Opmerking
up	activeren	ifconfig eth0 up	moet worden uitgevoerd na toekenning ip-adres
down	de-activeren	ifconfig eth0 down	.....
mtu	max in IP	ifconfig eth0 mtu 1500	Maximum transfer unit (aantal bytes per ip-pakket)
netmask	instellen Netmask	ifconfig eth0 netmask 255.255.255.0	Normaal niet nodig -auto herkenning.
broadcast	instellen broadcast	ifconfig eth broadcast 192.168.0.255	Normaal niet nodig -auto herkenning.
pointtopoint	directe verbinding	ifconfig <iplocal> pointtopoint <ipremote> up	directe verbinding met ander systeem
dynamic	dynamische verbinding		dhcp

voorbeeld instellen van ip-nummer op netwerkkaart eth0:

```
ifconfig eth0 10.1.1.1 broadcast 10.1.1.255 netmask 255.255.255.0 up
```

toevoegen nieuwe alias op netwerkkaart:

```
ifconfig eth0:2 192.168.6.3
```

Controle alle actieve en inactieve interfaces:

```
ifconfig -a
```

instellen ander subnetmask

```
ifconfig eth0:2 netmask 192.0.0.0
```

## **Netstat**

Vergaren van informatie over de actuele situatie:

netstat -i

## **Actieve netwerkverbindingen**

netstat -u(udp) of -t (tcp)

Overzicht routetabel:

netstat -r

## **Iptraf:**

menu-georiënteerd programma om te achterhalen welke:

- netwerk-interfaces gebruikt worden
- welke poorten gebruikt worden
- hoeveel pakketen verstuurd en ontvangen

Hij verzameld pas gegevens op het moment dat het geactiveerd wordt.

## **Routes:**

afbeelden van routetabel middels:

route

toevoegen van een route middels:

route add 196.168.13.0 eth0

toevoegen default route:

route add default ippp0

## **Forwarding:**

status opvragen met:

cat /proc/sys/net/ipv4/ip\_forward (indien 1 dan staat het aan, indien 0 dan staat het uit)

## **DNS:**

2 delen

### **Client:**

clientdeel ook wel resolver genoemd, configuratie via /etc/host.conf en /etc/resolv.conf

in etc/host.conf staat zoekvolgorde bv. Order hosts bind , hier wordt eerst in de hostfile gekeken en hierna in de dns. Bij gebruik DNS wordt DNS resolver gebruikt.

### **NIS:**

Network Information System, niet alleen een DNS mee op te zetten maar ook centraal gegevens administreren (bv. /etc/passwd)

## **Server:**

De DNS server (named, name server daemon, bind)beantwoordt vragen die het van DNS resolvers krijgt. De configuratie bestaat vaak uit 2 tabellen per domein: 1 voor opzoeken ip-adres naar naam en 2 voor opzoeken van naam bij ip-adres. Men kan ook een dns server zo configureren dat er zelf geen tabellen heeft maar alleen zoekopdrachten doorstuurt en het antwoord bewaard. Dit zijn caching only DNS servers. Let op ! Zodra een caching DNS server uit wordt gezet is zijn cache verdwenen, dit wordt nl. alleen in geheugen bewaard.

## **Commando's'**

hostname – naam van het systeem waarop wordt gewerkt

domainname: actuele NIS/YP domeinnaam op te vragen

dnsdomainname: domain waar het systeem onderdeel van is.

### **Systeemstart:**

De netwerkscripts staan in de directory /etc/rc.d of /boot/init.d.

In /etc/hostname staat de eigen hostname vermeld.

In /etc/hosts staat het bijbehorende ip-adres

Overige netwerken in /etc/networks, hierin ook het loopback interface.

### **Ip-verstrekking**

Printers met netwerkkaarten waarop geen ip-adres is in te stellen kunnen middels rarp, bootp en dhcp gebruikt worden.

### **RARP (Reverse Address Resolution Protocol)**

oudste methode en omgekeerde van ARP.

Toevoegen entry:

```
rarp -s printer 00:30:65:3d:3c:75
```

Opvragen met:

```
rarp -a
```

### **BOOTP**

werkt met een tabel, het /etc/bootptab bestand.

Hierin lijst met MAC adressen met ip-nummer

Tevens mogelijk: ip-adressen van DNS servers, subnetmasker, gateway  
bij toevoegen wel mac adres benodigd.

### **DHCP (Dynamic Host Control Protocol)**

pool van ipadressen met een leasetime

voordeel: geen MAC adressen te noteren.

Nadeel: geen vast ip-adres per mac adres

soms wel handig, denk aan printer

Gelukkig kunnen sommige dhcp daemons tevens bootp server zijn.

Maakt gebruik van /etc/dhcpd.conf

Hierin ook mogelijk om fixed ip adressen op te geven.

```
bv. host fantasia {  
    hardware ethernet 08:00:07:26:c0:a5;  
    fixed-address printer.bedrijf.nl;  
}
```

De host met dit MAC adres krijgt deze hostname en het ip-adres wordt via de resolver (DNS) achterhaalt. Let op ! Dan dient deze uiteraard wel in DNS zijn opgenomen of via /etc/hosts.

---

---

Netwerk-utilities:

### **Etherreal:**

Start Etherreal > Capture > Start

Selecteer de juiste(aangesloten netwerkkaart) eth0/eth1

zie bijvoorbeeld bij een ping dat er eerst een arp request komt waarna er icmp pakketjes worden gezonden.

Opmerkingen:  
Grafisch te starten.

Oordeel:  
Zeer uitgebreide tool en heel overzichtelijk.

### **Iptraf:**

Opmerking:  
x11 interface / Alleen TCP/UDP/ARP/RARP

Oordeel:  
Als er niets anders is wel aardig maar zeer beperkt en niet handig in het gebruik.

### **mtr:**

Opmerking:  
command based / combinatie van traceroute en ping

Oordeel:  
erg mager

### **netcat:**

Opmerking:  
Hiermee kun je zelf TCP en UDP pakketje maken en verzenden over je netwerk.  
bv. netcat 192.168.6.156 21 (via etherreal kun je zien dat hij wil connecten over FTP)

Oordeel:  
Heel handig maar wel voor cracks (wil je er veel mee doen)

### **ntop:**

Opmerking:  
command based / Ik kreeg het na een reboot pas aan de praat.  
Beperkte mogelijkheden.

(let op ntop -A -u wwwrun draaien was de melding na installatie, niet gedaan, en het draaide toch)

### **traffic-vis:**

Opmerking:  
command based / network traffic analyzer  
man 8 traffic-vis opvragen  
te starten met traffic-collector  
en dumpfile te vinden in /var/log/traffic-collector

Oordeel:  
weinig voorbeelden, onduidelijk  
niet voor beginners

### **ethtool:**

syntax: ethtool eth0  
Hiermee kun je je netwerksettings aanpassen bv. Speed 100Mb/s, Wake-on:g

### **nessus:**

Opmerking:  
Grafische portscanner en absoluut een aanrader.

Oordeel:  
zeer handige tool

Bron:

Plaatjes: <http://www.dmccormick.org/tcpip.htm>