# Computernetwerken?

## Uitwisselen informatie:

Er is een gemeenschappelijke fysieke verbinding

Meerdere computers gebruiken t.z.t. die gemeenschappeijlke verbinding

Computers kunnen rechtstreeks informatie met elkaar uitwisselen

## Computernetwerken:

Gemeenschappelijk medium

Computers kunnen rechtstreeks met elkaar uitwisselen

## Componenten:

Nodes met de nodige aansluitingen (computers)

Medium, kabels

Softwaar of programmatuur

## Soorten netwerken:

LAN: local area network

MAN: Metropolitan area network

WAN: wide area network

PAN: wide area network

VLAN: virtual LAN

## Protocollen:

Een set van afspraken heet protocol.

Worden opgeslagen in programma’s.

Dient voor communicatie tussen pc’s

## Protocollagen:

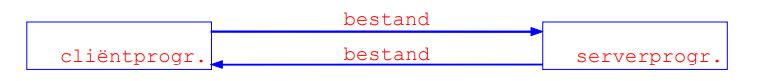
Een protocol bestaat uit vele lagen.

Voor goeie communicatie maken we gebruik van een toepassing laag (browser)

De fysieke laag is de hardware die dient voor de communicatie.

### Tussenlagen:

Dient voor de complexere communicatie.



## Vb. (bovenstaande):

Deelt “bericht” op in stukken

“Stuk” heet segment

Segmenten worden verstuurd naar een andere computer

Als er een fout gebeurt moet enkel het laatste “stuk” worden doorgestuurd en niet het hele bestand.

Meerdere communicaties “terzelfdertijd” mogelijk op 1 kabel.

## TCP/IP:

TCP/IP is een communicatieprotocol voor het netwerk.

## Afspraken:

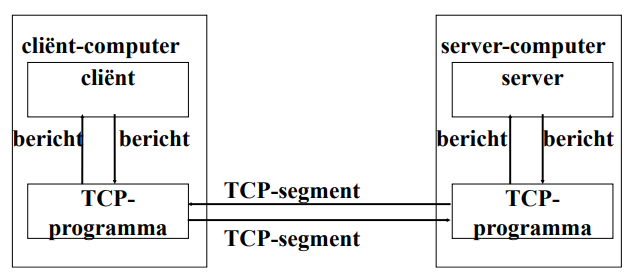
Elke computer heeft een uniek IP-adres.

Computer wordt aangesproken met IP-adres in combinatei met het poortnummer.

### Meerdere lagen:

TCP/IP-protocolsuite

TCP/IP-protocolstapel



## TCP:

Programma op de client en server.

Deze communiceren met elkaar.

Een bericht opdeelt in meerdere segmenten als dat nodig is.

De TCP laag werkt *onder* de IP laag

## IP:

IP-programma stuurt pakketten naar elkaar.

Een segment mogelijk opdeelt in meerder IP-pakketten.

## OSI-referentiemodel TCP/IP

7.Toepassingslaag 5. Toepassing laag 4. Toepassing

6. Presentatie laag

5. Sessie laag

4. Transport laag 4. Transport laag 3. Transport

3. Netwerk laag 3. Internet laag 2. Internet

2. Datalink laag 2. Datalink laag \

1. Fysieke laag 1. Fysieke laag / 1. Network access

# IP:

Tussenlaag bij communicatie tussen pc en server.

Elk netwerk krijgt een uniek IP-adres

Elke computer i/h netwerk krijgt uniek IP-adres

Vroeger: klasse

A: 0… /8

B: 10… /16

C: 110…/24

Nu: expliciet

## IP-Adressen:

32 bits

4 groepen van 8 bits

11011010 01001101 00110111 0111111 /21

Wordt 218.77.55.127 /21

/21 duidt het sub net aan.

## IPv6:

## Unicast:

Is toegewezen aan een enkele IPv6 interface.

Een pakket dat gestuurd wordt naar een unicast adres wordt enkel ontvaangen door die ene interface

### Global Unicast:

Analoog aan publiek IPv4 adres

Routeerbaar

### Link-local:

Wordt gebruikt om met devices te communiceren op dezelfde link of subnet.

Niet routeerbaar

### Loopback

::1/128 wordt gebruikt om:

Ip te testen

Pakketten naar zichzelf te zenden.

Kan niet aan een interface verbonden worden.

### Unspecified Address:

::/128

Kan niet aan een interface gegeven worden

Wordt alleen als bron gebruikt

### Unique Local

Analoog een private IPv4 adressen

In range van FC00::/7 tot FDFF::/7

Verplicht! Voor elk IPv6 address.

Begint met FE80::/10, eerste 10 bits zijn 1111 1110 10xx xxxx

Als jij zelf geen geeft maakt device er zelf een

Prefix lengte /64 (dit is niet nodig).

## EUI-64 proces:

Gebruik client zijn 484-bit Ethernet MAC adres

Plaats 16 bits in het midden van 48-bit Mac adres, maar de 7de bit wordt geflipt

Creert een 64-bit interface ID.

## EUI-64 Interface ID:

24-bit OUI van client MAC adres, maar de 7de bit wordt geflipt

Inserted 16-bit value FFFE.

24-bit device identifier van client MAC adres.

ICANN: nonprofitorganisatie die een aantal internet-gerelateerde taken uitvoert.

RIR: internationale organisatie die de toewijzing en registratie van internet nummers overziet.

## Global unicast address:

Uitgedeeld met eerste drie bits 001 of 2000::/3

Bestaat uit drie delen:

Global Routing Prefix

Subnet ID

Interface ID

Global Routing Prefix: dit is de prefix toegewezen door de ISP

Momenteel geven ISP’s een /48 global routing prefix aan klanten.

### SLAAC:

Stateless Address Autoconfiguration

Device verkrijgt prefix /64 van router

# Role of transport layer:

Temporary communication session between two applications

TCP/IP uses two protocols to achieve this:

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

Resposibilities:

Tracking the individual communication between applications on the source and destination hosts.

Segementing data for manageability and reassembling segmented data into streams of application data at the destination

Tracking individual conversations

Segmenting the data:

enables different communications,

provides the means to both send and receive data

Header added to each sement to identify it.

Reassemble segments

Identify the applications

### TCP:

Provides reliable delivery ensuring that all of the data arrives at the destination

Uses acknowledged delivery and other processes to ensure delivery

Makes larger demands on the network.

### UDP:

Provides just the basic functions for delivery – no reliability

Less overhead

### TCP of UDP:

There is a trade-off between the value of reliability and the burden it places on the network

Depends on the requirements of their application.

## TCP:

TCP transport is reliable because it supports packet delivery confirmation.

Three basic operations make this possible:

* Numbering and tracking data segments
* Acknowledging received data
* Retransmitting any unacknowledged data after a certain period of time

## UDP:

Some applications do not require that level of reliability

Adding overhead to ensure reliability for some application.

If reliability is not a factor UDP is a better protocol

## Which one is better?

### TCP:

application whose must be in specific order, if file needs to be in one whole file.

Examples: Databases, Web browsers, email clients.

### UDP:

Is a better choice for applications that can tolerate some data loss during transmission, but delays are unacceptable.

Examples: Live audio streaming, live video streaming, voice over IP (VoIP)

## TCP Features:

Establishing a session

Reliable delivery

Same-Order Delivery

Flow control

## Header:

20 bytes header.

## UDP Features:

No ordered Data Reconstruction

Connectionless

Unreliable Delivery

No flow control

## Header:

UDP is a stateless protocol.

8 bytes header.

## Multiple Separate Conversations.

Transport layer separates multiple communications

Different applications are sending and receiving.

Unique identifiers: port numbers.

### Port Numbers:

Source port:

* Source port number wordt dynamisch gekozen.
* An HTTP client is tracked trough the source port.

Destination Port:

* Used to identify an application
* A server can offer more than one service trough different ports

## Socket Pairs:

The combination of IP + port = socket.

Two sockets = socket pair.

Sockets enable multiple processes.

The source port is the return number.

It is the transport layer’s job to keep track of the sockets.

## Port Number Groups:

IANA: The Internet Assigned Numbers Authority, body responsible for assigning.

## The netstat command:

Unsecured TCP is a major security threat

Netstat is a network utility that can be used to verify active connections.

By default, the netstat command will resolve IP addresses to domain names

The -n option can be used to display IP addresses and port numbers.

## TCP server processes:

Each application process uses port

An individual server cannot have two services asasigned to the same port number

Port active = in use by application = anything accepted.

### Connection Establishemen

1. Client requests a client-to-server communication.
2. The server acknowledges the communication.
3. The client acknowledges the communication.

### Session termination:

1. Client sends a segment with the FIN flag set.
2. The server sends and ACK(acknowledge) flag.
3. The server sends FIN flag to the client.
4. The client responds with ACK flag.
5. when everything has been acknowledged, the session is closed.

### Three-way handshake

Establishes that the destination device is present

Verifies that the destination device has an active service and is accepting requests.

Informs the destination device that eh intends to establish a communication.

### Reliability

TCP segments use sequence numbers to identify

An initial sequence number (ISN) is random and is increment by the number of transmitted bytes.

TCP process buffers until completed

Segments received out of order are held

The data is delivered to the application layer when completed.

Window size: the amount of data before the acknowledgment must be received.

### Flow control:

Adjusts the rate of data flow.

Relies on header, called window size.

Endpoints can adjust the window size.

### Congestion avoidance:

Results in discarded packets.

Undelivered TCP segments triggers re-transmission.

The source can estimate a certain level of network congestion.

The source can reduce the number of bytes.

The source reduces the number of unacknowledged bytes

The destination is usually unaware of the network.

## UDP:

Provides the basic.

Lower overhead.

Practically no reliability.

### Initiation:

By client, selects a port

## TCP-examples:

Handles all transport layer related tasks

## UDP-examples:

Live video and multimedia applications

Simple requests and reply applications

Applications that handle reliability