Informatica Instituut, Faculteit Wiskunde en Informatica, UU.
In elektronische vorm beschikbaar gemaakt door de TBC van A−Eskwadraat.
Het college INFONW werd in 2004/2005 gegeven door Piet van Oostrum.

# Uitwerking[1] Netwerken, toets 3 (INFONW) 31 januari 2005

N.B. Dit zijn de open vragen, die 60% van het cijfer voor dit tentamen bepalen.

## Opgave 1

a) Wat is het voordeel van hiërarchische routering (padbepaling)?

b) Hoe wordt hiërarchische routering in het Internet gebruikt?

**Antwoorden:**

a) Hiërarchische padbepaling wordt gebruikt als een netwerk groot is. De routeringstabellen in de routers worden dan te groot en er moet teveel data wordenuitgewisseld. Door een hiërarchie te gebruiken wordt dit beperkt. Bovendien kunnen delen van de hiërarchie zelfstandig hun routering bepalen.

b) In het Internet wordt hiërarchische routering gebruikt doordat het in autonome systemen is opgedeeld. Bovendien kan in OSPF een autonoom systeem weer in areas worden ingedeeld. N.B. Hiërarchische routering heeft niets te maken met de DNS structuur.

## Opgave 2

Wanneer een computer (bijvoorbeeld een laptop) voor het eerst in een netwerk (Ethernet) komt, heeft hij nog geen IP-adres. Ook kent hij niet de MAC-adressen van andere computers op het netwerk.

a) Hoe komt de computer aan zijn IP-adres als het niet handmatig ingevoerd wordt? Leg ook uit hoe dit werkt.

b) Waar heeft de computer de MAC-adressen van andere computers op het netwerk voor nodig?

c) Hoe komt de computer aan het MAC-adres van een andere computer op het netwerk?

**Antwoorden:**

a) De computer krijgt meestal een IP-adres via DHCP. De computer stuurt een DHCP discoverbericht. Een DHCP-server biedt zijn dienst aan (ook met een broadcast IP-adres). Daarna zendt de computer een DHCP verzoek en de DHCP server stuurt een ACK. Alle berichten hebben het broadcast IP-adres als bestemmingsadres.

b) Het MAC-adres is nodig omdat dit in de frames gezet moet worden die naar andere computers op het netwerk gestuurd worden.

c) Hiervoor wordt het ARP-protocol gebruikt. De computer stuurt een ARP pakket uit met het broadcast MAC-adres, dat het gevraagde IP-adres bevat. De computer die dit IP-adres heeft, stuurt een antwoord terug. (Computers kunnen ook langskomende pakketten in de gaten houden en daar de relatie tussen IP-adres en MAC-adres uitvissen.

[1] Deze uitwerkingen zijn met de grootste zorg gemaakt. In geval van fouten kan de TBC niet verantwoordelijk worden gesteld, maar wordt zij wel graag op de hoogte gesteld: `tbc@A-Eskwadraat.nl`

## Opgave 3

Bekijk de gemiddelde vertraging die een frame oploopt bij zuiver Aloha en slotted Aloha als het netwerk een lage belasting heeft. Welke is kleiner? Leg ook uit waarom.

**Antwoord:**
Bij lage belasting spelen botsingen nauwelijks een rol. De voornaamste vertraging bij slotted Aloha is dan het wachten tot het begin van een slot (gemiddeld een halve slot-tijd). Bij zuiver Aloha hoeft dat niet, daar kan onmiddellijk met zenden worden begonnen. De gemiddelde vertraging bij zuiver Aloha is dus kleiner.
N.B. Vertraging is iets anders dan efficiëntie. Bij slotted Aloha is (bij grote belasting) de efficiëntie groter. Vergelijk het met het OV: de trein is efficiënter dan de auto bij het vervoeren van grote hoeveelheden mensen, maar de auto heeft een kleinere vertraging wanneer het niet druk is. Je kunt direct gaan rijden in plaats van wachten op de volgende trein.

## Opgave 4

Bij het afspelen van een audio-stream worden voor 3 achtereenvolgende pakketten de volgende end-to-end netwerkvertragingen gemeten: 10,50,20 msec.

a) Waar komen deze getallen vandaan?

b) Bereken het voortschrijdend gemiddelde $d_i$, de geschatte gemiddelde afwijking $v_i$ voor $i = 1, 2, 3$, en de afspeelvertraging die hieruit volgt. Neem $d_0 = v_0 = 0, u = 0.25, K = 4$. Geef de berekeningen duidelijk aan.

c) Wanneer kan de berekende afspeelvertraging gebruikt worden?

**Antwoord:**

a) De getallen worden berekend als het verschil van de aankomsttijd en de timestamp van het pakket $(r_i - t_i)$.

b) $d_i = (1 - u)d_{i-1} + u(r_i - t_i)$
$v_i = (1 - u)v_{i-1} + u|r_i - t_i - d_i|$
$d_0 = 0$
$d_1 = 0.75 \times 0 + 0.25 \times 10 = 2.5$
$d_2 = 0.75 \times 2.5 + 0.25 \times 50 = 14.375$
$d_3 = 0.75 \times 14.375 + 0.25 \times 20 = 15.781$
$v_0 = 0$
$v_1 = 0.75 \times 0 + 0.25 \times |10 - 2.5| = 1.875$
$v_2 = 0.75 \times 1.875 + 0.25 \times |50 - 14.375| = 10.312$
$v_3 = 0.75 \times 10.312 + 0.25 \times |20 = 15.781| = 8.789$
afspeelvertraging $= d_3 + Kv_3 = 15.781 + 4 \times 8.789 = 50.938$ msec.

c) De afspeelvertraging kan gebruikt worden na de eerstvolgende stilte. Een aaneengesloten serie pakketten moet met dezelfde afspeelvertraging afgespeeld worden, anders krijg je jitter. Daarom is de berekende afspeelvertraging bij het eerste pakket na een stilte bepalend voor de hele serie.

## Opgave 5

Stel: we hebben een gigabit (1 Gb/s) verbinding die een token-emmer-algoritme (in het boek 'leaky bucket' genoemd) gebruikt met een gemiddelde snelheid van 256 kbit/s (=0.25 Mbit/s) en een tokenvolume van 1 megabyte. We sturen over deze verbinding een videostroom met een gemiddelde snelheid van 700 kbit/s.

a) Als we beginnen met een volle token-emmer, hoe lang kan de stroom dan op 700 kbit/s gehouden worden?

b) Hoe groot moet de bucket zijn om een filmpje van 1 minuut af te spelen?

**Antwoord:**

a) De gemiddelde snelheid is gelijk aan de snelheid waarmee de bucket met tokens gevuld wordt. Wanneer deze snelheid $r$ is en de bucketgrootte $b$ dan kan in tijd $t$ beginnend met een volle bucket in totaal verstuurd worden $rt + b$. Als $s$ de snelheid van de datastroom is, dan hebben we nodig $st$. De tijd waarin we de datastroom kunnen volhouden wordt dan bepaald door $st = rt + b$ ofwel $t = \frac{b}{s-r}$. In dit voorbeeld is (als we kbit als eenheid nemen) $s = 700, r = 256$ en $b = 8388$ (1 megabyte = 8388 kbit). Dus $t = \frac{8388}{700-256} = 18.893$ sec. (Je kunt het ook zo zeggen: je hebt 700 kb/s nodig, de token bucket geeft 256 kb/s, dus je komt 444 kb/s tekort. De bucket kan dat 8388/444 sec. volhouden.

b) Omgekeerd: voor 1 minuut = 60 sec. heb je $60 \cdot 444$ kbits $= 26640$ kbits $= 3.176$ megabyte nodig.

N.B. Ik heb mega $= 1024^2$ genomen. Je mag ook mega $= 10^6$ nemen, dan worden de getallen een klein beetje anders.

## Opgave 6

SSL (TLS) en IPSec zijn twee verschillende manieren om beveiliging op Internetverbindingen te realiseren. Ze worden echter heel verschillend toegepast. Beschrijf voor elk van deze protocollen een situatie waarin deze de voorkeur verdient boven de andere en leg duidelijk uit waarom dit zo is. Gebruik bij deze uitleg ook de manier waarop hun werking verschilt.

**Antwoord:**
SSL wordt gebruikt tussen de applicatielaag en de transportlaag (als een soort opgevoerd TCP). Het moet specifiek in de applicaties ingebouwd worden. Het functioneert goed bij één specifieke TCP-verbinding. Dus bijvoorbeeld voor e-commerce of internetbankieren.
IPSec functioneert in de netwerklaag en vereist dus aangepaste routers of een aanpassing in het OS. Dit kan dus niet zomaar gebruikt worden voor de communicatie tussen twee willekeurige computers. Als het aanwezig is, wordt wel al het Internetverkeer beveiligd zonder aanpassing van de applicaties. Dus is het geschikt voor bijvoorbeeld telewerken of VPN's.

## Opgave 7

Leg uit waarom bij de encryptie van e-mailboodschappen (bijvoorbeeld met PGP) de voorkeur gegeven wordt aan een combinatie van symmetrische en public-key cryptografische algoritmen in plaats van simpelweg één van de twee.

**Antwoord:**
Symmetrische cryptografie heeft het probleem van sleuteldistributie, maar is snel. Asymmetrische cryptografie heeft geen probleem met de sleuteldistributie, maar is langzaam. Door ze te combineren, kun je de inhoud van een e-mail versleutelen met een symmetrische sessiesleutel, en deze sessiesleutel met een publieke sleutel. Omdat de sessiesleutel klein is, is dit toch relatief snel en combineer je de voordelen van beide methodes.

N.B. Dit zijn de meerkeuzevragen, die 40% van het cijfer bepalen.
N.B. De antwoorden op de volgende vragen zijn telkens **vet** gedrukt.

1. Routering in het Internet vindt plaats in de

   a) datalink laag

   b) **netwerk (internet) laag**

   c) transport laag

   d) applicatie laag

2. Een organisatie wil een blok IP-adressen hebben voor ca. 3000 computers. Ze krijgen een CIDR blok. Welk blok is geschikt?

a) 200.37.175.0/20

b) 210.50.175.0/21

c) **215.83.176.0/20**

d) 220.21.176.0/21

3. Wat is het voordeel van CSMA/CD boven zuiver Aloha?

   a) Stations moeten op vaste tijdstippen (slots) met zenden beginnen

   b) Een station moet eerst toestemming krijgen voor het mag zenden

   c) **Zendende stations controleren of een ander station ook aan het zenden is**

   d) Twee stations kunnen nooit op hetzelfde tijdstip beginnen met zenden

4. Twee CDMA-stations zenden elk een bit uit. A heeft code $(-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$ en B heeft $(-1\ -1\ +1\ -1\ +1\ +1\ +1\ -1)$. Een ontvanger ontvangt het sugnaal $(0\ 0\ -2\ +2\ 0\ -2\ 0\ +2\ )$. Welke bits hebben A en B uitgezonden?

   a) A een 0 en B een 0

   b) A een 0 en B een 1

   c) **A een 1 en B een 0**

   d) A een 1 en B een 1

5. Als in IP versie 4 een door een router ontvangen IP pakket te groot is voor de framegrootte van de datalink laag aan de uitgang van de router, wat doet deze router dan in het algemeen?

   a) De router zendt een ICMP bericht naar de afzender om zijn beklag te doen

   b) De router splitst het grote IP-pakket op in groepjes bytes die elk afzonderlijk wel passen in een frame.

   c) De router gooit het IP pakket weg zonder iets te melden

   d) **De router maakt van het grote IP pakket meerdere kleine IP pakketten die elk afzonderlijk wel passen in een frame.**

6. Als in IP versie 6 een door een router ontvangen IP pakket te groot is voor de framegrootte van de datalink laag aan de uitgang van de router, wat doet deze router dan in het algemeen?

   a) **De router zendt een ICMP bericht naar de afzender om zijn beklag te doen**

   b) De router splitst het grote IP-pakket op in groepjes bytes die elk afzonderlijk wel passen in een frame.

   c) De router gooit het IP pakket weg zonder iets te melden

   d) De router maakt van het grote IP pakket meerdere kleine IP pakketten die elk afzonderlijk wel passen in een frame.

7. Waardoor ontstaat bij het telefoneren over het Internet jitter meestal?

   a) digitaliseren van het geluid

   b) congestion control

   c) error correctie

   d) **queueing delays**

8. Een RTP pakket wordt met UDP verstuurd. In welke volgorde staan de headers in het frame?

   a) RTP IP UDP

b) RTP UDP IP

c) **IP UDP RTP**

d) IP RTP UDP

9. Wat is het essentiële verschil tussen cryptografie met symmetrische en met openbare sleutels?

a) Bij symmetrisch gebruik je dezelfde algoritme voor versleutelen en ontsleutelen

b) **Bij symmetrisch gebruik je dezelfde sleutel voor versleutelen en ontsleutelen**

c) Bij openbare hoef je geen sleutels geheim te houden

d) Bij openbare kun je sleutels zonder problemen via e-mail uitwisselen.