1 Klassiek lagenmodel vs. TCP/IP

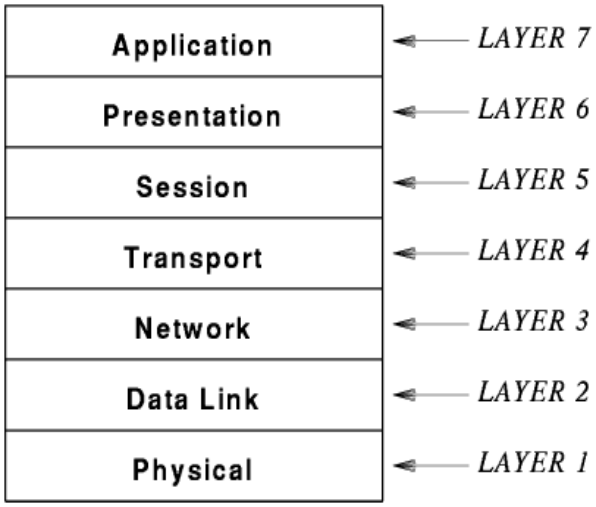
1.1 Inleiding

Om alle netwerkhardware met elkaar te laten communiceren zijn er communicatieprotocollen nodig. Deze verzameling afspraken zorgt ervoor dat we samen met de hardware een krachtig communicatiesysteem verkrijgen.
In dit hoofdstuk zullen we het klassiek lagenmodel bespreken en dit vervolgens toetsen aan het alom gebruikte TCP/IP-protocol.

1.2 Het 7 lagen OSI model

1.2.1 Situering

Een degelijk communicatiemodel is moeilijk in één grote bundel te vatten. Daarom maakt men gebruik van een protocolsuite, een groep kleinere protocollen die samen één geheel vormen.
Deze onderverdeling gebeurt via het *lagenmodel*. Een protocol-suite bestaat uit een verzameling van protocollen die overeen-komen met elk één van de lagen.
Zo werd voor de eerste netwerken door de *International Organization for Standardization (ISO)* een *7-layer Reference Model* gedefinieerd, ook wel het OSI-model genoemd.



Het werken met lagen was vooral bedoeld om makkelijker te werken en vooral om problemen sneller op te sporen en op te lossen.

1.2.2 De zeven lagen

1.2.2.1 Laag 1: Fysiek

Laag 1 komt overeen met de elementaire netwerkhardware. Deze geeft de gedetailleerde specificatie van de LAN-hardware. We hebben het hier over de netwerkbekabeling en de bijhorende specificaties (spanning, lichtpulsen, enz...)

1.2.2.2 Laag 2: Datalink

De protocollen van Laag 2 geven aan hoe data in frames moet worden geordend en hoe frames over een netwerk moeten worden verstuurd.

1.2.2.3 Laag 3: Netwerk

De protocollen voor Laag 3 bepalen hoe adressen worden toegekend en pakketten over het netwerk moeten worden verstuurd.

1.2.2.4 Laag 4: Transport

In Laag 4 vinden we de protocollen die een betrouwbare overdracht van data verzorgen. Deze protocollen behoren tot de meest complexe.

1.2.2.5 Laag 5: Sessie

Deze laag bevat de protocollen die aangeven hoe u een communicatiesessie met ander systeem tot stand brengt. Ook vindt u er de specificaties voor beveiligingsdetails als verificatie via wachtwoorden.

1.2.2.6 Laag 6: Presentatie

Hier zijn protocollen aanwezig die bepalen hoe data wordt weergegeven, dat is nodig omdat verschillende computermerken integers en tekens intern verschillend aanbieden. De protocollen van Laag 6 zorgen voor de onderlinge vertalingen van de representaties op de verschillende computers. Hier denken we vooral aan verweking van formaten zoals bijv. jpg, mp3, mpeg, enz...

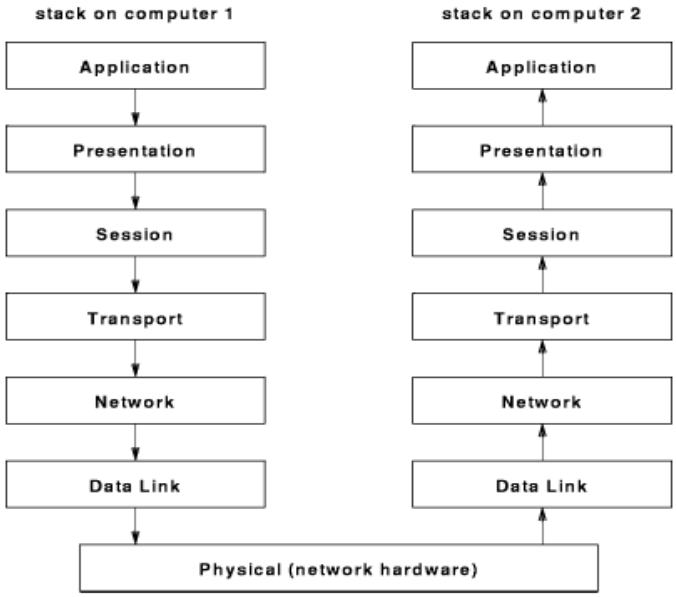
1.2.2.7 Laag 7: Applicatie

Elk protocol van Laag 7 specificeert hoe een bepaalde applicatie het netwerk gebruikt. Zo hoort bijvoorbeeld de specificatie voor een applicatie die bestanden tussen computers uitwisselt, in Laag 7. Het protocol geeft de details voor de manier waarop een applicatieprogramma op een computer een aanvraag doet (hoe

de naam van het gewenste bestand moet worden aangegeven) en hoe de applicatie op een andere computer antwoordt.

1.2.3 Stacks: gelaagde software

Protocollen die ontworpen zijn naar een gelaagd model zijn zo ontworpen dat ze steeds de gelaagde orde volgen. Voor elke laag is er een module. En elke module kan alleen corresponderen met de bovenliggende of onderliggende module (afhankelijk van verzenden of ontvangen).



De software bundel die een gehele suite van protocollen kan bevatten noemt men meestal een stack

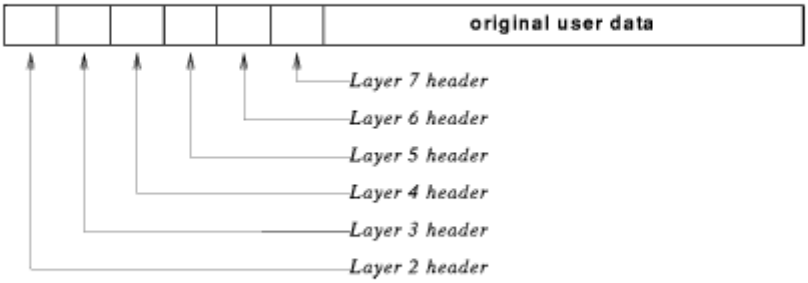
Er bestaan verschillende commerciële stacks. Deze zijn onafhankelijk van elkaar ontworpen en kunnen daarom niet onderling samenwerken.

Een aantal commerciële stacks die veel gebruikt worden zijn:

- Netware Novell Corporation
- AppleTalk Apple Computer Corporation
- DECNET Digital Equipment Corporation
- TCP/IP diverse

1.2.4 Werking gelaagde software

De werking van het gelaagde netwerk model rust op het toevoegen van extra informatie per laag die doorlopen wordt.
Dit tijdens het zenden.
Bij de ontvanger wordt er laag per laag de extra info verwijderd om zo terug de oorspronkelijke data te verkrijgen.
Vertrekkend van een datapakket wordt er al het ware een treintje gevormd met extra info vooraan, headers.
Omdat elke laag een header toevoegt spreken we over geneste headers.



1.2.5 Sequencing: pakketvolgorde en duplicatie voorkomen

Op verbindingloze netwerken kunnen de routes die de pakketten volgen, veranderen. Hierdoor kunnen de pakketten in een andere volgorde toekomen.
Hiervoor wordt er *sequencing* toegepast. Dit houdt in dat elk pakket van de afzender een volgnummer krijgt.

Sequencing wordt ook gebruikt om duplicatie te vermijden. Een slechtwerkend toestel binnen een CSMA/CD (Carrier Sense, Multiple Access/ Collision Detection) netwerk kan voor duplicatie zorgen. De ontvanger zal hier een geldige zending constateren terwijl de zender een botsing zal detecteren. De zender zal vervolgens nog eens zenden.

1.2.6 Pakketverlies

In computernetwerken gaan regelmatig pakketten verloren, ze komen nooit aan of geraken zodanig corrupt dat de ontvanger ze weggooit.

Hiervoor werd de hertransmissie in het leven geroepen.
Als een pakket geen positieve bevestiging krijgt van de ontvanger dan zal de zender dit pakket opnieuw versturen.
Deze bevestiging noemt men een acknowledgement of ACK.
Om overbelasting van het netwerk ten gevolge van hertransmissie te voorkomen, is er een maximaal aantal hertransmissies voorzien.

1.2.7 Stroomregeling tegen data-overloop

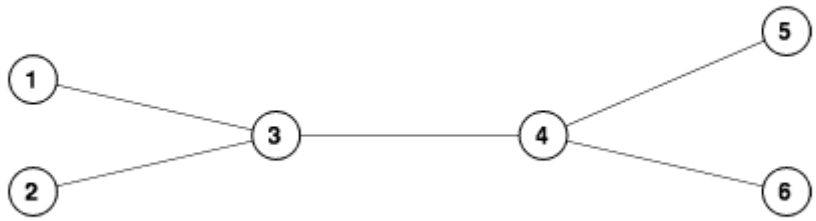
Tijdens datacommunicatie kunnen snelheidsverschillen tussen zender en ontvanger ontstaan. Als de zender te snel verstuurd kan er zich daardoor een *data overrun* voordoen.

Een eerste techniek om data-overloop tegen te gaan is de *stop-and-go* techniek. Hier verstuurd de zender telkens 1 pakket en wacht op een bevestiging om pas daarna het volgende pakket te versturen.
Dit systeem is heel fail-proof maar kampt met een groot verlies van bandbreedte tijdens het wachten.

Om een beter throughput te verkrijgen gebruiken moderne protocollen de *sliding window* technologie.
Hier wordt niet pakket per pakket verstuurd maar een veelvoud. Bijvoorbeeld vier pakketten direct na elkaar. Terwijl er per pakket een bevestiging komt schuift het venster verder, maar de volgende vier pakketten worden pas verzonden nadat de vorige allen bevestigd werden.

Zie ook http://www3.rad.com/networks/2004/sliding_window/

1.2.8 Mechanismen om netwerkcongestie te vermijden



Stel dat in bovenstaande figuur elk cijfer een netwerk voorstelt.
Zolang de toestellen in 1, 2 en 3 enerzijds en 4, 5 en 6 anderzijds onderling communiceren zullen er zich weinig of geen snelheidsproblemen voordoen.
Stel: er ontstaat veel communicatie tussen een toestel van netwerk 2 en een toestel van netwerk 5, en daarenboven nog eens intensive communicatie tussen toestellen van net 1 en net 6 enz... Al deze datatransfer loopt over de verbinding tussen netwerk 3 en 4.
Als er een bepaald moment meer pakketten aangeboden worden dan dat er verstuurd kunnen worden, spreken we van een *congestie*, een verstopping.
Als de congestie aanhoudt een pakketschakkeling geheugengebrek krijgen en pakketten weggooien. De verzender krijgt dus geen ACK en stuurt een kopie waardoor nog meer data door verbinding 3-4 moet. Nu wordt het netwerk zo goed als onbruikbaar en spreekt men over een *congestion-collaps*.

Er zijn twee benaderingen om een congestioncollaps tegen te gaan.
Een eerste oplossing speelt zich af in om het knooppunt dat verbonden is met de probleemverbinding. Van hieruit wordt ofwel een speciaal bericht naar de zender gestuurd of wordt er in de pakketheader een bit ingesteld zodat de ontvanger de bron kan verwittigen.
De tweede benadering houdt in dat pakketverlies wijst op congestie. Moderne netwerken zijn zo storingvrij dat pakketverlies meestal een gevolg van congestie is. Daarom gaat de zender ervan uit dat alle verlies het gevolg is van een congestie. Hierop zal de zender reageren door de zendfrequentie te verlagen.

Dit wordt geregeld door een frequentiecontrolemechanisme dat in sommige protocollen aanwezig is. Ook het verkleinen van de venstergrootte zorgt bij sliding-window-protocollen voor een vermindering van aantal verzonden pakketten.

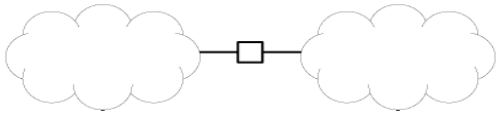
1.3 TCP/IP

1.3.1 Inleiding

Netwerktopologieën zijn meestal ontwikkeld voor een specifieke vereisten. Bijvoorbeeld een netwerk dat over kleine afstanden hoge snelheden haalt. Ook voor grote netwerken zoals een WAN bestaan er specifieke protocollen.
Daarom kan men zeggen dat er geen netwerktechnologie bestaat die volledige voldoet aan alle eisen voor alle soorten netwerken.
Vroeger bestond er geen mogelijkheid om netwerken aan elkaar te koppelen. Hierdoor moesten gebruikers steeds wisselen van werkstation als ze een bepaald netwerk nodig hadden voor een specifieke taak.
Deze dure werkmethode, duur wegens onproductief en veel dure hardware, zorgde voor een zoektocht naar een universeel systeem dat meerdere netwerken kan koppelen.
Uit deze zoektocht is het gegeven van ***internetwerken*** ontstaan. Men is erin geslaagd om meerder netwerken te verbinden tot 1 groot netwerk. Hierdoor kan elk werkstation vanuit elk aangesloten netwerk informatie versturen naar elk ander werkstation, zelfs al is de bestemmeling aangesloten in een ander netwerk.

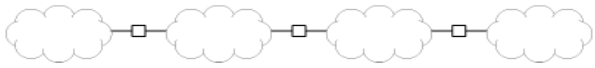
1.3.2 Fysieke verbinding van netwerken via routers

Als je verschillende soorten netwerken aan elkaar wil koppelen moet je gebruik maken van een *router.* Een router is een computer met als enige taak, netwerken verbinden. In deze computer zit een processor, geheugen, een netwekinterface per te verbinden netwerk.



Twee fysieke netwerken verbonden door een router.

Dankzij routers kan een organisatie die netwerktechnologie gebruiken die best past bij de toepassing. Deze routers zorgen ervoor dat alle netwerken verbonden worden.
Op deze manier wordt een *internet* gevormd.



Een internet, bestaand uit vier netwerken onderling verbonden door drie routers.

Routers kunnen, in tegenstelling tot bovenstaand schema, meer dan twee netwerkverbindingen hebben. Bovenstaand netwerk kan dus ook gevormd worden door één centrale router waaraan de vier netwerken gekoppeld worden.
Deze manier van werken wordt meestal vermeden. Daarvoor zijn twee redenen:

- Alle dataverkeer moet door de cpu en het geheugen van de router verwerkt worden. Een router het verkeer tussen een willekeurig aantal netwerken laten regelen zou een te zware belasting betekenen.
- Redundantie (= meer gebruiken dan eigenlijk nodig) verhoogt de bedrijfszekerheid van het internet. In de meeste protocolsuites zijn technieken aanwezig die het internetwerkverkeer controleren en bijsturen indien nodig.

1.3.3 Virtueel netwerk

Software ontwikkeld voor een internet geeft de gebruikers een beeld van één naadloos netwerk. Hierbij worden de details van fysieke netwerkverbindingen, fysieke adressen en routeringsinformatie verborgen. Gebruikers of toepassingssoftware merken niets van de onderliggende fysieke netwerken en de routers die ze verbinden.
We kunnen dus spreken over een virtueel netwerksysteem omdat het communicatiesysteem een abstractie is. Hiermee bedoelen we dat we niet tegenstaande de combinatie van hardware en software de illusie krijgen van een uniform netwerksysteem, dit systeem toch niet bestaat.

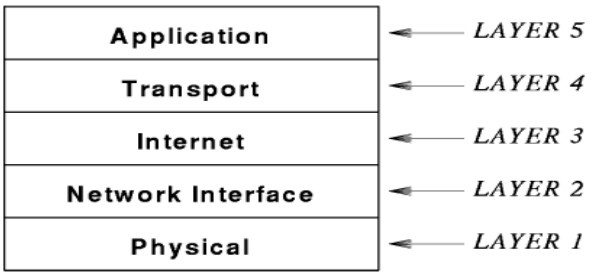
1.3.4 Ontstaan van de TCP/IP Protocolsuite.

Veel protocollen werden aangepast om te gebruiken voor een internet. Toch is het het eerste protocolset dat speciaal voor internet ontwikkeld werd het meest gebruikt. Dit is het *TCP/IP Internet Protocol* of kortweg het TCP/IP.
De ontwikkeling van TCP/IP gebeurde in de jaren 70 van de vorige eeuw. Hier was ARPA (*Advanced Research Projects Agency*) de voortrekker in het onderzoek. Gefinancierd door het Amerikaanse ministerie van Defensie.
Later, in de jaren tachtig, financierden de *National Science Foundation* en andere Amerikaanse ministeries de verdere ontwikkeling van TCP/IP en ook een groot internet om de protocollen te testen. Dit noemde men het ARPA-net, later zal dit uitgroeien tot het *World Wide Web*, het Internet.

Ondertussen is het TCP/IP protocol uitgegroeid tot het meest gebruikte protocol voor zowel netwerken van grote organisaties als kleine lan's van particulieren.

1.3.5 TCP/IP en het lagenmodel

Eerder bespraken we het 7-lagenmodel dat werd uitgewerkt voordat de internetwerken er waren. Hierdoor bevat het model geen specifieke laag voor internetprotocollen. Komt hier nog bij dat in het OSI-model er een volledige laag aan *session*-protocollen besteed wordt.
Heden ten dage is het een feit dat computersystemen zo goed als enkel nog bestaan uit gekoppelde privé werkstations en steeds minder grote computers met terminal schermen. Hierdoor wordt de sessielaag steeds minder belangrijk.
Het grootste gevolg is dat de TCP/IP ontwikkelaars een nieuw lagenmodel ontwikkelden.
Het TCP/IP-lagenmodel, ook wel het *Internet-lagenmodel* genoemd bevat vijf lagen. (zie onderstaand figuur)



Vier van deze lagen komen overeen met één of meer lagen van het OSI-model. Wat we niet terugvinden in het OSI-model is de ineternet-laag.

1.3.6 Overzicht van de TCP/IP-lagen

1.3.6.1 Laag 1: Fysieke laag

Laag 1 correspondeert met de elementaire netwerkhardware, net als laag 1 van het OSI-model

1.3.6.2 Laag 2: Netwerkinterface

Laag 2-protocollen geven aan hoe de data in frames moet worden ingedeeld en hoe een computer frames over het netwerk transporteert. Dit is vergelijkbaar met laag 2 van het OSI-model.

1.3.6.3 Laag 3: Internet

De protocollen in laag 3 bepalen het formaat van de paketten die via het internet worden verstuurd. Tevens geven ze aan welke mechanismen er worden gebruikt om de pakketten van een computer via één of meer routers naar een eindbestemming door te sturen. Hier vinden we concreet het IP gedeelte terug.

1.3.6.4 Laag 4: Transport

Net zoals in laag 4 van het OSI-model zorgen de protocollen hier voor een betrouwbare overdracht. Het TCP gedeelte is dan weer in deze laag terug te vinden.

1.3.6.5 Laag 5: Toepassing

Hier worden de referentielagen 6 en 7 uit het OSI-model samengevoegd. De hier actieve protocollen bepalen hoe een toepassing een internet gebruikt.

2 DHCP

2.1 Inleiding

De keuze van een protocolsuite legt een groot aantal details vast. Zo heb je het exacte pakketformaat, de header-grootte enz...
Toch zijn ook een aantal details variabel omdat deze per aangesloten toestel moeten verschillen. Bijvoorbeeld het IP-adres, subnet-masker, DNS-server-adres, enz...
De invulling van deze variabele details kunnen ofwel ingevuld worden door de installateur of automatisch via DHCP services.

2.2 Variabele instellingen via DHCP services

Bij gewone computersystemen maken meestal gebruik van het TCP/IP-protocol. Indien de netwerkinstellingen op automatisch staan, zal het in TCP/IP ingebouwde *Reverse Address Resolution Protocol (RARP)* ervoor zorgen dat de computer de juiste instellingen verkrijgt.
Eenvoudig uitgedrukt komt het erop neer dat de computer een RARP-aanvraag *(RARP-request)* uitstuurt en dat een server hierop reageert met een RARP-antwoord *(RARP-response)*
Tijdens zo'n rarp-aanvraag wordt het eigen IP op 0.0.0.0 gezet en vervolgens wordt de aanvraag *gebroadcast* over het volledige netwerk, m.a.w. Verstuurd naar 255.255.255.255 op poort 67.
Het antwoord van de DHCP server komt terug bij de aanvrager dankzij het feit dat bij de aanvraag ook het mac-adres meegestuurd wordt.

2.3 De TCP/IP invulling

De ontwerpers van het TCP/IP-protocol merkten al snel dat het theoretisch model dat uit verschillende stappen bestaat kon gecombineerd worden tot één stap, op voorwaarde dat de server in staat is meer dan één configuratie-item te geven.
Voor deze service werd het *BOOTstrap Protocol (BOOTP)* ontworpen.
Om configuratie-informatie te verkrijgen, stuurt de protocolsoftware een *BOOTP Request* broadcast-bericht. Een BOOTP-server die de aanvraagt ontvangt, plaatst de informatie in één *BOOTP Reply*-bericht en stuurt het antwoord terug naar de aanvragende computer. Zo kan een computer in één stap informatie ontvangen als het IP-adres, de naam en IP-adres van de server, router...

2.4 Dynamic Host Configuration Protocol

Om de configuratie te automatiseren werd DHCP ontwikkeld. In tegenstelling tot BOOTP heeft DHCP geen beheerder nodig. In plaats hiervan levert DHCP een mechanisme waarmee een computer zonder handmatige inmenging tot een nieuw netwerk kan bijtreden en een IP-adres kan krijgen. Men preekt hier ook over *plug-and-play netwerken*.
Een bijkomend pluspunt van DHCP is dat zowel computers die serversoftware als werkstations met clientsoftware bedient kunnen worden:

- Dankzij DHCP kan een pc met clientsoftware makkelijke naar een ander netwerk verplaatst worden zonder handmatige inmenging van een systeembeheerder.
- Computers die niet bedoeld zijn om mobiel te zijn en vooral servertaken draaien, kunnen een vast ip-adres krijgen via DHCP. Zo krijgen ze steeds hetzelfde ip-adres als de computer opnieuw opstart.

2.5 Hoe werkt DHCP?

Om beide bovenstaande typen computers van dienst te kunnen zijn, kan DHCP vrij schema hanteren. In plaats daarvan wordt een client/server-model gebruikt.
Als een computer start, wordt een *DHCP-request* gebroadcast waarop een server een *DHCP-Replay* terugstuurt.
Een DHCP-server kan bij het verwerken van aanvragen zowel overweg met vaste als variabele ip-adressen. Bij een aanvraag wordt een database geraadpleegd. Bevat deze een specifieke entry voor de computer, dan stuurt de server deze info terug. Als er geen info gevonden wordt kiest de server het volgende vrije IP-adres uit de pool en stuurt dit terug naar de aanvrager.

2.6 DHCP lease time

De opvraag toegekende adressen zijn in principe niet permanent. DHCP geeft voor een bepaalde periode een *lease* op het adres. Als deze lease afloopt, moet de computer met de DHCP-server onderhandelen over een verlenging van het gebruik. In principe zal DHCP een verlenging toestaan.

3 POP3-service van Windows 2003

3.1 Wat?

De POP3 service (Post Office Protocol) is een e-mail service die e-mail ontvangt. Om e-mail te kunnen verzenden moet je beschikken over een SMPT service (Simple Mail Transfer Protocol). Omdat de client de mail zou kunnen lezen, moet deze beschikken over een POP3 e-mail client software, zoals Outlook (Express).

Windows 2003 beschikt over een POP3 service. Hiermee kan je een lokale emailservice opzetten.

3.2 Oefeningen

3.2.1 Oefening 1: Installeren van de POP3 service

1. Installeer de POP3 service:
2. Open de console om onderdelen toe te voegen aan Windows.
3. Selecteer E-mail services. Merk op dat de SMTP-service automatisch wordt geïnstalleerd (als onderdeel van IIS)
4. Zorg ervoor dat de service iedere keer automatisch wordt gestart bij het starten van Windows (via services!)

3.2.2 Oefening 2: Instellen van de eigenschappen van de server

1. Open de POP3 service (Administrative tools)
2. Klik rechts op de naam van de pc (in de linker console) en kies "Properties".

Je kunt de volgende zaken instellen.

- **De Authenticatie-methode**: je kunt kiezen uit de volgende methodes:
  - ***Local Windows accounts authentication:*** de POP3 service wordt geïntegreerd in de lokale SAM. Voor elke emailgebruiker moet dus een account aangemaakt worden of aangemaakt zijn. De gebruikers worden toegevoegd aan de "POP3 gebruikers" groep. Deze gebruikers kunnen niet lokaal inloggen op de server.
    Dit type van authenticatie moet gebruikt worden als de mail server geen deel uitmaakt van een AD domein, of als je expliciet wil dat de gebruikers worden bewaard op de POP3 server.
  - ***Active Directory Integrated authentication:*** de POP3 service wordt geïntegreerd in de bestaande AD Directo-

ry. Gebruik deze manier van authenticatie als de server een lid is van een AD domein, of als de server een AD domein controller is.

- ***Encrypted password file authentication:*** deze authenticatie maakt een encrypted bestand aan met de gebruikers wachtwoord. Dit bestand wordt bewaard in de map van de mailbox van de gebruiker op de server. Gebruik deze methode als je niet beschikt over AD of als je geen gebruikers wil aanmaken op de lokale pc. Je kan hiermee mailboxen aanmaken zonder dat je een gebruiker moet aanmaken.

3. Kies voor "Local Windows accounts authentication"

- **Wijzigen van de standaardpoort.** Indien de waarde gewijzigd wordt, moeten de clients ook ingesteld worden om deze nieuwe poort te gebruiken.
- **Instellen van het niveau van de Event logging.** Je kunt kiezen uit:
  - None: er worden geen gebeurtenissen bijgehouden.
  - Low: alleen kritieke gebeurtenissen worden bijgehouden
  - Medium: kritieke gebeurtenissen en waarschuwingen worden bijgehouden
  - High: alle gebeurtenissen worden bijgehouden.
- **Wijzigen van de plaats waar de mailboxen** moeten bewaard worden: standaard zijn deze terug te vinden in inetpub\mailroot\mailbox.

Opmerkingen:
De root van een station kan niet gebruikt worden als mailbox opslagplaats.
Je kunt een map op het lokale toestel of een UNC-pad gebruiken. Je kunt geen stations gebruiken die zijn toegekend aan een UNC-pad.
Het is aangeraden om de mailbox opslagplaats te plaatsen op een NTFS-volume. Zorg ervoor dat de administrators volledig beheer hebben over de map!
Map voor de mailboxen: c:\mailbox

- **Require Secure Password Authentication (SPA) …:** indien je voor deze optie kiest, dan worden de gegevens van de ge-

bruikers (vb. het wachtwoord), versleuteld over het netwerk verstuurd. Dit is een veiligere manier van werken.

4. SPA niet inschakelen

- **Always create an associated user for new mailboxes:** deze optie zorgt ervoor dat als er een mailbox wordt aangemaakt voor een nog niet bestaande gebruiker, er automatisch een gebruiker wordt aangemaakt.

5. Gebruiker laten aanmaken

Belangrijke opmerking:
Na de wijzigingen moet de POP3 service gestopt en opnieuw opgestart worden. Indien dit niet werd gevraagd bij het afsluiten van het dialoogvenster, kan je dit als volgt oplossen: Klik op de naam van de server, kies All Tasks, kies daarna om de service opnieuw op te starten.

3.2.3 Oefening 3: Aanmaken van een domein

Met een maildomein wordt niet dezelfde entiteit bedoeld als een AD-domein. Als je echter werkt met een AD, is het aangeraden om het emaildomein te laten samenvallen met het AD-domein.

1. Klik rechts op de naam van de server en kies New, Domain
2. Geef de naam op van het domein in het vak Domain Name: sntx.local (x=nr van de pc). Klik op OK. Indien deze server op het Internet wordt geplaatst, moet je contact opnemen met de ISP om afspraken te maken over de domeinnaam (deze moet aangekocht worden) en hun DNS-servers moeten aangepast worden zodat er verwezen wordt naar jouw emailserver.

3.2.4 Oefening 4: Aanmaken van mailboxen

1. Maak de gebruiker Sophie aan (wachtwoord: snt) via gebruikersbeheer.
2. Open het domein (rechter panel).
3. Kies Add mailbox uit het linker panel.
4. Geef de naam van de mailbox op. De maximale lengte voor een naam van een mailbox is 20 tekens indien je werkt met "Local Windows Accounts Authentication" en 64 tekens als je werkt met "Encrypted password file authentication" of

"AD Integrated Authentication". De minimale lengte is gelijk aan 1. Volgende tekens mogen niet gebruikt worden: @ ( ) / \ [ ] : ; , " < > * = | ? +(deze mag wel bij Encrypted password file authentication)

5. Geef als naam sophie op. Vink "Create associated user for this mailbox" af, aangezien de gebruiker reeds werd aangemaakt. Klik op OK.
6. Wat is het emailadres van deze gebruiker?
7. Maal een mailbox aan voor Els. Aangezien de gebruiker Els nog niet bestaat, mag je het vinkje bij "Create associated user for this mailbox" niet afvinken. Het wachtwoord is gelijk aan snt. Controleer gebruikersbeheer. Controleer eveneens van welke groep Els lid is.
8. Maak een mailbox voor aan met jouw naam. Wachtwoorden = snt

3.2.5 Oefening 5: installatie van de client (vb Outlook Express)

1. Start Outlook Express
2. Tools, Accounts, Internet mail toevoegen (indien de wizard niet start)
   - Display name = jouw naam.
   - Email-address = jouw emailadres
   - Pop3 en SMTP = ip-adres van jouw emailserver
   - Account name = jouw emailadres
   - Password = jouw wachtwoord
   - Indien op de server SPA geactiveerd werd, moet dit vinkje ook worden aangezet bij de installatie van de client.

3. Installeer eveneens het emailadres van Els.
4. Test het account uit door mails naar Els te sturen.

3.2.6 Oefening 6: controle van de mailboxen op de harde schijf

1. Controleer de fysieke mailboxen op de harde schijf.
2. Welke extensie hebben de berichten?

3.2.7 Oefening 7: instellen van een quota

Om ervoor te zorgen dat de mailboxen niet te groot worden, is het aangeraden om quota's te plaatsen op de mailboxen.

1. Activeer de eigenschappen van station C (= station waarop mailroot is aangemaakt).

2. Ga naar het tabblad Quota.
3. Plaats een vinkje voor "Enable quota management"
4. Klik op "Quota entries"
5. Kies "New quota entry" uit het menu Quota
6. Select users: via de knop advanced is het mogelijk om de quota op te geven voor meerdere gebruikers. Stel quota in voor Els. OK.
7. Stel Quota en waarschuwingsniveau in (resp 5000 en 4500). OK.
8. Sluit het venster. Verlaat het dialoogvensters via de OK-knop.
9. Stuur naar Els via jouw email-adres een mail, met een bijlage die groter is dan 4500 Kb.

3.2.8 Oefening 8: verwijderen van een mailbox

1. Klik op de mailbox van Sophie en kies delete mailbox (ook mogelijk via rechtersnelmenu). Alle gegevens worden gewist!
2. Je kunt aanduiden, indien nodig, of de bijhorende gebruiker ook gewist moet worden. Laat de gebruiker verwijderen.
3. Controleer gebruikersbeheer.
4. Wat gebeurt er met de fysieke mailbox op de harde schijf?

3.2.9 Oefening 9: blokkeren van een mailbox

1. Zoek in de help op hoe je een mailbox kan blokkeren.
2. Test dit uit met de mailbox van Els.
3. Indien een mailbox is geblokkeerd, wat gebeurt er dan met de mail die wordt verzonden naar de mailbox.
4. Zorg dat de blokkering wordt opgeheven.

3.2.10 Oefening 10: wijzigen van het wachtwoord

1. Kan je via de console het wachtwoord van Els wijzigen in sntbrugge?
2. Wijzig het wachtwoord van Els.

3.2.11 Oefening 11: Remote connectie

1. Klik rechts op POP3 service (linker panel) en kies Connect.
2. Voer de naam van de server in waarmee je een connectie wil maken.
3. Maak een connectie met een andere POP3 server
4. Maak een nieuwe mailbox aan met jouw naam

3.2.12 Oefening 12: Wijzigen van een bestaande mailroot

1. Maak een map c:\newmailbox aan.
2. Wijzig in de eigenschappen van de POP3 service de mail-root.
3. Verplaats (niet kopiëren) alle mappen van c:\mailbox naar c:\newmailbox.
4. Controleer steeds of de machtigingen ok zijn van de nieuwe opslagplaats voor mail!
5. Stop en start de service opnieuw.

3.2.13 Oefening 13: Wijzigen van de standaardpoort

1. Wijzig de standaardpoort van de POP3 service in 120
2. Voer deze instelling uit in de client (eigenschappen emailaccount)

3.2.14 Oefening 14: verwijderen van een domein

1. Klik rechts op de naam van het domein en kies Delete.
2. Bevestig. Alle mailboxen worden eveneens verwijderd.

3.2.15 Oefening 16: gemeenschappelijk adresboek

1. Zet op het toestel met de projector het imagebestand van Windows 2003 AD server terug.
   - Installeer de POP3 service
   - Maak voor iedereen een mailbox aan. Gebruik hiervoor de naam van de cursist. Laat eveneens een gebruiker aanmaken in AD.
   - Maak een gedeelde map adresboek aan, iedereen volledig beheer.

2. Zet de andere toestellen klaar:
   - Pas computernaam en ip-adres aan
   - Plaats het toestel in het domein
   - Log in met jouw naam (zoals opgegeven op de server)
   - Configureer het emailaccount
   - Ga naar het register en open de sleutel HKCU\Software\Microsoft\wab\wab4\Wab File Name
     Wijzig de gegevens van (default) of (standaard) in \\<naam server>\adresboek\klas.wab

- Open outlook express en wijzig het adresboek. Opgelet: je moet de contacts plaatsen in shared contacts! Wat zie je?

4 Internet Information Services

4.1 Inleiding

Een Windows 2003 server kan fungeren als een webserver (HTTP), een file Transfer Protocol server (FTP), een Simple Mail Transport Protocol host (SMTP) of een Network News Transfer Protocol host (NNTP).

4.2 HTTP

Het HTTP kan je terugvinden in de applicatielaag van de TCP/IP stack. Dit protocol maakt het WWW mogelijk. HTTP zorgt ervoor dat je statische en dynamische pagina's kan publiceren op een Windows 2003 Server via de WWW Publishing Service.
HTTP is een client/server protocol: dit protocol verzorgt de communicatie tussen een HTTP server (webserver) en een HTTP client (webbrowser). De sessie wordt als volgt tot stand gebracht:

- De client gebruikt TCP om een connectie te maken met de server, standaard via poort 80. Er wordt een three-way handshake connectie tot stand gebracht.
  Indien je wenst te werken met poort 8080, of een andere poort, moet je na de aanvraag een dubbele punt toevoegen, gevolgd door het nummer van de poort.
- De client vraagt aan de server dmv een HTTP GET Request boodschap om een webpagina of een ander bestand. Hij kan dit doen door het adres in te typen in de Explorer of door te klikken op een hyperlink in een andere pagina.
- De server antwoordt door een aantal pakketten terug te zenden die de webpagina of het bestand bevatten.
- Indien HTTP Keep-Alives geactiveerd is, blijft de TCP connectie tussen de client en de server open. Op die manier kan er snel om extra pagina's gevraagd worden.

4.3 Oefeningen

4.3.1 Oefening 1: Installatie van de IIS service

1. Open op je server2003 het configuratiescherm
   - toevoegen software
   - Kies toevoegen/verwijderen Windows componenten
   - Application server, details

- Internet Information Services (IIS), details. Zeker nodig: Common files, Internet Information Services Manager, World Wide Web Services.
- OK, OK
- Next
- Finish.
- Sluit alle vensters.

2. Schakel op de server de internetbeveiliging uit:
   - Open het configuratiescherm, toevoegen software
   - Kies toevoegen/verwijderen Windows componenten
   - Vink "Internet Explorer Enhanced Security Configuration" af.
   - Next
   - Finish

4.3.2 Oefening 2: Default Website

1. Standaard worden de bestanden bewaard in de map c:\Inetpub\wwwroot. Open de map en bekijk de inhoud. Open het bestand iisstart.htm. Dit bestand zal weergegeven worden.

2. Je kan een connectie maken met de lokale site op één van de volgende manieren:
   - Start
   - Uitvoeren
   - http://127.0.0.1
   - Open Internet Explorer en geef als adres http://127.0.0.1 of localhost of http://<servernaam>
   - Via de IIS console: Start, programs, Administrative tools, Internet Information Service (IIS) Manager. Open websites in het rechterpaneel. Klik rechts op Default Website en kies Browse.

3. Je kan een connectie maken met de remote site op één van de volgende manieren:
   - Open Internet Explorer en geef als adres http://<remote-servernaam>
   - Open Internet Explorer en geef als adres http://<remote-ipadres>

- Open Internet Explorer en geef als adres http://<remote-DNS-naam>

4.3.3 Oefening 3: Aanmaken van andere Website

Binnen een webserver kan je verschillende websites aanmaken. Iedere website wordt beschouwd als een aparte server: virtuele server. Het is alsof de server volledig aan de website toebehoort.

1. Voeg eerst een IP-adres toe aan de server (eigenschappen netwerk, eigenschappen TCP/IP, advanced). Kies als ip-adres het standaard ip-adres + 50.
2. Maak en map c:\newweb aan.
3. Plaats in deze map het volgende bestand (index.htm). Je kan dit bestand aanmaken via het kladblok:

   <html>
   <head>
   <title>Welkom aan de SNT </title>
   </head>
   <body>
   <p>Deze Cursus gaat over internet-werken.
   </body>
   </html>

4. Klik rechts op Websites in IIS-beheer en kies nieuw, Web Site. De Wizard wordt gestart. Kies Next.
5. Voer "Nieuwe website" als omschrijving in. Next.
6. Geef het juist aangemaakte IP-adres op en kies next.
7. Specificeer het pad naar de nieuwe homedirectory (c:\newweb). Anoniem inloggen toelaten. Next.
8. Wijzig eventueel de machtigingen. Next.
9. Finish.
10. Testen van de website: surf naar http://<nieuw ip-adres>

4.3.4 Oefening 4: wijzigen van de poort

1. Klik in IIS-beheer rechts op "Nieuwe website" (linkerpaneel). Activeer de eigenschappen. Tabblad website: wijzig de TCP-poort in 8080. OK. Merk op dat deze instellingen tijdens het configureren van de website had kunnen gebeuren.
2. Testen van de website: surf naar http://<nieuw ip-adres>:8080

4.3.5 Oefening 5: Virtuele directories

Stel dat je een directory wenst toe te voegen aan een website, maar fysisch is deze directory opgeslagen op een andere plaats (al dan niet remote).

4.3.5.1 Werkwijze 1:

1. Maak een map c:\virtueel aan.
2. Plaats in deze map het bestand index.htm met de volgende inhoud:

```
<html>
<head>
<title>Werken met virtuele directories</title>
</head>
<body>
<p>Dit is een voorbeeld van een virtuele directory
</body>
</html>
```

3. Klik rechts in IIS-beheer op de site waaraan een virtuele directory moet toegevoegd worden. In ons geval de is dit de "Default website". Kies Nieuw, Virtuele map. De wizard wordt gestart. Kies Next.
4. Geef als alias "Virtueel" op voor de virtuele map. Next.
5. Geef het pad op naar de map die moet toegevoegd worden aan de website. Next.
6. Stel eventueel de machtigingen in. Next.
7. Finish.
8. Testen: surf naar http://127.0.0.1/virtueel

4.3.5.2 Werkwijze 2 (lokaal):

1. Maak de map c:\oefen aan.
2. Plaats in deze map het bestand index.html met de volgende inhoud:

```
<html>
<head>
<title>Werken met virtuele directories 2</title>
</head>
<body>
<p>Dit is een tweede voorbeeld van een virtuele di
     rectory
</body>
</html>
```

3. Klik rechts op de map in de Verkenner.

4. Kies eigenschappen, tabblad Web sharing.
5. Kies de Website waaronder deze moet geplaatst worden (uit de vervolgkeuzelijst). Kies "Nieuwe website"
6. Kies Deel deze map en vul de aliasnaam (virtueel2) en de machtigingen in.
7. Testen: surf naar http://127.0.0.1/virtueel2:8080
8. Hoe kan je ervoor zorgen dat de shares niet worden weergeven via netwerkomgeving?

4.4 FTP

4.4.1 Inleiding

Via FTP is het mogelijk om bestanden te kopiëren over een internetwerk. In Windows 2000 wordt gebruik gemaakt van de FTP Publishing service. FTP is een client/server protocol. Hierbij maakt de FTP-client een connectie met poort 21 van de server. Dit is de standaard TCP poort dat de FTP-server gebruikt om na te gaan of een client een connectie wenst te maken. Eénmaal dat de connectie is ontstaan, wordt er een willekeurige poort boven 1023 toegekend aan de client. De connectie is klaar!

4.4.2 Oefening 1: toevoegen van de ftp-service

1. Open het configuratiescherm, toevoegen software
2. Kies toevoegen/verwijderen Windows componenten
3. Application server, details
4. Internet Information Services (IIS), details. Zorg ervoor dat de ftp-service ook aangevinkt staat.
5. OK, OK
6. Next
7. Tijdens de installatie is de cd nodig.
8. Finish. Sluit alle vensters.
9. Next, Finish

4.4.3 Oefening 2: Default Website

1. Standaard worden de bestanden bewaard in de map c:\Inetpub\ftproot.
2. Open de map en plaats hierin een aantal bestanden: oefen.txt, tekening.bmp, lijst.snt
3. Je kan een connectie maken met de lokale ftp-site op één van de volgende manieren:

- Start, Uitvoeren, ftp://127.0.0.1
  Dubbelklik op de verschillende bestanden. Wat kan je besluiten?
- Open Internet Explorer en geef als adres ftp://127.0.0.1 of localhost of ftp://<servernaam>
- Via de IIS beheer: klik rechts op Default FTPsite en kies Browse.

4. Je kan een connectie maken met de remote site op één van de volgende manieren:
   - Open Internet Explorer en geef als adres ftp://<remote-servernaam>
   - Open Internet Explorer en geef als adres ftp://<remote-ipadres>
   - Open Internet Explorer en geef als adres ftp://<remote-DNS-naam>

4.4.4 Oefening 3: Aanmaken van andere FTPsite

Op dezelfde manier als bij de WWW-service, kan je ook hier virtuele FTP-servers aanmaken.

1. Voeg eerst een IP-adres toe aan de server (eigenschappen netwerk, eigenschappen TCP/IP, advanced). Gebruik hetzelfde ip-adres als bij http.
2. Maak een map c:\nieuwftp aan en plaats een drietal bestanden in de map.
3. Klik rechts op FTPsite (IIS-beheer) en kies nieuw, FTP Site. De Wizard wordt gestart. Kies Next.
4. Voer als omschrijving “Nieuwe ftp” in. Next.
5. Geef het juiste IP-adres op en kies next.
6. Specificeer het pad naar de nieuwe homedirectory. Next.
7. Wijzig eventueel de machtigingen. Next.
8. Finish.
9. Testen van de website: surf naar ftp://<nieuw ip-adres>/nieuwe ftp

4.4.5 Oefening 4: wijzigen van de poort

1. Klik in IIS-beheer rechts op “Nieuwe ftp” (linkerpaneel). Activeer de eigenschappen. Tabblad website: wijzig de TCP-poort in 100. OK. Merk op dat deze instellingen tijdens het configureren van de website had kunnen gebeuren.
2. Testen van de website: surf naar ftp://<nieuw ip-adres>:100

4.4.6 Oefening 5: Virtuele directories

Stel dat je een directory wenst toe te voegen aan een ftpsite, maar fysisch is deze directory opgeslagen op een andere plaats (al dan niet remote).

1. Maak een map c:\virtueel aan.
2. Plaats in deze map drie bestanden:
3. Klik rechts in IIS-beheer op de site waaraan een virtuele directory moet toegevoegd worden. In ons geval is dit de "Default FTP-site". Kies Nieuw, Virtuele map. De wizard wordt gestart. Kies Next.
4. Geef als alias "Virtueelftp" op voor de virtuele map. Next.
5. Geef het pad op naar de map die moet toegevoegd worden aan de ftpsite. Next.
6. Stel eventueel de machtigingen in. Next.
7. Finish.
8. Testen: surf naar ftp://127.0.0.1/virtueelftp

4.4.7 Oefening 6: FTP- en Dos

Via de opdracht FTP [-s:bestandsnaam][hostnaam] kan je een verbinding opstarten vanaf de dosprompt.

- -S: bestandsnaam: specificeert een tekstbestand dat FTP-opdrachten bevat. Deze opdrachten worden automatisch uitgevoerd nadat FTP is gestart.
- Hostnaam: specificeert de hostnaam of het IP-adres van de computer waarmee een verbinding wordt gemaakt. Indien geen hostnaam wordt opgegeven kan nog steeds later een verbinding worden gemaakt.

Starten van een FTP-sessie:

- FTP <ipadres>
- Er wordt gevraagd om een gebruikersnaam op te geven. Indien het toegelaten is om anoniem in te loggen, voer dan het volgende in: anonymous <enter>.
- Er wordt gevraagd naar het wachtwoord. Indien je anoniem mag inloggen, druk op <enter>.
- Zoek in de help de verschillende opdrachten op.

4.5 NNTP

4.5.1 Inleiding

NNTP is een TCP/IP toepassingsprotocol dat de basis vormt voor het USENET systeem of voor nieuwsgroepen (internetwerken of intranet).

NNTP is zowel een client/server als een server/server protocol met de volgende functionaliteiten:

- Een NNTP-client (nieuwslezer) kan een connectie maken met de server om een lijst te downloaden van alle mogelijke nieuwsgroepen op de server. De client kan berichten lezen, antwoorden op bestaande berichten of zelf een nieuw bericht posten.
- De NNTP-host kan de lijst met nieuwsgroepen repliceren naar een andere host op het internetwerk.

4.5.2 Default NNTP Virtual Server

Standaard worden de bestanden bewaard in de map c:\Inetpub\nntpfile\root.
Je kan de volgende items onderscheiden:

- Newsgroups: er worden drie standaardgroepen aangemaakt. Control.cancel (nodig om berichten te annuleren door clients), Control.newsgroup (nodig om nieuwe groepen te maken door clients) en control.rmgroup (nodig om groepen te verwijderen door clients)
- Expiration policies:
- Virtual directories: hier kan je een aantal gegevens bewaren van de nieuwsgroepserver
- Current sessions: hier kan je zien wie er momenteel een verbinding heeft gemaakt en eventueel kan je verbindingen verbreken.

4.5.3 Aanmaken van een nieuwe NNTP Virtual Server

- Klik rechts op de servernaam
- Kies nieuw, virtuele server uit het snelmenu
- Geef een beschrijving op. Next.
- Geef het IP-adres en poort (standaard 119) op. Next.
- Geef het pad op dat gebruikt moet worden voor de interne bestanden van de server. Dit zijn oa tijdelijke bestanden.

- Is dit een lokaal pad of op een netwerkshare?
- Geef het pad op waar de gegevens moeten bewaard worden.
- Finish.

4.5.4 Expiration Policy

Hier kan je aanduiden hoelang artikels moeten blijven in een nieuwsgroep vooraleer deze worden verwijderd.

- Klik rechts op de expiration policy en kies new, expiration policy uit het snelmenu.
- Geef een beschrijving op voor de policy.
- Geef aan of deze policy moet toegepast worden op alle nieuwsgroepen van de virtuele server, of enkel op een (aantal) groepen. Je kan de * gebruiken in de groepsnaam, om een aantal groepen op te geven.
- Finish

Open Expiration policy om de regel te zien.

4.5.5 Nieuwe newsgroepen toevoegen

- Klik rechts op Newsgroups in de juiste server en kies Nieuw uit het menu Acties.
- Geef een weergave naam op voor de nieuwsgroep. Next.
- Geef een beschrijving en een pretty-name op. Next.
- Finish.

4.5.6 Nieuwsgroepserver heropbouwen

Dit is nodig als je manueel bestanden wist:

- Stop de NNTP virtuele server (selecteer de server en klik rechts en kies stop).
- Klik rechts op de server, All tasks, Rebuild server.
- Herstart de server.

4.6 SMTP

SMTP is een populair TCP/IP toepassingsprotocol dat de basis vormt van (Internet) E-mail. Dit protocol wordt gebruikt om e-mails te verzenden van een SMTP host naar een andere SMTP host over een internetwerk. Het SMTP protocol kan echter geen berichten bewaren, zodat een gebruiker deze later kan lezen. Dus beide pc’s moeten online zijn! Een oplossing voor dit probleem, was de ontwikkeling van een nieuw protocol POP (Post Office

Protocol) en IMAP versie 4 (Internet Message Access Protocol). Deze server kan niet beschouwd worden als een volwaardige e-mail server. Daartoe moet je gebruik maken van andere servers zoals de Microsoft Exchange Server.

4.7 Eigenschappen van services

4.7.1 Instellingen op server niveau

- Verbinding maken met een server die IIS draait: klik rechts op IIS in de manager, en kies connect. Geef de (DNS)naam of IP-adres op van een server
- Backups maken en/of terugzetten van de configuratie van een server: klik rechts op de naam van de server en kies Backup/restore configuration uit het menu All tasks. Via de knop Create Backup wordt er een backup aangemaakt met de opgegeven naam in de map system32\inetsrv\MetaBack. Deze informatie in binaire vorm is specifiek voor de server waarvan deze werd aangemaakt. Indien Windows 2003 opnieuw wordt geïnstalleerd op het toestel kan je hier echter geen gebruik van maken. Via de knop Restore kan je de vorige instellingen terugzetten. Opgelet: om een backup terug te zetten, moeten alle IIS-services gestopt zijn!

4.7.2 Eigenschappen van de WWW Publishing service

4.7.2.1 Tabblad Website

1. Beschrijving: de naam die wordt weergeven in de IIS-console van de website.
2. IP-adres: kies het ip-adres van de website uit de keuzelijst. Indien je geen IP-adres toewijst, reageert deze site op alle IP-adressen die aan deze computer en niet aan andere sites is toegewezen. Slechts één website kan de melding (Alle niet toegekende ip-adressen) krijgen.
3. TCP-poort: standaard is de poort gelijk aan 80, maar je kan elke geldige vrije poort kiezen boven 1023. Via deze werkwijze is het mogelijk om een extra beveiliging in te voeren: naast de url, moet een client ook het nummer van de poort kennen. Voorbeeld: www.snt.be:8080
4. Geavanceerd: hierdoor kan je gebruik maken van domeinnamen (zie DNS-server).
5. SSL-poort: dit is nodig als je werkt met een beveiligde website (Secure Sockets Layer). De standaardpoort is 443.

Clients moeten wel het nummer van de poort aanvragen vooraleer ze toegang krijgen tot deze website.

6. Time-out van de verbinding: dit is het aantal seconden waarna de server de verbinding met een inactieve gebruiker verbreekt.
7. HTTP-keepalives inschakelen: hiermee kan een client de verbinding met de server open houden, zodat de verbinding niet telkens opnieuw hoeft te worden geopend voor elke nieuwe aanvraag.
8. Vastleggen in een logboek inschakelen:
   - Microsoft IIS-indeling: een vaste ASCII-indeling.
   - ODBC-registratie: vaste indeling in een databank
   - Uitgebreide W3C-indeling: aanpasbare ASCII-indeling

   Via eigenschappen kan je de frequentie, bestandslokatie, ... instellen. Ook de gegevens die moeten bewaard worden kunnen aangeduid worden.

4.7.2.2 Tabblad Service

1. Run WWW service IIS 5.0 isolation mode: voor de compabiliteit is de IIS 5.0 geïsoleerde mode soms nodig.
2. Http compression: bestanden die gecomprimeerd worden vooraleer ze verzonden worden naar een compression-enabled client.

4.7.2.3 Tabblad Performantie

1. Limiteren van de bandbreedte.
2. Aanduiden hoeveel maal de website zal aangesproken worden per dag (schatting). Dit staat in combinatie met de IIS cache. Indien geen beperking, kies dan voor oneindig.

4.7.2.4 Tabblad Basismap

1. Vooreerst kan je aanduiden waar de inhoud geplaatst is. Je hebt de keuze uit: een map op deze computer, een share op een andere computer of een omleiding naar een url. Afhankelijk van de keuze kan je vervolgens de plaats aanduiden.
2. Toelatingen:
   - Toegang tot scriptbron: de gebruikers krijgen toegang tot de broncode van scripts (zoals ASP) wanneer de machteging Lezen of Schrijven is ingesteld.
   - Lezen: de gebruikers kunnen bestanden of mappen lezen en/of downloaden.

- Schrijven: de gebruikers kunnen bestanden en bijhorende eigenschappen uploaden.
- Bladeren door mappen: de gebruiken kan een hypertext-lijst van de bestanden en submappen in de virtuele map bekijken, als er geen standaard homepagina aanwezig is.
- Bezoeken in logboek vastleggen: in het tabblad website moet het opnemen van gebeurtenissen in het logboek vastgelegd zijn.
- De bron indexeren: de map wordt door de Microsoft Indexing Service opgenomen in een tekstindex van de website.

3. Instellingen voor de applicaties. Voorbeeld: Machtigingen uitvoeren: hiermee kan je het gewenste niveau van uitvoeren selecteren.
   - Geen: geen scripts (vb ASP) of uitvoerbare bestanden uitvoeren op de server.
   - Alleen Scripts: alleen scripts zoals ASP-toepassingen uitvoeren op de server.
   - Scripts en uitvoerbare bestanden: scripts en uitvoerbare bestanden mogen uitgevoerd worden op de server.

4.7.2.5 Tabblad Documenten

1. Standaarddocumenten inschakelen: op die manier kan je aanduiden dat je wenst gebruik te maken van een standaarddocument. Je kan eveneens de volgorde aanduiden waarnaar gezocht moet worden. Bovendien kan je een document toevoegen of verwijderen.
2. Voettekst van document inschakelen: hiermee kan je automatisch een voettekst (enkel HTML-code) toevoegen aan elk document.

4.7.2.6 Tabblad mapbeveiliging

Opgelet: de NTFS-beveiliging op bestanden heeft voorrang!

1. Anonieme toegang en verificatiemethoden bewerken:
   - Anonieme toegang en verificatiemethoden: de gebruikers krijgen anonieme toegang via een gastaccount.
   - Basisverificatie: gebruikersnaam en wachtwoord moeten ingevoerd worden (gebruikersbeheer). De wachtwoorden worden ongecodeerd over het netwerk verzonden. Er kan een standaarddomeinnaam opgegeven worden.

- Verificatiesamenvatting: in plaats van het wachtwoord, wordt een hash-waarde over het netwerk verzonden. Deze methode werkt ongeacht of er proxyservers of firewalls aanwezig zijn.
- Geïntegreerde Windows-verificatie: de huidige gebruikersnaam en wachtwoord wordt gebruikt. Wordt het meest gebruikt op intranets!

2. Ip-adressen: hier kan een aantal computers toelaten of hen de toegang verbieden via hun IP-adres (één computer of een aantal computers) of via de DNS-naam (domein).
3. Beveiligde communicatie: hier kan je de toegang beveiligen door gebruik te maken van het SSL protocol. De toegang tot een dergelijke website gebeurt via https:// ipv http://. Vooraleer je hiervan gebruik kan maken, moet je een certificaat aanvragen bij een publieke Certificate authorithy (zoals Verisign) of moet je op een lokale server de service installeren.

4.7.2.7 Tabblad http-headers

In dit venster kan je waarden instellen die naar de browser worden gezonden en in de koptekst van de HTML-pagina wordt opgenomen. Zo kan je een vervaldatum opnemen in tijdsgebonden informatie. De browser vergelijkt de huidige datum met de vervaldatum om aan te duiden of er gebruik moet gemaakt worden van de pagina in de cache, of moet er een bijgewerkte pagina van de server gehaald worden.

4.7.2.8 Aangepaste foutberichten

Hiermee kan je de foutberichten die naar een client wordt gestuurd bij een fout, aanpassen.

4.7.3 Eigenschappen van de website zelf

Volgende tabbladen verschijnen bij het openen van de eigenschappen van een website:

- Website
- Performance
- ISAPI filters
- Home Directory
- Documents
- Directory Security

- http-Headers
- Custom errors

Deze instellingen hebben voorrang op deze van de webservice zelf.

4.7.4 Eigenschappen van de FTP Publishing service

4.7.4.1 Tabblad FTP-site

Analoog als bij http, op het volgende na:
Via de knop huidige sessies, kan je zien wie er momenteel een connectie heeft. Bovendien is het mogelijk om het aantal gelijktijdige verbindingen te beperken. Je kan ook verbindingen verbreken.

4.7.4.2 Tabblad beveiligingsaccounts

In dit venster kan je aanduiden of een gebruiker mag anoniem aanmelden of niet.

- Anoniem aanmelden toelaten aangevinkt en alleen anoniem aanmelden toelaten aangevinkt: alleen anonieme toegang is mogelijk.
- Anoniem aanmelden toelaten aangevinkt en alleen anomiem aanmelden toelaten afgevinkt: anonieme toegang wordt eerst gecontroleerd, vervolgens basis authenticatie (di gebruikers die lokaal mogen inloggen op de IIS server).
- Anoniem aanmelden toelaten afgevinkt: alleen basis authenticatie is mogelijk.

FTP-siteoperators vormen een speciale groep gebruikers met beperkte beheerderrechten voor hun FTP-site. Ze kunnen enkel eigenschappen beheren die betrekking hebben tot hun site.

4.7.4.3 Tabblad berichten

Volgende berichten zijn mogelijk: welkomstbericht, Afsluitbericht en een bericht wanneer het maximale aantal verbindingen is overschreven.

4.7.4.4 Tabblad Basismap

1. Map op deze computer of share op een ander computer.
2. Plaats van de map.
3. Toegang: lezen en/of schrijven. Maw mogen ze alleen kunnen downloaden of mogen ze ook uploaden.
4. Bezoeken in een logboek vastleggen?
5. Stijl van weergave: Unix of DOS.

4.7.4.5 Tabblad Directory Security

Hier kan je aanduiden welke IP-adressen zijn toegelaten en welke niet. Standaard worden alle IP-adressen toegelaten.

Opmerking: de eigenschappen op een FTP-site zelf hebben voorrang!

4.7.5 Eigenschappen van NNTP server

4.7.5.1 Tabblad algemeen

- Naam van de virtuele server.
- Ip-adres
- Connecties en logging: zie ook web service.
- Path header: wordt meegeven in Path lijn van de NNTP header.

4.7.5.2 Tabblad Access

Hier kan je de gewenste authenticatiemethoden aanduiden. Zie ook Web- en ftp-servers.

4.7.5.3 Tabblad settings

- Mogen de clients posten naar de server?
- Limiteren van de maximale grootte van een bericht.
- Limiteren van de maximale hoeveelheid die tijdens één connectie kan gepost worden.

Je kan gebruik maken van gemodereerde groepen: de moderator ontvangt alle opgestuurde berichten, die hij vervolgens kan accepteren of weigeren. Berichten kunnen via STMP naar de moderator gestuurd worden of ze kunnen direct geplaatst worden in de map Pickup van de virtuele server. Vervolgens worden de berichten doorgestuurd naar de geselecteerde moderator.

4.7.5.4 Tabblad security

Hier kan je zoals bij www en ftp aanduiden wie de server kan beheren.

5 Openvpn

5.1 Bronnen

Alle programma's en informatie, tevens installatie handleidingen zijn te vinden op htt://www.openvpn.net

5.2 Installatie stappenplan

5.2.1 De server

- Download de laatste versie van openvpn
- installeer openvpn op uw server
- genereer de nodige sleutelbestanden (1 voor server en 1 voor client) aan de hand van de bestanden dit te vinden zijn in de folder c:\program files\openvpn\easy-rsa. De werkwijze lees je in README.txt.
- Configureer het serverbestand server.ovpn
  - een standaard voorbeeld van dit bestand vind je in de folder c:\program files\openvpn\sample-config.
  - Open dit voorbeeld bestand en pas het aan naar jou opstelling.
  - LET OP DE VOLGENDE PUNTEN:
    - Gebruik routing NIET bridging
    - zet zeker alle firewalls uit
  - Sla het aangepaste server.ovpn bestand op in de folder c:\program files\openvpn\config
- Start openvpnserv.exe te vinden in c:\program files\openvpn\bin
- kijk na of de server effectief actief is. Pas eventuele fouten aan.
- Fouten kun je meestal terugvinden in de logbestanden in de folder c:\program files\openvpn\log

5.2.2 Het werkstation

- Download de laatste versie van openvpn
- installeer openvpn op uw werkstation
- copieer de sleutel voor het werkstation naar c:\program files\openvpn\config
- Configureer het clientbestand client.ovpn

- een standaard voorbeeld van dit bestand vind je in de folder c:\program files\openvpn\sample-config.
- Open dit voorbeeld bestand en pas het aan naar jou opstelling.
- LET OP DE VOLGENDE PUNTEN:
  - Let op de overeenkomsten met de serverconfiguratie
- Sla het aangepaste client.ovpn bestand op in de folder c:\program files\openvpn\config

- Start openvpn.exe te vinden in c:\program files\openvpn\bin
- kijk na of de client effectief actief is. Pas eventuele fouten aan.
- Fouten kun je meestal terugvinden in de logbestanden in de folder c:\

5.2.3 Testen

Ping naar het vpn-ip van de server.