THUISNETWERKEN

Peer-to-Peer netwerken tot 10 PC's

Hardware- en softwarematig opzetten van een Peer-to-Peer netwerk
Beheer van gebruikers en hun machtigingen

Carl Maegerman
www.lesgever.be

INHOUDSOPGAVE

1 Inleiding

De personal computer is stilletjes aan een vetrouwde machine in de “huiskamer”. Een drie- à viertal jaar terug heeft vader een pc gekocht en die naarstig gebruikt. De opgroeiende kinderen hebben in de loop van deze tijd ook de PC ontdekt. Het spelen van spelletjes en het maken van werkjes voor school op de pc is dagelijkse kost. De PC is te druk bezet en vader beslist om een tweede pc aan te kopen.

Uiteraard volgt deze PC de laatste ontwikkeling en is Internet-toegang een must. Maar de kinderen, MSN-fanaten, zien de snelle Telenet/ADSL-toegang waardoor communiceren met hun vrienden nog gemakkelijker en vooral sneller gaat dan met de trage analoge modem. De nieuwe PC wordt opnieuw druk bezet en de “oude PC” blijft staan.

Vader zit dus nog steeds met hetzelfde probleem. De oplossing : een netwerk tussen de twee pc’s waardoor de kinderen met hun eigen PC ook op het internet kunnen via Telenet/ADSL.

Dit fenomeen doet zich dagelijks voor bij de Vlaamse huisgezinnen. Waar vroeger networking (gebruik van een netwerk) enkel in bedrijven werd gebruikt is er een sterk groeiende behoefte naar kleine thuisnetwerken waardoor een aantal “bronnen” gezamenlijk kunnen worden gebruikt.

Dit is ook de aanleiding om te starten met een cursus netwerken. Een cursus die bestaat uit drie delen : inleiding tot netwerken en client-server netwerken (deel 1 en 2).

In het eerste deel wordt uitgegaan van de hierboven geschetste situatie waarbij een gezin een twee à drie PC’s heeft die om verschillende redenen met mekaar moeten communiceren.

In de twee volgende delen belichten we de meer professionele toepassing van netwerken. Hierbij spreken we over client-server netwerken waarbij een speciale computer, de “SERVER” het centrale deel van het grote netwerk is. Dit is uiteraard niet van toepassing in een gezinsituatie of een KMO waar een aantal medewerkers samen hun gegevens moeten kunnen delen en in gemeenschap moeten kunnen gebruiken.

Inleiding tot netwerken behandelt de installatie en het gebruik van kleine netwerken. Kleine netwerken bevatten van twee tot een tiental computers en andere gemeenschappelijke toestellen. Dit is het uitgangspunt voor deze cursus. Dit betekent niet dat er in een klein netwerk geen centrale server kan

gebruikt worden, maar de extra kosten die daarmee gepaard gaan wegen soms niet op tegen de voordelen van dit systeem.

In deze cursus gebruiken we Windows XP Professional omdat deze het meest geschikt is om in een netwerk te gebruiken. Het is echter wel zo dat mocht je Windows XP Home Edition gebruiken de manier van werken eigenlijk hetzelfde is. Dus het is zeker niet nodig om Windows XP Professional te installeren maar als je de mogelijkheid hebt om dit te doen is het aan te raden.

Netwerken basis – Labo 001 – Installatie Windows XP Professional

In een eerste hoofdstuk “Netwerken : wat en waarom ?” beschrijven we de functie van een netwerk en belichten we het waarom van netwerken. In de loop van de jaren zijn verschillende vormen ontstaan. Deze vormen belichten we vanuit informatieve overwegingen.

In het tweede deel van de cursus gaan we onmiddellijk van start met de installatie van het netwerk. Daarbij geven we een overzicht van de verschillende onderdelen en hun onderlinge samenwerking.

Na de “hardware”-installatie van je netwerk moeten uiteraard een aantal parameters e.d. geconfigureerd worden wil je een goed functionerend netwerk hebben. In deel drie gaan we stap-voor-stap te werk bij de instelling van je verschillende pc in het netwerk.

Uit de inleiding hebben we begrepen dat er een behoefte is ontstaan naar netwerken. Welke functionaliteiten een netwerk heeft en hoe deze te gebruiken vormt het onderwerp van het vierde hoofdstuk van deze cursus.

De leerstof wordt in de vorm van praktische oefeningen, labo’s genoemd, aangeleerd en herhaald. De bedoeling is dat je na het labo eigenlijk deze taak zelfstandig zou moeten kunnen uitvoeren. Uit ervaring blijkt dat dit niet na éénmaal oefenen mogelijk is vandaar dat we bij de labo’s heel wat herhaling zullen inbouwen zodanig dat een aantal vaardigheden “gedrild” worden.

In het laatste hoofdstuk van deze cursus zullen we de connectie van ons netwerk(je) met de buitenwereld bespreken. In een klein netwerk is er meestal geen communicatie met andere netwerken (zoals verbindingen van bijkantoren met het hoofdkantoor, of van winkels met de administratieve zetel). In

kleine netwerkjes spreken tegenwoordig enkel met het Internet. Dit wordt dan ook het thema voor het laatste hoofdstuk.

Na deze cursus kan je een drie-tal pc's in een netwerk plaatsen. Naast deze fysieke installatie kan je de verschillende pc's in het netwerk configureren zodanig dat alle functionaliteiten van een netwerk ter beschikking zijn van de gebruikers. Dit gaat van het gebruiken van een zelfde harde schijf, printer, ... tot het gemeenschappelijk gebruik van de internettoegang.

Je zal merken dat deze opdracht "kinderspel" wordt voor jou.

2 Wat is een netwerk?

In zijn eenvoudigste vorm bestaat een netwerk uit 2 computers die met elkaar verbonden zijn.

Alle netwerkvormen, hoe ingewikkeld ze ook zijn, stammen af van dit principe.

Netwerken zijn ontstaan vanuit de behoefte om gegevens van computer naar computer te verhuizen zonder hiervoor externe opslagmedia te moeten gebruiken. In een netwerk is het mogelijk gegevens van op een andere computer te raadplegen zonder veel moeite. Het delen van een printer is ook een belangrijke behoefte geweest om netwerken op te bouwen.

Een netwerk is dus een geheel van computers, randapparatuur en bekabeling met als functie het beschikbaar maken van data en apparatuur aan meerdere gebruikers.

Een eenvoudig netwerk dat bestaat uit enkele computers en een printer.

Netwerken verschillen echter onderling sterk in grootte.

Afhankelijk van de grootte van het netwerk zullen ook verschillende vormen van netwerk ontstaan. Elk van deze netwerktopologieën (weergave van alle fysieke netwerkverbindingen) heeft zijn eigenheid. Op basis van de geografisch oppervlakte het netwerk bestrijkt spreken we van een Local Area Network (LAN), een Metropolitan Area Network (MAN) of een Wide Area Network (WAN).

3 Waarom een netwerk

3.1 Historisch

In de beginjaren 80 (de eerste IBM-PC kwam op de markt) was informaticamateriaal ontzetten duur. Een klein voorbeeldje : een harde schijf van 15 Mb (sic) kostte in die tijd al snel € 10.000,- (sic). Voor een matrix-printer betaalde je al snel 5 à 8000 Euro, terwijl je voor de de eerste IBM PC 16.500 € neertelde.

Een kantoor dat twee computers en een printer kocht had al snel een serieuse investering gedaan. Alleen kon de gebruiker van de tweede pc geen afdrukken maken en moest hij met zijn diskette naar de pc gaan waar de printer geïnstalleerd was. De andere gebruiker moest dan even stoppen en het document van de collega moest eerst ingeladen worden om te kunnen afdrukken. Dit is nu ondenkbaar, maar zo moest het vroeger gezien de hoge kostprijs van een tweede printer. Een tweede printer kopen was onverantwoord.

Vandaar dat gezocht werd naar een goedkopere naarmate de behoefte groeide om verschillende toestellen en informatie (documenten, gegevens, ...) gemeenschappelijk te gebruiken. Al gauw werd gewerkt aan onderdelen die communicatie tussen computers mogelijk moesten maken (netwerkkaarten en bekabeling).

Vanuit de behoefte om informatie en apparatuur gezamelijk te gebruiken ontstond stilaan het netwerk-gebruik.

3.2 Eigen situatie

Als je even in je eigen situatie (thuis, kantoor, werk, …) gaat kijken dan zal je al snel ontdekken dat ook jij behoefte hebt om gegevens of toestellen te delen.

3.2.1 Gegevens

Gezamelijk gebruik van documenten : Je collega heeft een type invulformulier gemaakt waardoor er heel wat tijd wordt bespaard doordat je niet steeds het document volledig opnieuw moet intikken. Het zou interessant zijn dat je tien andere collega's ook dit document kunnen gebruiken. Je kan nu dit document door middel van een diskette op elke PC kopiëren maar van zodra dat er iets verandert in het originele document moet je telkens op de verschillende pc's de nieuwe versie kopiëren. Het zou veel gemakkelijker zijn als iedereen de originele versie vanop die ene pc zou kunnen gebruiken. Van zodra een wijziging in het origineel is aangebracht gebruikt iedereen onmiddellijk de nieuwe versie.

Gezamelijk gebruik van gegevens : op de afdeling boekhouding maken verschillend personen fakturen. Eén van de bediende is verantwoordelijk voor adreswijzigingen van klanten in te brengen. Wanneer deze

nieuwe adresgegevens op elke PC door middel van een diskette zouden moeten worden gekopieerd zouden heel wat fakturen naar klanten naar oude adressen gestuurd worden. Door het klantenbestand gemeenschappelijk te gebruiken wordt elke adreswijziging onmiddellijk van kracht bij het faktureren van de klant.

3.2.2 Randapparatuur

Gebruik van een dure laserprinter : thuis heb je een dure laserprinter gekocht en uiteraard op je PC aangesloten. Je zoon die, op zijn eigen kamer, ook een PC staan heeft, wil ook gebruik maken van deze printer. De printer elke keer verhuizen van de ene ruimte naar de andere is ook niet de meest elegante oplossing. Vandaar dat je een middel moet vinden zodanig dat je zoon op je printer kan afdrukken. Een netwerkkabel en twee netwerkkaarten kunnen hier de oplossing brengen.

Gebruik van je internet-aansluiting : ondertussen heb je ook een telenet aansluiting en wil je dochter ... op die andere kamer ... gebruik maken van je PC om op internet te surfen. Maar daar ben jij niet zo op gesteld. Jouw PC is jouw PC ! Terwijl je toch al een netwerkje hebt met de pc van je zoon kan je ook de pc van je dochter in het netwerk leggen en kan ze via het netwerk gebruik maken van je Telenet-modem en surfen op het Net zonder je maar één moment te storen. Wat een uitvinding dat netwerk .....

3.2.3 Toepassingen

Gebruik van e-mail en agenda : op de verkoopsafdeling wil de verkoopsdirecteur steeds weten waar en wanneer een verkoper bij klanten is. Om dit te weten te komen koopt de directeur een agenda- en email-programma dat op zijn pc draait. Alle verkopers kunnen via het netwerk hun afspraken in de agenda invullen. De directeur en de andere verkopers kunnen de agenda raadplegen en zo te weet komen waar de verschillende verkopers zich bevinden. De directeur wil zijn verkopers op de hoogte brengen van een aantal verkoopscijfers. Een eigen email-adres voor elke verkoper is hier de oplossing. Een goed email-programma dat ook op het netwerk wordt geplaatst geeft de mogelijkheid dat de verschillende gebruikers op het netwerk met elkaar en met de buitenwereld door middel van e-mail kunnen communiceren.

4 Soorten netwerken

4.1 LAN

Een Local Area Netwerk bevindt zich meestal in een beperkte geografische ruimte. Een lokaal, een afdeling bestaande uit meerdere burelen, een gebouw, een campus gelokaliseerd op één plaats zijn voorbeelden waarin we spreken over een LAN. LAN gebruikt, gezien zijn beperkte geografische verspreiding, geen communicatiemiddellen zoals telefoonlijnen, ... Alle computers worden met elkaar verbonden door netwerkkabels zonder gebruik te maken van tussenliggende communicatietoestellen zoals modems e.d.

Voorbeeld : het netwerk is de klas, netwerk in je kantoor of de twee pc's die je thuis met elkaar verbonden hebt.

4.2 MAN

Een Metropolitan Area Netwerk ligt verspreid over een grotere oppervlakte, alhoewel deze ook beperkt is. We spreken hier bijvoorbeeld over een netwerk dat verschillende gebouwen in een zelfde gemeente verbindt. Of van een netwerk dat verschillende universiteitscampussen in eenzelfde streek verbindt. Het grote verschil met een LAN is het gebruik van extra communicatietoestellen om de verschillende netwerken te verbinden.

Voorbeeld : het netwerk dat de verschillende gemeentelijke diensten (burgerlijke stand, politie, gemeentehuis, sportdienst, ...) met elkaar verbinden.

4.3 WAN

Wordt je netwerk nog wat groter en ga je verschillende filialen van je bedrijf, die zich in verschillende gemeenten, landen, ... bevinden, onderling verbinden dat spreken we eerder van een Wide Area Network. Er is zeer weinig verschil tussen een MAN en een WAN buiten de geografische verspreiding van de verschillende onderlinge netwerken. Door deze verschillende verspreiding is het soms nodig van andere communicatiemiddelen te gebruiken (bvb. sattelietverbindingen, ...).

Voorbeeld : het netwerk van geldautomaten (Bancontact, Banksys, ...), computernetwerk van bedrijven zoals IBM, Microsoft, Philips, ..., het internet

Een MAN/WAN is eigenlijk het aan elkaar sluiten van verschillende LAN's (een subnet van een groter netwerk) door middel van speciale communicatietoestellen. Het opzetten van een LAN is dan ook de basis

van een grotere WAN. Gezien de specificiteit van de communicatiemiddelen die nu en in de toekomst op de markt zijn en nog zullen verschijnen, is het aan te raden om gespecialiseerde firma's aan te spreken voor dit deel van je netwerk dat instaat voor de communicatie tussen de verschillende LAN's die in je netwerk zitten. Hierbij denken we bijvoorbeeld aan firma's zoals Belgacom, Telenet, ... die dergelijke gespecialiseerde diensten aanbieden.

Het installeren van een eigen LAN moet echter binnen de mogelijkheden van deze cursus (en het vervolg) liggen. Daarbij starten we met een klein netwerkje van 2 à 10 PC's en gaan we in een tweede deel van deze cursus (Client-server netwerken) de grotere netwerken bespreken.

5 Soorten LAN's

Een netwerk ontstaat uiteraard vanuit een behoefte van communicatie. Bij het starten van een klein bedrijfje zal de zaakvoerder één PC kopen om zijn klanten bij te houden, om zijn brieven te tikken, om zijn fakturen te maken, ... De volledige administratie van het bedrijf gebeurt op deze éné PC.

Het bedrijfje groeit. Er komen meer klanten en de zaakvoerder heeft geen tijd meer om zelf de volledige administratie bij te houden. Een eerste medewerker wordt aangeworven en dus ook een nieuwe PC verschijnt in het bedrijf. Alle gegevens van het bedrijf staan echter op de PC van de "baas". Dus : een netwerkje moet de oplossing bieden. De medewerker kan nu de klantgegevens van op de eerste pc halen en zo zijn eigen werk vanop zijn eigen pc uitvoeren met gegevens die op een andere pc staan.

De firma haalt wat verkopers in huis en daardoor stijgt de verkoop, het aantal klanten, de omzet en dus ook het werk.... Enkele medewerkers worden bij aangeworven en uiteraard met elk zijn bureel en pc. Doordat elke medewerker ook contact moet hebben met de pc van de "baas" wordt het netwerk uitgebreid. De pc van de "baas" wordt nu door iedereen aangesproken waardoor deze overbelast wordt en de zaakvoerder niet comfortabel meer kan werken op zijn pc. De snelheid waarmee nu informatie kan opgevraagd worden is zo laag geworden dat het niet meer werkbaar is.

De pc van de "baas" is een (file-)server geworden maar eigenlijk is het een gewone pc die daar niet voor aangepast is. Een speciale server en de nodige uitbreidingen worden gekocht en stilaan evoleert het kleine netwerkje van 2 à 3 pc's (peer-to-peer netwerk) naar een volwaardig groot netwerk waarbij bepaalde toestellen (de pc van de baas) in functie staan van alle gebruikers van het netwerk (dedicated toestellen). Gezien de specificiteit van deze functies worden speciale toestellen gekocht (servers) en komen we tot een "server-based" netwerk.

5.1 Point-to-Point netwerken

Een LAN dat bestaat uit twee computers.

Deze computers kunnen dan elkaars gegevens en randapparaten gebruiken.

5.2 Peer-to-Peer netwerken (= gedecentraliseerd netwerk)

5.2.1 Eigenschap

Een peer-to-peer netwerk is te omschrijvien als een netwerk waarbij de verschillende clients aan elkaar gekoppeld zijn en waarbij elke client evenwaardig in de hiërachie van het netwerk. Geen van de deelnemende clients neemt het beheer van het netwerk waar. Elke gebruiker kan zelf bepalen of andere gebruikers van het netwerk gegevens op zijn harde schijf mogen lezen/bewaren/schrijven. Of iemand een document op zijn printer mag afdrukken, ... Het is de gebruiker van de pc die het beheer van zijn eigen pc in handen heeft.

Daardoor wordt het soms **moeilijk werkbaar**. In een netwerk van 5 pc's bewaart elkeen meestal zijn documenten op zijn eigen pc. Wil iemand anders deze tekst gebruiken moet de "beheerder" (meestal iemand die iets meer van computers kent dan zijn collega's) de toegang tot deze pc configureren. De beheerder loopt van pc tot pc om dit alles in orde en werkbaar te houden.

Alle documenten in het netwerk staan verspreid over alle pc's. Zoek je een bepaald document dan kan dit nogal eens duren voor je dit gevonden hebt. Je weet niet precies waar het document zich bevindt. De eigenaar van het document of een andere netwerkgebruiker kan het verplaatst hebben. Dit kan toch wel wat ergenis opwekken.

Een **veiligheidskopie** niemen van deze docoumenten is ook al een heikele opdracht. Wil je bijvoorbeeld 's nachts (wanneer niemand werkt) een veiligheidskopie (backup) nemen dan moeten alle pc's aanstaan. Van de pc's die uitgezet zijn bij het verlaten van het kantoor kan geen backup genomen worden. Doordat de gebruiker zelf kan beslissen waar hij zijn gegevens bewaart is het mogelijk dat de folder waar deze zijn documenten bewaart niet in de procedure van de veiligheidskopie is opgenomen.

Dit zijn een aantal nadelen van een peer-to-peer netwerk. Het heeft een uiteraard ook een aantal voordelen. Het grootste voordeel is dat men voor een minimale investering aan hardware (Windows ondersteunt peer-to-peer netwerken) communicatie tussen verschillende pc's mogelijk wordt. Verschillende bronnen kunnen dus op een goedkope manier ter beschikking gesteld worden van alle

gebruikers. Door tijds- en financiële besparingen (bvb. geen twee printers moeten kopen voor twee gebruikers – één is voldoende) is de investering voor een peer-to-peer netwerken snel terug verdiend.

Gezien de minimale beheerstaken is het een netwerk dat snel kan gelegd worden en waarvoor geen specifieke kennis nodig is. Weten hoe je een netwerk leggen en hoe je werkstations te configureren is voldoende.

5.2.2 Grootte

Een peer-to-peer netwerk beperkt zich meestal tot een tiental pc's. Wordt je netwerk groter dan moet je gaan denken aan de aanschaf van een centrale server (gezien zijn specifieke capaciteiten). De snelheid van een peer-to-peer netwerk met meer dan 10 pc's zal in sommige gevallen abominabel zijn.

5.2.3 Kosten

Zoals hoger gezien zijn de kosten minimaal. Een netwerkkaart in elke pc (ongeveer 40 € /kaart), netwerkkabel (ongeveer 1€/m) en nog wat bijkomende onderdelen afhankelijk van het type netwerk je wilt leggen (terminator, t-stukjes, hub/switch, RJ45-connectoren, ...). Een kostprijs van 50 €/pc zal een goede raming zijn van de kostprijs van een peer-to-peer netwerk.

5.2.4 Besturingssysteem

Qua besturingssysteem is er ook geen enkel probleem omdat Windows vanaf de versie Windows 3.11, en dus ook alle latere versies een peer-to-peer-netwerk module in zich hebben. Enkel het configureren van deze netwerksoftware vraagt wat kennis, maar daarvoor zit je op deze cursus, ... of niet soms ?

5.2.5 Implementatie

Zoals reeds voldoende benadrukt is het configureren van het netwerk niet zo een moeilijke opdracht. Op elke pc een aantal netwerkparameters instellen en klaar-is-kees. Het netwerk zoekt zelf de andere clients enkel moeten de gebruikers de bronnen die zij ter beschikking willen stellen in het netwerk, gedeeld plaatsen.

5.2.6 Toepasbaarheid

Dit netwerktype is overal toepasbaar. Van zodra je denkt aan communicatie tussen twee pc's of het gezamenlijk gebruiken van een toestel kan je een peer-to-peer netwerk leggen. Privé-toepassingen (delen van een printer of internet-toegang) tot het netwerk van een middelgrote KMO met een aantal werkstations kunnen van het type peer-to-peer zijn.

5.2.7 Algemene overweging

Een peer-to-peer netwerk is zeer eenvoudig in gebruik. Het behoeft geen specifieke kennis en is zeer goedkoop in installatie. Een groot nadeel is de beveiliging van het netwerk. Doordat elke gebruiker zijn eigen pc beheert is het onbegonnen werk om dergelijk netwerk tot in de details te beveiligen. Dit zal dan ook één van de grote redenen zijn dat men beslist om naar een server-based netwerk over te stappen.

5.3 Client-Server of Domein netwerken (= gecentraliseerd netwerk)

5.3.1 Eigenschap

Een Client-Server netwerk (ook soms Server-Based netwerk genoemd) begint als een uit-de-kluiten-gewassen peer-to-peer netwerk. Het is een netwerk waarbij een server (en de nodige netwerksoftware) het netwerk beheert, controleert en beveiligt.

Een netwerkserver (hardware) draait een client-server-besturingssysteem zoals Windows NT Server, Windows 2000 Server, Windows 2003 Server, Linux, ... waardoor het beheer (waar mogen documenten geplaatst worden, wie mag welke documenten bekijken, lezen, ..., wie heeft toegang tot bepaalde gedeelde bronnen, ...) centraal geregeld wordt door een netwerkbeheerder.

Op elk werkstation kan een gebruiker inloggen op het netwerk, het beheerssysteem bepaalt welke toegangsrechten een gebruiker heeft. Door deze toegangsrechten wordt de vrijheid van de gebruiker beperkt. Hierdoor wordt het netwerk beheersbaar en controleerbaar, wat de bruikbaarheid en de veiligheid bevordert.

Fysiek is er slechts één groot verschil tussen een peer-to-peer en een client-server netwerk : deze laatste heeft een hardware server met een speciaal netwerk-besturingssysteem waardoor grotere netwerken mogelijk zijn.

5.3.2 Grootte

Server-based netwerken beginnen klein. Vanaf een 10-tal gebruikers is het al verantwoord om een server in je netwerk te plaatsen. Een server-based netwerk kan zeer groot worden tot verschillende duizenden pc’s in één netwerk. Uiteraard zal dit niet door één server beheerd worden, maar zullen daarvoor meerdere servers in het netwerk geplaatst worden.

5.3.3 Kosten

De meerkost zit vooral in de aanschaf van een server (vanaf ong. € 3000,-) en het speciale besturingssysteem (vanaf ong. € 1500). In een klein netwerk moet men geen beheerder in het kostenplaatje

steken (een collega zal dit wel doen tijdens zijn uren). In een groter netwerk wordt een netwerkbeheerder echter wel nodig en drijft dit uiteraard ook de kosten op.

5.3.4 Besturingssysteem

Een speciaal besturingssysteem zoals Windows 2000, Windows 2003, Novell Netware, Linux of nog andere is nodig. Deze software staat in voor het beheer van het netwerk. De netwerk-beheerder (Administrator) staat in voor het beheer.

5.3.5 Implementatie

Het configureren van een client-server netwerk is geen sinecure. Kennis van het netwerkbesturingssysteem is noodzakelijk. Vandaar dat de cursus “Client-server netwerken” ingericht wordt.

Ervaring en dagelijks bezig zijn met deze materie zijn een must wil je een goede netwerkbeheerder worden. Een netwerk van een 50-tal pc geeft al een parttime job voor een netwerk-administrator (beheerder).

5.3.6 Toepasbaarheid

Gezien de hogere kostprijs (naast de netwerkkaarten in de pc’s en de bekabeling die ook hier nodig is) is dit soort netwerken maar mogelijk bij grotere firma’s waar verschillende pc in een netwerk moeten worden geplaatst. Privé is dit voorlopig geen haalbare kaart. Maar in informatica weet je maar nooit. Alhoewel dat ik niet verwacht dat in privé-omgevingen zal gewerkt worden met servers en speciale netwerk software.

5.3.7 Algemene overweging

Een server-based (client-server) netwerk is enkel voor grotere netwerken waar beheersbaarheid en veiligheid van de gegevens zeer belangrijk is. Het vraagt een goede kennis de netwerksoftware. Gezien de grootte van dergelijke netwerken is een netwerkbeheerder algauw geen overbodige luxe.

5.4 WLAN

Deze afkorting staat voor **Wireless LAN** en duidt op een LAN waarin draadloze verbindingen worden gebruikt tussen computers.

Dit soort netwerk kan gebruikt worden op plaatsen waar het niet mogelijk is om bekabeling te leggen.

Let op voor War-chalking!!!

Het aanbrengen van merktekens (meestal met krijt) op de buitenkant van gebouwen, waardoor passanten kunnen zien dat er een WLAN draait. Bij War-chalking worden diverse symbolen gebruikt om aan te geven of het WLAN voor iedereen (binnen en buiten) toegankelijk is, of dat een wachtwoord vereist is. War-chalkers maken gebruik van snuffelsoftware om WLAN's op te sporen.

Een site waar uw WLAN misschien vermeld is **www.wardrivemap.com**

5.5 Hybride netwerken

In vele netwerken worden **Client-Server netwerken** gecombineerd met **Peer-to-Peer netwerken**. Dergelijke netwerken noemt men hybride netwerken.

Zo een netwerk beschikt over een Client-Server operating system zoals Windows 2000 of Windows NT. Deze software wordt gebruikt voor centrale opslag van de bestanden en de validatie van de gebruikers. Ook de backup wordt verzorgt door de server.

De client computers kunnen zich echter onderling verbinden voor printersharing of het gebruik van lokale data. Niet al de shared resources bevinden zich dus op de servers.

Hybride netwerken zijn vaak zéér nuttig, maar moeilijk te onderhouden en ook is niet altijd duidelijk wie voor wat verantwoordelijk is!

5.6 Samenvattend overzicht

Samenvattend kunnen we stellen dat er twee soorten netwerken zijn : peer-to-peer netwerken en client-server netwerken. Beiden hebben dezelfde grootte doelstelling : communicatie tussen verschillende computers en andere toestellen. Gezien de specifieke problemen (beheersbaarheid en veiligheid) bij een

groter wordend netwerk is een peer-to-peer netwerk voor kleine netwerken, terwijl een client-server netwerk noodzakelijk is bij veel netwerkgebruikers.

Er is een duidelijk verschil in het prijskaartje : een peer-to-peer netwerk is goedkoop en even efficient in kleine netwerken. Een client-server netwerk kost, gezien de extra investeringen, heel wat meer en is dus enkel te verantwoorden in grote netwerken.

Wanneer je vreest voor de veiligheid van je gegevens en deze veiligheid is belangrijker dan de extra kostprijs, dan moet je een client-server netwerk nemen ook al heb je maar 5 of 6 pc’s in je netwerk. Sommige software bestaat enkel in een client-server versie. In dergelijke situaties moet je wel naar een server-based netwerk gaan alhoewel je misschien maar 3 of 4 pc’s in je organisatie gebruikt.

6 Hoe een netwerk maken

6.1 Netwerk topologieën

Netwerktopologie betekent de beschrijving van hoe een netwerk er uit ziet, de fysische plaatsing van de computers, bekabeling en apparatuur. Het gaat dus over het ontwerp van het netwerk. Meestal kan zo een ontwerp in een diagram weergegeven worden.

Gegevens worden tussen computers onderling doorgegeven door middel van elektrische signalen op de kabel(s) die hen verbinden. Opdat een computer zou herkennen dat een signaal voor hem bestemd is moet iedere computer een adres hebben en moet het signaal het bestemmings-adres met zich meedragen. Het is zo dat niet de computer een adres heeft, maar de netwerkkaart die erin zit heeft wel een adres. Dit adres zit hardwarematig ingebakken in de kaart door de leverancier van de kaart. De leverancier van de kaart zorg ervoor dat het adres wereldwijd uniek is.

Om communicatie tussen twee computers te hebben is er dus altijd minstens een adres nodig. Samen met het adres wordt de te verzenden data omgezet in signalen op de bekabeling.

Het is de topologie die bepaald hoe die signalen hun weg vinden en hoe de computers er op reageren.

Er zijn 3 standaard topologiën.

- Bus
- Ster
- Ring

6.1.1 Bus

Dit is de eenvoudigste en meest gebruikte topologie. Het bestaat uit een lange kabel waarin alle apparatuur is aangesloten. Vergelijk het met een straat waarin ieder huis op de waterleiding is aangesloten.

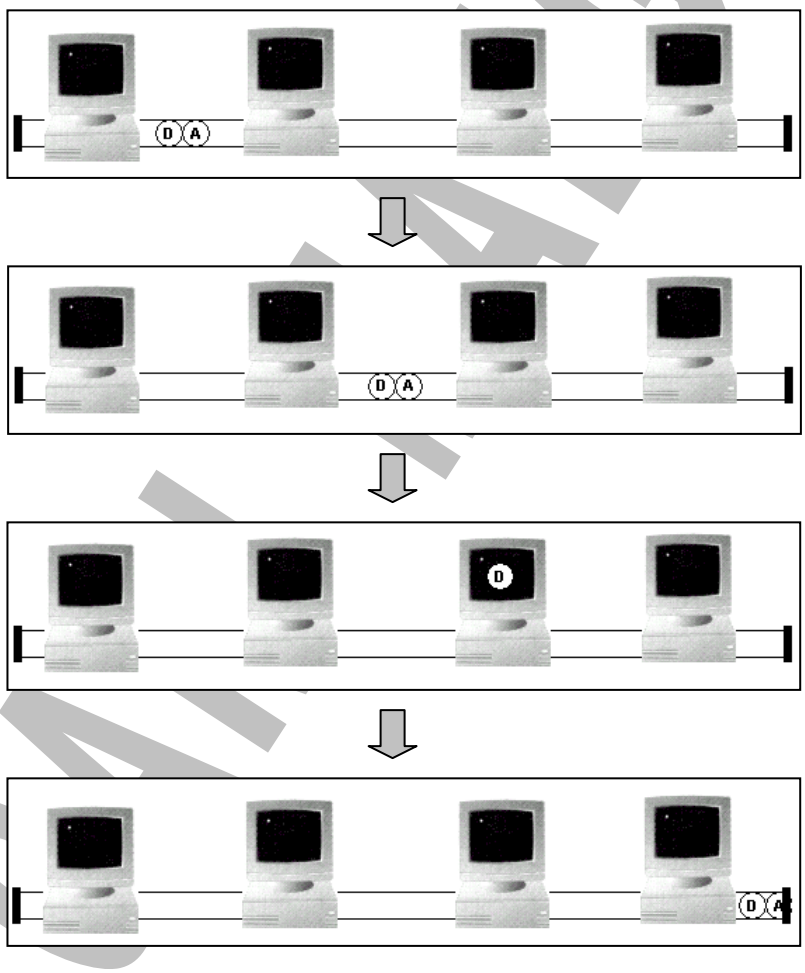
Het signaal passeert alle computers. Hierdoor ontvangt iedere computer het signaal, terwijl het slechts voor 1 bepaalde computer bestemd is. Een computer die een signaal krijgt die niet voor hem bestemd is doet hier verder niets mee. Het signaal zal zijn weg verder zetten totdat het de computer tegenkomt waarvoor het bestemd is. Daarna is het signaal niet meer aanwezig op de kabel.

Wanneer er een signaal gegeven wordt, bestemd voor een computer die niet bestaat komt het op het eind van de kabel. Hierdoor stopt het signaal met bestaan.

Op het ganse netwerk kan slechts 1 computer tegelijkertijd verzenden. De andere moeten wachten. Hoe meer computers in het netwerk, hoe trager het netwerk zal gaan. Dit is een belangrijk nadeel van de Bus topologië

6.1.1.1 Werking

- Een computer die iets zendt stuurt de data, voorafgegaand door het adres, op de bus.
- Het pakket komt voorbij iedere computer op het netwerk. Elke computer gaat op zijn beurt na of het pakket voor hem bestemd is. Is het niet voor hem bestemd hoeft de computer niets te doen, het pakketje zet vanzelf zijn weg verder.
- Komt het pakketje aan bij de bestemmingscomputer dan zal deze het verwerken.
- Is er geen enkele computer die aan het bestemmingsadres voldoet zal het pakketje geabsorbeerd worden door de terminator.



6.1.1.2 De noodzaak van een terminator

Een terminator op het eind van een kabel zorgt ervoor dat het signaal waarvan de bestemming niet bestaat van de kabel verdwijnt. De terminator absorbeert als het ware het signaal. Zonder die terminator zou het signaal blijven op het netwerk circuleren en zou het onmogelijk zijn een tweede signaal te sturen. Hierdoor ligt het ganse netwerk plat.

6.1.1.3 Breuken in de kabel

Door een breuk in de kabel wordt het netwerk ongewild in tweeën gesplitst. Dit heeft niet alleen als gevolg dat een computer in het ene deel geen computer in het andere deel kan bereiken, maar door de breuk ontstaan twee netwerken die elk een einde hebben die geen terminator heeft. Beide stukken zullen niet meer werken.

6.1.1.4 Passieve technologie.

De bus is een passieve topologie. Dit wil zeggen de netwerk-onderdelen sturen het binnenkomende signaal, dat niet voor hen bestemd is, niet uit zichzelf verder. Het signaal zal zonder tussenkomst van de netwerkkaart zijn weg verder zetten. Dit heeft als voordeel dat wanneer een computer defect is dit geen invloed heeft op de rest van het netwerk.

6.1.1.5 Uitbreiding van het netwerk.

Om een bestaand netwerk uit te breiden moet de kabel dus langer gemaakt worden.

Dit kan door een nieuw stuk kabel aan de bestaande te hangen door een barrel connector. Een barrel connector is dus een metalen stuk om tussen twee einden kabel te steken die het signaal verder leidt. Probleem hierbij is dat het signaal veel zwakker wordt en dit kan tot vertraging en niet werken van het netwerk leiden.

Beter is een repeater te plaatsen. Dit is een apparaat die twee stukken kabel aan elkaar verbindt en het signaal elektrisch versterkt. Zo kan het signaal veel verder reizen en toch nog correct ontvangen worden.

6.1.2 Star

In de star topologie zijn de computers geconnecteerd via een centraal stuk apparatuur. Dit is de hub. Elke computer heeft een kabel die naar de hub leidt. Een hub heeft dus minstens zoveel uitgangen als er computers zijn. Signalen van een computer komen in de hub aan en deze stuurt het signaal over elke andere uitgang verder. De signalen worden toch naar elke computer gestuurd. Elk van hen moet controleren of het voor hen bestemd is.

Door deze topologie valt het probleem van terminator weg, want elke netwerkkaart absorbeert het signaal.

Een breuk in een kabel levert slechts een probleem op voor die ene computer aan deze kabel verbonden. De rest van het netwerk kan verder werken.

Dit zijn voordelen tegenover de bus technologie. Nadeel is dat een hub dient aangeschaft te worden en dat heel wat meer bekabeling moet aanwezig zijn.

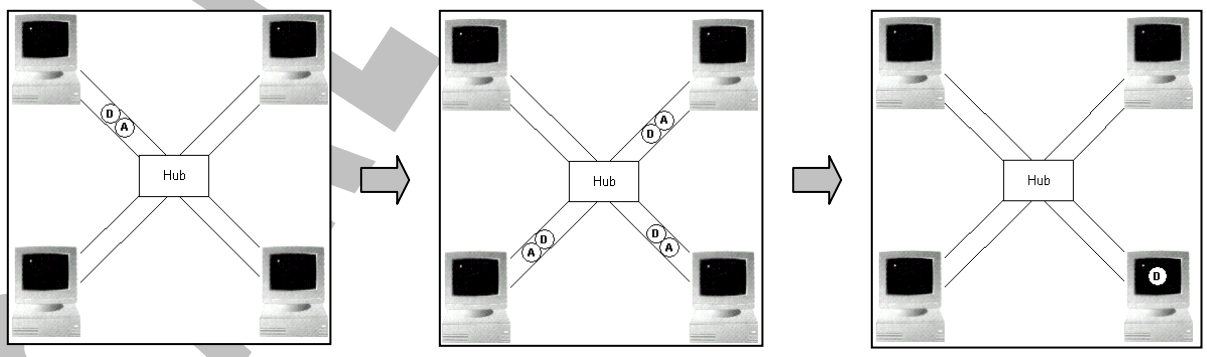
Ander voordeel is dat een computer een signaal kan sturen vanaf dat een ander signaal is vetrokken uit de hub.

Hubs zijn momenteel vrij goedkoop en in alle maten en vormen leverbaar. Moderne versies van hubs zijn intelligenter. Ze sturen het signaal niet langer naar alle andere uitgangen, maar weten naar welke uitgang precies het signaal verder moet gestuurd worden. Men spreekt niet meer van hubs, maar van stacks of switches.

De computers moeten het signaal dat niet voor hen bestemd is, niet verder sturen, want elke computer is als het ware het eindpunt. Het is de hub die de signalen verderstuurt. Star is dus ook een passieve topologië.

6.1.2.1 Werking

- De computer stuur het adres en de data naar de hub.
- De hub stuurt het pakket op elke uitgang verder waardoor elke computer het pakket ontvangt en evalueert of het voor hem bestemd is.
- De computer voor wie het pakket bestemd is verwerkt het.



6.1.3 Star bus

Dit is de combinatie van een star en een bus. Hier zijn meerdere hubs aanwezig die aan elkaar verboden zijn via 1 kabel (=bus), maar rond elk van de hubs is er een ster-topologië.

Deze combinatie topologie komt typisch voor in kantoren met verdiepingen. Op elke verdieping is er een hub voorzien. Verticaal over de verdiepingen heen is er een kabel.

Momenteel ziet men meer en meer star topologiën komen. Dit komt voort uit de duidelijke voordelen tegenover de bus topologie en de lage prijzen van de hubs.

6.1.4 Ring

In een ring topologie hangen de computers aan één kabel zoals in de bus topologie, maar deze kabel eindigt waar hij begint. Er zijn geen terminators nodig.

In de ring loopt constant een signaal rond, het stopt nooit. Het zijn wel de computers die het signaal verder moeten sturen. Daarom is dit een actieve topologie. Eén voor één krijgt iedere computer het signaal dat ze zelf moeten verdersturen. Als een netwerkkaart van één computer defect is ligt ook het ganse netwerk uit.

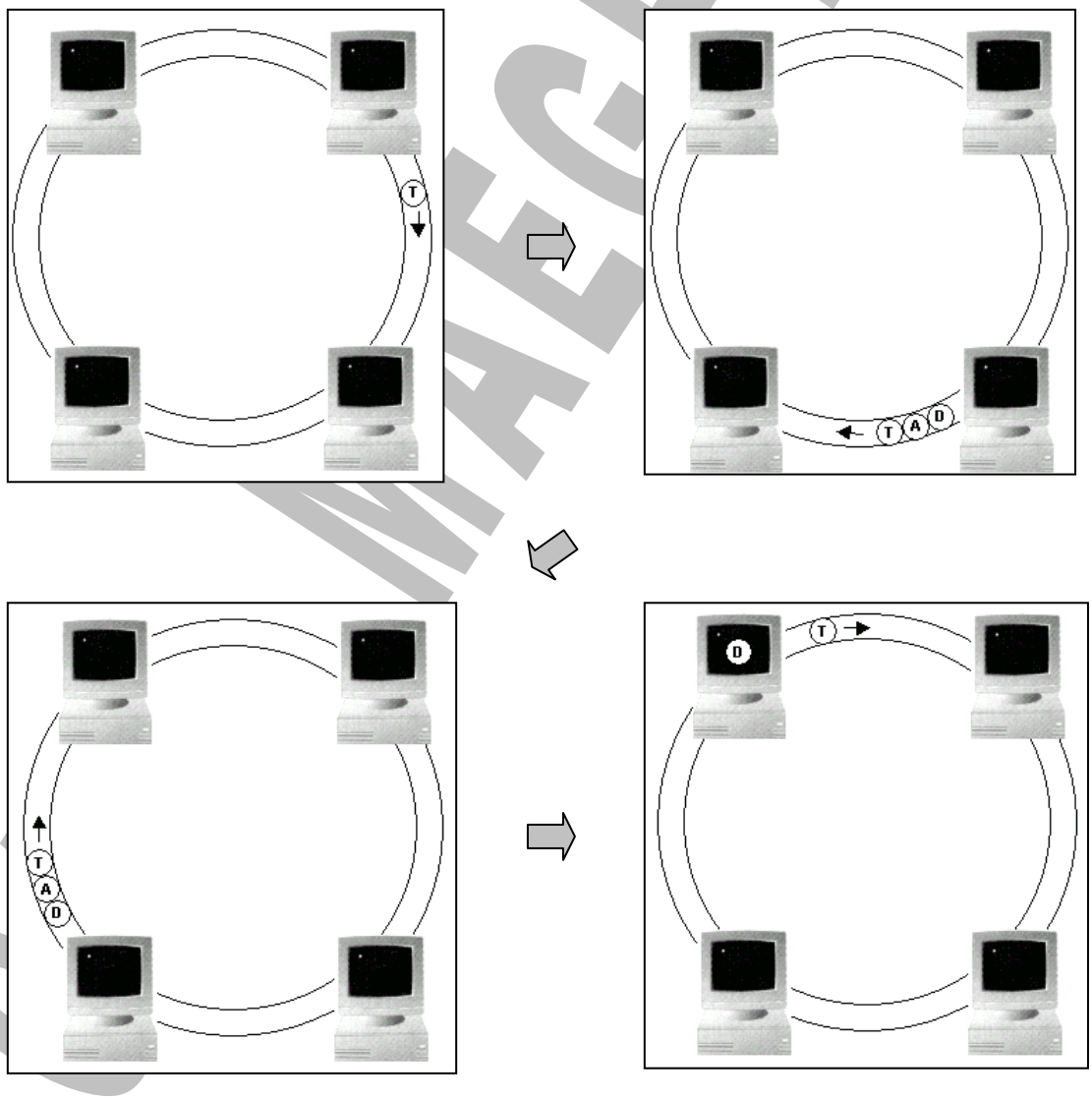
Het signaal dat rondgestuurd wordt noemt met het token. Wanneer het token in een computer terecht komt kan hij dit signaal aanvullen met een bestemmings-adres en het verder sturen naar de volgende computer. Deze zal het signalen binnenkrijgen en gebruiken als het voor hem bestemd is en verder sturen wanneer niet. Wanneer een computer een signaal binnenkrijgt kan hij het token gebruiken om terug een ander computer te contacteren.

Wanneer de computer beslist niets verder te sturen, stuurt hij het token verder naar de volgende computer die het op zijn beurt kan gebruiken.

Het lijkt alsof dit alles heel traag zal werken, maar dit is niet zo. Een tokensignaal draait in een ring van 200 meter ongeveer 10.000 keer rond in 1 seconde.

6.1.4.1 Werking

- Het token circuleert op het netwerk.
- Een computer die iets wil zenden wacht tot het token passeert en plaatst er het bestemmings-adres en de data achter. Het token is nu niet meer vrij en kan niet meer door een andere computer gebruikt worden.
- De volgende computer in de ring ontvangt de serie van token, adres en data. De computer evalueert aan de hand van het bestemmings-adres of het pakket voor hem bestemd is. Zoniet stuurt hij het verder.
- Wanneer de computer die de serie ontvangt wel het bestemmings-adres is, verwerkt deze de data. Onmiddellijk daarna stuurt hij het vrije token zonder bestemmings-adres en data terug op de ring. Hierdoor is het token terug vrij en kan een andere computer het gebruiken om data te verzenden.



6.2 Bouwstenen van een netwerk

Uit de definitie blijkt dat een netwerk uit verschillende onderdelen bestaat. Een overzicht van de verschillende mogelijke toestellen die in een netwerk elk hun eigen functie hebben is belangrijk om inzicht te krijgen in de werking van een klein tot groot netwerk.

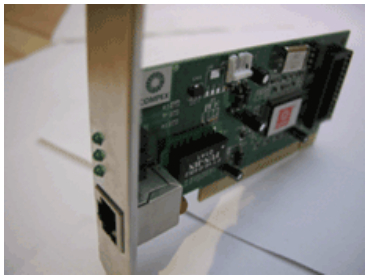
Niet alle toestellen in dit overzicht zullen in elk netwerk zitten. Afhankelijk van de functie, de grootte en de financiële mogelijkheden zal een keuze gemaakt worden uit de verschillende apparaten.

6.2.1 Bouwstenen voor een thuisnetwerk

6.2.1.1 Netwerkkaart voor een PC

Voordat je het eigenlijke netwerk gaat aanleggen moet elke computer uitgerust zijn met een netwerkkaart.

Vaak hebben computers een ingebouwde netwerkkaart op het moederbord. Zo niet, dan wordt er gebruik gemaakt van een PCI netwerkkaart die in een PCI slot op het moedebord gezet wordt (zie afbeelding).



De gangbare snelheid voor netwerkaarten was 10/100 Mbits. Tegenwoordig is 1 Gigabit de gangbare snelheid. 1 Gigabit maakt een doorvoersnelheid van zo'n 1000 Mb per seconde mogelijk, mits er aan de andere kant ook een 1 Gigabitskaart aanwezig is natuurlijk.

Netwerken basis – Labo 002 – Installatie van een netwerkkaart

6.2.1.2 PC-kaart (PCMCIA-kaart) voor een notebook

Deze kaart heeft de vorm van een dikke netwerkkaart en wordt gebruikt (althans vroeger) om draagbare computers (waar geen netwerkkaart ingebouwd zit) aan te sluiten op het netwerk. De huidige generatie van portables heeft een netwerkkaart ingebouwd waardoor deze PC-kaarten vermoedelijk in deze functie stilaan zullen verdwijnen. De PC-kaart wordt nu nog wel gebruikt om draagbare computers op een draadloos netwerk aan te sluiten. Doch nu ook al beginnen de producenten van draagbare computers een draadloze netwerkinterface te integreren.

6.2.1.3 Draadloze netwerk-interface voor een PC of notebook

Een “wireless”-netwerkinterface is een zender die aan de client wordt gekoppeld zodanig dat deze kan verbinding maken met een “wireless”-station. Deze interface (recentelijk op de markt – dus nog heel wat evolutie te verwachten) kunnen in de vorm van een netwerkkaart, PC-kaart of USB-zendstation gekocht worden. Zij hebben telkens dezelfde functie. Signalen die draadloos verzonden worden door het station op te vangen en door te geven aan de client die op zijn beurt signalen terug zendt naar het station.

6.2.1.4 Modem

Een modem is een apparaat dat 2 computers (of andere apparaten) met elkaar verbindt over een telefoonlijn. Aangezien de telefoonlijn slechts analoge signalen kan verzenden moet hier een omzetting van digitale signalen naar analoge signalen gebeuren. Dit is de belangrijkste taak van de modem. Het signaal moet ge**MO**duleerd worden en aan de ander kant van de lijn ge**DEM**oduleerd worden.

Een modem kan ofwel intern in de computer ingebouwd worden ofwel aangesloten worden op de RS232 communicatiepoort (serieel).

De standaard die in modems gebruikt worden is de Hayes standaard. Hierdoor kunnen communicatie-programma’s alle modems besturen.

De modem is een zeer traag apparaat, maar hieraan ligt het feit dat onze telefoonlijnen nooit voorzien zijn om er data over te transporteren.

De snelheid van een modem wordt uitgedrukt in Baudrate. Dit is de snelheid waarover een signaal verstuurd wordt over de lijn. Het gaat hier wel over ongecomprimeerde data. Vroeger kwam 300 baud overeen met 300 bps. Door compressie-algoritmen kan een 28.800 baud modem momenteel tot 115200 bps verzenden.

Verwar deze apparaten NIET met breedband-modems!!!

Het principe van een binair signaal omzetten naar een ander is hetzelfde, maar dan met een technologie die veel hogere datatransfersnelheden toelaat (kabel-modem of ADSL-modem)

6.2.1.5 Hub en switch

Een hub of switch is een netwerkkruispunt. Hubs en switches zijn voorzien van poorten om UTP kabels in te steken. Je kunt zo netwerkcomputers met elkaar verbinden.

Een hub en een switch voeren dezelfde taak uit op een verschillende manier. Een switch stuurt data direct naar de juiste computer door, terwijl een hub data stuurt naar alle computers in een netwerk. De computers beslissen dan zelf of de data voor hen bestemd is of niet.

Het snelheidsverschil is voor thuisnetwerken echter niet merkbaar bij het surfen op internet, maar wel bij het versturen van bestanden tussen netwerkcomputers. Een switch is aan te raden, zeker gezien het geringe prijsverschil met een hub.

Het uitzicht van beide is gelijk. Op het zicht is het dus niet mogelijk een onderscheid te maken tussen een hub en een switch. In het gebruik daarentegen voel je duidelijk een snelheidsverschil.

Op dit moment wordt eigenlijk nog alleen switches verkocht. Er worden echter in oudere netwerken nog altijd hubs gebruikt. Stilaan worden die wel vervangen en zullen op termijn hubs verdwijnen uit het “straatbeeld”.

6.2.1.6 Router

Een router is een apparaat dat simpel gezegd 'verkeer regelt' tussen twee netwerken. In een thuisnetwerk staat de router tussen het thuisnetwerk en het grootste netwerk ter wereld, het internet. De router is daartoe aan de ene kant verbonden met een internet modem en aan de andere kant met het thuisnetwerk.

Routen kan met behulp van een hardware router of een software router.

Een **hardware router** is een apparaat dat speciaal gemaakt is om te router (zie afbeelding). Een router is vaak gelijk voorzien van een switch. Je kan er dus direct netwerkcomputers in pluggen zonder dat je daar nog een aparte switch of hub voor nodig hebt.

Een hardware router van SMC. Zoals je ziet kun je in de ingebouwde switch aan de achterkant direct een aantal (4) UTP kabels steken.

Een **software router** is een computer waarop routing software draait. Gebruik je een computer als router, dan gebruik je een aparte switch. De router computer is voorzien van twee netwerkverbindingen: een met de modem en een met de hub of switch.

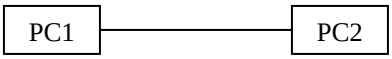
Het **voordeel van een hardware router** is dat je maar 1 klein apparaatje hebt dat constant aan staat om een internetverbinding voor alle netwerkcomputers mogelijk te maken. Dit kost minder energie, maakt minder herrie en neemt minder ruimte in.

Bij het gebruik van een software router moet de computer met de routing software (bijvoorbeeld Windows ICS) aan staan als de rest van het netwerk gebruik wil maken van internet. Dit kost dus relatief veel energie, etc.

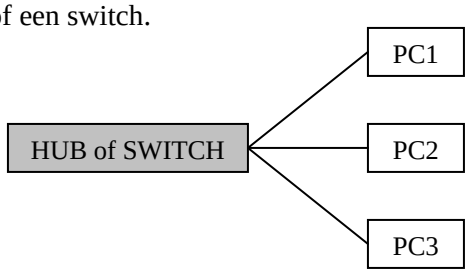
Het **voordeel van een software router** is weer dat je er met behulp van software leuke trucken mee kunt uithalen (snelheidslimieten instellen, een firewall naar eigen keuze gebruiken, etc).

6.2.1.7 Verschillende opstellingen om een thuisnetwerk aan te leggen

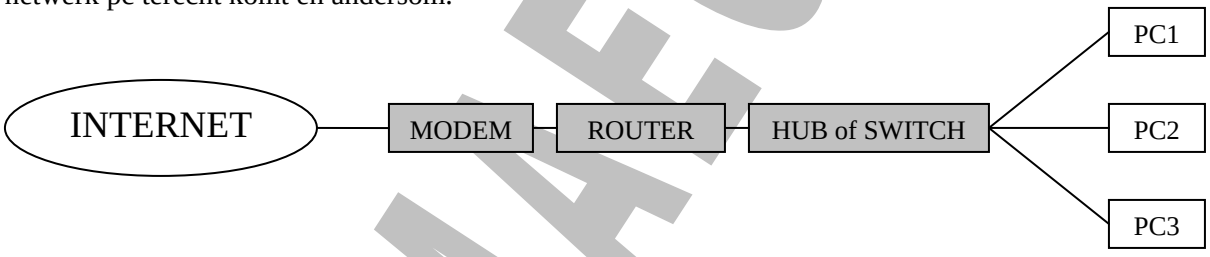
Het simpelste thuisnetwerk bestaat uit 2 computers die verbonden zijn met een crossover UTP kabel. Er is geen switch of hub nodig.



Wil je een netwerk aanleggen met meer dan 2 computers dan worden de netwerkcomputers verbonden met een hub of een switch.

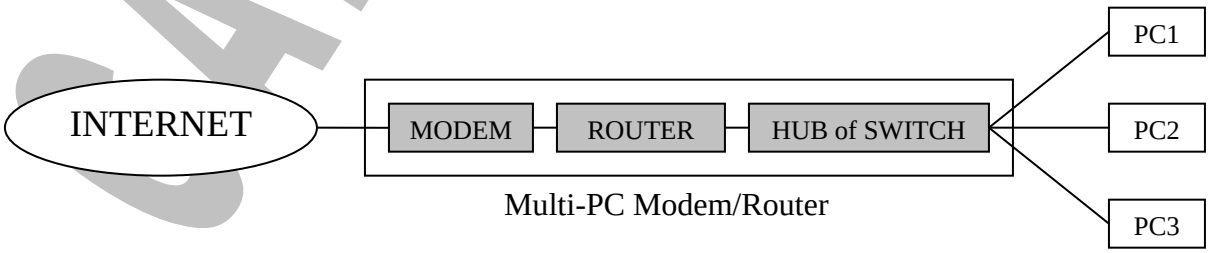


Als je op je netwerk een internetverbinding gaat delen dan moet er tussen de twee netwerken, internet en het thuisnetwerk, een apparaat staan dat het verkeer regelt: een router. De router komt tussen de switch of hub en de modem. De belangrijkste taak van de router is zorgen dat verkeer vanaf het internet op de juiste netwerk pc terecht komt en andersom.

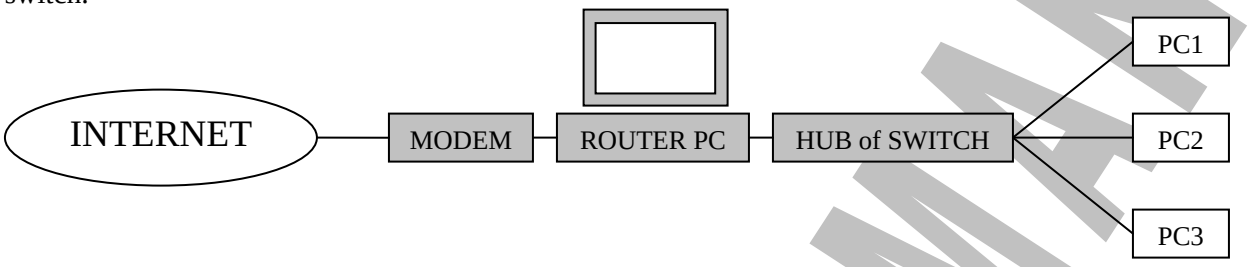


Gecombineerde modems, routers en switches

Het overzicht van een thuisnetwerk met gedeelde internetverbinding hierboven is de meest gangbare opstelling voor een thuisnetwerk. De modem, router en hub of switch kunnen 3 verschillende apparaten zijn, maar er zijn ook geïntegreerde oplossingen verkrijgbaar. Een hardware router heeft bijvoorbeeld bijna altijd een ingebouwde switch. Meestal kan je daarom op een hardware router direct 4 tot 8 computers aansluiten. Onder de naam modemrouter of multi-pc modem worden apparaten verkocht, die zowel een modem, een router als een switch ingebouwd hebben. Een echte totaaloplossing dus. Vaak hangt het van de internetprovider af welke oplossingen aangeboden en ondersteund worden.



Bij een netwerk met software routing zijn modem, router pc en hub of switch aparte apparaten. De router pc heeft twee netwerkverbdindingen, één verbinding met de modem en één verbinding met de hub of switch.



6.2.2 Bouwstenen voor grotere netwerken

6.2.2.1 Server

Een server is een speciale computer die een centrale rol speelt in grotere netwerken. Gezien de belangrijkheid van dit toestel heeft een server ook een betere architectuur dan een gewone pc. Snellere interne communicatie, een snellere en grotere harde schijf (meestal meerdere harde schijven), een betere beveiliging tegen gegevensverlies (backup, RAID-controllers, ...) zijn enkele eigenschappen van een server.

In dit verhaal zullen we het ook hebben over DHCP-servers, DNS-servers, e.d. Daarbij wordt meestal een software-pakket bedoeld die een specifieke functie vervult in het netwerk. We spreken hier ook over een “server” terwijl het een programma is.

Een server kan dus in twee betekenissen voorkomen : hardware (computer) en/of software (programma). Een (software)server draait meestal op een (hardware)server. Er kunnen dus ook verschillende (software)servers op één (hardware)server draaien.

Samengevat kan je stellen : een server is een toestel of programma met een zeer specifieke controlerende of beherende functie in het netwerk.

6.2.2.2 Client

De gebruikers in een netwerk hebben toegang tot het netwerk via een client. Een client is meestal een PC met de nodige software die gebruik maakt van gegevens en toestellen op het netwerk. Een client noemt men ook “host”. Eigenlijk is een server ook een client van het netwerk. Het is echter een client met een speciale functie : controle en beheer van het netwerk.

6.2.2.3 Communicatie-media

De verschillende clients in het netwerk moeten per definitie met elkaar kunnen communiceren. Deze communicatie verloopt via verschillende media (kabels, zenders, ...).

6.2.2.4 Repeater

Signalen die over netwerkbekabeling gestuurd worden verzwakken na een bepaalde afstand. De repeater is een apparaat die er voor zorgt die signalen gehergenereerd worden. De repeater ontvangt het zwakke signaal en stuurt het versterkt signaal verder.

Repeaters kunnen ook gebruikt worden om van een bepaald kabeltype naar een ander kabeltype over te gaan. Repeaters bekijken de inhoud van de signalen niet. Hierdoor werkt een repeater op de physical layer.

Dit is het eenvoudigste en goedkoopste netwerkapparaat.

6.2.2.5 Bridge

Een bridge kan zoals een repeater het netwerk groter maken, maar doet meer. Terwijl een repeater elk signaal dat binnenkomt verder zendt zal een bridge slechts een deel van de signalen verder sturen.

Door een bridge te plaatsen krijgt men dus 2 netwerken. Een links en een rechts. De bridge oordeelt of een binnenkomend signaal voor het linkse of het rechtse deel bestemd is. Op basis hiervan zal het signaal doorgezonden worden of niet. Dit gebeurd door het controleren van het bestemmings-adres. Ligt het bestemmings-adres aan dezelfde kant als de verzender dan wordt het niet verder gezonden, zoniet wordt het verder gezonden op elke andere poort.

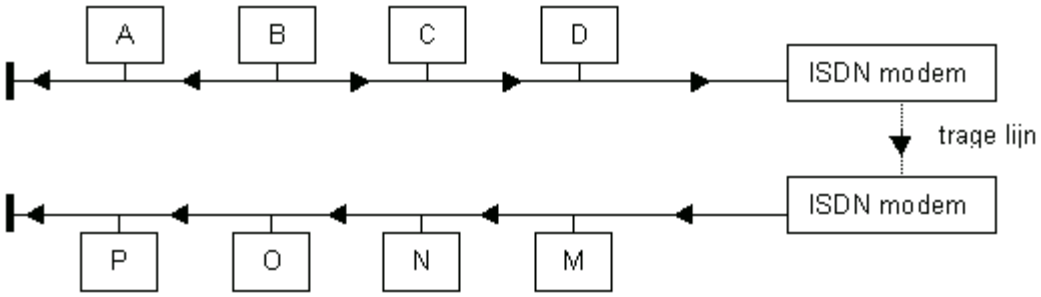
Een bridge wordt vooral gebruikt om een netwerk onder te verdelen in meerdere subnetwerken. Hierdoor wordt de traagheid van grote netwerken te omzeild.

Daar een signaal dat een computer over de kabel stuurt elke andere computer moet bereiken kan dit bij een groot aantal computers een traag netwerk opleveren. Wanneer een deel van de computers gescheiden zijn van de rest door een trage verbinding (modem of ISDN) zal dit zeker een probleem opleveren. Door net voor en net na de trage verbinding een bridge te plaatsen, wordt vermeden dat een signaal dat voor hetzelfde deel van het netwerk bestemd is als de zender, over deze trage lijn gaat.

Voorbeeld: Een netwerk bestaande uit 2 delen, elk met een 20-tal computers, gescheiden door een ISDN modem. Het netwerk werkt op 10 Mbs, de ISDN-lijn slechts op 64 Kbps. Het netwerk werkt dus 160 x sneller dan de trage verbinding ertussen.

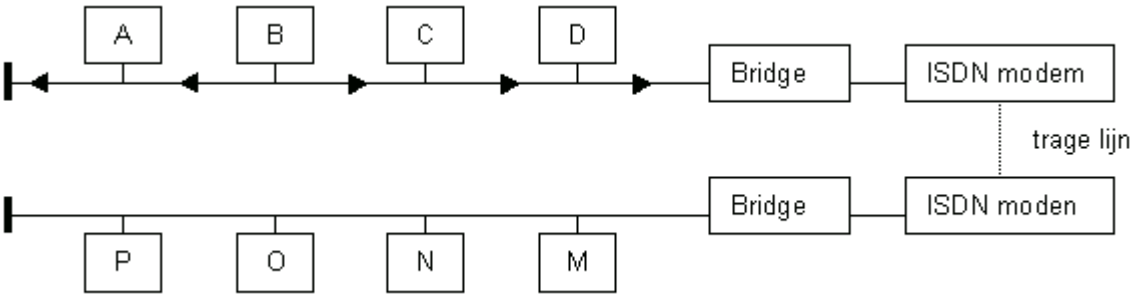
Situatie zonder bridge

Computer B zendt een signaal dat voor computer A bestemd is. In bepaalde gevallen komt het signaal over de trage lijn toch in het tweede netwerk terecht. De rest van het netwerk kan niet verder werken zolang het signaal niet geabsorbeerd is door de terminator.



Situatie met bridge

Computer B zendt een signaal dat voor computer A bestemd is. Wanneer het signaal op de bridge komt zal het niet verder gezonden worden aangezien de bridge weet dat de bestemmings-computers toch niet aan de ander kant kunnen liggen. De bridge absorbeert het signaal en het netwerk kan onmiddellijk verder werken.



Bridges bekijken dus ieder pakket. Ze onderzoeken het adres. Hierdoor werken bridges op de data link layer. Ze beslissen enkel over het al dan niet doorsturen van een pakket. Ze kunnen geen beslissing nemen over welke van de uitgangen moet genomen worden voor het vlugst bij de bestemming te zijn.

6.2.2.6 Router (uitgebreid)

Routers verdelen zoals bridges netwerken in meerdere subnetwerken, maar doen op hun beurt ook meer. Terwijl een bridge een signaal dat voor een ander deelnetwerk bestemd is op elke poort verder zendt zal een router dit slecht op 1 uitgangspoort verder sturen. Het is mogelijk ieder deelnetwerk een uniek nummer toe te kennen. De computers in een deelnetwerk weten dit netwerknummer. Dit netwerknummer wordt bij bepaalde netwerkprotocollen meegezonden met het bestemming-adres. Een router weet ook welke subnetwerken zich achter welke poort situeren. De router kijkt niet meer naar het bestemmingsadres in de data link layer, maar naar het netwerknummer in de network layer. Aan de hand hiervan zal de router beslissen op welke poort het signaal verder gezet moet worden.

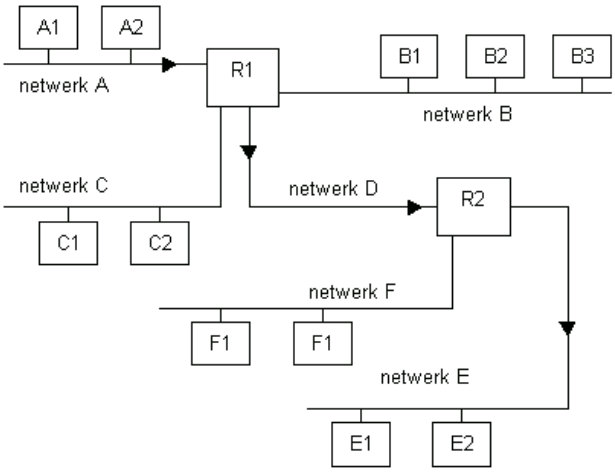
Routers worden gebruikt om netwerk in te delen in logische segmenten. Een bepaald segment kan dus van een ander gescheiden zijn door de router. De router zal intelligent gaan oordelen welk pakket naar welke poort gestuurd moet worden. Een router weet niet alleen het netwerknummer van het netwerk waaraan hij gekoppeld is maar ook van de netwerksegmenten verderop in het netwerk. Hierdoor kan de router beslissen welke de beste (=kortste) manier is voor het pakket om bij zijn bestemming te komen. De volgende router zal dit op zijn beurt ook doen.

Een router moet dus constant bijhouden welke netwerken er rond zich heen situeren, want een bepaald netwerksegment kan uitvallen of een betere weg om het te bereiken (=route) kan er bijkomen. Vandaar dat routers complexe en dure apparaten zijn.

Routers zijn het belangrijkste onderdeel van het internet. Internet is inderdaad een gigantisch groot netwerk van meerdere netwerksegmenten.

Een pakket moet gezonden worden van computer A2 naar computer E1. Computer A2 bevindt zich in subnetwerk A en computer E1 in subnetwerk E.

Het signaal komt binnen op router R1, deze beslist om het signaal verder te sturen naar netwerk D. Netwerk B en C krijgen het signaal niet. Router R2 krijgt het pakket en stuurt het verder naar netwerk E. Dit is het netwerksegment van de bestemmeling.



6.2.2.7 BRouter

Een Brouter is een apparaat dat tegelijkertijd bridge als router is. In normale omstandigheden werkt het identiek als een router. Pas wanneer een netwerkprotocol gebruikt wordt waarin geen netwerknummer met het signaal is meegegeven zal het principe van de bridge werken.

6.2.2.8 Gateway

Gateways zijn toestellen die totaal verschillende netwerken aan elkaar kunnen koppelen. Met totaal verschillend wordt bedoeld dat zowel bekabeling, topologie als netwerkprotocol verschillend kunnen zijn. Hierdoor moet ieder pakket volledig vertaald worden. Gateways zijn heel duur en dikwijls op maat gebouwd voor specifieke doeleinden. Bij connectie tussen normale LAN netwerken en een mainframe zijn ze zeker nodig.

6.2.2.9 Grote Switches

Switches zijn de nieuwste technologische aanwinsten in de netwerkwereld. Het zijn de duurste en ingewikkeldste apparaten. Om een netwerk groter en nog sneller te kunnen maken zijn manieren ontwikkeld om de pakketten nog sneller door te sturen. Om die snelheidswinst te halen worden de pakketten door de switch in kleinere pakketjes opgedeeld. Deze worden tegelijkertijd over verschillende netwerksegmenten naar de bestemming gestuurd. Door de switch geplaatst bij de bestemming worden alle pakketjes terug verzameld en in de correcte volgorde gezet.

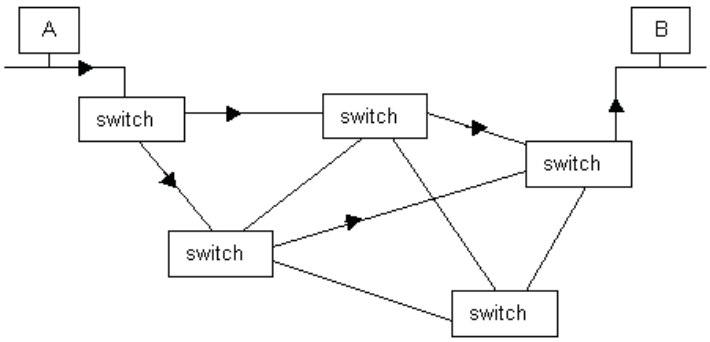
Switches gebruiken dus een Virtual Circuit van zender naar bestemming. Dit Virtual Circuit is de combinatie en opeenvolging van verschillende netwerken. Een Virtual Circuit kan tijdelijk (voor de tijdspanne van de verzending) of permanent zijn.

Switches worden gebruikt om geografisch grote gebieden te overspannen. Het zijn de grote communicatiereuzen die ze gebruiken om netwerk te verbinden.

Sommige switches vervullen ook routing functionaliteiten. Hierdoor zijn ze de schakels tussen de netwerken die het internet opmaken.

Er zijn 2 switching technieken :

- Frame relay
- ATM (asynchronous transfer mode)



6.3 Netwerk bekabeling

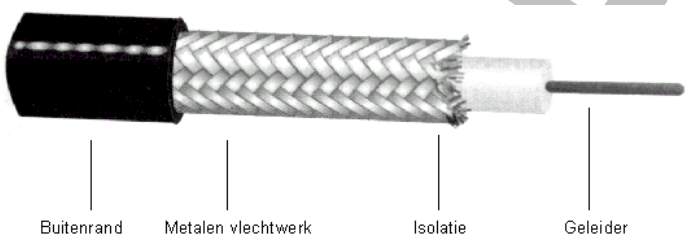
De bekabeling is de ruggegraat van het netwerk. Ze dient om de signalen en hiermee de gegevens van de ene pc naar de andere pc over te brengen. Er zijn verschillende types die kunnen gebruikt worden. Elk heeft zijn specifieke eigenschappen. Binnen elke type zijn er meerdere kwaliteiten.

Er zijn 3 groepen van typen :

- Coax kabel
- Twisted pair
- Fiber-optic

6.3.1 Coax

Coax bestaat uit een vaste koperen geleider die omgeven is door de isolatie, een metalen vlechtwerk en daarrond een plastic buitenrand. Langs de koperen geleider verplaatst het elektrische signaal zich. De isolatie houdt de geleider tegen om contact te hebben met andere geleiders. Het metalen vlechtwerk houdt elektrische signalen die van buitenaf kommen tegen, zodat ze het signaal op de geleider niet storen. De coax kabel heeft een heel sterke weerstand tegen storende signalen van buitenaf.



6.3.1.1 Types

Thin coax

Een buigzame kabel met een dikte van 0.25 inch. De kabel wordt rechtstreeks op de netwerkkaart aangesloten. De kabel is goedkoop en eenvoudig te installeren. Hierdoor wordt hij vaakst gebruikt in kantoren.

Thick coax

Een onbuigzame kabel van 0.5 inch doorsnede. De kabel wordt op een apart apparaatje los van de computer aangesloten. Dit apparaatje is op zijn beurt aan de computer gekoppeld. Thick coax heeft als voordeel dat het signaal erover verder kan gestuurd worden dan bij Thin. De weerstand tegen signalen van buitenaf is nog sterker. In industrieën en voor grotere afstanden is dit de aangewezen kabel.

Coax lijkt op de normale kabel die we kennen van de kabel-TV. Toch zijn ze niet onderling uitwisselbaar. Het verschil zit hem in de weerstandsfactor.

Crosstalk: is een storing van het signaal dat optreedt door dat meerdere kabels te dicht bij elkaar liggen. Hierdoor beïnvloedt de ene de andere kabel.
Attenuation: is het verlies van de signaalsterkte over een lange afstand.

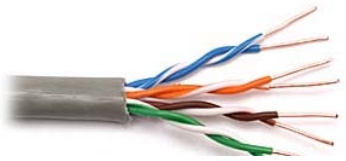
6.3.2 Twisted-pair

Twisted-pair bestaat uit twee geïsoleerde koperen draden die rond elkaar zijn gedraaid. De kabels voor normale telefonie zijn ook twisted-pair kabel. Doordat in vele kantoren reeds (ongebruikte) telefoonkabels liggen kunnen deze gebruikt worden.

6.3.2.1 Types

UTP (Unshielded Twisted-Pair)

staat voor Unshielded twisted-pair. Deze is flexibeler, maar heeft geen metaalfolie, enkel een plastiek omhulsel (net als STP).

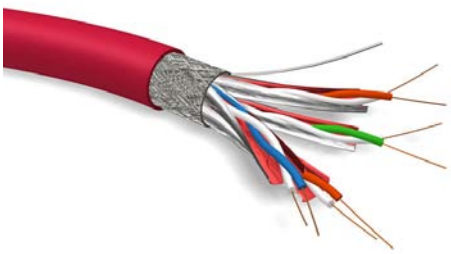


FTP (Foiled Twisted-Pair)

staat voor Foiled twisted-pair. Deze heeft enkel een metaalfolie om alle draden heen, niet per paar draden.

STP (Shielded Twisted-Pair)

staat voor Shielded twisted-pair. Dit houdt in dat iedere paar van draden omhuld is met een metaalfolie en dat het geheel van deze paren ook nog eens omhuld is met zo'n folie.



6.3.2.2 Categorieën

Onthou de volgende 3 categorieën van dit soort bekabeling. Een hogere categorie betekent een betere kwaliteit

5	Hoge snelheid tot 100 Mbps – UTP cat5
5e	Snelheid tot 1 Gbps – FTP cat5e
6	Snelheid tot 1 Gbps – STP cat6

Netwerken basis – Labo 003 – Straight- & Crossed-cable

6.3.3 Fiber Optic

Dit is glasvezel bekabeling. Hier is geen elektrische signaal maar er zijn lichtpulsen. Vanzelfsprekend is dit een heel snel medium. Het heeft totaal geen last van elektrische storingen.
Belangrijk bij dit soort kabels is, dat het signaal niet opgevangen worden van buitenaf. Hierdoor is het een veilige bekabeling, de data kan niet gestolen worden.

De kabel bestaat uit 2 heel dunne cilinders van glas. Deze zijn nogmaals door glas of plastic omgeven. Dit alles is nogmaals omgeven door een buitenrand in Kevlar. In de cilinder passeert de lichtpuls. Elke cilinder wordt in één richting gebruikt.

Snelheden kunnen tot 1 Gbps gaan.

Het nadeel van fiber optic kabels is dat ze heel erg duur zijn en dat het specialistenwerk is om ze te installeren.

7 Configuratie van een Point-to-Point netwerk

We gaan telkens **2 PC's verbinden d.m.v. een cross-cable** en we baseren ons hiervoor op het schema van het volgende labo:

Netwerken basis – Labo 004 – Point-to-Point netwerk

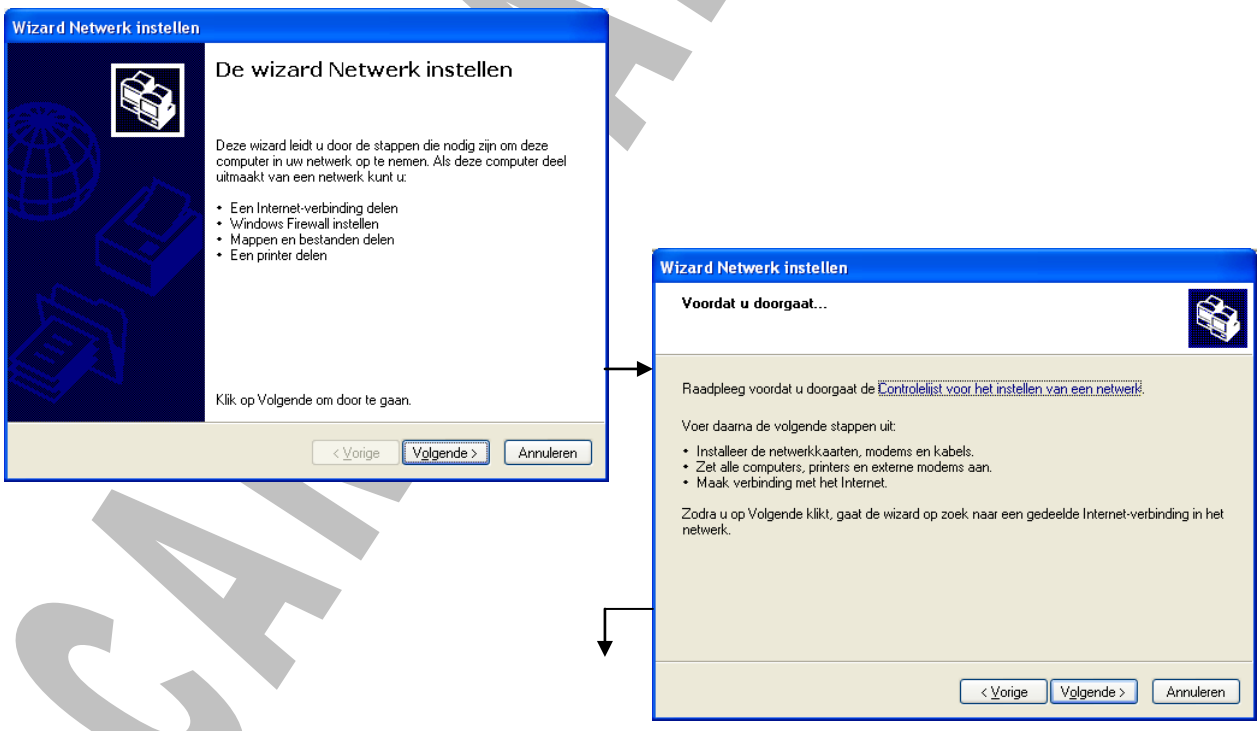
Om een PC in een Point-to-Point netwerk op te nemen gaat u als volgt tewerk:

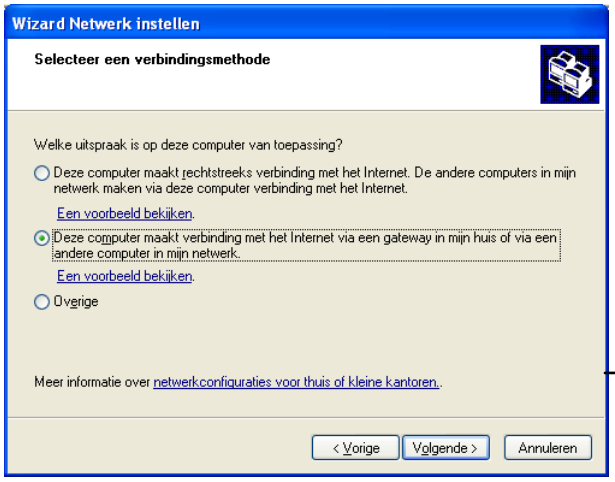
7.1 Instellen van de PC via "Wizard Netwerk instellen"

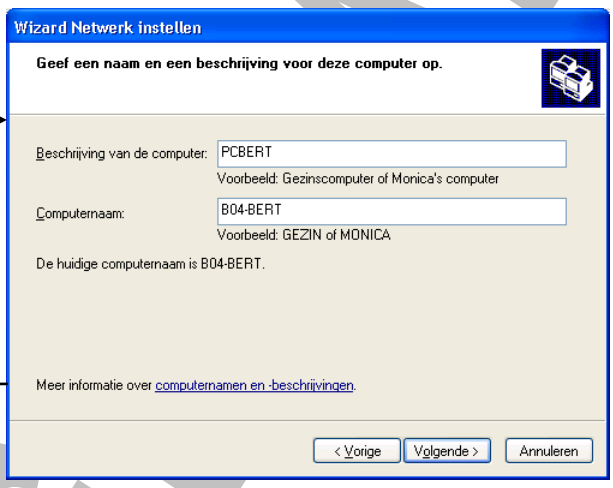
Deze wizard zorgt ervoor dat u via een hulpprogramma (Wizard) de volgende zaken zult instellen:

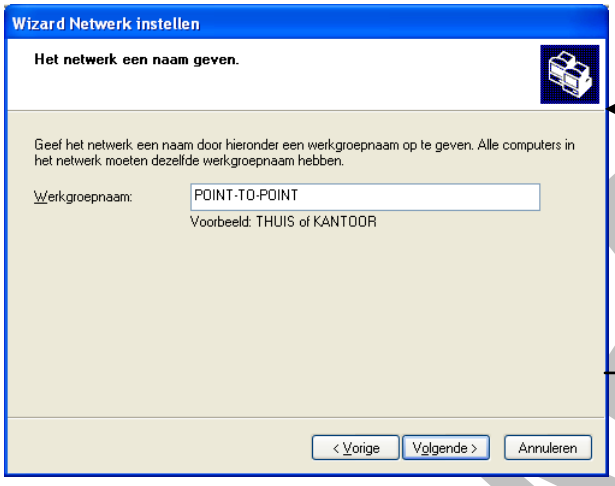
- Verbindingsmethode met het internet
- Beschrijving van de computer
- Computernaam
- Werkgroepnaam
- Bestands- en printerdeling

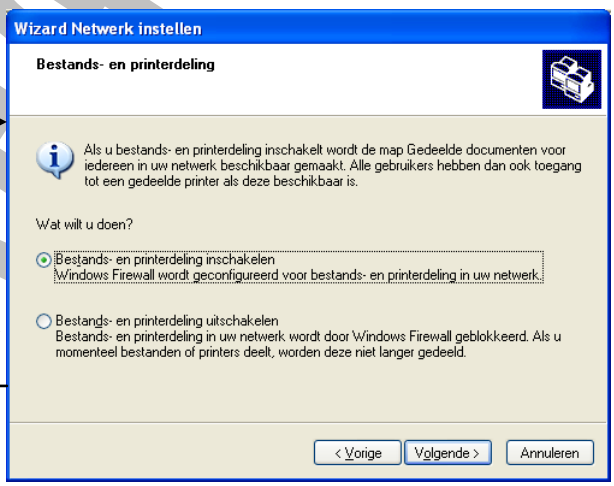
Om de wizard op te starten klikt u op: **Start – Configuratiescherm – Netwerk- en Internet verbindingen – Een thuisnetwerk of klein bedrijfsnetwerk instellen**

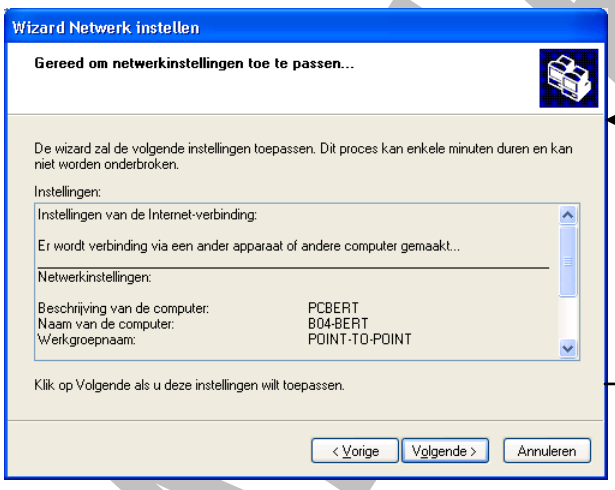


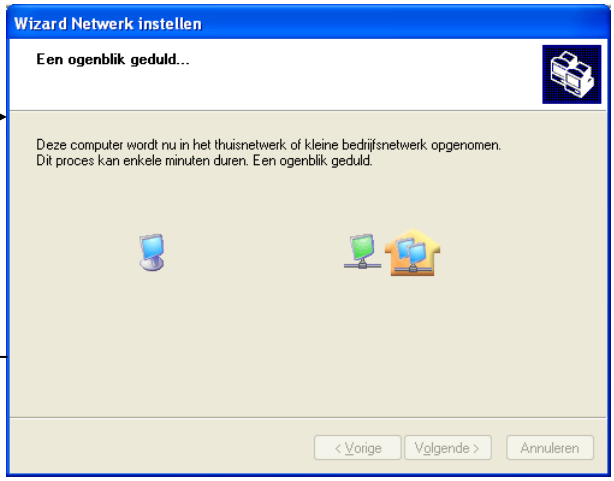


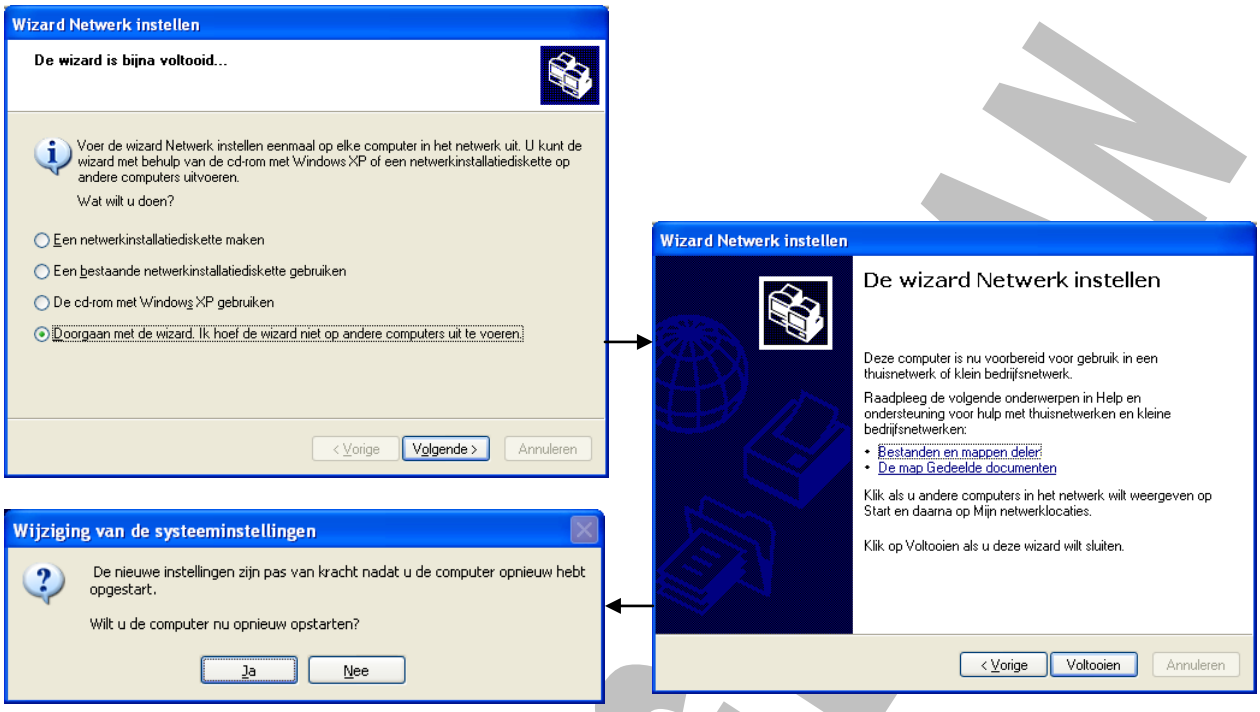






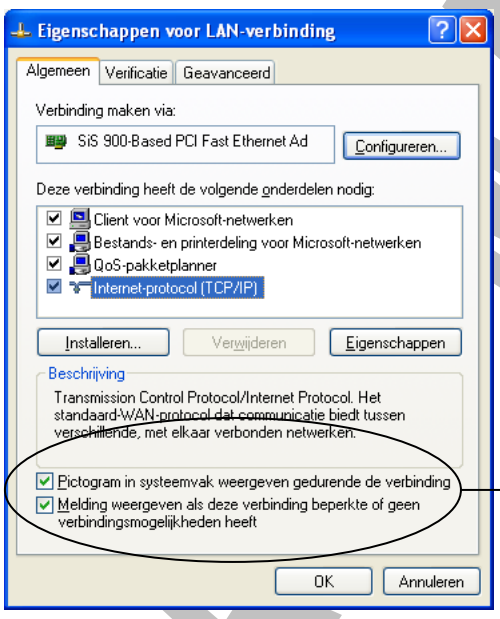






Kies nu: **Start – Configuratiescherm – Netwerk- en Internet verbindingen – Netwerkverbindingen**

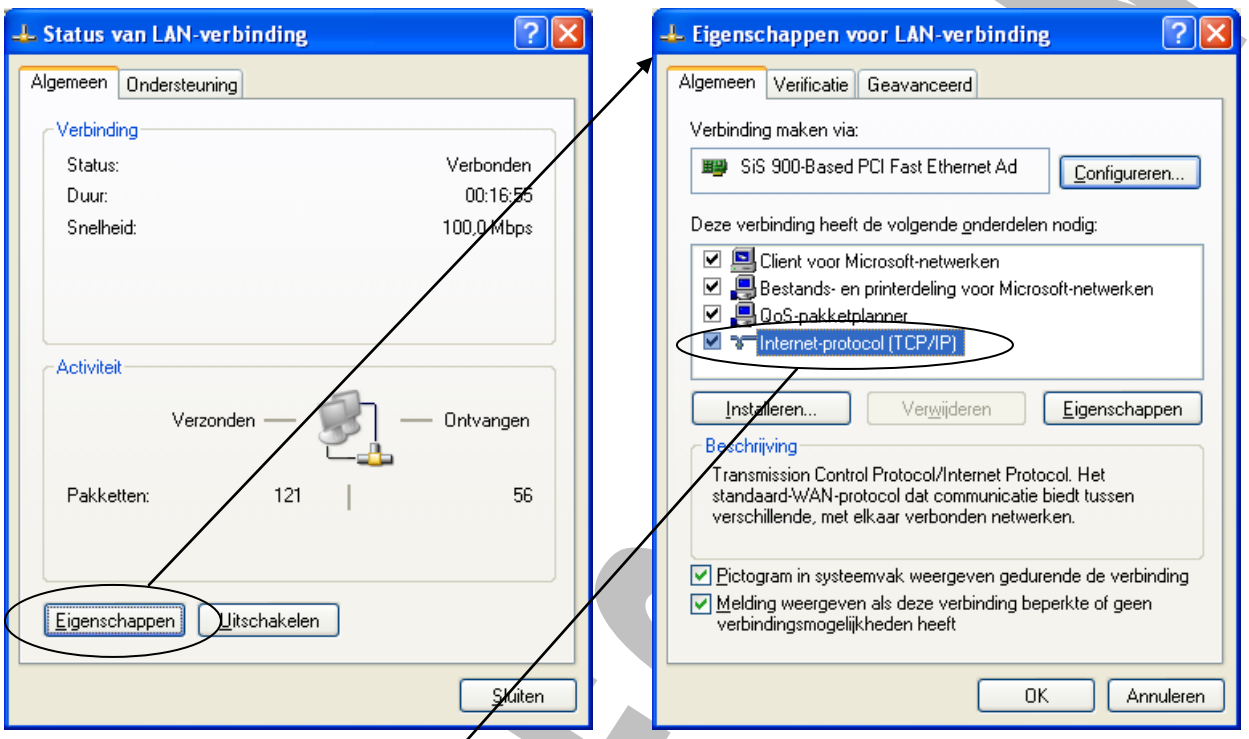
Klik met de rechter muisknop op de **LAN verbinding** en klik op het item **Eigenschappen**



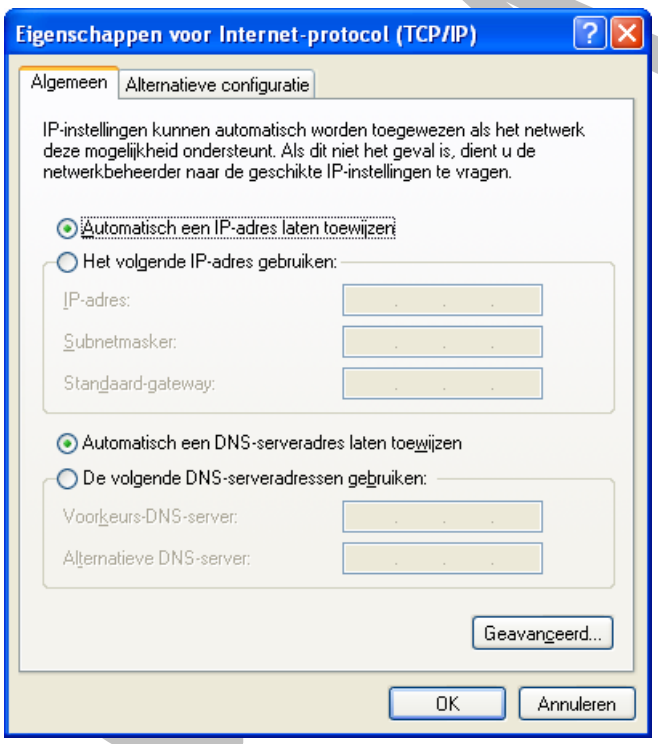
Zet het vinkje aan bij **"Pictogram in systeemvak weergeven gedurende de verbinding"**.

U kunt nu aan dit pictogram ook direct merken of de **LAN-verbinding onderbroken** wordt.

Dit pictogram stelt u ook in staat om de volgende keer met een **dubbelklik op dit pictogram**, het venster **"Status van de LAN-verbinding"** op te roepen.



U dubbelklikt nu op **"Internet-protocol (TCP/IP)"** en dan krijgt u het volgende venster.



In dit venster staat voor een Point-to-Point verbinding alles op automatisch.

De IP-nummers worden automatisch toegewezen.

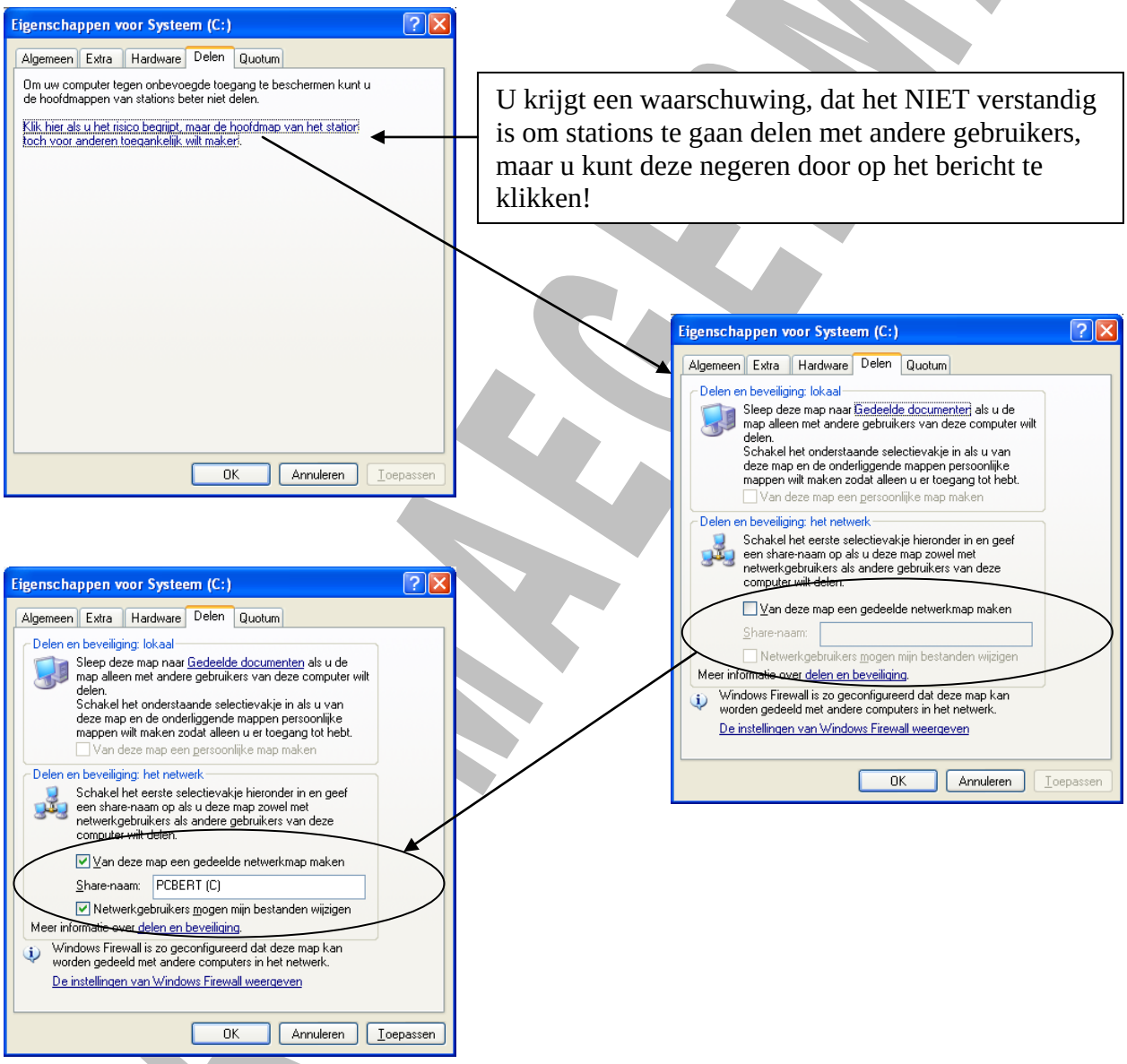
8 Stations en mappen delen bij een Point-to-Point netwerk

Als de beide PC's nu met elkaar verbonden zijn, dan kan men stations en mappen gaan delen tussen beide PC's. Hiervoor gaan we als volgt tewerk:

8.1 Station delen

Open de verkenner op **PCBERT** en klik met de rechter muisknop op het **station C:**

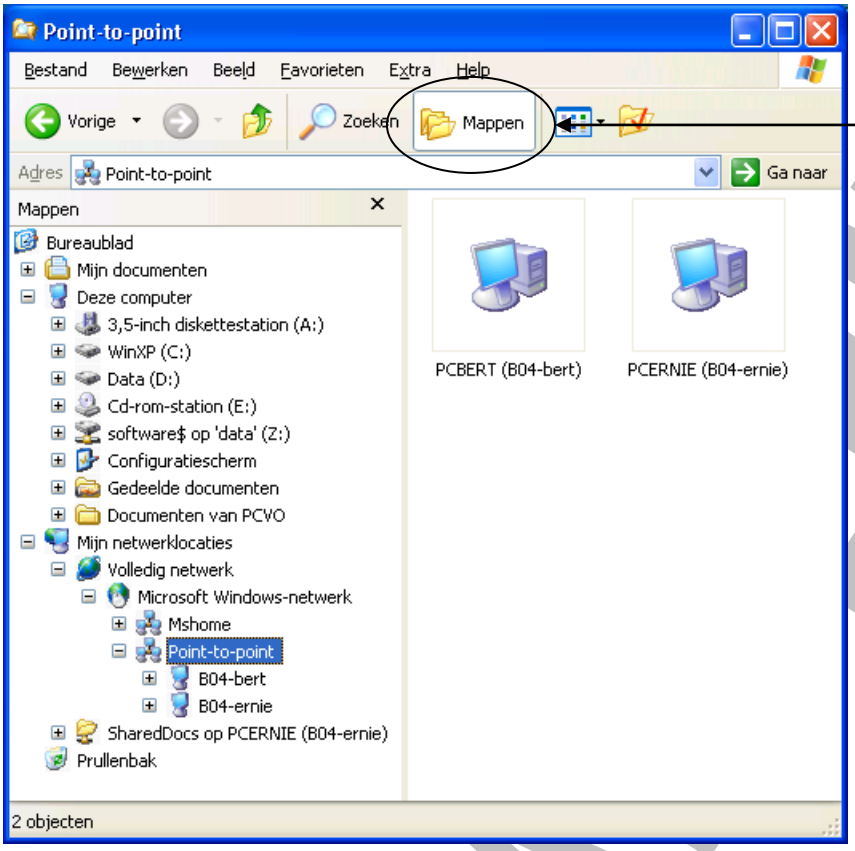
Kies in het snelmenu het item **Delen en beveiliging…**



Men kan nu op **PCERNIE** de het station **PCBERT (C)** gaan bekijken en men heeft volledige toegang tot de bestanden die op dit station staan.

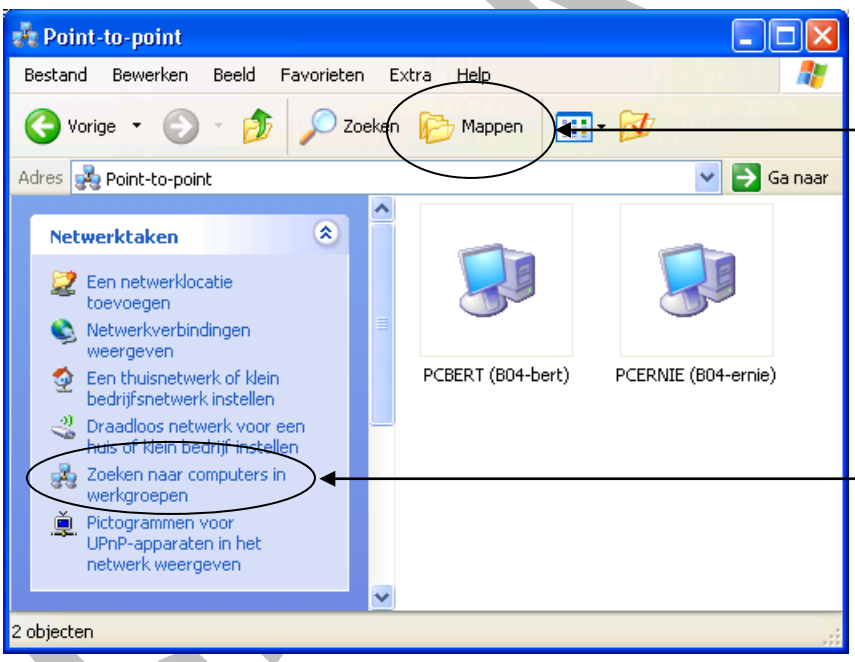
HÉÉL GEVAARLIJK!!! – Dus zet dit na ons experimentjes maar vlug terug UIT!!!

8.2 Netwerk verkennen met de verkenner



Knop Mappen IN
Men kan **ALLE werkgroepen** ineens bekijken en daarnaast ziet men ook **ALLE gedeelde stations en mappen**

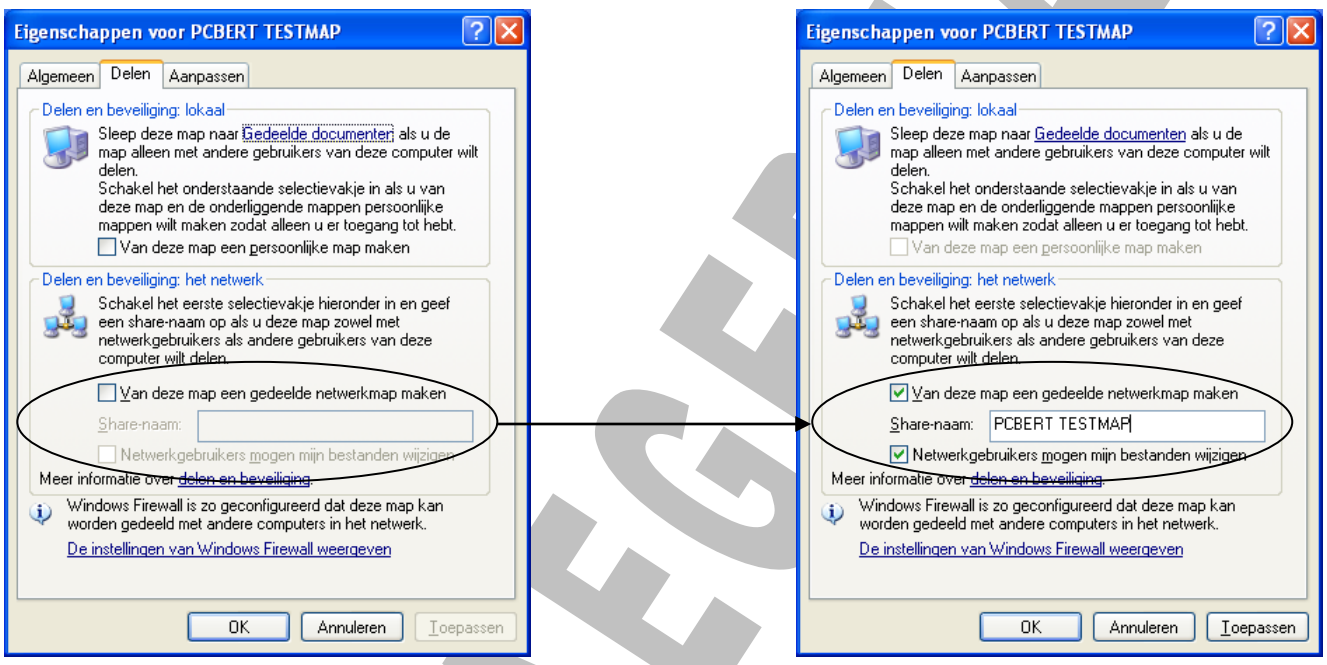
Soms ziet een beginnende netwerkbeheerder dan door het bos de bomen niet meer!!!



Knop Mappen UIT
Men kan **ALLE PC's** opzoeken die in **dezelfde werkgroep zitten als de PC die men gebruikt**.

8.3 Map delen

- Maak een nieuwe map aan op **PCBERT** op het **bureaublad** en noem ze **PCBERT TESTMAP**
- Klik met de rechter muisknop op deze map
- Kies in het snelmenu het item **Delen en beveiliging…**



De map **PCBERT TESTMAP en zijn inhoud** is nu volledig toegankelijk vanop **PCERNIE**.

Gedeelde mappen noemt met ook **SHARES**.

9 Configuratie van een Peer-to-Peer netwerk

We gaan nu **alle PC's verbinden d.m.v. een straight-cables met een SWITCH** en we baseren ons hiervoor op het schema van het volgende labo:

Netwerken basis – Labo 005 – Peer-to-Peer netwerk 1

Om een PC in een Peer-to-Peer netwerk op te nemen gaat u tewerk als in het hoofdstuk **"Configuratie van een Point-to-Point netwerk"**.

10 Stations en mappen delen bij een Peer-to-Peer netwerk

Alle PC's die geconfigureerd zijn kunnen nu terug stations en mappen gaan delen. Dit gebeurt op net dezelfde manier als bij een Point-to-Point netwerk.

In het volgende labo herconfigureren wij ons netwerk met 2 werkgroepen i.p.v. 1 werkgroep.

Netwerken basis – Labo 006 – Peer-to-Peer netwerk 2

Bekijk nog eens goed in de verkenner hoe het netwerk er dan uitziet!!!

11 Netwerkverbindingen maken naar gedeelde mappen

In het Engels wordt dit **shares** (=gedeelde) **mappen** (=netwerkverbinding maken) genoemd

11.1 Shares "mappen"

Als u nu bepaalde shares veel moet raadplegen, kunt u ze beter "mappen", d.w.z. een stationsletter toekennen aan deze netwerkmap.

Dit doet men als volgt:

- Open de **verkenner**
- Kies **Extra – Netwerkverbinding maken…**

- Kies een **stationsletter** uit , die u wilt toekennen aan de share
- **Blader** naar de shares die u wilt "mappen" of **typ** \\[servernaam]\[netwerkmapnaam]
- Vergeet ook niet het vinkje **"Opnieuw verbinding maken bij aanmelden"** aan te vinken, want dit zal u telkens terug aanmelden bij deze share als u herstart
- Nadat u op **"Voltooien"** geklikt hebt zult u in de verkenner nu het nieuwe station herkennen

11.2 Shares “mappen” via batchfile

Het kan nu zijn dat iemand de verbinding met uw “gemapte” share **verbreekt**.

Dit doet u door **op de stationsletter met de rechter muisknop te klikken** en te kiezen voor **“Netwerkverbinding verbreken”**.

Dit vermijdt u door uw share te “mappen” d.m.v. een **batchfile** die via een DOS commando de betreffende share zal “mappen”. Hiervoor gebruikt u het commando **NET USE**.

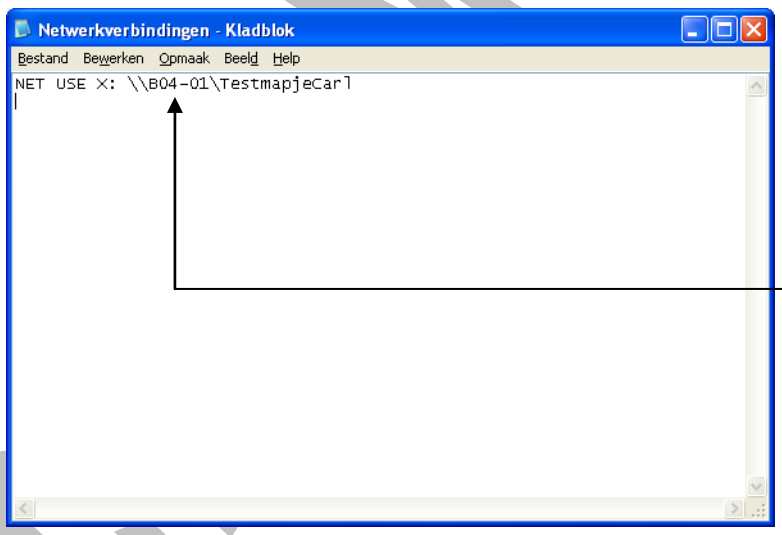
Opdat deze batchfile **telkens zou uitgevoerd worden als u de PC opstart**, moet u deze batchfile in de map **“Opstarten”** zetten van **“All Users”**.

Deze map vindt u op de volgende locatie:
C:\Documents and Settings\All Users\Menu Start\Programma's\Opstarten

De batchfile zelf kunt maken in **kladblok** en opslaan als een **.BAT** bestand.

Ga als volgt tewerk:

- Ik maak zelf eerst een **share** aan op **PC01** en noem dit **“TestmapjeCarl”**
- Open op de **andere PC’s** het programma **Kladblok**
- Typ hier het volgende commando **NET USE X: \\B04-01\TestmapjeCarl** en druk op **ENTER**



B04-01 kan men ook vervangen door het IP-adres van de PC.
In dit geval 10.0.0.1

LET OP: indien men het commando vervangt door **NET USE X: \\10.0.0.1\TestmapjeCarl** zal het vinden van de betreffende PC op het netwerk sneller gebeuren!

- Kies dan **Bestand – Opslaan**
- Ga naar de volgende locatie
  C:\Documents and Settings\All Users\Menu Start\Programma's\Opstarten
- Geef de volgende bestandsnaam in en let op dat u deze tussen **aanhalingstekens** zet!!!
  "Netwerkverbindingen.bat"
- Sluit nu Kladblok af en controleer of dit bestand zich op de gewenste locatie bevindt.
- Herstart de PC en kijk of er opnieuw een verbinding gemaakt wordt met de share.

Het volgende probleem kan zich nu toch nog voordoen:
De computer start op en voert de BATCH-file uit voordat de netwerkverbinding tot stand gekomen is. Zo heeft het NET USE commando niet de mogelijkheid om de netwerkverbinding te maken!

12 Printers delen in een Peer-to-Peer netwerk

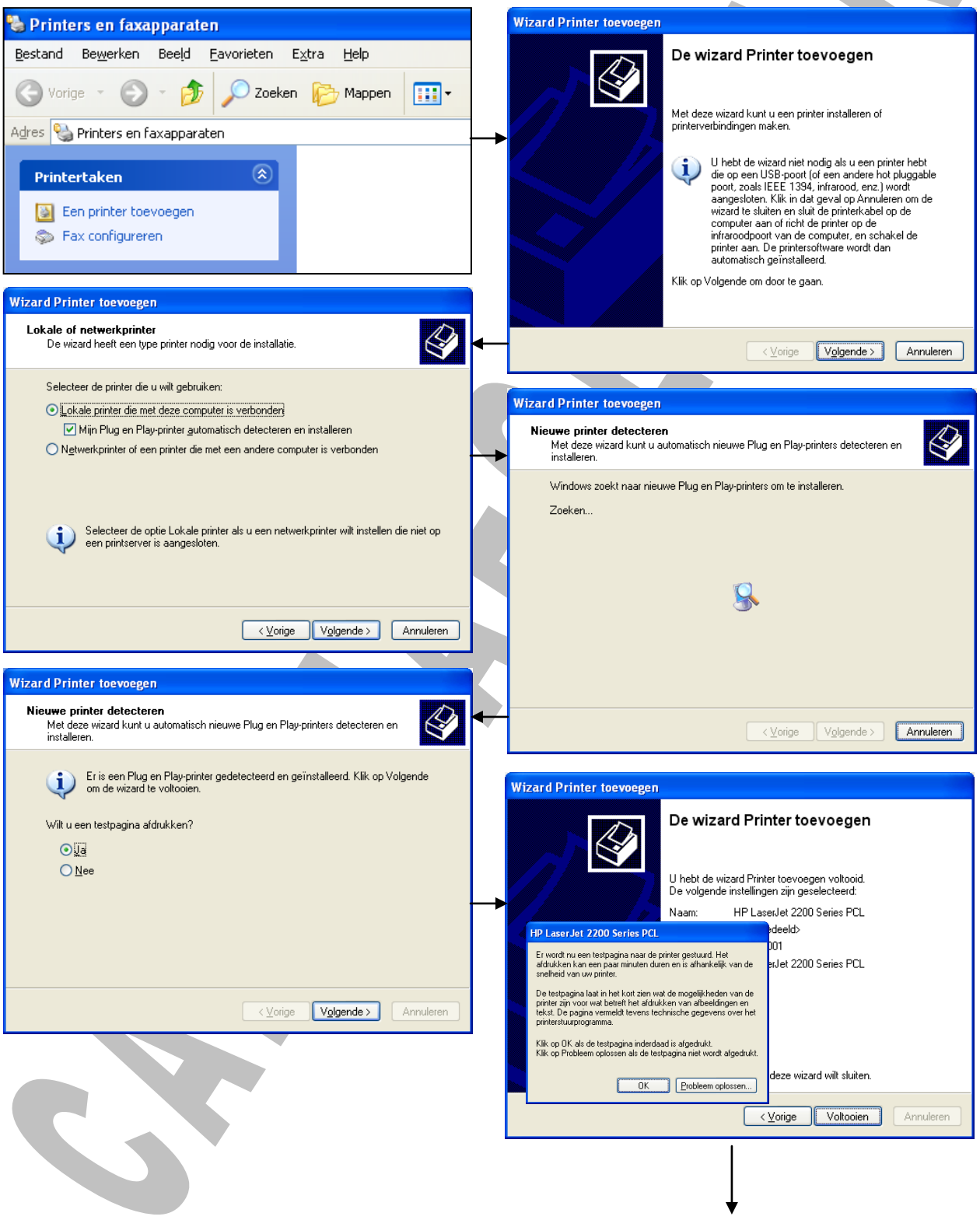
We gaan ervan uit dat de printer verbonden is met één van de PC's via zijn **parallelle poort (LPT)**.
In ons geval is deze PC namelijk **PC01**!

Wij zullen dus als volgt tewerk gaan:

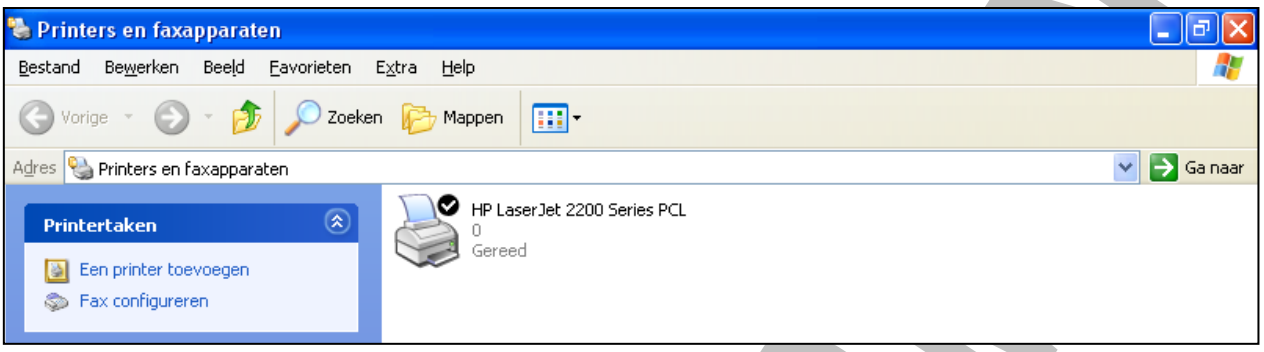
- Installeer eerst de printer op PC01
- Deel deze printer dan op PC01
- Installeer de printer van PC01 op de andere PC's die op het netwerk aangesloten zijn

12.1 Printer installeren op de PC waarop hij aangesloten is via de parallelle poort (LPT)

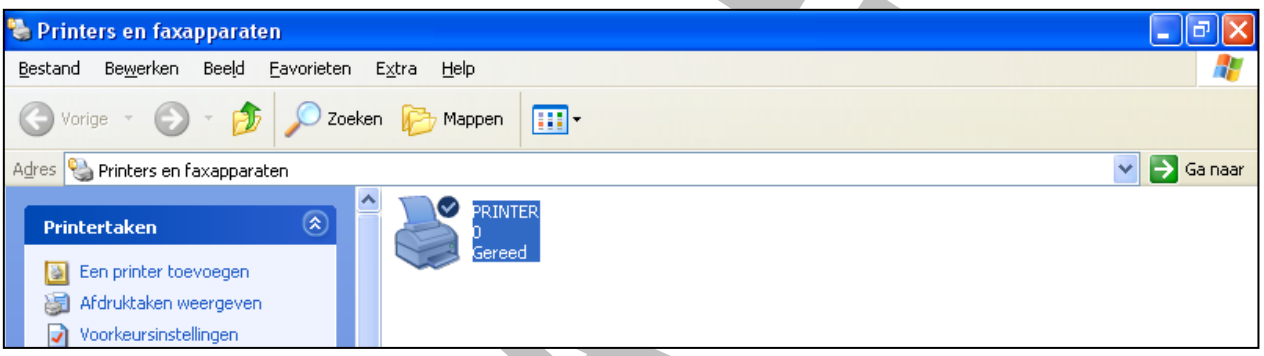
Kies **Start – Printers- en faxapparaten**



De printer is nu geïnstalleerd op PC01 en verschijnt in het venster **"Printers en faxapparaten"**



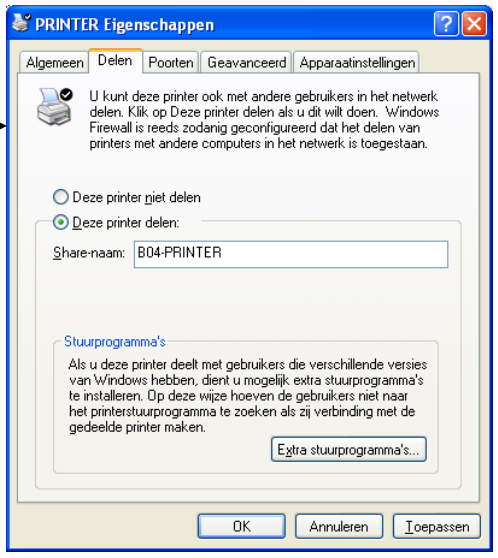
Men kan nu de beschrijving van de printer wijzigen door met de rechter muistoets op het pictogram van de printer te klikken en daarna **Naam wijzigen** te kiezen. (kies in ons voorbeeld **PRINTER** als naam)



12.2 De printer delen op de PC waarop hij aangesloten is

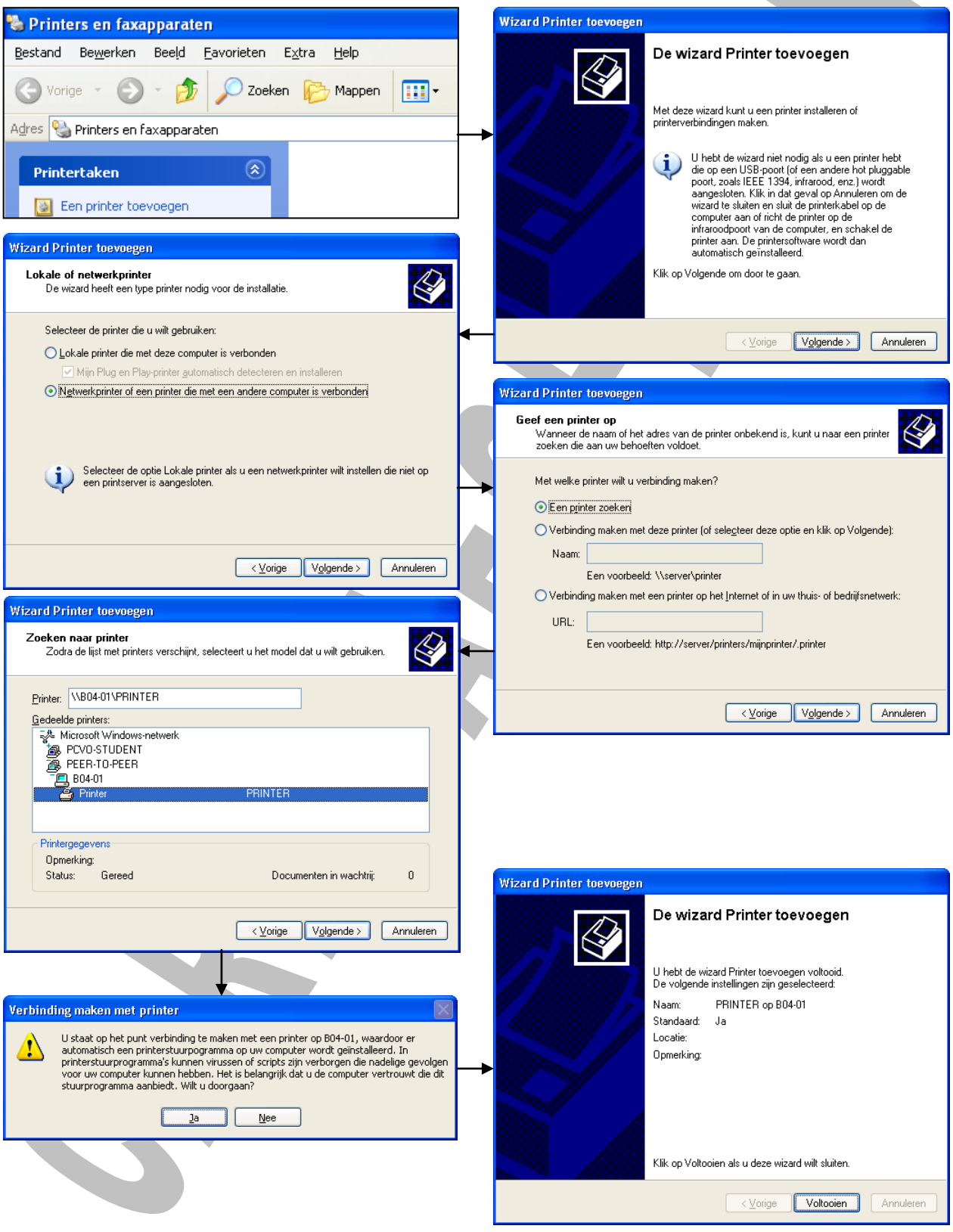
Om een printer in een Peer-to-Peer netwerk op te nemen gaat u als volgt tewerk:

- Kies **Start – Printers en faxapparaten – Klik met de rechtermuisknop op de printer die u wilt delen**
- Kies in het snelmenu het item **Delen…**



12.3 Printer installeren op een andere PC's in het netwerk

Kies **Start – Printers- en faxapparaten**



13 TCP / IP

Staat voor **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol

TCP/IP is het veelgebruikte netwerk protocol. Het heeft zijn oorsprong in de Unix-wereld. Door de opkomst van het internet heeft TCP aan belangrijkheid gewonnen ook buiten deze Unix-wereld.

TCP/IP is een open standaard. Alle eigenschappen, definities, concepten en werkwijzen zijn openlijk op het Internet gepubliceerd. Elke onderdeel van de standaard is beschreven in de zogenaamde RFC's (Request for Comments). Dit maakt het mogelijk voor veel kleine software-firma's uitbreidingen op de standaard te ontwikkelen. Het is mogelijk om een voorstel tot wijzigingen in de dienen.

TCP/IP is niet de eigendom van een bepaalde firma, het is een non-proprietary protocol. Hierdoor kan het protocol overal gebruikt worden zonder licentie-rechten te moeten betalen aan een firma. Mede door dit feit heeft het internet zich zo vlug kunnen ontwikkelen.

TCP/IP is een heel uitgebreid en rijk protocol. Het is niet alleen het protocol zelf dat van belang is, maar ook de vele programma's en mogelijkheden errond. (FTP, HTTP, …)

De belangrijkste eigenschap van TCP/IP is dat door het adressering-algoritme meerdere netwerken onderscheiden kunnen worden en in een hiërarchie kunnen geplaatst worden.

13.1 IP-Nummer

Iedere computer heeft een uniek nummer in een TCP/IP netwerk. Het internet is een gigantisch netwerk van meerder computers. Elke computer op het net heeft dus een IP nummer.

Het nummer bestaat uit een 32 bits lang getal.

Hierdoor zijn er in principe 2 tot de macht 32 = 4.294.967.296 mogelijk adressen.

Een 32 bits lang getal is meestal te moeilijk om te onthouden of op te schrijven. Daarvoor wordt het getal opgesplitst in 4 keer 8 bits. Elke 8 bits vormen 1 byte. Elke byte heeft een waarde van 0 tot 255. De 4 bytes worden gescheiden door puntjes. Hierdoor is een adres eenvoudiger memoriseerbaar en kan het zonder fout ingetikt worden. Dit noemt men de **dotted-decimal notation**.

Voorbeeld:

11000001000010100001111000000010

Na opdeling in 4 bytes.

11000001 00001010 00011110 00000010

De dotted-decimal notation is dan:

193.10.30.2

Typ in GOOGLE de trefwoorden “network calculators” in om een omreken-site te vinden.

13.2 Klasses van IP adressen.

Met een IP nummer worden tegelijkertijd 2 elementen weergegeven:

- Het netwerk nummer
- Het computer nummer

Samen vormen ze het unieke nummer. Het netwerknummer is van belang om meerdere computers onder te brengen in een subnetwerk.

Er zijn 3 categorieën van adressen.

Klasse A : Hiervan betekent de eerste byte het netwerknummer en de 3 volgende bytes het computernummer.

NNNNNNNN	CCCCCCCC	CCCCCCCC	CCCCCCCC

De eerste byte heeft een waarde van 0 tot 127.

Er zijn 126 netwerken, die elk 16 777 214 computers kunnen hebben.

Klasse B : Hiervan zijn de eerste twee bytes het netwerknummer en de volgende 2 bytes het computernummer.

NNNNNNNN	NNNNNNNN	CCCCCCCC	CCCCCCCC

De eerste byte heeft een waarde van 128 tot 191

Er zijn 16 384 netwerken, die elk 65 534 computers kunnen hebben.

Klasse C : Hiervan zijn de eerste drie bytes het netwerknummer en de vierde byte het computernummer.

NNNNNNNN	NNNNNNNN	NNNNNNNN	CCCCCCCC

De eerste byte heeft een waarde van 192 tot 223.

Er zijn 2 097 152 netwerken met elk 254 computers.

Verder zijn er nog **Klasse D** en **klasse E** adressen die voorlopig niet gebruikt worden.

13.3 Er zijn ook enkele gereserveerde adressen :

- **0.0.0.0** (all zeros) kan niet gebruikt worden
- **255.255.255.255** (all ones) kan ook niet gebruikt worden.
- **127.0.0.1** Het loopback adres. Met dit adres wordt steeds de eigen computer bedoeld. Om het even vanop welke computer zal het versturen van data naar 127.0.0.1 resulteren in het sturen van de data naar zichzelf.
- Alle adressen die **eindigen op 255** kunnen ook niet aan een computer toegewezen worden. Door van de laatste byte een 255 te maken wordt de data naar alle computers verzonden die zich in het sub-netwerk bevinden. Dit is het **broadcast adress**.
- Alle adressen van **244.0.0.1 tot 255.255.255.255** worden niet gebruikt om een computer te bepalen. Het zijn deels experimentele adressen.

13.4 Beheer van IP adressen.

Om computers in het internet te kunnen zetten moeten ze een IP-nummer hebben die uniek is over de gehele wereld.

De adressen worden beheerd door het **NIC** (Network Information Center).

Een adres moet door een firma aangekocht worden bij deze instantie. Naargelang de grootte van de firma zal een adres uit een bepaalde klasse aangekocht worden. Een firma die heel veel computers op het internet wil, zal een adres uit klasse A willen. Hierdoor hebben ze een heel brede computer range. Ze zijn vrij hierbinnen zelf nog eens een hiërarchie te bedenken. Grote firma's zijn er niet veel, vandaar het geringe aantal netwerknummers. Wel zijn er heel veel kleine firma's die slechts een beperkt aantal computers op het net willen. Deze opteren dan voor een C adres.

Alle klasse A adressen zijn momenteel uitgedeeld aan de firma's zoals Apple, IBM …

13.5 Hoe een klasse herkennen.

Aan de hand van het adres kan men bepalen in welk klasse een adres zich bevindt. Hierdoor moet de eerste byte naar binair omgezet worden. Aan de hand van het aantal leidende eenen (binaire 1) in de byte is de klasse te bepalen.

Begint met	Klasse
0	A
10	B
110	C
1110	D
1111	E

13.6 Verschil tussen PRIVATE en PUBLIC IP-adressen

Er zijn twee soorten IP adressen, namelijk PRIVATE en PUBLIC IP adressen.

PRIVATE IP adressen zijn IP adressen die NIET voorkomen op het internet. Deze IP adressen worden in principe alleen gebruikt voor bedrijfs en thuis netwerken.

Meest gebruikte PRIVATE IP adressen reeksen zijn:

- **10.0.0.0 - 10.255.255.255 Dit is de range die wij in onze klas gaan gebruiken!!!**
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255 Dit is de range die meestal voor thuisnetwerken gebruikt wordt

PUBLIC IP adressen zijn alle overige adressen. Houd er rekening mee dat er op het Internet alleen naar unieke IP adressen zijn (1 IP adres komt maar 1 keer voor). Een postbode kan ook geen post bezorgen als er in België twee huizen zijn met het zelfde adres.

13.7 Subnetmask

Een subnetmask is een reeks van bits die definiëren wat het netwerk nummer en wat het computernummer is van een IP adres. Een 1 staat voor het netwerk adres, een 0 voor het computernummer. In een subnetmask zal altijd een reeks van 1-en gevolgd worden door een reeks van 0-en. Nooit zal na een 0 terug een 1 voorkomen. De mogelijke subnetmasks zijn dus.

10000000 00000000 00000000 00000000
11000000 00000000 00000000 00000000
...
11111111 11111111 11111111 11111100
11111111 11111111 11111111 11111110

In klasse A is de eerste byte het netwerknummer en de volgende 3 het computernummer.

Hierdoor is het subnetmask 11111111 0000000 0000000 0000000.
In dotted-decimal notitie is dit 255.0.0.0

Klasse	Subnetmask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

13.8 Subnetting

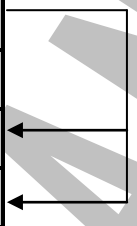
Naast de drie standaard klassen kan ook een ander klasseringsprincipe gebruikt worden. Dit komt voor bij netwerken die niet aan het internet gekoppeld worden of voor het verder indelen van de computernetwerken van grote firma's. Dit kan door een subnetmask te gebruiken die tussen de standaard subnetmask van de klassen ligt.

Stel: een firma heeft een adressen range in klasse C nl. 205.101.55.X . Hierdoor heeft het 1 netwerk van 254 computers.

Het standaard subnetmask is dus	255.255.255.0
Dit komt overeen met	11111111 11111111 11111111 00000000

Een bepaald adres in de range van de firma is 205.101.55.91

11001101	01100101	00110111	01011011	**ipnr**
11111111	11111111	11111111	00000000	**subnetmask**
11001101	01100101	00110111		**netwerknummer**
			01011011	**computernummer**



Dit betekent computer nummer 91 in netwerk 205.101.55.

De firma wil dit netwerk nogmaals opdelen in meerdere subnetwerken. Dit kan het door het subnetmask te verbreden.

Het nieuw subnetmask wordt 11111111 11111111 11111111 11100000

Hierdoor zijn 6 nieuw netwerken mogelijk nl.

11111111 11111111 11111111 001

11111111 11111111 11111111 010

11111111 11111111 11111111 011

11111111 11111111 11111111 100

11111111 11111111 11111111 101

11111111 11111111 11111111 110

Hierdoor liggen de computers

11111111 11111111 11111111 00100001

11111111 11111111 11111111 01000001

elk in een ander netwerk.

In dotted-decimal notitie zijn dit volgende 6 netwerk nummers:

205.101.55.32

205.101.55.64

205.101.55.96

205.101.55.128

205.101.55.160

205.101.55.192

14 Configuratie v/e Peer-to-Peer netwerk (met IP-nummers)

We configureren nu alle PC's eerst zoals we gezien hebben in **Labo 005**, maar we zullen iedere computer nog een IP nummer meegeven. We baseren ons hiervoor op het schema van **Labo 007**.

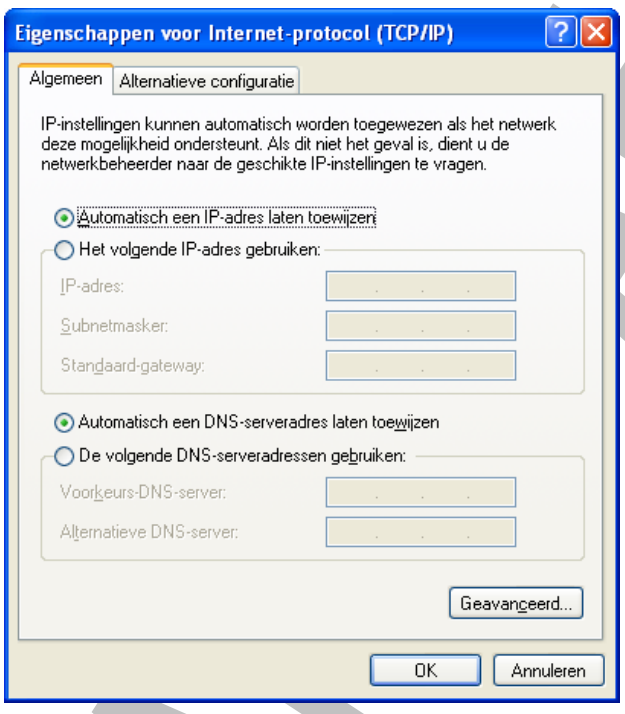
Netwerken basis – Labo 007 – Peer-to-Peer netwerk 1 (IP)

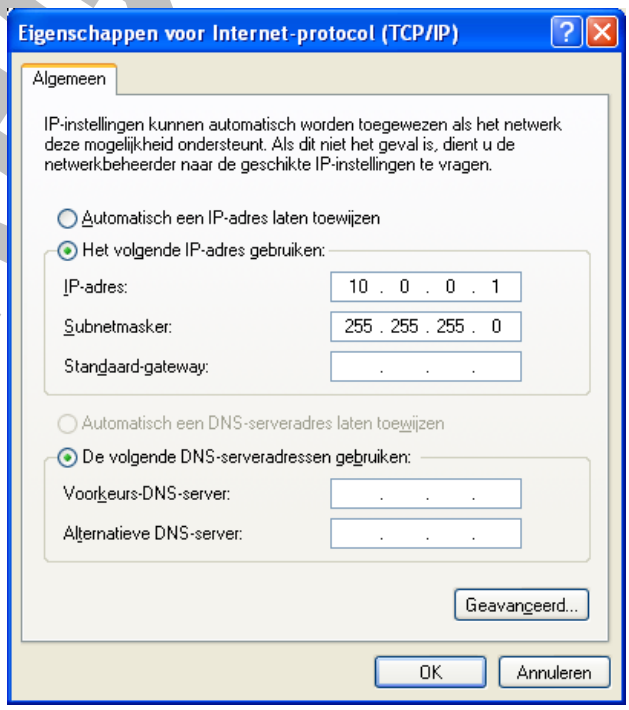
U gaat als volgt tewerk:

- PC's configureren zoals in Labo 005
- Elke PC een IP nummer geven

Voor het laatste item te verwezelijken gaat u als volgt tewerk:

- Dubbelklik op het pictogram met de 2 computertjes in het systeemvak..
- Klik op de knop **"Eigenschappen"**.
- Dubbelklik op **"Internet-protocol (TCP/IP)"** en dan krijgt u het volgende venster.





- Klik op het keuzerondje **"Het volgende IP-adres gebruiken"**.
- Vul het IP-adres in. Gebruik **SPATIE** om naar het volgende veld te springen.
- Na het invullen van het laatste veld, drukt u op **TAB** en zo wordt automatisch het Subnetmasker ingevuld.

15 Enkele netwerkcommando's

Nu de PC's geconfigurrerd zijn met IP-adressen kunnen we de volgende zaken eens uitproberen:

- IPCONFIG
- PING – verbinding uittesten van uw PC met een ander apparaat (PC, switch, router, enz…)
- TRACERT
- Adres-vak van de browser
- NET VIEW
- NET USE

15.1 IPCONFIG

IPCONFIG /?	Vraagt de mogelijkheden van dit commando op
IPCONFIG	Vraagt een summier overzicht van de IP instellingen op
IPCONFIG /all	Vraagt een uitgebreid overzicht van de IP instellingen op
IPCONFIG /release	Verwijdert het IP-adres van de PC
IPCONFIG /renew	Vraagt een nieuw IP-adres aan bij de DHCP-server

15.2 PING

PING /?	Vraagt de mogelijkheden van dit commando op
PING 127.0.0.1	LoopBack om de netwerkkaart uit te testen
PING [eigen IP-adres]	Test de verbinding uit tussen jouw PC en het eerstvolgende apparaat
PING [ander IP-adres]	Test de verbinding uit tussen jouw PC en een ander apparaat

15.3 TRACERT

TRACERT /?	Vraagt de mogelijkheden van dit commando op
TRACERT [ander IP-adres]	Geeft de weg weer die men volgt tussen jouw PC en het ander adres

15.4 Adres-vak van de browser

\\[IP-adres PC]	Maakt verbinding met een bepaalde PC via zijn IP-adres
[IP-adres netwerkprinter]	Maakt verbinding met het configuratiescherm van een netwerkprinter

15.5 NET VIEW

NET VIEW	Toont een overzicht van alle clients op het netwerk

15.6 NET USE

NET USE	Kent een stationsletter toe aan een share (gedeelde map)

16 Installatie en configuratie van een netwerkprinter (RJ45)

Als het netwerk gebruik maakt van een printer die **via de parallelle (LPT) poort** aangesloten is op één van de PC's van het netwerk, dan moet de PC in kwestie ook steeds aan staan wil men de printer door een andere PC van het netwerk laten gebruiken.

Men kan dit vermijden door gebruik te maken van een "echte" netwerkprinter. Deze laatste kan men, net zoals een netwerkkaart, via een **RJ45 connector** op het netwerk aansluiten.

16.1 IP-adres toekennen aan de netwerkprinter

We moeten aan deze printer een IP-adres toekennen die in **dezelfde range** valt als de andere PC's die deze printer willen gebruiken.

Dit kan men op de volgende manieren kan toekennen:

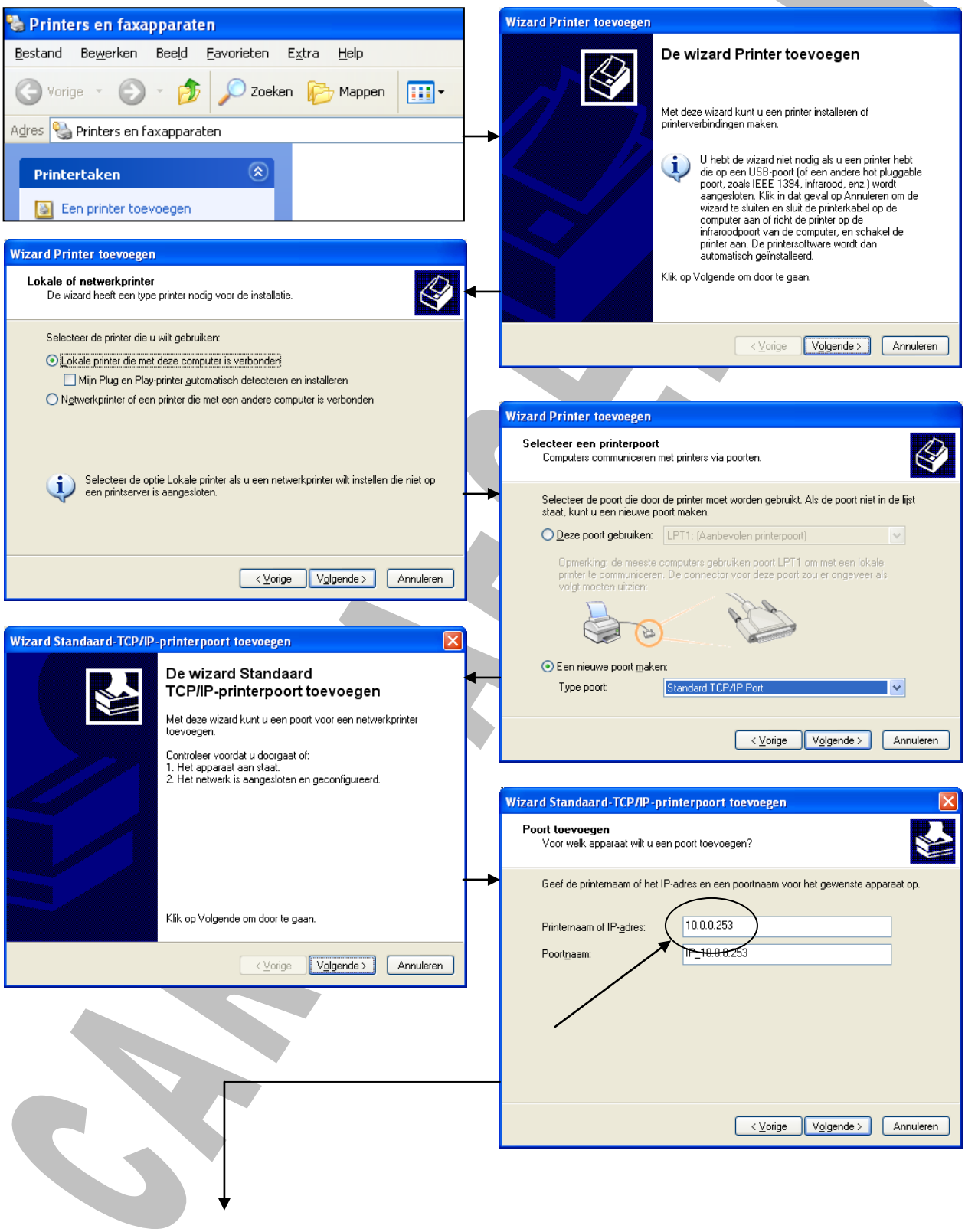
- Via **toetsen op de printer** zelf.
- Door zijn huidig IP-adres in te vullen op de adresbalk van uw browser (dit adres komt men te weten door de printer zijn configuratiegegevens te laten afdrukken) en dan in het **configuratiescherm van de printer** de nodige wijzigingen aan het IP-adres door te voeren.
  De PC zijn IP-adres moet in dezelfde range liggen als dat van de printer!!!!!
- Via speciale software zoals **HP Web Jetadmin**.

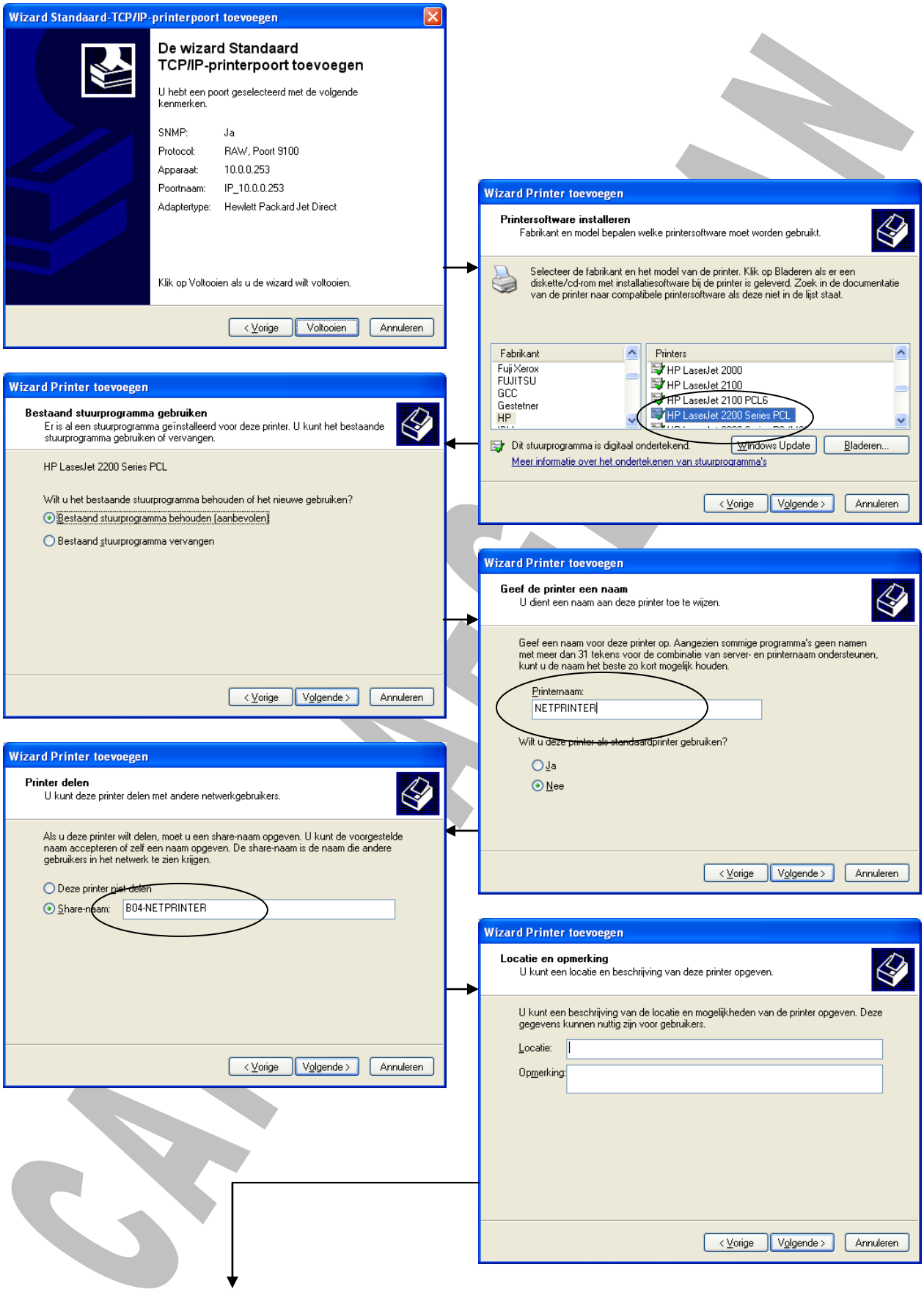
We baseren ons hiervoor op het schema van **Labo 008** om dit uit te proberen.

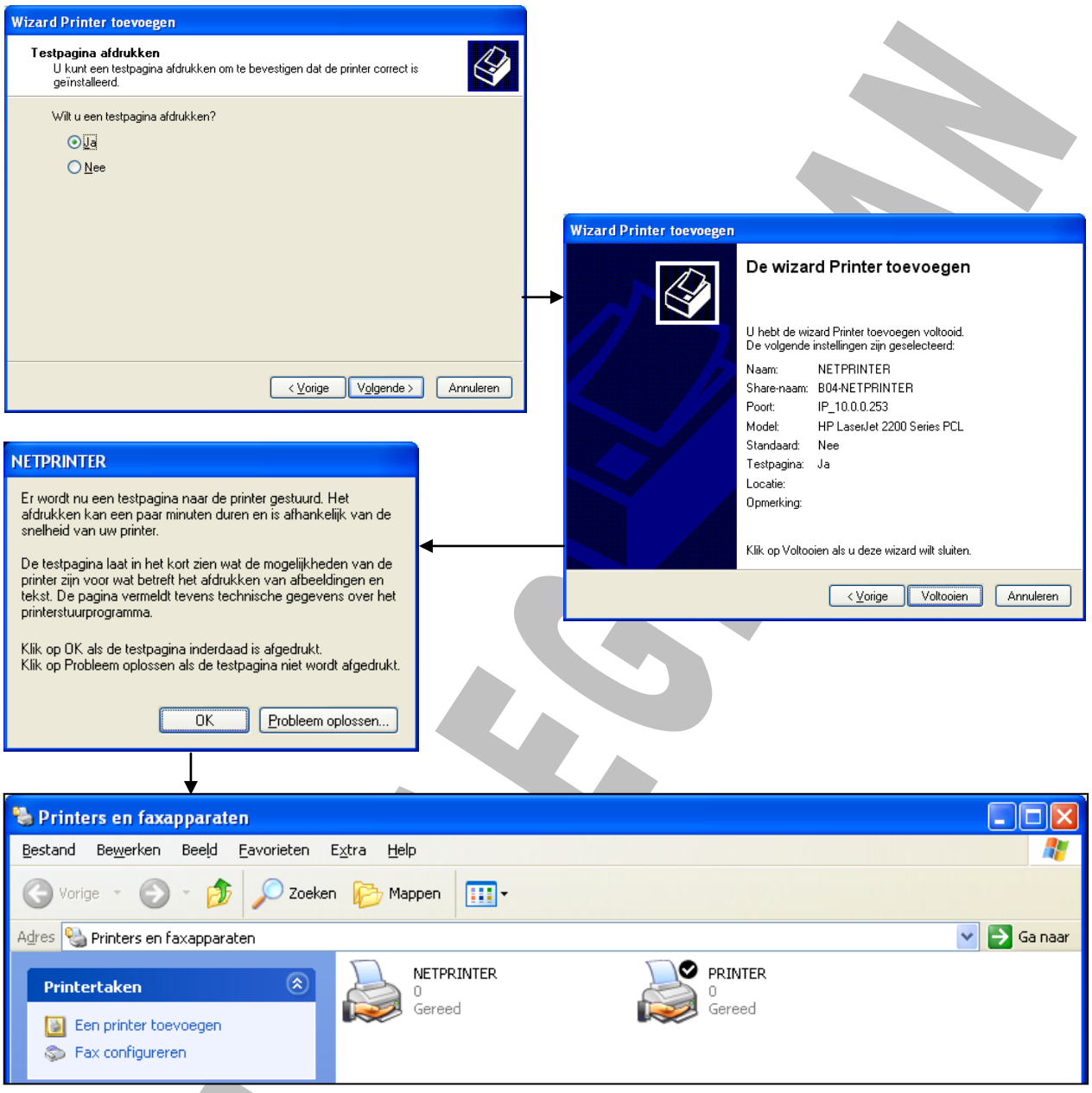
Netwerken basis – Labo 008 – Peer-to-Peer netwerk 2 (IP)

16.2 Printer installeren en delen op één PC in het netwerk

Kies **Start – Printers- en faxapparaten**




Wizard Standaard-TCP/IP-printerpoort toevoegen
De wizard Standaard TCP/IP-printerpoort toevoegen
U hebt een poort geselecteerd met de volgende kenmerken.
SNMP: Ja
Protocol: RAW, Poort 9100
Apparaat: 10.0.0.253
Poortnaam: IP_10.0.0.253
Adaptertype: Hewlett Packard Jet Direct
Klik op Voltooien als u de wizard wilt voltooien.
< Vorige
Voltooien
Annuleren
Wizard Printer toevoegen
Printersoftware installeren
Fabrikant en model bepalen welke printersoftware moet worden gebruikt.
Selecteer de fabrikant en het model van de printer. Klik op Bladeren als er een diskette/cd-rom met installatiesoftware bij de printer is geleverd. Zoek in de documentatie van de printer naar compatibele printersoftware als deze niet in de lijst staat.
Fabrikant
Fuji Xerox
FUJITSU
GCC
Gestetner
HP
Printers
HP LaserJet 2000
HP LaserJet 2100
HP LaserJet 2100 PCL6
HP LaserJet 2200 Series PCL
Dit stuurprogramma is digitaal ondertekend.
Windows Update
Bladeren...
Meer informatie over het ondertekenen van stuurprogramma's
< Vorige
Volgende >
Annuleren
Wizard Printer toevoegen
Bestaand stuurprogramma gebruiken
Er is al een stuurprogramma geïnstalleerd voor deze printer. U kunt het bestaande stuurprogramma gebruiken of vervangen.
HP LaserJet 2200 Series PCL
Wilt u het bestaande stuurprogramma behouden of het nieuwe gebruiken?
Bestaand stuurprogramma behouden (aanbevolen)
Bestaand stuurprogramma vervangen
< Vorige
Volgende >
Annuleren
Wizard Printer toevoegen
Geef de printer een naam
U dient een naam aan deze printer toe te wijzen.
Geef een naam voor deze printer op. Aangezien sommige programma's geen namen met meer dan 31 tekens voor de combinatie van server- en printernaam ondersteunen, kunt u de naam het beste zo kort mogelijk houden.
Printernaam:
NETPRINTER
Wilt u deze printer als standaardprinter gebruiken?
Ja
Nee
< Vorige
Volgende >
Annuleren
Wizard Printer toevoegen
Printer delen
U kunt deze printer delen met andere netwerkgebruikers.
Als u deze printer wilt delen, moet u een share-naam opgeven. U kunt de voorgestelde naam accepteren of zelf een naam opgeven. De share-naam is de naam die andere gebruikers in het netwerk te zien krijgen.
Deze printer niet delen
Share-naam:
B04-NETPRINTER
< Vorige
Volgende >
Annuleren
Wizard Printer toevoegen
Locatie en opmerking
U kunt een locatie en beschrijving van deze printer opgeven.
U kunt een beschrijving van de locatie en mogelijkheden van de printer opgeven. Deze gegevens kunnen nuttig zijn voor gebruikers.
Locatie:
Opmerking:
< Vorige
Volgende >
Annuleren



De andere PC's in het netwerk kunnen deze printer nu automatisch gebruiken!!!

17 Hardware router als gateway gebruiken

U zult misschien ondertussen ook gemerkt hebben dat we nu niet meer in staat zijn om via de browser op het internet te surfen.

Om dit terug te kunnen doen moeten we gebruik maken van een hardware router.

Onze netwerk zal er dan uitzien zoals in **Labo 009** of **Labo 010**.

Netwerken basis – Labo 009 – Peer-to-Peer netwerk 3 (IP)

Netwerken basis – Labo 010 – Peer-to-Peer netwerk 4 (IP)

We onderscheiden twee soorten routers:

- Met RJ45 poorten, dan spreken we gewoon van een **ROUTER**
- Met RJ45 poorten en draadloos, dan spreken we van een **WLAN ROUTER (WI-FI)**

17.1 ROUTER

17.1.1 Configuratie ROUTER

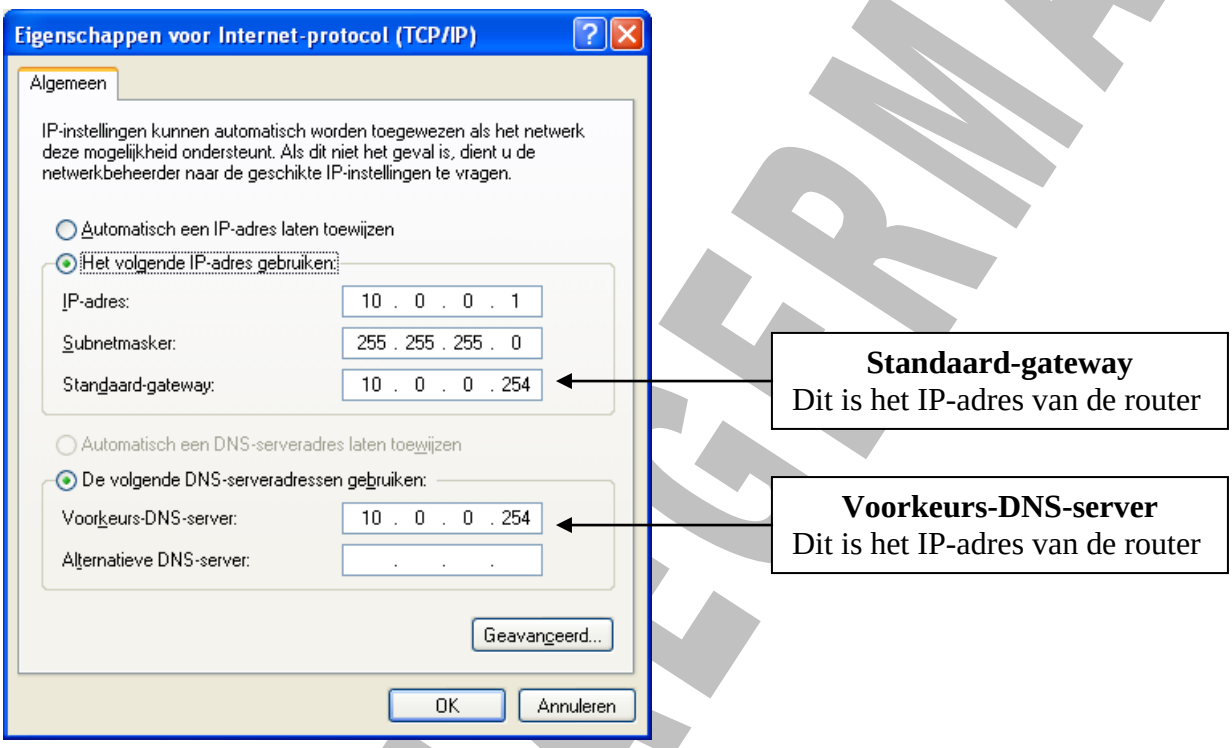
Voor het configureren van de ROUTER gaat men als volgt tewerk:

- We sluiten het toestel aan (PC's en internet) en zetten het onder spanning
- We starten onze browser (bvb. Explorer) op en typen het IP-adres in van de router (dit vindt men in het boekje dat bij de router geleverd is, dit is meestal **192.168.1.1**). Let op dat u uw PC even in dezelfde range plaatst (bvb. **192.168.1.x**)
- Hierna wordt ons een login gevraagd (meestal **gebruikersnaam: admin** en **wachtwoord: admin**)
- Nu krijgt u toegang tot de instellingen van de router (dit kan er voor iedere router anders uitzien)
- U verandert hier nu zijn IP-adres (in ons geval bvb. **10.0.0.254**)
- En u verandert ook zijn Subnet Mask (in ons geval bvb. **255.255.255.0**)
- Als laatste verandert u ook **het wachtwoord** dat u toegang geeft tot deze instellingen
- Vergeet niet de **instellingen op te slaan**
- Hierna zet u uw PC terug in dezelfde range van de router (bij ons bvb. **10.0.0.x**) en u probeert nog even via de browser toegang te krijgen tot zijn IP-adres (dit is nu in ons geval bvb. **10.0.0.254**)
- Het **nieuwe paswoord** moet hierbij gebruikt worden

17.1.2 Configuratie PC's

Als de ROUTER ingesteld is, gaat u elk van de PC's die hiermee verbinding moeten hebben gaan instellen. Dit doet u als volgt:

- Ga naar het venster **"Eigenschappen voor Internet protocol (TCP/IP)"** en stelt daar de volgende zaken in



17.1.2.1 Standaard-gateway (Gateway = Toegangspoort)

Dit is een punt in uw netwerk dat verbonden is met een ander netwerk. De computers of systemen (in ons geval de ROUTER) die in het netwerk het verkeer regelen tussen het LAN en het INTERNET zijn GATEWAYS.

In ons geval moet hier dus het IP-adres van onze ROUTER ingevuld zijn, daar dit apparaat bij dienst doet als gateway. Indien dit niet opgegeven is kan men niet op het internet surfen via deze router.

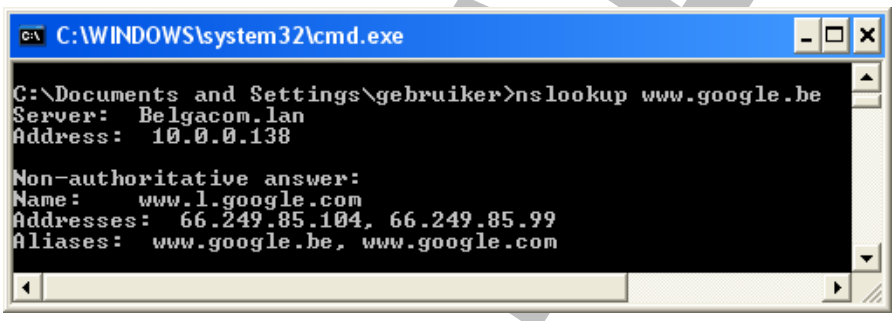
17.1.2.2 Voorkeurs-DNS-server (DNS = Domain Name System)

Dit systeem is de schakel tussen internetdomeinnamen (bvb. www.google.be) en hun bijhorend IP-adres. De DNS-servers van uw provider leggen de link tussen de door u opgevraagde domeinnaam en het correcte IP-adres.

In de praktijk zorgt dit er dus voor dat wij internetdomeinnamen kunnen intypen in het adresvak van onze browser zoals www.google.be i.p.v. het IP-adres van de website. Dit systeem is er gekomen omdat deze domeinnamen gemakkelijker te onthouden zijn dan IP-adressen.
Als u nu bvb. **GEEN DNS-server** zou instelllen, dan zal u enkel in staat zijn om via IP-adressen te surfen naar een bepaalde website.

U kunt echter zo'n IP-adres opvragen op de volgende manier:

- Zet eerst in het venster **"Eigenschappen voor Internet protocol (TCP/IP)"** alles op **AUTOMATISCH**
- Kies **Start – Uitvoeren – typ hier cmd en druk ENTER** om het DOS venster op te roepen
- Typ het volgende commando in: **nslookup www.google.be** en druk op **ENTER**
- U ziet de volgende informatie verschijnen, waaronder het IP-adres van de gevraagde website



- U kunt in het DOS venster iets selecteren door **rechts te klikken** in dit venster en te kiezen voor **Markeren**
- Daarna **selecteert u het IP-adres** en drukt u op **ENTER** op dit te kopiëren
- Ga nu naar de browser, klik in het **adres-vak** en druk **CTRL + V** om het IP-adres te plakken
- U ziet nu dat u de website van Google opvraagt

Vergeet niet uw IP-instellingen terug te zetten naar de laatste instellingen na deze test!!!

17.2 WLAN ROUTER (WI-FI)

Men kan nu i.p.v. de ROUTER ook een ROUTER met geïntegreerd ACCESS POINT (= WLAN ROUTER) gebruiken.

Deze router zal het mogelijk maken om draadloze verbindingen tot stand te brengen tussen de PC's en de WLAN ROUTER.

17.2.1 Beveiliging WLAN

Daar een draadloos netwerk kwetsbaarder is voor aanvallen van buitenaf, zullen wij door bijkomende instellingen in de WLAN ROUTER dit soort netwerken extra beveiligen.

17.2.1.1 Vuistregels voor een veilig WLAN

Wil men dus zijn WLAN beveiligen, dan kan men het best de volgende vuistregels in acht nemen:

- Zorg voor een gebruikersnaam en wachtwoord voor het configuratiescherm van uw ROUTER (zie vroeger)
- Activeer WEP of WPA
- Schakel SSID-broadcasting uit
- Voorzie uw shares van wachtwoorden (zie vroeger)
- Stel een MAC-adresfilter in voor WiFi-toegang
- Configureer uw firewall
- Blokkeer de radiosignalen van uw antenne in één bepaalde richting

Deze verschillende mogelijkheden bespreken we hierna

17.2.1.2 WEP (Wired Equivalent Privacy) en WPA (WiFi Protected Access)

Dit zijn de twee bekendste beveiligingsmethodes voor WLAN's.

WEP versleutelt de data die door de ether wordt gestuurd, maar is – zeker als er gebruik wordt gemaakt van oudere routers – redelijk eenvoudig te kraken.

Encryptie via WEP of WPA heeft bovendien invloed op de snelheid van uw netwerk. Dit kunt u afleiden uit de volgende tabel:

Transport snelheid bij het doorsturen v/e bestand van 250MB	
Zonder encryptie	2 MB/s
WPA	1,3 MB/s
WEP	1,1 MB/s

WPA is een WiFi-standaard die bedoeld is als uitbreiding op de beveiligingsfuncties van WEP.

WPA en WEP kunnen beschouwd worden als basisbeveiliging, die u altijd moet instellen om toevallige passanten buiten de deur te kunnen houden.

Het instellen doet u door een **wachtwoord** op te geven, waarna u de WLAN ROUTER of het ACCESS POINT moet herstarten. Kies hierbij ook voor een zo sterk mogelijke versleuteling bijvoorbeeld **128-bit encryptie**.

Verder verdient het aanbeveling alleen bepaalde computers toegang tot uw WLAN te verschaffen. Daartoe vult u in uw WLAN ROUTER of ACCESS POINT op een lijstje de geautoriseerde MAC-adressen in.

Een **MAC-adres** is een uniek adres van uw netwerkadapter.

Het MAC-adres van uw netwerkadapter kunt u vinden door in het DOS-venster het commando **IPCONFIG /all** in te typen. U ziet dan onder **Physical Adress** het MAC-adres van uw netwerkadapter.

17.2.1.3 SSID (Service Set Identifier)

Een SSID is een tekenreeks van 32 karakters die staat vermeld in de header van elk pakketje dat over een WLAN wordt verstuurd. De **header** bevat de naam van de zender en het ontvangende ACCESS POINT van het pakketje.

De meeste WLAN ROUTERS of ACCESS POINTS hebben een standaard **SSID die gebaseerd is op de merknaam** en zo **ingesteld is dat deze zichzelf bekend maakt in de ether**.

Wilt u dus dat uw buren of passanten niet weten dat u een WLAN hebt, dan zet u bij voorkeur **SSID-broadcasting UIT**.

Er bestaan echter **diverse softwaretooltjes** die WLAN's opsporen die GEEN gebruik maken van SSID. Dus 100% veilig is dit ook alweer niet.

17.2.1.4 MAC-adresfilter en IP-adres

Als u nu in de WLAN ROUTER alle MAC-adressen van de computers ingegeven hebt van de computers die verbinding mogen maken met dit toestel, dan nog is dit ook niet 100% veilig.

Hackers kunnen deze MAC-adressen met niet al te veel moeite klonen, en zo zich voordoen als één van de computers die toegang hebben tot uw WLAN.

De meeste WLAN ROUTERS zijn zo ingesteld dat ze automatisch IP-adressen uitgeven via een ingebouwde **DHCP-server**.

DHCP (Dynamic Host Configuration Protocol)
Dit is een communicatieprotocol waarmee systeembeheerders de verdeling van IP-adressen binnen hun netwerk centraal kunnen beheren.

Als er in een WLAN maar weinig gebruikers zijn, is het aan te raden DHCP uit te schakelen en met statische IP-adressen te werken. Dit is dan alweer een beveiliging waar hackers door moeten!

17.2.1.5 Firewall instellen

Het internet draait al sinds de vroege jaren 70 op TCP / IP, een relatief eenvoudige combinatie van twee protocollen die zorgt voor de adressering en veilige verzending van datapakketjes.

- **IP** (**I**nternet **P**rotocol)
  Breekt de datastroom die een computer genereert op in kleine pakketjes en voorziet deze van IP-adres en prioriteitslabels
- **TCP** (**T**ransmission **C**ontrol **P**rotocol)
  Garandeert op zijn beurt dat de pakketjes worden verzonden en dat ze daadwerkelijk aankomen op hun bestemmingsadres. Mochten er pakketjes ontbreken, dan wordt het verzoek nogmaals verstuurd. Bij aankomst assembleert TCP de datastroom en geeft deze door aan de ontvangende machine.

Een firewall scheidt uw computer of netwerk van de rest van het internet en controleert de integriteit van alle IP-pakketjes die naar binnen en naar buiten willen. De firewall accepteert de datastroom en vergelijkt de IP-headers met de door u gedefinieerde firewallregels. Op basis van deze regels worden de datapakketjes doorgelaten of de toegang tot uw domein ontzegd. Een firewall vertrouwt daarbij op twee basismethodes:

- Hij consulteert vooraf opgestelde lijsten van vertrouwde bronadressen
- Hij consulteert vooraf opgestelde lijsten van toegestane poorten

IP-poorten

Bij een verbinding met het internet worden er gegevens van en naar de computer verzonden door applicaties zoals de browser en e-mailprogramma's. Daarbij dient de PC te weten welke gegevens voor welk programma bedoeld zijn. Door voor elk programma een aparte poort te reserveren, zijn de gegevens op het juiste "adres" af te leveren. Deze primaire toegangspunten tot uw systeem noemen we IP-poorten.

Dit zijn **virtuele poorten**, geen fysieke poorten zoals USB-aansluitingen.

Over het algemeen zijn zend- en ontvangstpoorten op de communicerende machines gelijk aan elkaar. In totaal zijn er ruim 65.000 poorten, via welke programma's en services op uw computer kunnen communiceren. Om uw machine op een degelijke manier af te sluiten, moet uw firewall dus alle poorten in de gaten houden. Gelukkig is er een eenvoudige methode om deze klus te klaren, waarbij alles standaard wordt afgesloten, behalve de poorten die u definieert.

Welke poorten openstellen?

Enkel belangrijke poorten die u dient op te nemen in de firewall configuratie zijn:

- http: poort 80
- FTP: poort 21
- SMTP: poort 25
- POP3: poort 110
- Login (Login Host Protocol): poort 49
- Auth(Authentication service): poort 113
- MSN (chatprotocol): poort 1863

Het belang van een CENTRALE SERVER of HARDWARE ROUTER met ingebouwde firewall

Als u één van beide hebt dan hoeft u de client PC's van uw netwerk niet van extra persoonlijke firewalls te voorzien.

17.2.1.6 Antennes afschermen

Wilt u dat het radiosignaal van uw WLAN ROUTER maar in een beperkt gebied te ontvangen is, dan kunt u dit op 2 manieren doen:

- Deflectors aanbrengen (u kunt dit ook maken met Aluminium folie)
- Zendkracht van uw WLAN ROUTER of ACCESS POINT terugschroeven

Op deze manier moeten Hackers al binnen het zendgebied komen (meestal binnen uw huis of bedrijf), als ze willen inbreken op uw WLAN.

Het blokkeren van signalen kan tegenwoordig ook gebeuren met verf (zie www.forcefieldwireless.com).

17.2.1.7 Apart SUBNET instellen voor het WLAN

Een extra beveiligingsmethode is een draadloos netwerk inrichten, apart van het bestaand bekabeld netwerk, door gebruik te maken van een **apart subnet**, en een **eigen router en firewall** voor zowel het WiFi-netwerk als het bekabeld netwerk.

Nog beter is een volledig standalone WiFi-netwerk dat niet verbonden is met het bekabelde netwerk.

Het gebruik van een **ander subnet** (vaak wordt standaard voor 255.255.255.0 gekozen) voorziet in een fysieke scheiding van beide netwerken en biedt een vangnet tegen hackers als alle andere beveiligingsmaatregelen gefaald hebben.

De **firewall** moet ervoor zorgen dat alleen geautoriseerd verkeer van het draadloos naar het bekabeld netwerk mag gaan, de rest moet worden geblokkeerd.

Zet u een **draadloos netwerk alleen in voor internettoegang**, dan is het verstandig om daarvoor een WLAN ROUTER of ACCESS POINT te gebruiken, die voor een aparte verbinding zorgt. Toegang tot het bekabeld thuis- of bedrijfsnetwerk is dan niet mogelijk.

17.2.1.8 Conclusie

Een honderd procent veilige omgeving is een utopie. De veiligste computer is er één zonder besturingssysteem en toetsenbord, opgeborgen in een kluis. Het veiligste WLAN is een niet actief WiFi-

netwerk. Men kan dus alleen hopen dat als u enkele beveiligingen inbouwt, de “hacker” het liever eens bij uw buren probeert!

Om dit alles nu in de praktijk even uit te testen, baseren wij ons op Labo 011

Netwerken basis – Labo 011 – Peer-to-Peer netwerk 5 (IP)

17.2.2 Configuratie WLAN ROUTER

Stel het **IP-adres**, het **Subnetmasker** en het **admin wachtwoord** van de WLAN ROUTER in zoals we gezien hebben bij de configuratie van een “gewone” ROUTER.

Vergeet ook niet de **WEP of WPA codering in te stellen** (later meer hierover) en **de sleutel te noteren**, want die laatste zal u moeten ingeven bij het configureren van de PC’s die zich willen verbinden met de WLAN ROUTER!!!

17.2.3 Configuratie draadloze PC’s

Wij dienen bij iedere PC een draadloze netwerkadapter te installeren.

Deze kunnen onder de volgende vormen voorkomen:

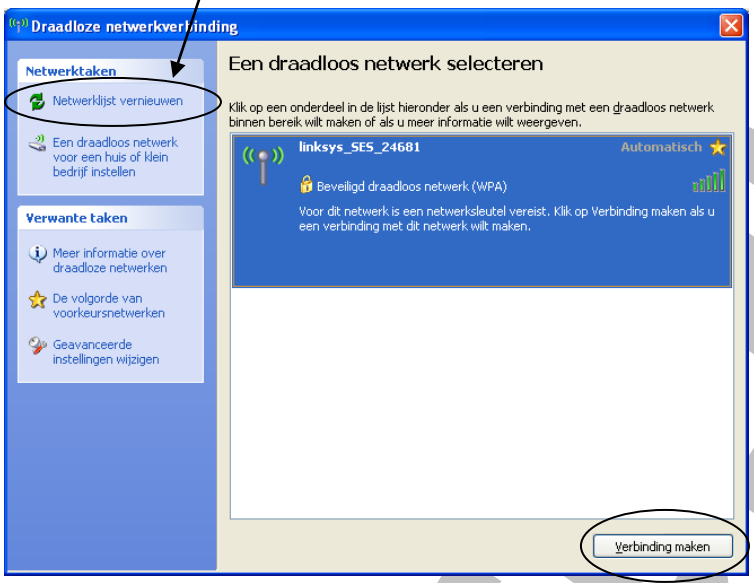
- PCI kaart
- PC Card
- Ingebouwd op het moederbord
- USB apparaat

In ons netwerk zullen wij gebruik maken van WLAN USB-adapters. Voor andere adapters blijft de werkwijze principieel hetzelfde, alleen moet men andere hardware gebruiken.

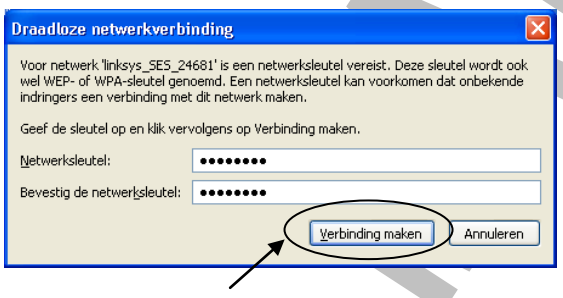
Deze adapters installeren wij als volgt:

- Zorg ervoor dat de WLAN ROUTER **aan** staat
- Steek de **WLAN USB adapter** in de PC
- **Installeer de drivers** die bijgeleverd zijn op CD (in de klas staan ze ook op het netwerk)
- Men krijgt na voltooiïng van de installatie in het systeemvak het volgende pictogram te zien  Dit duidt op een draadloze verbinding die niet actief is

- **Dubbelklik op dit pictogram** en men krijgt een lijst van de gevonden draadloze routers
  Ziet men zijn WLAN ROUTER niet tevoorschijn komen, klik dan een paar maal op **"Netwerklijst vernieuwen"**. De herkenning van zo'n draadloos signaal kan nogal op zich laten wachten!



- **Duid de router aan** met welke je verbinding wilt en druk op de knop **"Verbinding maken"**
- Nu wordt u (indien ingesteld in de router) de WEP of WPA sleutel gevraagd. Vul deze 2x in!



- Klik op **"Verbinding maken"**
- Na een tijdje verandert het pictogram in het systeemvak verandert nu in het volgende 
- U bent nu in staat via de WLAN ROUTER te **surfen** (**ALS** de IP-instellingen op **AUTOMATISCH** staan, anders moet men via TCP/IP eigenschappen alles juist zetten!!!)

18 Het netwerk aanbieden aan gebruikers

Nu het netwerk is opgezet zal men alle gebruikers een **"account"** geven om zich aan te melden op het netwerk en deze accounts bepaalde **"machtigingen"** toekennen.

18.1 Accounts

Elke gebruiker krijgt een account. Dit bevat zijn of haar naam en een wachtwoord. Daarmee krijgt de gebruiker toegang tot die delen op uw computer die u vrijgeeft voor gebruik (shares).

Voor elke account wordt een eigen map "Mijn documenten" aangemaakt, waar de gebruiker zijn eigen bestanden in kan plaatsen.

18.1.1 Soorten accounts

Windows XP heeft standaard 3 accounts:

- **Administrator**
  Alle rechten
- **Account met eigen naam**
  Is gemaakt bij de installatie van Windows XP en heeft ook alle rechten
- **Gast**
  Is standaard uitgeschakeld. **Indien ingeschakeld** (zie **Start – Configuratiescherm – Gebruikersaccounts – Klik op Gast – Schakel hem in**) kan iedereen zich als Gast aanmelden en toegang krijgen tot alle mappen en printers die niet met een wachtwoord afgeschermd zijn.

18.1.2 Account aanmaken

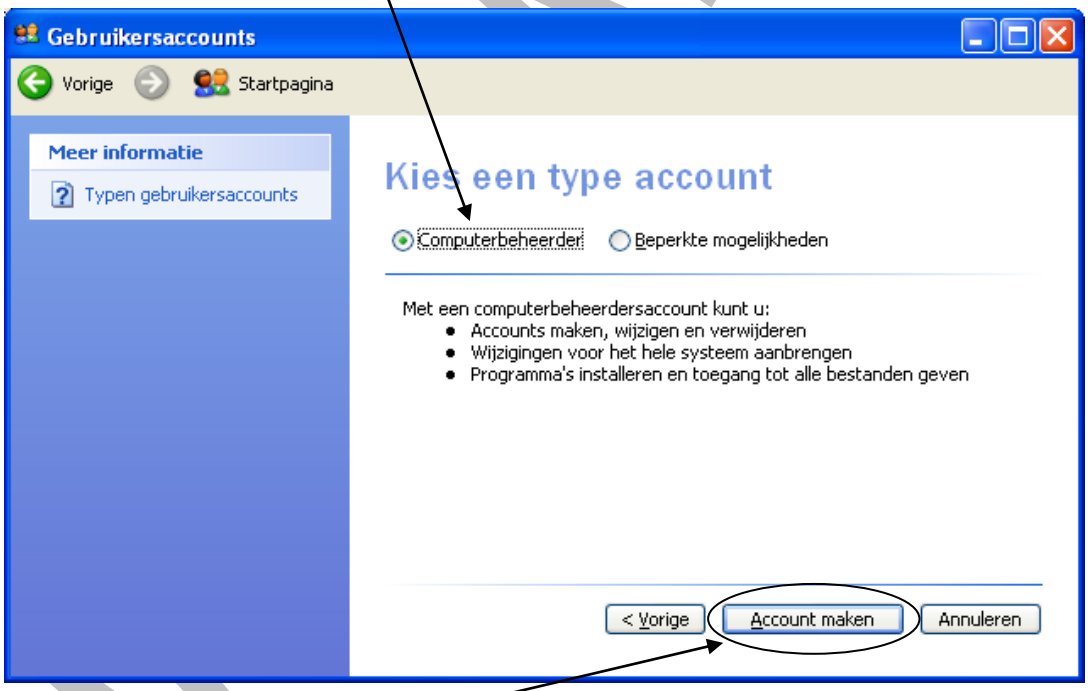
Klik op **Start – Configuratiescherm – Gebruikersaccounts – Een nieuwe account maken**

Kies nu het type account:

- **Computerbeheerder**
  - Mag accounts aanmaken, wijzigen en verwijderen.
  - Mag programma's en drivers installeren.
  - Mag de Registry aanpassen en andere systeeminstellingen wijzigen.
  - Toegang tot mappen, bestanden en printers instellen.
- **Beperkte mogelijkheden**
  - Mag eigen wachtwoord veranderen.
  - Mag voor eigen gebruik de achtergrond en andere instellingen voor het bureaublad wijzigen, deze wijzigingen zijn niet van toepassing voor andere gebruikers.
  - Eigen bestanden in de map **"Mijn documenten"** en in submappen daarvan plaatsen en bekijken.
  - Bestanden in de map **"Gedeelde documenten"** plaatsen en bekijken.

De map **"Mijn documenten"** wordt pas aangemaakt **als de gebruiker zich voor de eerste keer aanmeldt**. Deze map krijgt de naam die u als gebruikersnaam hebt opgegeven. U kunt de gebruikersnaam achteraf veranderen, zonder dat de aanmeldnaam en de naam van de map veranderen.

Kies hier **Computerbeheerder**



Klik op **"Account maken"**

18.1.3 Account aanpassen

Klik op **Start – Configuratiescherm – Gebruikersaccounts**

Klik op de account die u zojuist hebt gemaakt om een venster te openen met de volgende opties:

- **De naam wijzigen**
  - Verander een naam als deze conflicten oplevert met dezelfde naam van een andere gebruiker, of als u spaties in de naam wilt plaatsen.
  - **Let op:** hiermee verandert u niet de aanmeldnaam, alleen de naam die in het **welkomstscherm** en het menu **Start** wordt weergegeven.
- **Een wachtwoord instellen**
  - Geef een **wachtwoord** op volgens onderstaande beschrijving.
- **Andere afbeelding kiezen**
  - Wijzig de **afbeelding** die wordt weergegeven op het **aanmeldscherm** en het menu **Start**.
- **Het type account wijzigen**
  - Van **Computerbeheerder** naar **Beperkte mogelijkheden** of omgekeerd.
- **De account verwijderen**
  - Verwijdert de account, waarbij u moet opgeven of u de bestanden in de map **"Mijn documenten"** wilt behouden of verwijderen.

18.1.3.1 Een wachtwoord instellen

Standaard krijgt een account **geen** wachtwoord (ook de Administrator niet)!

Als u Windows XP als upgrade over een oudere versie van Windows hebt geïnstalleerd, zijn alle wachtwoorden verwijderd.

Een wachtwoord mag maximaal 127 tekens lang zijn. Gebruik echter minimaal 8 tekens en wissel hoofdletters af met kleine letters, cijfers en andere tekens.

Voorbeeld: dKL75#_sV5

Dit soort wachtwoorden zijn lastig te onthouden maar eveneens lastig te kraken!!!

Elke gebruiker kan zijn of haar eigen wachtwoord veranderen. Elke gebruiker die Computerbeheerder is, kan wachtwoorden van alle accounts veranderen.

Wij stellen het wachtwoord van **Gebruiker1** in op **aaa** en als geheugensteun gebruiken we het zinnetje **"drie maal de eerste letter van het alfabet"**

Maak nu een tweede gebruiker (Computerbeheerder) aan met de naam **Gebruiker2** en geef hem als wachtwoord **bbb** en als geheugensteun het zinnetje **"drie maal de tweede letter van het alfabet"**.

Na het maken van de twee gebruikers, sluiten we de computer af en starten terug op.

We zien nu het welkomstscherm met de twee nieuwe gebruikers: **Gebruiker1** en **Gebruiker2**

We loggen nu eerst eens in met elk van de twee gebruikers (zodanig dat hun eigen mappen in de hoofdmap **"Documents and Settings"** aangemaakt worden).

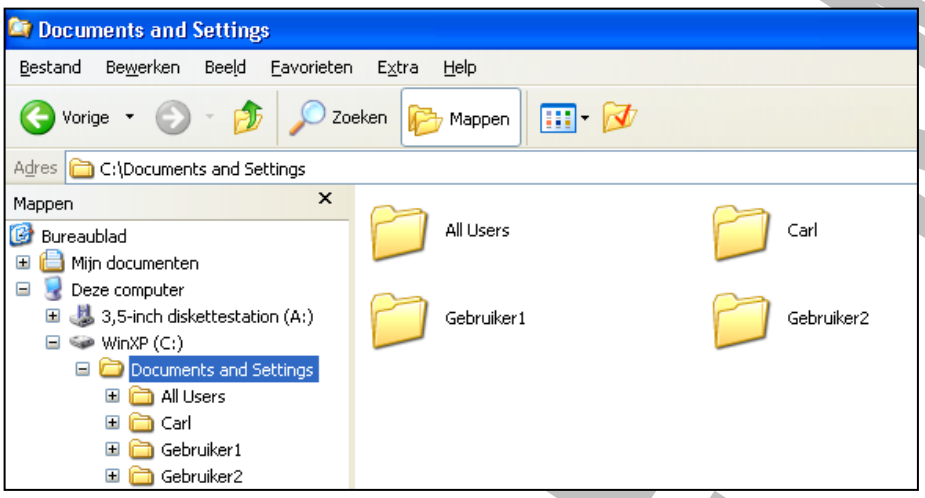
We kunnen nu ook gemakkelijk "switchen" van de ene account naar de andere, door te klikken op: **Start – Afmelden – Andere gebruiker**.

LET OP

Door te switchen van de ene naar de andere gebruiker, blijven alle de aangemelde gebruikers wel aangemeld. Wil men dus effectief een gebruiker afmelden dan klikt men op:

Start – Afmelden – Afmelden.

Switch nu naar de Standaard Computerbeheerder en controleer even in de verkenner of alle gebruikers hun eigen map gekregen hebben in de hoofdmap **"Documents and Settings"**.



In deze account map worden alle gegevens van de betreffende account bewaard!!!

- Men kan nu terug switchen naar **Gebruiker1**
- Daar wijzigt men de **achtergrond van het bureaublad** en plaatst men een **snelkoppeling naar "Kladblok"** op het bureaublad
- Dan switched men naar **Gebruiker2**
- Men wijzigt daar ook de **achtergrond naar nog iets anders** en plaatst een **snelkoppeling naar "Rekenmachine"** op het bureaublad

Switched men nu van de ene naar de andere account, dan merkt men dat deze instellingen behouden blijven!!!

Maak nu nog een derde account aan met de naam **Gebruiker3** en geef hem het wachtwoord **ccc** en als geheugensteun het zinnetje **"drie maal de derde letter van het alfabet"**. Daarna switch je naar deze gebruiker en je stelt terug enkel bureaubladinstellingen van deze gebruiker in.

18.1.3.2 Andere afbeelding kiezen

Indien nu de pictogrammen van de accounts je niet aanstaan, kan je deze veranderen als volgt:

- Kies **Start – Configuratiescherm – Gebruikersaccounts**
- Daar klik je op **Gebruiker1**
- Kies het item “Andere afbeelding kiezen”
- De rest wijst zichzelf uit

Geef **Gebruiker2** en **Gebruiker3** ook een andere afbeelding.

18.1.3.3 Het type account wijzigen

Men kan ook achteraf het type van account wijzigen, dit doet men als volgt:

- Kies **Start – Configuratiescherm – Gebruikersaccounts**
- Daar klik je op **Gebruiker1**
- Kies het item “Het type account wijzigen”
- Men kan er nu een account van maken met beperkte mogelijkheden

Maak van **Gebruiker2** en **Gebruiker3** ook een account met beperkte mogelijkheden.

18.1.3.4 De account verwijderen

Als men nu als **Computerbeheerder ingelogd** is dan kan men ook andere accounts verwijderen, dit doet men als volgt:

- Log in met de standaard **computerbeheerder**
- Kies **Start – Configuratiescherm – Gebruikersaccounts**
- Daar klik je op **Gebruiker3**
- Kies het item “De account verwijderen”
- De account **Gebruiker3** is weg

Sluit nu de computer volledig af!

18.1.4 De administrator in het welkomstvenster weergeven

Standaard verschijnen alle gebruikers met een account op een computer in het welkomstvenster. De Administrator verschijnt satndaard alleen in het welkomstvenster als u in veilige modus start.

Het is ook een stuk veiliger als u uw eigen account **Beperkte mogelijkheden** heeft. Omdat u dan niet meer het recht hebt om programma's te installeren, kunnen ook virussen, Trojaanse paarden en andere kwaadwillige programma's niet veel meer beginnen. U moet zich specifiek als **Administrator** aanmelden als u beheerstaken wilt uitvoeren.

U kunt zich op twee manieren als Administrator aanmelden:

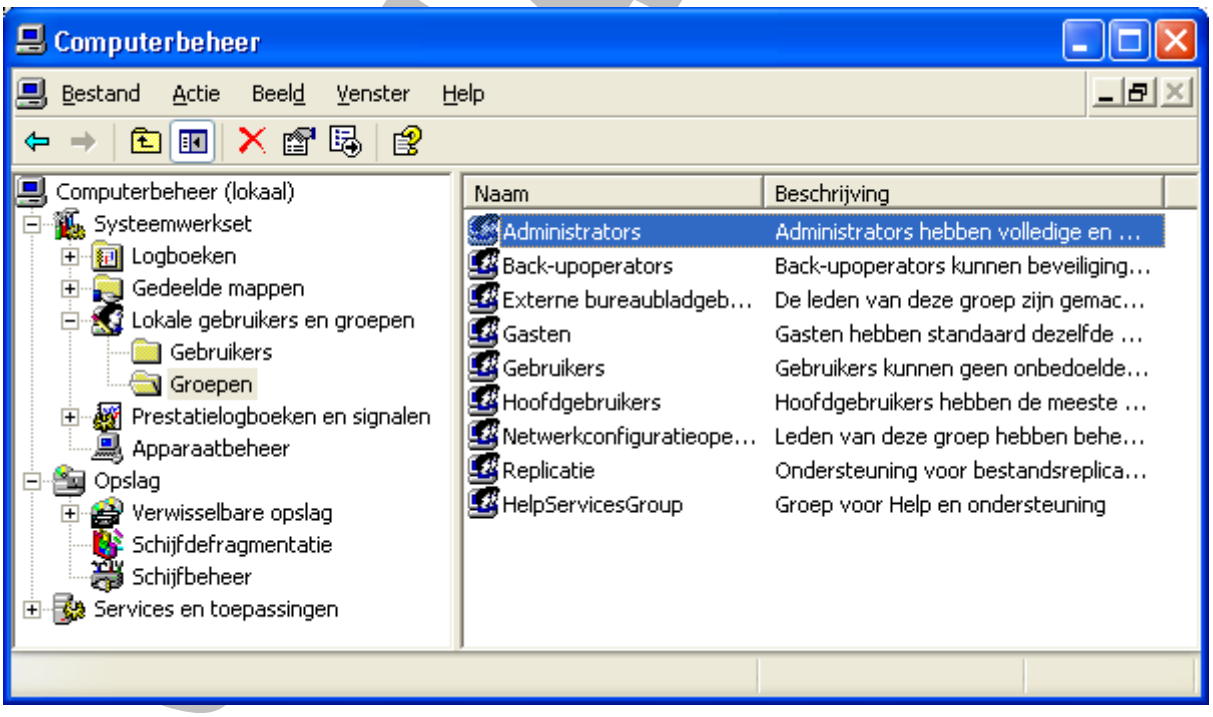
18.1.4.1 Via een toetsencombinatie bij het welkomstvenster

Als het normale welkomstvenster verschijnt, drukt u 2x na elkaar op CTRL + ALT + DEL. U krijgt nu een venster waar u zich als Administrator met het juiste wachtwoord kunt aanmelden.

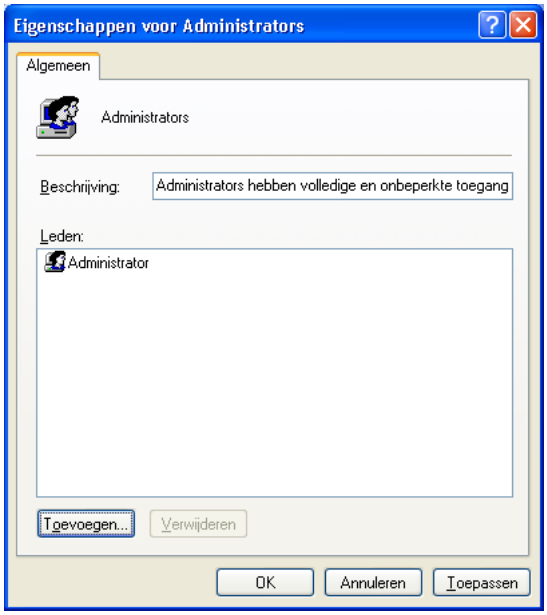
18.1.4.2 Voeg de Administrator toe aan het welkomstvenster

Dit kan u doen door de volgende stappen uit te voeren:

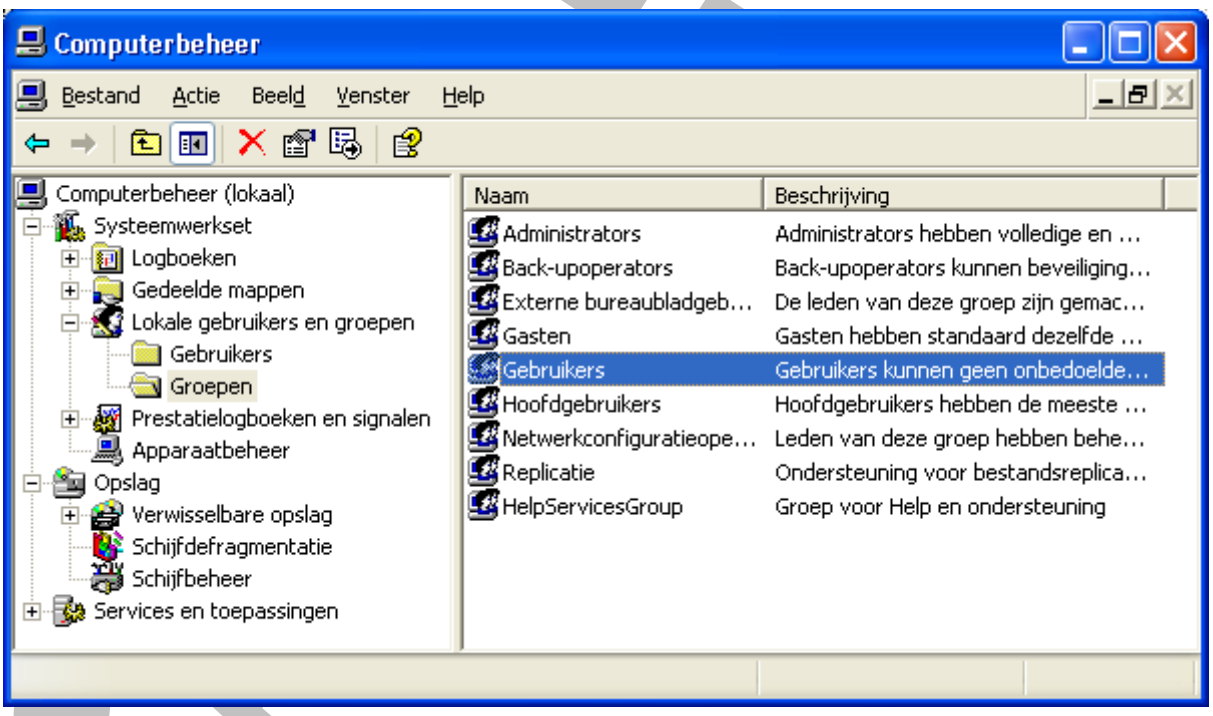
- Klik op **Start**, **rechtsklik op Deze computer** en kies **Beheren**
- In het venster **Computerbeheer** kiest u het item **Lokale gebruikers en groepen**, waar u eerst op **Groepen** klikt en vervolgens **dubbelklikt** op **Administrators** (rechter gedeelte)



- In het venster dat u nu krijgt, verwijdert u **ALLE** accounts, **behalve Administrator** en sluit het venster



- Klik nu op Gebruikers of Hoofdgebruikers en voeg de gebruikers toe die u hebt verwijderd (anders zijn ze niet meer zichtbaar in het welkomstvenster)

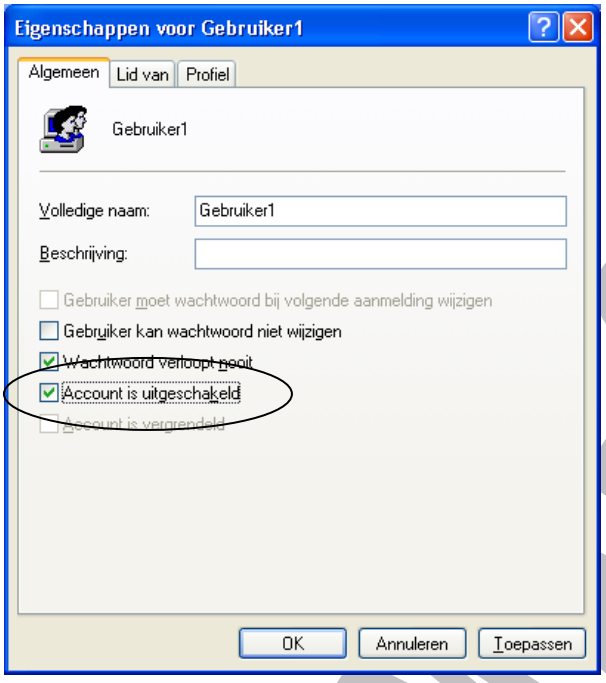


Voortaan verschijnt de gebruiker Administrator in het welkomstvenster!

18.1.5 Accounts uitschakelen

Wilt u nu een gebruiker **TIJDELIJK** de toegang tot een systeem ontzeggen (zonder zijn gegevens te verliezen), dan kan men deze account uitschakelen door de volgende stappen uit te voeren:

- Open terug het venster **Computerbeheer**
- Klik eerst op de map **Gebruikers**
- Dubbelklik nu op **Gebruiker1** en u krijgt het volgende venster (als u deze wilt uitschakelen)
- Zet een vinkje bij **"Account is uitgeschakeld"**



U zult deze account niet meer zien bij het welkomstvenster!

U kunt een account ook uit en aan schakelen via de opdrachtregel als volgt:

- Open het opdrachtvenster en typ **Net user [naam] /active:no**
- Schakel de account weer in met **Net user [naam] /active:yes**

18.2 Groepen

In het venster **Computerbeheer** staan bij **Lokale gebruikers en groepen** de verschillende groepen van Windows XP. U kunt hier gebruikers aan groepen toevoegen of ze verwijderen.

Administrators	Gebruikers die Computerbeheerder zijn
Gebruikers	Gebruikers hebben beperkte rechten. Ze kunnen • hun eigen account aanpassen • programma's starten • bestanden in hun documentmappen maken, wijzigen en verwijderen • bestanden in gedeelde documentmappen bekijken • machtigingen bekijken
Hoofdgebruikers	Mogen hetzelfde als Gebruikers. Verder kunnen ze • mappen delen • lokale printers maken en beheren • lokale gebruikers en groepen maken
Back-upoperators	Mogen back-ups maken en terugzetten
Netwerkconfiguratieoperators	Mogen netwerkonderdelen installeren en configureren
Gast	Kan • mappen en printers zonder wachtwoordbescherming gebruiken • kan geen wachtwoord voor zichzelf maken of veranderen

18.2.1 Een gebruiker aan een groep toevoegen

U kunt een gebruiker aan een groep toevoegen op de volgende manier:

- Open het venster **Computerbeheer**
- Ga naar de map **Groepen** in de map **Lokale gebruikers en groepen**
- Dubbelklik op de groep **Gebruikers** (in ons geval is dit de groep waar we iets willen aan toevoegen) en u ziet het venster **Eigenschappen voor [groepsnaam]**
- Daar klikt u op de knop **Toevoegen**
    - **Typ** nu de naam van de gebruiker(s) die u wilt toevoegen of
    - Klik op **Geavanceerd** en op **Nu zoeken** om een lijst met gebruikers te openen, **selecteer de naam of namen** en klik op **OK** om ze toe te voegen

18.2.2 Een nieuwe groep maken

Om een nieuwe groep te maken, klikt u in het venster **Computerbeheer** op **Lokale gebruikers en groepen**, dan op **Groepen** en kies vervolgens in het **menu Actie** voor **item Nieuwe groep**

18.3 Werkgroepen

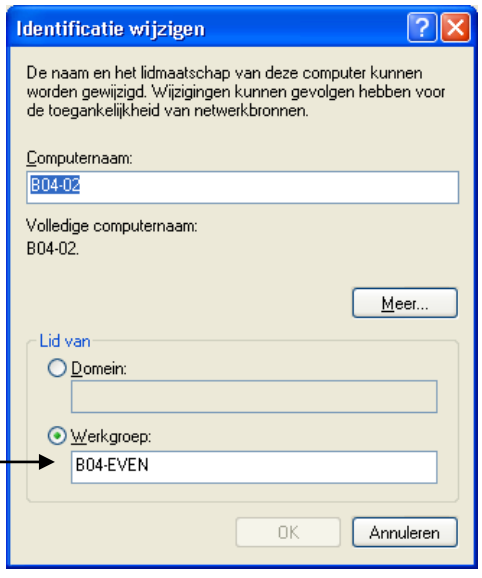
De hiervoor beschreven manier om accounts te maken, is bedoeld voor gebruik binnen **WERKGROEPEN**.

Een werkgroep (ook wel peer-to-peer netwerk genoemd) is een reeks computers die **allemaal dezelfde werkgroepnaam** hebben. De gebruikers van deze computers hebben toegang tot alle andere computers binnen dezelfde werkgroep, als op die computers een account voor de betreffende gebruiker is gemaakt.

U kunt ook een paar algemene accounts maken, bvb. Econoom, Administratie, Directie. Iedereen die de betreffende functie nodig heeft, meldt zich dan onder die naam aan.

Bij het installeren van Windows is al gevraagd naar de naam van de werkgroep. U past deze op de volgende manier aan:

- Ga naar **Start** en rechtsklik op **Deze computer**
- Kies het item **Eigenschappen**
- Ga naar het tabblad **Computernaam**
- Klik op de knop **Wijzigen** en u krijgt het volgende venster



- Typ de naam van de werkgroep in het vak **Werkgroep**

Zorg ervoor dat ALLE computers binnen het netwerk die zichtbaar moeten zijn voor de gebruikers, dezelfde werkgroepnaam krijgen!

19 Beveiliging

U moet uw computers beveiligen tegen aanvallen van buitenaf, en dan met name vanaf het internet, maar ook van binnenuit. De gebruikers mogen op andere computers alleen toegang hebben tot mappen en bestanden die ze nodig hebben. Indringers vanaf het internet zullen proberen virussen, Trojaanse paarden, spyware en andere ongewenste bestanden te installeren.

19.1 Bestanden en mappen beveiligen voorbereiding

Voor een goede beveiliging moet u eerst twee onderdelen instellen, als dat nog niet is gebeurd:

- De vaste schijf moet geformatteerd zijn in NTFS, omdat u dan bestanden en mappen kunt beschermen met rechten en wachtwoorden.
- Eenvoudig delen van bestanden moet zijn uitgeschakeld, omdat iedere gebruiker anders alles mag doen in de mappen waar hij toegang toe heeft.

19.1.1 Van FAT of FAT32 naar NTFS

U kunt een schijf achteraf converteren van FAT of FAT32 naar NTFS, maar niet omgekeerd. U doet dit als volgt:

Typ op de opdrachtregel **convert d: /fs:ntfs**

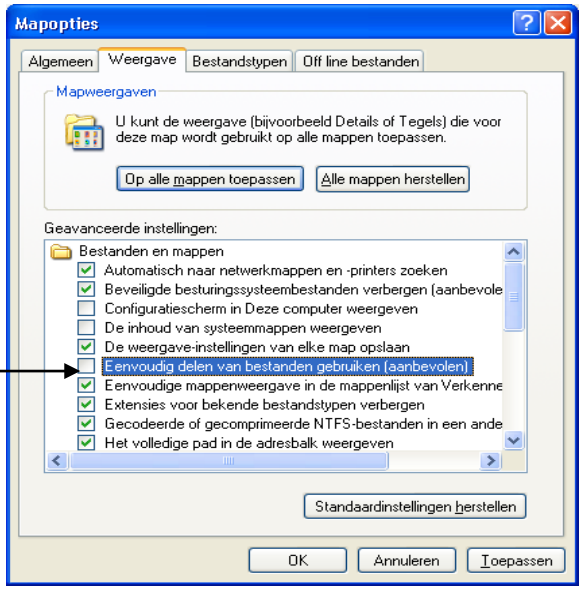
- d: is de schijf die u wilt converteren

Als u de startschijf wilt converteren, moet u de computer herstarten. De conversie wordt tijdens het herstarten uitgevoerd. Bij de conversie krijgen de systeemmappen al de juiste machtigingen toegewezen.

19.1.2 Eenvoudig delen uitschakelen

- Ga naar het **Configuratiescherm**
- Kies **Extra – Mapopties**
- Klik op de tab **Weergave**

Schakel het selectievakje “Eenvoudig delen van bestanden gebruiken” UIT



19.2 Het beveiligen van mappen en/of bestanden t.o.v. gebruikers

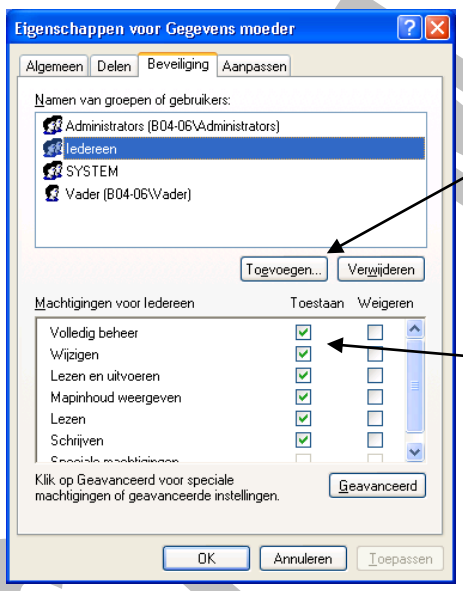
19.2.1 Hoe gaan we tewerk

Netwerken basis – Labo 012 – Gezinsnetwerkje

Het is zéér belangrijk dat op de verschillende PC's van het netwerk, identiek dezelfde gebruikers (gebruikersnaam en wachtwoord) ingesteld zijn. Anders kunt u gegarandeerd problemen verwachten met machtigingen!!!

Doe de voorbereidende stappen zoals opgesomd in het labo en werk dan verder volgens de volgende stappen om de juiste machtigingen in te stellen:

- Overtuig je ervan dat je **Eenvoudig delen** uitgeschakeld hebt, zie **Verkenner openen – Extra mapopties – Vinkje Eenvoudig delen uitschakelen**
- Klik bvb. op de map **"Gegevens moeder"** met de rechter muistoets
- Kies voor **Delen en beveiliging…**
- Ga naar het tabblad **Beveiliging** (hier kan men instellen wat groepen en gebruikers, **in de toekomst**, als **maximale machtigingen** kunnen hebben)
    - Voeg hier de groep **Iedereen** toe en geef hem **volledig beheer** (van de andere blijf je af)



Voeg de groep **Iedereen** toe.

Zie bijlage achteraan in de cursus

De toegevoegde groep **Iedereen** moet als machtiging **Volledig beheer** hebben

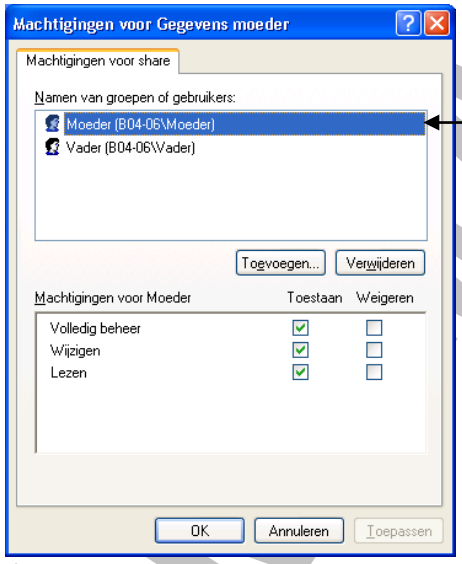
- Ga nu naar het tabblad **Delen**
- Je activeert het keuzerondje **"Deze map delen"**

LET OP

Bij deze netwerken kan dit alles erg lang duren, je moet dus echt veel geduld hebben om het resultaat te zien van iets wat je ingesteld hebt.
!!! RUSTIG BLIJVEN EN AFWACHTEN !!!

- Klik nu op de knop **Machtigingen**
- Het venster **"Machtigingen voor Gegevens moeder"** verschijnt

  In dit venster stelt men dan de **effectieve machtigingen** in!!!



LET OP

Hier mogen enkel de gebruikers staan die **VIA HET NETWERK** uw gedeelde map mogen benaderen.

Denk eraan dat je **PER GEBRUIKER** de **JUISTE MACHTIGINGEN** moet instellen!!!

Om dit te testen dient u dus op een **ANDERE COMPUTER IN HET NETWERK** te checken of u de gedeelde map van **UW COMPUTER** kunt benaderen op de juiste manier.

Op de volgende pagina staat een kort overzicht van wat de selectievakjes doen, die men kan aanduiden.

De map krijgt nu een **handje** onder het pictogram om aan te duiden dat ze gedeeld wordt via het netwerk.

Gedeelde map

19.2.2 Verborgen shares

Een bijzondere manier om een gedeelde map te beveiligen, is door deze onzichtbaar te maken.

- Open de **verkenner**
- Selecteer de **map** die u wilt delen en verbergen
- Klik met de **rechtermuisknop**
- Kies in het snelmenu **Delen en beveiliging**
- Het eigenschappenvenster verschijnt, met het tabblad **Delen** actief.
- Selecteer **Deze map delen** en plaats achter de naam in het vak Share-naam een **$**-teken
- Klik tenslotte op **OK**

Een map die u op deze manier verbergt, is nog altijd bereikbaar voor de gebruikers die de naam kennen.

Elke schijf heeft standaard een share: C$, D$. Deze kunt u niet uitschakelen.

19.3 Nog wat extra informatie i.v.m. machtigingen

19.3.1 Soorten machtigingen

Machtigingen bepalen wat iemand mag doen met een map, bestand of printer. De machtigingen worden vastgelegd in een **ACL** (**A**ccess **C**ontrol **L**ist). U kunt de volgende machtigingen aan gebruikers en groepen toewijzen:

Volledig beheer	De gebruiker of groep heeft alle onderstaande rechten. Deze worden alle automatisch geselecteerd.
Wijzigen	Mag bestanden lezen, veranderen en verwijderen, maar geen machtigingen toekennen of het eigendom overnemen.
Lezen	Bestanden weergeven, machtigingen bekijken, bestanden synchroniseren.

19.3.2 Machtigingen toewijzen

De eigenaar van een map (degene die de map heeft gemaakt of die het eigendom van de map heeft overgenomen), de leden van de groep Administrators en specifiek daartoe geautoriseerde gebruikers hebben het recht om machtigingen toe te wijzen.

- Ga naar het venster **"Machtigingen voor Gedeelde map PC##"** verschijnt
- Selecteer de naam van de groep of gebruiker waarvoor u de machtigingen wilt instellen, of klik op **Toevoegen** en voeg een naam toe.

Ken machtigingen zoveel mogelijk aan **groepen** toe. U hoeft dan alleen nog maar gebruikers die deze machtigingen nodig hebben aan de groep toe te voegen.

- Selecteer in de kolom **Toestaan** de rechten die u toestaat.

Gebruik niet de kolom **Weigeren**. Deze is bedoeld voor complexe netwerken. De uiteindelijke rechten zijn heel lastig te bepalen als u in beide kolommen selecteert. Gebruik ook niet de optie **Speciale machtigingen**, behalve als u precies weet wat deze inhouden. U maakt het beheer anders alleen maar bijzonder onoverzichtelijk.

19.3.3 Testen

Test de machtigingen door u aan te melden **vanaf een andere computer** in het netwerk, waarbij u een naam gebruikt waaraan u machtigingen hebt toegewezen.

Controleer of u alleen de mappen en bestanden kunt zien waarvoor u rechten hebt toegekend. Controleer ook of u een bestand kunt maken in een map waarop u alleen leesrechten hebt toegekend, bijvoorbeeld door een bestand vanuit een andere map te kopiëren.

Mocht u meer kunnen doen dan had verwacht, dan is de oorzaak vaak dat de gebruiker lid is van een groep die meer rechten heeft dan hij of zij persoonlijk heeft gekregen.

19.4 Herhalingsoefening op beveiliging en machtigingen

Als oefening op de voorgaande leerstof, gaan we een klein netwerk opstellen met enkele gebruikers.

Netwerken basis – Labo 013 – Beveiliging en machtigingen

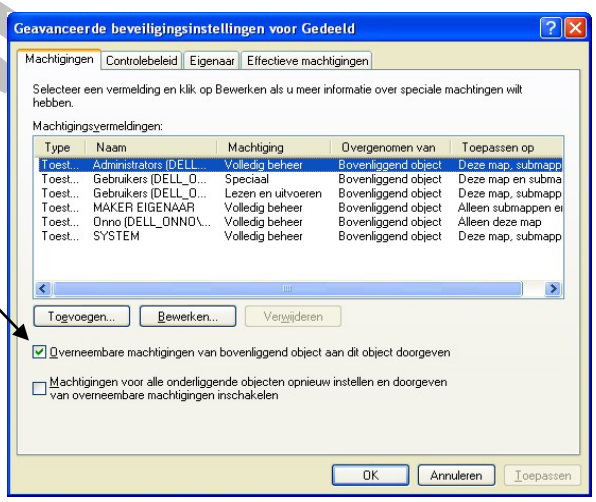
19.5 Machtigingen complexer

Gaan we nu terug even naar tabblad **Beveiliging** van de gedeelde map

Drukken we nu op de knop **Geavanceerd**, dan krijgen we nog een ander venster, waar we nog complexere instellingen kunnen ingeven.

19.5.1 Submappen en hun machtigingen

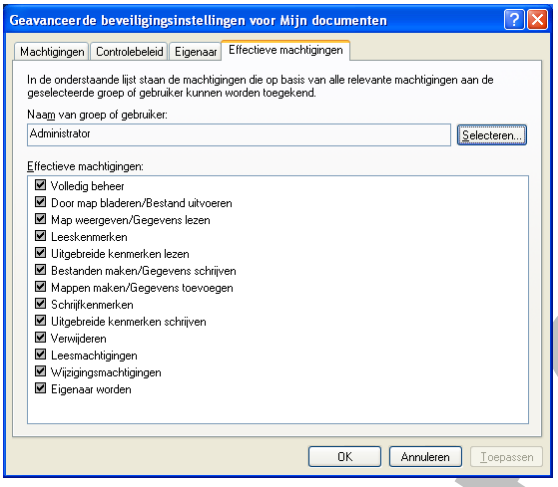
Standaard zullen de machtigingen die u voor een map toekent, zijn ook van toepassing op de submappen. U kunt in het tabblad **Machtigingen** controleren voor wie machtigingen zijn overgenomen voor submappen en voor bestanden in die mappen.



19.5.2 Machtigingen controleren

Controleren of een gebruiker wel de juiste rechten heeft (inclusief de overgeërfde rechten van bvb. De gebruikersgroep waar hij inzit) doet men als volgt.

- Open het tabblad **Beveiliging** voor de map waarvan u de rechten wilt controleren
- Klik op **Geavanceerd** en open het tabblad **Effectieve machtigingen**
- Typ de **naam** van degene van wie u de rechten wilt controleren. Alle beschikbare rechten worden aangevinkt



19.5.3 Machtigingen voor printers

Standaard krijgen alle gebruikers het recht om printopdrachten te maken en hun eigen printopdrachten te pauzeren, herstarten en verwijderen.

De groepen **Administrators** en **Hoofdgebruikers** kunnen printers en afdrukwachtrijen beheren.

De standaardmachtigingen zijn:

Afdrukken	Documenten afdrukken Eigen documenten beheren Eigenschappen van eigen documenten wijzigen
Printers beheren	Printer delen en verwijderen Printer onderbreken en herstarten Eigenschappen van printer veranderen Machtigingen veranderen
Documenten beheren	Documenten van anderen beheren

19.6 LogMeIn – Computers op afstand bedienen via het internet

Er is een eenvoudige (en gratis) mogelijkheid om computers op afstand te bedienen via het internet, **zonder kennis van het IP-adres** van deze computers.

Hierna volgen de stappen welke men moet ondernemen om dit te verwezenlijken.

19.6.1 Gratis account maken op LogMeIn

Waar:

Op een willekeurige PC met een internetverbinding.

Hoe:

Maak op www.logmein.com een FREE account aan. Men heeft hiervoor de volgende gegevens nodig:

- Een geldig email adres
- Een paswoord dat men zelf zal kiezen

19.6.2 PC op afstand bedienen via het internet

Waar:

Op de PC die je wilt bedienen op afstand via het internet.

Je moet het volgende dus doen op **iedere PC** die je wilt bedienen op afstand via het internet.

Hoe:

- Neem plaats achter de PC die je later wilt bedienen op afstand via het internet.
- Surf naar www.logmein.com en login met je gegevens die je in het vorig puntje aangemaakt hebt.
- Voeg de PC in, bij de lijst van PC's die je kunt bedienen op afstand via het internet.
- Je zal dan een scriptje moeten installeren op deze PC.
- Meldt je af.
- Vanaf nu kan je vanaf een PC met internetverbinding, deze laatst bijgevoegde PC bedienen.

Bijzonderheden:

- Als op de PC die je bedient op afstand via het internet, gebruikers gedefinieerd zijn, dan moet je de login van een "beheerder" van deze PC kennen, wil je deze PC kunnen bedienen.
- Je kan in je LogMeIn account, een **"secundaire" gebruiker** toevoegen, die dan ook **jou PC's of een deel er van** kan bedienen op afstand (zie groepen instellen en secundaire gebruiker instellen)

19.7 Automatische updates

De eerste stap voor de beveiliging van de toegang buiten het lokale netwerk is het inschakelen van **Automatische updates**. Microsoft brengt regelmatig patches uit in verband met beveiligingslekken in Windows XP. Schakel Automatische updates in om ervoor te zorgen dat deze automatisch worden geïnstalleerd. Bij de installatie van SP2 is Automatische updates ingeschakeld. U kunt de status controleren:

- Open in het **Configuratiescherm** het **Beveiligingscentrum**
- Achter **Automatische updates** moet **Ingeschakeld** staan
- Klik als dat niet het geval is op de koppeling **Automatische updates** en stel in dat u deze automatisch wilt ontvangen, hoe vaak (het liefst dagelijks) en op welk tijdstip

19.8 ActiveX-besturingselementen

Een van de manieren waarop kwalijke elementen worden verspreid, is via ActiveX-besturingselementen. Na de installatie van SP2 worden deze standaard door Internet Explorer geweigerd – en andere browsers kunnen er niet mee overweg.

Vandaar dat ik persoonlijk met de browser **Chrome** of **Firefox** werk!

Zodra een site een ActiveX-control wil laden, verschijnt een balk bovenin het venster van Internet Explorer.

- Klik in de balk. Een menu verschijnt
- Geef aan of u het besturingselement wilt laden

Veel van deze besturingselementen zijn bedoeld om een webpagina levendiger te maken

- Kent en vertrouwt u de site? Dan kunt u doorgaan
- Geen idee om welke site het gaat? NIET laden

19.9 Firewalls

Firewalls beschermen de computers binnen een netwerk tegen inbraak van buitenaf – het internet dus. Een firewall is een programma op een computer, router of gateway die de toegang tot bepaalde “poorten” bewaakt.

Een “poort” is een adres voor een toepassing. Zo is poort 80 de toegang tot een webserver, poort 25 tot een e-mailserver, enz… . Een firewall sluit alle poorten af, behalve degene die u nodig hebt.

19.9.1 Controleer uw beveiliging

Op het internet zijn er verschillende diensten die uw beveiliging (al dan niet tegen betaling) kunnen controleren, zoals:

- Shields Up! (www.grc.com)
- HackerWatch.org (www.hackerwatch.org/probe)
- AuditMyPC (www.auditmypc.com)

Voer een test op één van deze (of alle) sites uit om te zien in hoeverre uw computer zichtbaar is vanaf het internet.

19.9.2 Microsoft Firewall

Een van de belangrijkste nieuwe onderdelen van SP2 is de Firewall.

De Firewall houdt alle binnenkomende verkeer tegen, behalve het verkeer dat u toestemming geeft om door te gaan. Een aantal onderdelen is standaard al ingeschakeld.

Om te zien welke doet u het volgende:

- Klik in het **Beveiligingscentrum** op de knop **Firewall instellingen**
- Klik op het tabblad **Uitzonderingen**
- Voor alle programma's die worden doorgelaten staat een vinkje

U kunt eenvoudig programma's toevoegen, door op de knop **Programma toevoegen** te klikken.

19.9.3 Andere Firewalls

Een nadeel van de Firewall van Microsoft is dat alleen binnenkomend verkeer wordt geblokkeerd. Het is echter nog altijd mogelijk dat u Spyware, Trojaanse paarden en andere ongewenste programma's binnenkrijgt die, zonder dat u het merkt, zelf verbinding met het internet maken en allerlei berichten verzenden.

19.9.3.1 ZoneAlarm

ZoneAlarm (www.zonelabs.com) bestaat in verschillende uitvoeringen.

De eenvoudigste versie is gratis. De kracht van ZoneAlarm is dat de computer volledig onzichtbaar wordt gemaakt voor het internet (stealth-modus) en dat voor elk programma dat verbinding met internet of het

lokale netwerk wil maken, eerst eenmalig om toestemming wordt gevraagd. Het resultaat van deze toestemming wordt opgeslagen in een lijst die u altijd achteraf kunt aanpassen.

Andere programma's die soortgelijke functies verichten:

- Norton Personal Firewall (zie Norton Internet Security)
- McAfee Personal Firewall Plus (zie McAfee Internet Security Suite)
- BitDefender Professional (Antivirus, Antispam en Firewall in één packet)

De Firewall van Microsoft wordt door de meeste Firewallprogramma's uitgeschakeld.

19.10 Antivirus

De meeste virussen worden verspreid via e-mail. De ontvanger opent zijn bericht of een bijlage en het virus kan zijn werk gaan doen.

De beste beveiliging tegen virussen is dan ook: NIET ZOMAAR e-mailberichten te openen.

De ontvanger moet er een gewoonte van maken om elk bericht van een onbekende afzender direct te verwijderen.

19.10.1 Voorbeeldvenster

Veel e-mailprogramma's geven echter standaard een voorbeeldweergave. Schakel deze bij voorkeur UIT. In de meeste gevallen wordt een virus echter pas geactiveerd als u de bijlage opent!!!

19.10.2 Antivirusprogramma's

De volgende zijn gratis te downloaden:

- AVG Free Edition (www.grisoft.com) – Mijn persoonlijke voorkeur
- Avast! 4 Home edition (www.avast.com)
- AntiVir (www.hbedv.com)

20 Bijlage

20.1 Service Pack 2

Normaal gesproken is het delen van mappen op de harde schijf een eenvoudige zaak. Behalve wanneer de **andere gebruikers op uw netwerk geen toegang** krijgen tot uw gedeelde map.

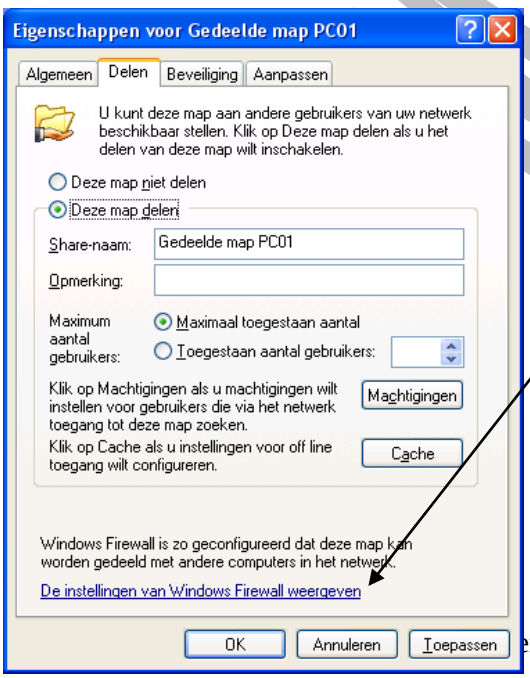
Probeer in eerste instantie geen ingewikkelde dingen, maar deel de map en geef iedereen **Volledig beheer**. Blijf van het **tabblad Beveiliging rechten** af.

Controleer of andere netwerkgebruikers u wel 'zien' in het netwerk. Daarvoor moeten zij bijvoorbeeld **tot dezelfde werkgroep behoren** en uw **IP-adres kunnen benaderen**.

Dit laatste kan een probleem opleveren als u een **firewall** gebruikt.

Dit is bijvoorbeeld het geval wanneer u **Windows XP Service Pack 2** hebt geïnstalleerd. Deze nuttige update stelt een strenger beveiligingsniveau in en schakelt de nieuwe **Windows Firewall** standaard in. De instellingen van de firewall bepalen of anderen toegang kunnen krijgen tot de 'server':

Het is mogelijk om vanuit de eigenschappen van een gedeelde map naar de firewall-instellingen te gaan.



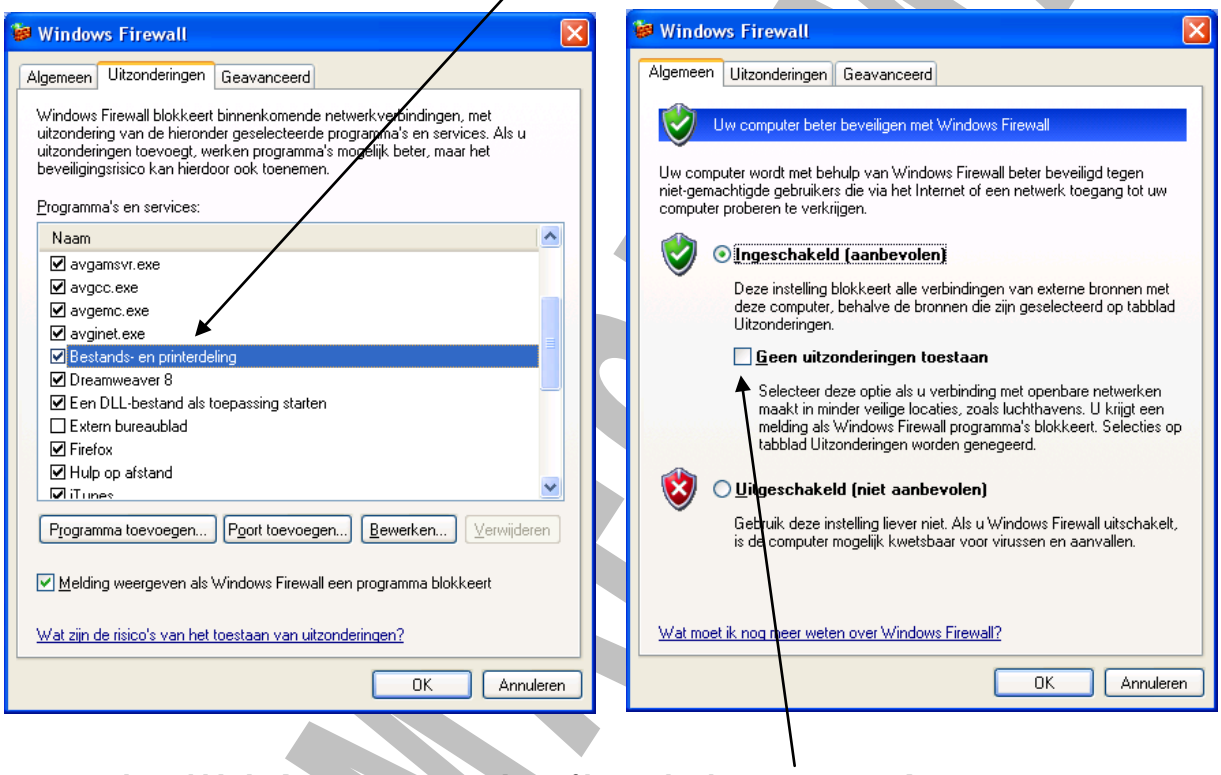
1. Rechtsklik op de gedeelde map en kies **Delen en beveiliging**.
2. Onderin het **tabblad Delen** vindt u informatie over de firewall. Als het goed is staat er Windows Firewall is zo geconfigureerd dat deze map kan worden gedeeld met andere computers in het netwerk.
3. Klik op de link **De instellingen voor Windows Firewall weergeven** om Windows Firewall te openen.

en is de volgende:

1. Kies op de server **Start - Configuratiescherm** en klik op **Beveiligingscentrum**.
2. Klik hier op de optie **Windows Firewall**.

Als je de eigenschappen van de firewall ziet gaan we verder:

1. Open in de Windows Firewall het **tabblad Uitzonderingen**.
2. Controleer of er een vinkje staat voor **Bestands- en printerdeling**. Zet deze optie aan indien het vinkje uit staat.



3. Open het tabblad **Algemeen** en controleer of het vinkje bij **Geen uitzonderingen toestaan uit staat**.
4. Sluit hierna Windows Firewall met de knop **OK**.

Nu moet het delen van mappen geen problemen meer opleveren.

20.2 Gebruikers en groepen toevoegen

- Klik op **Toevoegen** om het dialoogvenster **Gebruikers of Groepen selecteren** te openen

- Typ de naam of namen, gescheiden door puntkomma's
- Klik op **Namen controleren** om de volledige namen in te vullen. Als een naam niet op de computer bekend is, verschijnt een dialoogvenster. Binnen een werkgroep kunt u geen andere locatie opgeven, al is deze optie wel aanwezig. Als dit dialoogvenster verschijnt, betekent dit dat een account voor de gebruiker of groep niet op uw computer bekend is.

In plaats van namen te typen, kunt u ook op **Geavanceerd** en op **Nu zoeken** klikken om een lijst met beschikbare namen te openen.

20.2.1 SID

Elke account heeft een uniek **SID** (**S**ecurity **ID**). Als u een account verwijdert en vervolgens opnieuw aanmaakt, is de SID veranderd. U moet dan alle machtigingen opnieuw instellen.

20.2.2 CACLS

Een andere manier om machtigingen te bekijken en toe te wijzen is met **CACLS** (**C**ontrol **ACLS**) op de opdrachtregel:

- **Cacls *** geeft een overzicht van alle bestanden in de actuele map
- **Cacls *.doc** geeft een overzicht van alle bestanden met de extensie .doc
- **Cacls h05.doc** geeft een overzicht van het bestand h05.doc

Met de parameter **/G [naam]:x** krijgt de gebruiker **naam** het recht **x**.

De rechten zijn:

R	Lezen
W	Schrijven
C	Wijzigen
F	Volledig beheer

Met de parameter **/R [naam]** worden de rechten van gebruiker **naam** ingetrokken. Hierbij is ook de parameter **/E** (bewerken) nodig.

Met de parameter **/D [naam]** wordt de gebruiker **naam** de toegang geweigerd.