Inhoud leereenheid 3

Lokale netwerken

Introductie

Leerkern

1 Inleiding
2 Historische ontwikkeling
3 Structuur en componenten van een LAN
  3.1 Netwerkstations
  3.2 Bekabelingssystemen en draadloze verbindingen
  3.3 Netwerktopologie
  3.4 Netwerkapparatuur
  3.5 Netwerkprotocollen
  3.6 Netwerkprogrammatuur
  3.7 Toepassingen
4 Beveiliging van een LAN
  4.1 Toegangsbeveiliging
  4.1 Firewall
  4.3 Back-up

Terugkoppeling

– Uitwerking van de opgaven

Leereenheid 3

Lokale netwerken

INTRODUCTIE

In de vorige leereenheid hebben wij onder andere internet behandeld, momenteel het dominante wereldwijde elektronische netwerk. Op kleinere schaal is binnen organisaties het lokale netwerk van belang als technisch hulpmiddel voor informatievoorziening en communicatie.
In deze leereenheid gaan wij nader in op het local area network (LAN). Wij zullen naast de technische aspecten van dit communicatietechnologische hulpmiddel ook een aantal organisatorische aspecten de revue laten passeren. Tevens zullen we nagaan welke functionaliteit via LAN-implementaties gerealiseerd kan worden. Alleen de hoofdlijnen worden behandeld.

LEERDOELEN

Na het bestuderen van deze leereenheid wordt verwacht dat u

- kunt aangeven wat onder een local area network (LAN) verstaan wordt
- de oorsprong en ontwikkeling van het LAN kunt beschrijven
- de belangrijkste actoren rond het beheer van een LAN kunt benoemen
- de specifieke functies kunt benoemen die door een LAN ondersteund worden
- de onderliggende technische componenten kunt benoemen
- de onderliggende communicatiemedia kunt benoemen
- een probleemsituatie die zich voordoet rond het gebruik van een LAN, kunt analyseren in haar context.

Studeeraanwijzing

De verwachte studielast bedraagt 3 uur.

LEERKERN

1 Inleiding

Wat is een LAN?

Met de term local area networks worden lokale netwerken aangeduid van onderling gekoppelde computers en randapparatuur. Een LAN is in het algemeen geografisch beperkt van enkele tientallen meters tot maximaal enkele kilometers en beperkt tot één organisatie. In het algemeen zal een LAN ook gekoppeld zijn aan systemen buiten dit LAN, bijvoorbeeld aan internet, maar het kan in het algemeen toch als een afgebakende lokale structuur gezien worden.
De verantwoordelijkheid voor het beheer van het LAN is in handen van de organisatie die gebruikmaakt van een LAN. Eventueel kan de uitvoering van het beheer uitbesteed zijn, maar de verantwoordelijkheid blijft toch veelal liggen bij de organisatie die een LAN gebruikt.

Inmiddels is de omschrijving van een LAN niet meer alleen van toepassing op de koppeling van computers in grote bedrijven of overheidsinstellingen. Ook bij het midden- en kleinbedrijf (MKB) worden LAN's steeds meer gemeengoed, maar ook bij particulieren treft men steeds vaker een LAN aan, naarmate in veel huishoudens meer dan een computer in gebruik is en hiermee een klein netwerkje wordt gerealiseerd.

Ten opzichte van de hiervoor genoemde eigenschappen zullen er ongetwijfeld tegenvoorbeelden te vinden zijn bij specifieke implementaties. Een LAN kan zich over veel grotere afstanden uitstrekken dan hiervoor aangegeven (de studiecentra van de Open Universiteit Nederland kunnen bijvoorbeeld als onderdeel gezien worden van een landelijk gespreid LAN), er kan van een openbare infrastructuur gebruikgemaakt worden en de verantwoordelijkheid voor het beheer kan buiten de gebruikersorganisatie liggen. Door de gemaakte afbakening krijgt u echter een eerste indruk van wat onder een LAN verstaan wordt.

2 Historische ontwikkeling

Lokale netwerken hebben zich in het midden van de jaren tachtig ontwikkeld, een ontwikkeling die niet los gezien kan worden van de manier waarop organisaties zich in die tijd ontwikkelden. Enigszins clichématig kunnen deze verschillen in benadering binnen bedrijven als volgt naast elkaar gezet worden.

LAN: decentralisatie van centrale verwerking

Organisaties die al gewend waren aan krachtige centrale mainframes en andere soorten servers, zagen de ontwikkeling van het lokale netwerk als een ontwikkeling in de richting van decentralisatie. Op afdelingen ontstonden netwerken van computers met lokale servers. Deze ontwikkeling was een gevolg van analyses waaruit bleek dat veel van het netwerkverkeer tussen computers zich hoofdzakelijk beperkte tot de computers binnen één afdeling. Door de servers binnen die afdeling te plaatsen, kon een kostenbesparing gerealiseerd worden en kon een meer toegespitste dienstverlening aan de betreffende afdeling geboden worden. De servers en werkplekken namen deels de functies van de centrale systemen over. De centrale automatiseringsafdeling bood ondersteuning bij het vormgeven van de LAN-architectuur en zorgde voor de koppeling en integratie met de centrale systemen.

LAN: van eilandautomatisering naar koppeling van systemen

Aan de andere kant ontstonden de LAN-oplossingen vanuit organisaties met een minder centralistische informatievoorziening. Het betrof dan bijvoorbeeld organisaties zonder centrale ict-voorzieningen of er waren op het decentrale niveau redenen om het centrale beleid te ontwijken en decentraal LAN-voorzieningen te creëren los van de centrale automatiseringsafdeling. Hier werden dus computers aan elkaar gekoppeld die tot die tijd los van elkaar functioneerden.
In de loop der tijd werden deze lokale LAN's in het algemeen wel weer aan elkaar gekoppeld in een organisatiebrede infrastructuur. Een motief om toch te koppelen aan zo'n centrale infrastructuur was de opkomst van internet, e-mailverkeer en het intranet. Door op één punt in een organisatie een koppeling met internet te realiseren, konden kosten bespaard worden en kon de infrastructuur beter beheerd worden. Bovendien ontstond de mogelijkheid om de informatie- en

communicatievoorzieningen te versterken via het opzetten van intranetten en e-mail.

De laatste jaren zijn twee ontwikkelingen van belang voor de evolutie van LAN's. Allereerst heeft de opkomst van draadloze netwerken ervoor gezorgd dat werkplekken minder afhankelijk zijn geworden van bekabeling. Vooral voor laptops zijn hiermee nieuwe mogelijkheden ontstaan om deze flexibeler in te zetten binnen en buiten gebouwen. Een tweede ontwikkeling betreft de invoering van nieuwe diensten zoals voice over IP (VOIP). Met deze techniek wordt het mogelijk om het traditionele telefoonverkeer te integreren in datagerichte netwerken zoals een LAN. In leereenheid 4 zullen we dieper op deze ontwikkeling ingaan.

3 Structuur en componenten van een LAN

De volgende elementen die samen een LAN afbakenen, worden achtereenvolgens behandeld:
– netwerkstations
– bekabelingssysteem en draadloze verbindingen
– netwerktopologie
– netwerkapparatuur
– netwerkprotocollen
– netwerkprogrammatuur
– toepassingen.

3.1 NETWERKSTATIONS

Een netwerkstation is een apparaat dat als zelfstandige eenheid aan het netwerk gekoppeld is. Voorbeelden hiervan zijn onder andere een computer, een printer, een scanner of een ander apparaat dat rechtstreeks aan een lokaal netwerk gekoppeld kan worden.

3.2 BEKABELINGSSYSTEMEN EN DRAADLOZE VERBINDINGEN

De netwerkstations vormen de knooppunten in een netwerk. Om de knooppunten in een lokaal netwerk met elkaar gegevens te kunnen laten uitwisselen, is een verbinding tussen de stations noodzakelijk. De uitwisseling verloopt momenteel nog veelal via kabels, maar kan ook via draadloze verbindingen plaatsvinden.

In organisaties met honderden werkplekken, verdeeld over meerdere verdiepingen en gebouwen worden de kabels niet direct gekoppeld aan de netwerkapparatuur, maar gebruikt men veelal zogenaamde patch panels (zie figuur 3.1). In een patch panel komen alle netwerkverbindingen van bijvoorbeeld een verdieping op één centrale plek bij elkaar, waardoor het beheer van complexe bekabelingsinfrastructuren aanzienlijk vereenvoudigd wordt.

FIGUUR 3.1 Een patch panel

Draadloze systemen worden in LAN's veelal ingezet om mobiele netwerkstations zoals laptops te koppelen aan het netwerk.

CAT 5 en WiFi

Drie voorbeelden van verbindingstypen zijn:
– CAT 5: de momenteel gangbare standaard voor bekabeling waarbij uitwisseling van elektronische signalen via twisted-pairkabels plaatsvindt; een twisted-pairkabel bestaat uit een aantal paren koperdraden, waarbij elk paar om elkaar heen is gedraaid
– WiFi: wireless fidelity, een standaard voor draadloze uitwisseling van informatie via radiosignalen
– glasvezel: uitwisseling van gegevens via laserlicht door dunne kabels van glas.

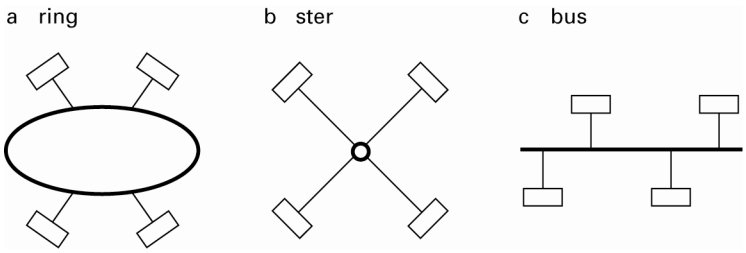
3.3 NETWERKTOPOLOGIE

Netwerktopologie

De *netwerktopologie* beschrijft de structuur waarmee de netwerkapparaten aan elkaar gekoppeld zijn. De protocollen beschrijven op welke manier de gegevens uitgewisseld worden tussen deze apparaten.

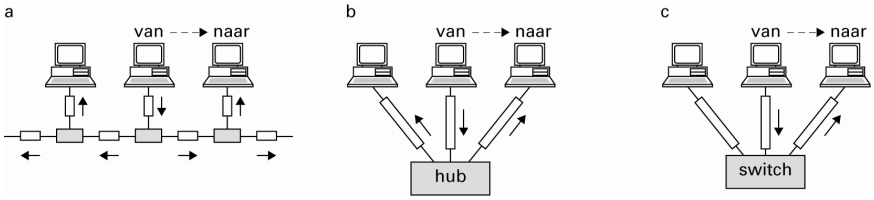
Bus
Ster
Ring

Netwerktopologieën nemen tegenwoordig meestal de vorm van een bus of een ster aan. Ringstructuren die in het begin van de LAN-ontwikkeling nog gebruikelijk waren, komen tegenwoordig nauwelijks nog voor. Figuur 3.2 toont de drie genoemde topologieën.



FIGUUR 3.2 De drie basale netwerktopologieën

De netwerktopologie bepaalt op welke manier gegevens in het netwerk uitgewisseld worden. In figuur 3.3 zijn een aantal configuraties weergeven.

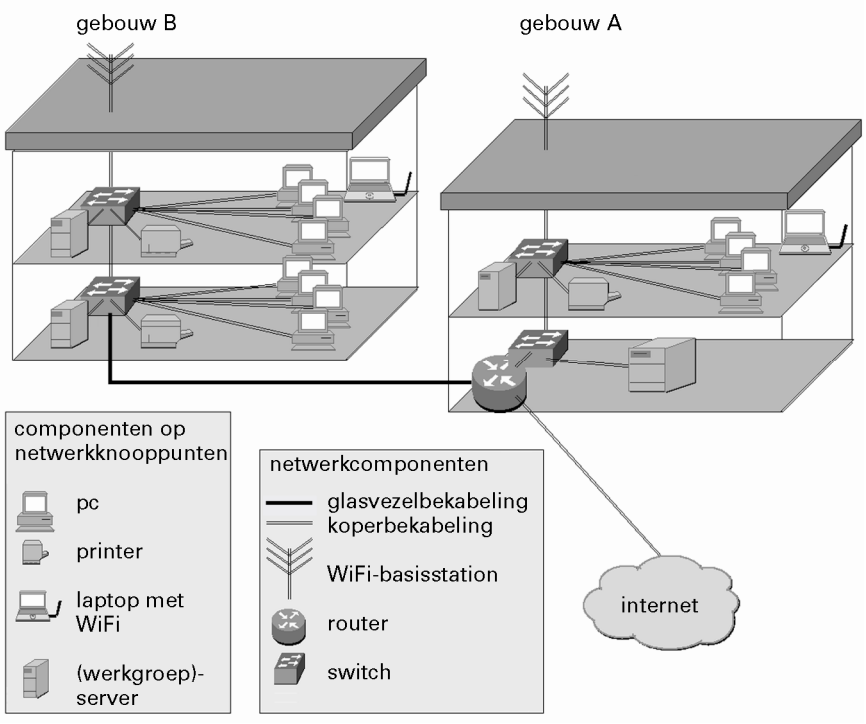


FIGUUR 3.3 De drie meest voorkomende topologieën in de huidige LAN's

Configuratie a: de datapakketten gaan via de bekabeling naar *alle* aangesloten netwerkstations. Alleen het netwerkstation waarvoor een pakket bestemd is, verwerkt het pakket.
Configuratie b: het datapakket gaat via de bekabeling en de *hub* naar *alle* aangesloten netwerkstations. Alleen het netwerkstation waarvoor een pakket bestemd is, verwerkt het pakket.
Configuratie c: het datapakket wordt via de *switch* alleen naar het bestemde netwerkstation doorgestuurd.

OPGAVE 3.1

Figuur 3.4 toont een typische netwerkconfiguratie bij een volledig geschakeld netwerk (dat wil zeggen dat elke computer direct op een switch aangesloten is) op een locatie met twee gebouwen met elk twee verdiepingen.



FIGUUR 3.4 Typische LAN-topologie

Probeer zo goed mogelijk de configuratie te beschrijven die weergegeven wordt. Begin bij de binnenkomende internetaansluiting en doorloop de verschillende verdiepingen. Geef ook aan in hoeverre er nog verder gewerkt kan worden wanneer één van de verbindingstypen uitvalt (internet, glasvezel tussen gebouwen, verbindingen tussen switches binnen een gebouw, de verbinding naar een pc).
Ga er hierbij van uit dat elke gebruiker de programmatuur voor de kantoortoepassingen en de persoonlijke gegevens van de server op de verdieping haalt, terwijl de centrale server op de benedenverdieping in gebouw a toepassingen en gegevens aanbiedt voor het gehele bedrijf.

3.4 NETWERKAPPARATUUR

Netwerkkaarten, modems, routers en switches zijn voorbeelden van netwerkapparatuur. Die netwerkapparatuur zorgt ervoor dat de informatiepakketten in het netwerk zo efficiënt mogelijk beschikbaar gesteld worden aan de netwerkstations in het netwerk waarvoor een bepaald informatiepakket bedoeld is.

Netwerkkaart

Om een koppeling tot stand te brengen tussen een netwerkstation en het netwerk is een specifieke network interface card (NIC) noodzakelijk. Afhankelijk van de bekabeling en het gehanteerde netwerkinterface verschilt de *netwerkkaart*. Ook in geval van een draadloze aansluiting is een antenne met aanvullende apparatuur nodig om radiosignalen uit te wisselen met het draadloze basisstation dat zorgt voor de koppeling aan de rest van het LAN.

Ethernet
Token-ring

Voorbeelden: de *ethernet*kaart is tegenwoordig de meest gebruikte netwerkkaart. *Token-ring* netwerkkaarten komen nog sporadisch voor in grotere organisaties met vooral IBM-apparatuur. In de paragraaf over netwerkinterfaces zullen de protocollen die ten grondslag liggen aan ethernet en Token-ring kort behandeld worden.

WiFi

Voor een draadloze verbinding van een pc met het netwerk middels WiFi wordt gebruikgemaakt van een speciale netwerkaansluiting op de pc die zich naar het besturingssysteem en de toepassingen in het algemeen echter op vergelijkbare manier manifesteert als een met kabels aangesloten network interface card (NIC).

FIGUUR 3.5 WiFi-hardware

Om grotere aantallen apparaten doelmatig aan een netwerk te kunnen koppelen, wordt specifieke netwerkapparatuur ingezet, die ervoor kan zorgen dat meerdere apparaten een netwerkaansluiting delen.

Hub

Switch

Wanneer er onvoldoende aansluitpunten beschikbaar zijn in een bepaalde ruimte, worden vaak *hubs* ingezet waardoor verschillende computers een verbinding kunnen delen. Het nadeel van een hub is dat de beschikbare bandbreedte die door het netwerk aangeboden wordt door de aan de hub aangesloten pc's gedeeld wordt. Bij een *switch* is dit niet het geval. Een switch zorgt ervoor dat de beschikbare bandbreedte zo efficiënt mogelijk verdeeld wordt. Bij een volledig geschakeld netwerk (dat wil zeggen dat alle pc's direct aan de switch gekoppeld zijn) kan elk werkstation beschikken over de volledige bandbreedte die het netwerk biedt, doordat alle computers direct in een stervorm op de switch aangesloten worden.

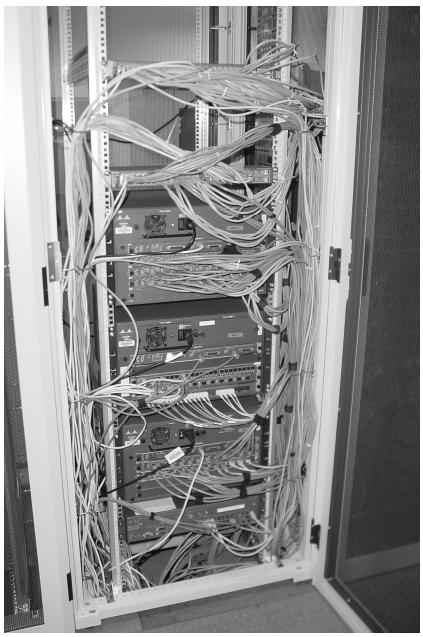
FIGUUR 3.6 Hub

Modem

De koppeling met de buitenwereld zal in veel gevallen totstandkomen via een *modem*. Dit apparaat zal internettoegang bieden via een ADSL- of een kabelaansluiting of via een reguliere analoge telefoonverbinding (minder voor de hand liggend voor de koppeling van een LAN, omdat het opbouwen van de verbinding steeds enige tijd duurt en de snelheid ook beperkt is).
Een digitale telefoonverbinding op basis van ISDN is een andere manier van koppelen aan een modem die vaak door kleinere bedrijven en particulieren gekozen wordt. Grotere organisaties zullen digitaal koppelen via een vaste verbinding. De hogescholen en universiteiten in Nederland zijn bijvoorbeeld gekoppeld via SURFnet.

Router

Op het koppelvlak tussen LAN en WAN (wide area network, het netwerk tussen organisaties) wordt in het algemeen een *router* geplaatst. In leereenheid 2 zagen wij reeds hoe een router een pakket naar het volgende netwerkstation stuurt. De router kan echter ook fungeren als firewall, dat wil zeggen dat de router pakketten met gegevens met een bepaalde herkomst of een bepaald adres kan weren. In de paragraaf over de beveiliging van een LAN gaan wij hier nader op in.



FIGUUR 3.7 Routers en switches

3.5 NETWERKPROTOCOLLEN

De netwerkprotocollen zorgen ervoor dat de gegevens correct via het netwerk verstuurd worden en door het juiste netwerkstation geïnterpreteerd en verwerkt worden. Zoals wij in de vorige leereenheid over communicatieprotocollen van internet reeds zagen, wordt het netwerkverkeer in een aantal lagen afgehandeld. Elke laag vervult een specifieke functie bij de regulering van het netwerkverkeer, waarbij elke laag zijn eigen protocollen kent waarin is vastgelegd op welke manier communicatie met de identieke netwerklaag op de aangesloten netwerkstations mogelijk is.

LAN-protocollen

In het begin van de jaren tachtig werden, ter ondersteuning van de in die tijd opkomende LAN-netwerken, specifieke *protocollen* voor dit type netwerken ontwikkeld. Deze protocollen waren bedoeld om netwerken te ondersteunen van beperkte omvang (zowel naar aantal aangesloten netwerkstations als naar geografische omvang).
Bij het ontwerpen van de netwerkarchitectuur van een LAN kon men ervan uitgaan dat een beperkt aantal stations over beperkte afstand aan elkaar gekoppeld werd, bijvoorbeeld om een afdeling netwerkvoorzieningen te bieden.

In leereenheid 2 (paragraaf 2.4) hebt u al kennisgemaakt met de gelaagdheid van internet. In lokale netwerken kan een vergelijkbare gelaagde structuur onderkend worden die bestaat uit: de fysische laag, de datalinklaag, de netwerklaag, de transportlaag en de toepassingslagen.

Fysische laag

De *fysische laag* wordt ingevuld door de al dan niet draadloze verbindingen die reeds hiervoor bij de LAN-bekabelingssystemen behandeld werden.

Datalinklaag

Frame

Het probleem waar een LAN-ontwerper op het niveau van de *datalinklaag* voor staat, is om ervoor te zorgen dat problemen opgelost worden, zoals de afhandeling van *frames* die gelijktijd op het netwerk geplaatst worden

(frame is de gebruikelijke naamgeving voor een gegevenspakket in een LAN).

Door ervoor te zorgen dat stations niet tegelijkertijd een frame op het netwerk kunnen plaatsen, kan dit probleem voorkomen worden. Omdat frames echter een eindige tijd op het netwerk aanwezig zijn, is er ook een mogelijkheid ingebouwd om botsingen te detecteren. Wanneer een botsing gedetecteerd wordt, zal het station dat het laatst een frame op het netwerk geplaatst had, dit frame na een vast bepaalde tijd opnieuw plaatsen. Deze techniek noemt men CSMA/CD (carrier sense multiple access with collission detection).

CSMA/CD

Het nadeel van dit protocol is dat bij grote aantallen stations veel botsingen voor kunnen komen, waardoor de capaciteit van het netwerk flink achteruit kan gaan.
Een andere manier om het probleem van de botsende frames op te lossen, is door voortdurend een *token* over het netwerk te laten circuleren wanneer er geen gegevens uitgewisseld worden. Een station dat een of meer frames wil versturen, pakt dit token op en verstuurt zijn frames. Wanneer dit station klaar is met het zenden van zijn frames, zal dit station het token weer op het netwerk plaatsen (vrijgeven) en krijgen andere stations de mogelijkheid om frames op het netwerk te plaatsen. Om te vermijden dat een station teveel frames aanbiedt en dus het netwerk langere tijd voor zich opeist, mag een station het token slechts een beperkte tijd vasthouden. Met deze techniek (met noemt dit *token-passing*) kunnen dus geen frames meer botsen en kunnen ze om deze reden ook niet verloren gaan. Token-passing heeft als voordeel dat voor tijdskritische communicatieprocessen goed te bepalen is hoelang het transport van een bepaalde hoeveelheid gegevens duurt. Het nadeel is echter dat deze standaard vereist dat de bekabeling altijd ringvormig gesloten dient te zijn. Het verwijderen van een station zonder de verbinding te herstellen, kan het hele netwerk platleggen.

Token-passing

Ethernet

De datalinklaag wordt binnen LAN's momenteel veelal ingevuld door het *ethernet*protocol. Dit is een implementatie van het CSMA/CD-protocol. Dit protocol werd al rond 1973 ontwikkeld.

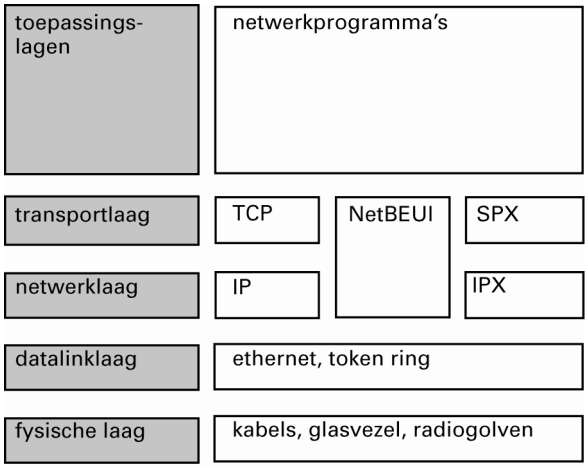
Token ring

Het *token-ring*protocol is een ander LAN-protocol voor de datalinklaag. Token ring is gebaseerd op het token-passingprincipe. Dit protocol is later ontstaan dan het ethernetprotocol en is eigenlijk een betrouwbaarder protocol, zeker bij grotere aantallen aangesloten stations. Het grote succes van het ethernetprotocol ten opzichte van het token-ringprotocol toont weer eens aan dat niet de beste technische oplossing hoeft te overleven.
De bandbreedte die door het ethernetprotocol wordt ondersteund, is explosief gestegen van 10 Mbps in de begindagen tot 10 Gbps vandaag de dag, terwijl ook de afstanden die overbrugd kunnen worden, zijn toegenomen van enkele tientallen meters tot wel 70 kilometer, zodat een LAN dus ook ingezet kan worden als een goedkoop alternatief voor een WAN.
Dat ethernet zich al die tijd heeft kunnen handhaven, is vooral te verklaren door de opkomst van de switched netwerken, waardoor elk station in feite een eigen verbinding heeft met de switch en dus geen botsingen van frames meer voor zullen komen.

Netwerklaag en transportlaag

TCP/IP, IPX/SPX, NetBEUI

Door de integratie van het internet en het LAN, sinds het begin van de jaren negentig, kan de transport- en de netwerklaag ook in LAN's gerealiseerd worden met TCP/IP, zoals op het WAN 'internet' al veel langer het geval was. Er bestaan echter ook specifieke LAN-protocollen zoals: IPX/SPX en NetBEUI. Figuur 3.8 toont een overzicht.



FIGUUR 3.8 De protocollagen bij een typisch LAN

De protocollen IPX/SPX en NetBEUI worden nog steeds ondersteund door de meeste moderne besturingssystemen.
Het protocol IPX/SPX (internetwork packet exchange / sequenced packet exchange) werd ontwikkeld in combinatie met het Novell. Het protocol NetBEUI (NetBIOS extended user interface) is vooral door IBM en Microsoft geadopteerd en geïntegreerd met de netwerkbesturingssystemen van deze bedrijven.
De verschillende protocollen kunnen naast elkaar gebruikt worden in een besturingssysteem zoals Windows. Omdat TCP/IP in het algemeen voldoende functionaliteit biedt, zijn de specifieke LAN-protocollen in het algemeen niet meer noodzakelijk voor de goede werking van een LAN. Zo kan de aansturing van de typische functies van de netwerkbesturingssystemen van Windows evengoed via TCP/IP verlopen als via NetBEUI.

Beveiliging door gebruik specifieke protocollen

Een motief om toch de specifieke LAN-protocollen op de netwerk- en transportlaag te gebruiken, kan bijvoorbeeld *beveiliging* zijn. Op een server die men van buiten het LAN absoluut niet toegankelijk wil maken, kan men bijvoorbeeld uitsluitend het NetBEUI-protocol installeren. Omdat dit protocol alleen binnen het LAN functioneert, is de betreffende server van buitenaf niet bereikbaar. Uiteraard kan men dan geen toepassingen op deze server installeren die typische internetprotocollen gebruiken, zodat deze server bijvoorbeeld niet als webserver kan functioneren.

Toepassingslaag

Bovenop de transportlaag kunnen nog een aantal lagen onderscheiden worden. Deze lagen vatten wij hier samen met de benaming *toepassingslagen*. De uitsplitsing in deze lagen zal in dit introducerende blok niet verder behandeld worden maar hieronder slechts genoemd worden. Een belangrijke reden hiervoor is dat deze lagen bij de meeste toepassingen van TCP/IP-netwerken niet helder onderscheiden worden.

OSI-referentiemodel

Open systems interconnection

De lagenstructuur die wij in dit blok als referentie gebruiken, bestaat uit vijf lagen is een variant van een algemener model: het *OSI-referentiemodel* dat in 1978 werd opgesteld. Dit model bestaat uit zeven lagen. Ten opzichte van het in dit blok gehanteerd 5-lagenmodel is de toepassingslaag opgedeeld in drie lagen: de sessie-, presentatie- en applicatielaag.

Samenvatting van de vier behandelde netwerklagen
De transportlaag zorgt ervoor dat de integriteit van de gegevenspakketten gewaarborgd wordt bij het transport tussen zender en ontvanger. De apparatuur en programmatuur bewaakt de kwaliteit van de verbinding, heft door buffering zoveel als technisch mogelijk is verschillen in tussentijdse transportsnelheden op en zorgt ervoor dat de gegevenspakketten in de juiste volgorde door de ontvangende computer verwerkt kunnen worden.
De netwerklaag zorgt ervoor dat de pakketten bij het juiste netwerkstation terechtkomen. De apparatuur en programmatuur zorgt ervoor dat elk pakket via het meest optimale pad tussen zender en ontvanger, gegeven de specifieke omstandigheden, verstuurd wordt en kan ook informatie verzamelen voor het doorberekenen van kosten voor het gebruik van het netwerk.
De datalinklaag zorgt voor de correcte stroom van de pakketten van en naar de netwerkstations. De apparatuur en programmatuur zorgt ervoor dat er geen verlies van gegevens optreedt tussen knooppunten in het netwerk, lost problemen op wanneer pakketten gelijktijdig bij een knooppunt in een netwerk arriveren en corrigeert zonodig en zo mogelijk de fouten tijdens het transport.
De fysische laag zorgt voor de correcte werking van de fysieke verbinding tussen de systemen waartussen de pakketten uitgewisseld worden. De apparatuur en programmatuur zorgt ervoor dat het juiste transportmedium bekend is, de transmissiesnelheid bekend is en de juiste stekkers en pluggen gebruikt worden.

3.6 NETWERKPROGRAMMATUUR

De netwerkprogramma's zorgen ervoor dat beschikbare diensten op eenvoudige manier toegankelijk zijn vanuit de verschillende stations. Bij moderne besturingssystemen zoals Windows XP/Vista of Linux is de specifieke netwerkprogrammatuur reeds ingebouwd, zodat de netwerkfunctie niet meer te onderscheiden is van de andere functies van zo'n besturingssysteem.

3.7 TOEPASSINGEN

Typische LAN-toepassingen die aangeboden worden aan de gebruikers, zijn:
– het delen van schijfruimte
– het delen van printers en andere randapparatuur
– het delen van toegang tot externe netwerken zoals het internet
– de installatie en het beheer van toepassingen vanuit een centraal punt
– delen van lokale databases
– toegang tot servers met gegevens in databases die van belang zijn voor de gehele organisatie, internet en intranetvoorzieningen
– toegangscontrole van personen
– centraal beheer van apparatuur en programmatuur.

De meest gebruikte toepassing in een LAN is veelal een verzameling van programmatuur voor tekstverwerking, het rekenen met spreadsheets, het maken van presentaties en het werken met elektronische kaartenbakken. De toegang tot het internet en het gebruik van e-mail zijn veel voorkomende toepassingen.

OPGAVE 3.2

Ga na hoe de verschillende elementen die in deze paragraaf genoemd zijn, in uw situatie ingevuld zijn voor de organisatie waarvoor u werkt of voor uw thuisnetwerk, wanneer u thuis een LAN hebt.

4 Beveiliging van een LAN

Wanneer u thuis een netwerk hebt of in een werksituatie gebruikmaakt van een LAN, wilt u natuurlijk veilig kunnen werken. U wilt dat de geïnstalleerde toepassingen en de daarbij behorende gegevens beschikbaar zijn, dat niemand uw gegevens zonder uw instemming kan benaderen en uw verbinding met de buitenwereld beschikbaar is voor het ophalen van informatie en het communiceren met andere personen.

Beschikbaarheid, integriteit, vertrouwelijkheid

U stelt daarmee eisen ten aanzien van *beschikbaarheid*, *integriteit* en *vertrouwelijkheid* van de voorzieningen waarover u beschikt. Deze beveiligingseisen brengen allerlei technische maatregelen met zich mee waarvan wij er hier drie zullen behandelen: toegangsbeveiliging, firewall en back-up.

4.1 TOEGANGSBEVEILIGING

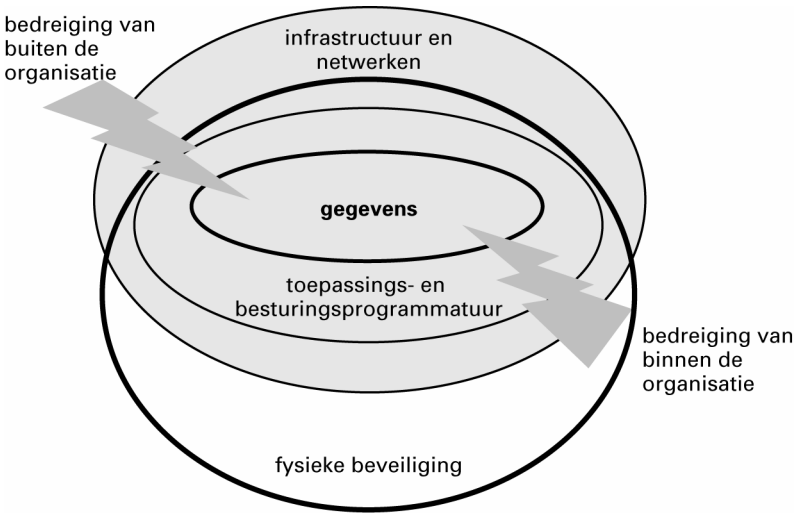
Toegangs-beveiliging

De voorzieningen die voor de gebruiker beschikbaar zijn via een LAN, worden tegen onrechtmatig gebruik beveiligd via *toegangsbeveiliging* (bijvoorbeeld met een gebruikersnaam en een wachtwoord). In het algemeen zal de toegang tot het LAN zelf reeds beveiligd zijn, zodat alleen daartoe geautoriseerde personen toegang hebben tot de netwerkvoorzieningen.

De toegangsbeveiliging zorgt er verder voor dat groepen van personen die mogelijk wel toegang hebben tot het LAN, uitsluitend en alleen toegang hebben tot de specifieke, voor de betreffende groep van personen bedoelde toepassingen, gegevens en communicatievoorzieningen.

Lagenmodel toegangsbeveiliging

Zoals wij reeds bij de netwerkinfrastructuur zagen, is ook beveiliging op te delen in niveaus, in dit geval niveaus van beveiliging. Een globaal model van beveiliging laat zien hoe de toegangsbeveiliging van het netwerk en de toepassingen geïntegreerd moet worden met andere vormen van toegangsbeveiliging.
Het *lagenmodel* geeft aan dat de kern, waar het bij beveiliging in essentie om gaat, de beveiliging van gegevens is (zie figuur 3.9).



FIGUUR 3.9 Lagenmodel toegangsbeveiliging

De fysieke omgeving (gebouwen en dergelijke), de infrastructuur en de programmatuur zijn vaak eenvoudig te herstellen, bijvoorbeeld door een uitwijkcontract af te sluiten, zodat bij calamiteiten op voorzieningen elders teruggevallen kan worden. Wanneer echter bedrijfsgegevens verloren gaan, worden de meeste organisaties in de kern van hun dienstverlening geraakt. Naarmate het voor bijvoorbeeld dienstverleners belangrijker wordt dat de diensten via een netwerk van buiten de organisatie toegankelijk zijn, wordt de bescherming van de toegang tot het netwerk een item op zich. Maar ook in dat geval ligt de uitdaging toch veelal in het beschermen van gegevens. Die bescherming dient ervoor te zorgen dat de integriteit van de gegevens behouden blijft, maar ook de vertrouwelijkheid via deze maatregelen wordt gewaarborgd.
Toen organisaties nog nauwelijks gebruikmaakten van externe netwerken, was de fysieke beveiliging de eerste beveiligingslinie. Grote rekencentra werden als moderne kastelen tegen indringers beveiligd via camera's en pasjessystemen. De fysieke beveiliging speelt voor de interne beveiliging nog steeds een belangrijke rol. Maar zoals wij reeds zagen, neemt de beveiliging van het externe netwerk in belang toe.
Is voor een indringer de fysieke beveiliging, dan wel de netwerkbeveiliging genomen, dan kan de programmatuur nog een vorm van beveiliging bieden.
De beveiligingsmaatregelen in de besturingsprogrammatuur en de toepassingsprogrammatuur dragen er dus toe bij dat de gegevens voor ongewenste toegang afgeschermd worden.
De beveiliging in de communicatietechnologische componenten heeft uiteraard vooral betrekking op de technische componenten van het netwerk.

OPGAVE 3.3
Geef voor elk van de in paragraaf 3 genoemde componenten van een LAN-netwerk voorbeelden van beveiligingsmaatregelen.

De meest gebruikte vorm van beveiliging waarmee de vertrouwelijkheid veilig gesteld wordt, is nog steeds de verplichting om gebruikersnaam en wachtwoord in te voeren in een toepassing. Steeds vaker worden echter meer betrouwbare voorzieningen gehanteerd zoals chipkaarten en meer

geavanceerde voorzieningen als biometrische identificatie waarmee unieke lichaamseigenschappen gebruikt worden, zoals de structuur van de iris of de vingerafdruk.

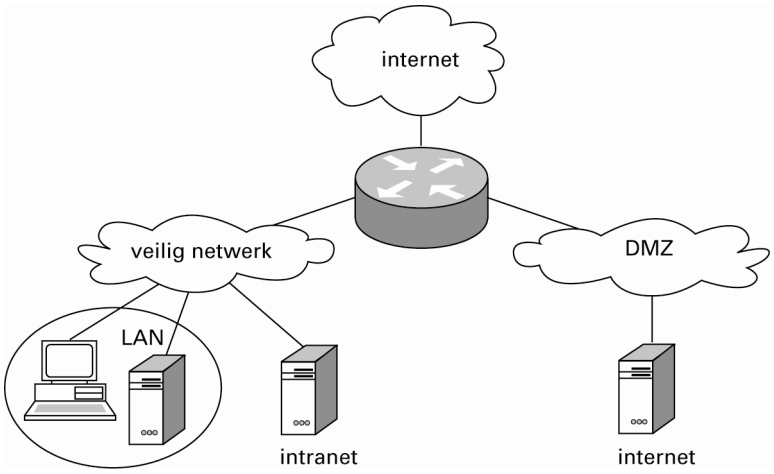
4.2 FIREWALL

Firewall — Brandwerende muur

Een manier van beveiligen vormt het selectief tegengehouden van IP-pakketten door een zogenaamde *firewall* (brandwerende muur). Met deze manier van beveiligen wordt generiek de toegang van delen van het interne netwerk voor buitenstaanders afgegrendeld. Deze firewall wordt meestal geïmplementeerd in netwerkapparatuur zoals routers, maar ook servers kunnen de functie vervullen om pakketten op het netwerk te screenen.
Een veel toegepaste strategie is om intern twee netwerken op te zetten. Het ene netwerk wordt maximaal beschermd. De werkplekken in het veilige netwerk kunnen wel een verbinding naar de buitenwereld opzetten, maar er kan geen verbinding op initiatief vanuit de buitenwereld opgezet worden naar systemen in het veilige netwerk. Dit wil dus niet zeggen dat geen gegevens van binnen naar buiten getransporteerd kunnen worden. Een gebruiker uit het veilige netwerk kan zondermeer het initiatief nemen om een bestand via FTP te verplaatsen naar een computer buiten de organisatie, maar een buitenstaander kan dit initiatief dus *niet* nemen.
Naast het veilige netwerk wordt een tweede netwerk opgezet van waaruit wel diensten aan de buitenwereld aangeboden kunnen worden die ook geïnitieerd kunnen worden vanuit de buitenwereld.

DMZ — Demilitarized zone

Dit deel van het netwerk wordt vaak aangeduid met *demilitarized zone* (DMZ). De servers in de DMZ kan men meer specifiek in de gaten houden en beschermen tegen inbraken. Bovendien kan men ervoor kiezen op deze servers zo weinig mogelijk gegevens te plaatsen, maar de gegevens te plaatsen op servers in het veilige netwerk. Deze gegevens worden uitgewisseld met de webserver via een extra beveiligde (via de firewall) en bewaakte (via netwerkbeheerprogrammatuur) verbinding (zie figuur 3.10). Wanneer de servers in de DMZ aangevallen worden, komen er in ieder geval geen vertrouwelijke interne gegevens beschikbaar.



FIGUUR 3.10 Bescherming van een netwerk via een firewall in combinatie met een demilitarized zone

Op deze manier wordt een beperkte vorm van beveiliging geboden tegen hackers die systemen binnen zouden willen dringen. Dit is geen absolute vorm van beveiliging, omdat er ook in deze configuratie noch allerlei inbraakmogelijkheden bestaan, bijvoorbeeld door het stelen van wachtwoorden van de beheerprogrammatuur of het gebruiken van fouten in programma's.

4.3 BACK-UP

Back-up

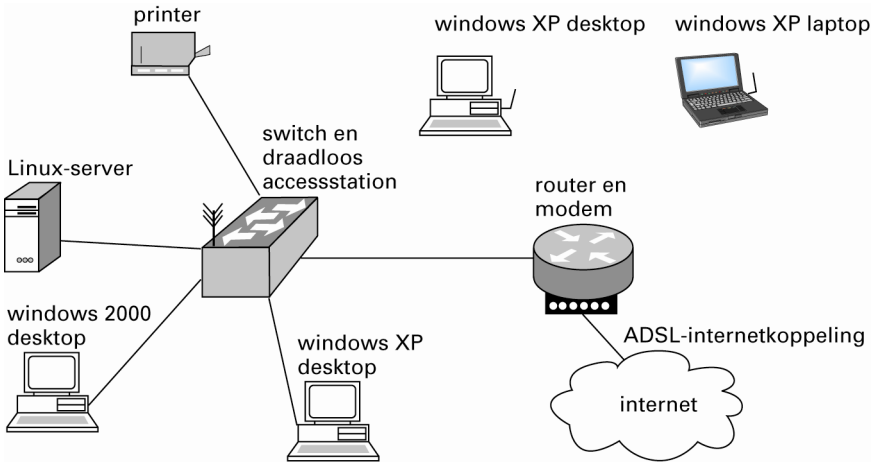
Om te voorkomen dat gegevens toch op de een of andere manier verloren gaan, worden er periodiek *back-ups* gemaakt van deze gegevens. Dit is een oplossing om de beschikbaarheid van gegevens veilig te stellen.
Back-ups worden op dit moment vaak nog op tapes geplaatst. In de toekomst zullen steeds meer back-ups op optische media geplaatst worden. De cd-rom en vooral de dvd zijn bij uitstek geschikt om gegevens over een langere periode stabiel vast te houden.

TERUGKOPPELING

Uitwerking van de opgaven

3.1 In gebouw A komt een externe internetaansluiting binnen. De router op de begane grond van gebouw A is via een koperverbinding gekoppeld aan de switch in dit gebouw en via een glasvezelverbinding naar de switch op de begane grond in gebouw B. Verder is in beide gebouwen de switch op de begane grond gekoppeld aan de switch op de tweede verdieping.
In beide gebouwen zijn op de begane grond de servers gekoppeld aan de switches die daar staan. Op de eerste verdieping van zowel gebouw A als gebouw B zijn de pc's en printers direct gekoppeld aan de switches die daar staan. Hieraan zijn ook de werkgroepservers gekoppeld die gegevens en toepassingen aanbieden voor de gebruikers op deze verdiepingen. Aan deze switches zijn ook de draadloze basisstations gekoppeld waarmee de laptops in dit gebouw verbinding kunnen maken.
In gebouw B treft u op de begane grond een aantal pc's, een printer en een werkgroepserver aan die zijn gekoppeld aan de switch aldaar. De werkgroepserver biedt gegevens en toepassingen voor gebruikers op de begane grond.
Wanneer de internetverbinding uitvalt, heeft geen enkele pc in beide gebouwen meer toegang tot het internet, maar er kan wel verder gewerkt worden met de kantoortoepassingen en de centrale toepassingen. Valt de glasvezelverbinding tussen de gebouwen uit, dan zijn in gebouw A nog alle voorzieningen beschikbaar maar kan men niet meer communiceren met de werkplekken in gebouw B. In gebouw B daarentegen kan men alleen nog werken met de kantoortoepassingen.
Valt de verbinding tussen de switches in een gebouw weg, dan kunnen de gebruikers op de getroffen verdieping alleen nog werken met de kantoortoepassingen. Valt een verbinding naar een pc uit, dan treft dat alleen de gebruiker van de betreffende pc. Valt een WiFi-basisstation uit, dan wordt hierdoor alleen de communicatiefunctie van de laptop getroffen die van dit station afhankelijk is.

3.2 Als referentie beschrijven wij hier een betrekkelijk omvangrijke configuratie die thuis staat bij één van de auteurs van deze cursus (zie figuur 3.11).



FIGUUR 3.11 Mogelijke configuratie van een privé-LAN

Netwerkstations
4 pc's (3 desktops en 1 laptop), een printer
Bekabelingssysteem en draadloos netwerk
CAT 5-bekabeling met ethernet, draadloos WiFi-netwerk, externe koppeling via een router-modem-combinatie aan ADSL
Netwerkinterfaces
TCP/IP
Netwerkprogrammatuur
De Windows-2000- en Windows-XP-werkplekken hebben ingebouwde netwerkprogrammatuur voor het verlenen van toegang en het delen van schijfruimte. Er is een softwarematige firewall (selectief uitsluiten van connecties naar de werkplek via TCP/IP) geïnstalleerd op de werkplekken. In het netwerk is ook een Linux-server opgenomen die voorzien is van een webserver (Apache). Via de server worden webpagina's beschikbaar gesteld voor gebruikers in het LAN, maar ook voor toegang vanuit internet.
Netwerkapparatuur
De netwerkapparatuur in dit netwerk bestaat uit een modem-router-combinatie en een switch die gecombineerd is met een draadloos WiFi-accessstation. Alle computers hebben een netwerkkaart, terwijl twee pc's beschikken over een draadloze koppeling naar het centrale WiFi-station.
Netwerktopologie
De pc's met een kabelverbinding zijn stervormig gekoppeld aan de switch.
Toepassingen
Op de werkplekken worden de volgende toepassingen gebruikt: Windows- en Linux-kantoortoepassingen, internetbrowser, e-mailclient, FTP-client, back-upprogrammatuur voor back-up naar cd's en diverse specifieke persoonlijke toepassingen.

3.3 Voorbeelden van beveiligingsmaatregelen
– Netwerkstations worden fysiek afgeschermd voor onbevoegden door het netwerkstation met een kabel aan de tafel te verankeren.
– Bekabeling wordt gekozen voor glasfiber zodat het netwerkverkeer niet afgetapt kan worden.
– Netwerktopologie krijgt een zodanige vorm dat het niet mogelijk is om door overbelasting op één plek het gehele netwerk plat te leggen.
– Netwerkapparatuur wordt beveiligd met wachtwoorden zodat onbevoegden geen wijziging in de instellingen aan kunnen brengen.
– Netwerkprotocollen: er wordt een firewall ingericht in een router die informatiepakketten kan blokkeren die afkomstig zijn van ongewenste bronnen.
– Netwerkprogrammatuur: iedere persoon moet zich eerst identificeren voordat toegang verkregen wordt tot de toepassingen.
– Toepassingen worden zodanig ontwikkeld dat er geen achterdeurtjes zijn waarmee onbevoegden toegang kunnen krijgen tot bepaalde programmatuur of gegevens.