1 Algemeen

1.1 Definities en begrippen

Een alomvattende, eenduidige definitie van een computernetwerk bestaat niet. Wel is er een aantal kenmerkende eigenschappen te geven welke gezamenlijk een operationele beschrijving van een computernetwerk geeft:

- Een computernetwerk bestaat uit een verzameling computersystemen (i.e. zelfstandige informatieverwerkende entiteiten)
- Deze computersystemen zijn aan elkaar gekoppeld door communicatieverbindingen, en
- Kunnen, via de communicatie verbindingen, interacties met elkaar hebben. Deze interacties volgen precieze interactievoorschriften (protocol), en
- Het geheel van informatieverwerking en interacties staat den dienst van een of meerdere specifieke (gebruikers-) doelen.

Een computersysteem is *zelfstandig* in die zin dat deze een informatieverwerkende taak kan uitvoeren. De *communicatieverbindingen* zijn nodig omdat de computersystemen geografisch verspreid zijn. De *topologie* van een computernetwerk en de geografische afstand van de computersystemen spelen een belangrijke rol. Ter aanduiding van de geografische spreiding van een computernetwerk onderscheidt men vaak *Local Area Networks* (LAN's), *Metrapolitan Area Networks* (MAN's) en *Wide Area Networks* (WAN's).

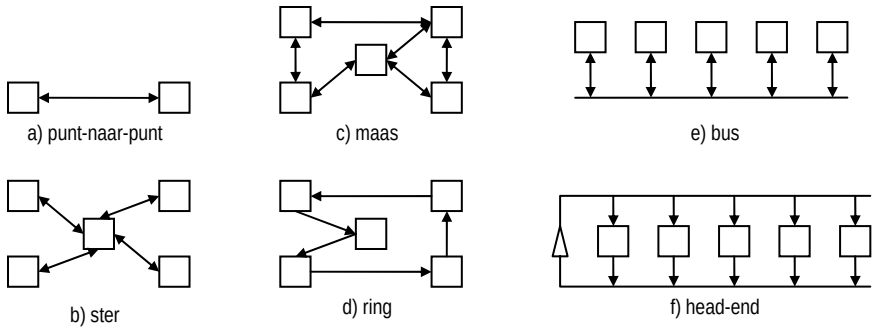
De *interactievoorschriften* voor interacties tussen computersystemen wordt een *protocol* genoemd. Protocollen worden doorgaans in protocolspecificaties vastgelegd, belangrijke aspecten hierin zijn de semantiek en syntaxis van de interacties. Ook is het essentieel dat een protocolspecificatie alleen die zaken voorschrijft die essentieel zijn voor het goed verlopen van de interacties: onderspecificatie is in deze funest en overspecificatie onwenselijk. Verder moet een protocol onafhankelijk zijn van mogelijke implementatiekeuzen. Achterliggende gedachte van deze eis is dat computernetwerken moeten kunnen worden opgebouwd met computersystemen van verschillende fabrikanten.

Een computernetwerk dient een gebruikersdoel. De term *gebruiker* dient hierbij in een ruime betekenis te worden opgevat: het zou een persoon kunnen zijn, maar ook een applicatieprogramma (bijvoorbeeld een bedrijfsapplicatie of een web-browser). Bekeken vanuit het gebruikersdoel, is het feit dat er een computer netwerk wordt gebruikt, bestaande uit computersystemen, verbindingen, protocollen etc. niet van belang. Het centrale concept waarmee het gebruikers aspect wordt gevangen en van

de interne structuur en werking wordt geabstraheerd is het concept *dienst* (of *service*).

1.2 Netwerktopologieën en Schakeltechnieken

De *topologie* van een computernetwerk wordt uitgedrukt in termen van de computersystemen en de communicatieverbindingen tussen deze systemen. Op het eerste gezicht lijkt de beste netwerktopologie die waarbij ieder computersysteem met ieder ander computersysteem is verbonden. Communicatieverbindingen zijn echter kostbaar. Bovendien, niet ieder computersysteem communiceert met ieder ander computersysteem, en in de loop van de tijd zullen er nieuwe computersystemen aan het netwerk worden aangesloten, en andere computer systemen worden losgekoppeld. Men streeft daarom naar optimalisatie van de verbindingsstructuren, hetgeen aanleiding geeft tot specifieke topologieën zoals: punt-naar-punt, ster, maasvorm, ring, bus en head-end (zie Figuur 1).



Figuur 1: Netwerktopologieën.

Punt-naar-punt topologie (Figuur 1.a): hierbij worden twee computersystemen met een communicatieverbinding met elkaar verbonden. Deze wordt doorgaans toegepast om grote geografische afstanden te overbruggen, bijvoorbeeld transatlantische verbinden.

Stertopologie (Figuur 1.b): in een stertopologie is een centraal computersysteem aanwezig en alle overige system zijn met een punt-naar-punt verbinding aan dit centrale systeem gekoppeld. Deze topologie komt voor in oudere netwerken met gecentraliseerde intelligentie, en in zogenaamde toegangsnetwerken, bijvoorbeeld om een thuis-PC toegang tot het Internet te geven.

De *maastopologie* (Figuur 1.c): in een maastopologie worden diverse computersystemen d.m.v. punt-naar-punt verbindingen met elkaar verbonden zodanig dat er meerderen mazen worden gevormd. Dit type topologie komt veelvuldig voor in netwerken die een grote geografisch gebied beslaan,

bijvoorbeeld een land of continent. Een belangrijk kenmerk is dat er meerdere routes bestaan voor de communicatie tussen twee computersystemen, waardoor de kwetsbaarheid verkleind wordt.

In de *ringtopologie* (Figuur 1.d): in een ringtopologie is een computersysteem met twee, zogenaamde buren, verbonden zodanig dat er een ring ontstaat. Een bronsysteem verstuurt de informatie via de ring, de buur verwerkt de informatie indien deze voor dit systeem bestemd is, en anders verstuurt deze het door naar de volgende buur. Dit type topologie zijn vooral te vinden in lokale netwerken.

De *bustopologie* (Figuur 1.e): in de bus topologie wordt gebruik gemaakt van 1 enkel fysiek medium (bijvoorbeeld coaxkabel) waarop meerdere computer systemen zijn aangesloten. Ieder systeem kan informatie versturen en ontvangen via het medium. Meerdere systemen mogen echter niet gelijktijdig informatie versturen. Dit geeft aanleiding tot het gebruik van een protocol om de toegang (i.e. het gebruik) van het medium te regelen: een zogenaamd Medium Access Control protocol. Dit type topologie komt vooral voor in lokale netwerken

De *head-endtopologie* (Figuur 1.f): de head-endtopologie bestaat uit een up-link (voor het versturen van informatie) en een down-link (voor het ontvangen van informatie). Ieder computersysteem is verbonden aan de up-link en de down-link. De up-link en down-link zijn zelf weer via een versterker aan elkaar gekoppeld. Deze topologie wordt o.a. gebruikt het televisie-kabelnetwerk geschikt te maken voor telefoon- en Internet-diensten.

In een computernetwerk vinden interacties plaatst tussen de computersystemen. Anders gesteld, ze wisselen informatie uit middels berichten. Er bestaan een aantal, verschillende technieken voor berichtenuitwisseling, t.w.: circuit-geschakelde, pakketgeschakelde en berichtgeschakelde netwerken. Computernetwerken zijn tegenwoordig allemaal pakketgeschakelde netwerken, en daarom zullen we alleen deze hier introduceren.

In een *pakketgeschakeld netwerk* worden gegevens verstuurd in pakketten, of *packets*, met een gegeven maximale of vaste lengte. Een *segmentation and reassembly* mechanisme zorgt ervoor dat de zender een bericht van willekeurige lengte opdeelt in één of meer pakketten (segmentation) en dat de ontvanger het oorspronkelijke berichten weer samenstelt uit de ontvangen pakketten (reassembly). Omdat de maximale lengte van de pakketten vaststaat, kan de verwerking in (schakel-) systemen efficiënt plaatsvinden. Er bestaan twee verschillende subklassen van pakketgeschakelde netwerken: virtueel circuit-geschakelde netwerken en datagram-geschakelde netwerken. In een virtueel circuit-geschakeld netwerk volgen alle pakketten dezelfde route door het netwerk van bron naar bestemming, in het netwerk (de netwerksystemen) wordt informatie opgebouwd om dit te bereiken; ATM netwerken behoren tot deze subklasse. In een

datagram-geschakeld netwerk worden alle pakketten onafhankelijk van elkaar door het netwerk vervoerd. Hierdoor is het mogelijk dat pakketten behorend tot hetzelfde bericht (als gevolg van segmentatie) verschillende routes door het netwerk volgen en in een andere volgorde aankomen bij de ontvanger; IP netwerken behoren tot deze subklasse.

1.3 Netwerkarchitectuur

De complexiteit van computernetwerken is in de loop van de tijd steeds verder toegenomen. Hiervoor zijn een aantal oorzaken aan te wijzen. Eindgebruikers stellen steeds hogere eisen aan computernetwerkgebaseerde toepassingen, waardoor een steeds grotere diversiteit aan toepassingsgerichte functies en diensten nodig is. Deze diversiteit uit zich onder andere in sterk verschillende eisen ten aanzien van de geleverde kwaliteit van de communicatie, zoals voor datacommunicatie, spraak en video. Gegeven het feit dat er al zeer vele verschillende netwerk- en communicatietechnologieën bestaan, en dit aantal in de toekomst alleen maar zal toenemen, ontstaat het probleem van integratie en samenwerking van die verschillende technologieën. Om dit soort complexiteitsproblemen het hoofd te bieden, is het noodzakelijk om structuur aan te brengen in de discussie over en het ontwerpen, implementeren en operationaliseren van computernetwerken. Voor dit doel, wordt traditioneel een zogenaamde horizontale en verticale structuur aangebracht. Binnen deze structurering wordt vervolgens een aantal belangrijke beschrijvingsconcepten gebruikt die het mogelijk maken om computernetwerken op verschillende abstractie- c.q. detail niveaus te beschouwen; deze concepten zijn: service en protocol.

Algemene Structureringprincipes

Zoals hiervoor aangegeven, wordt bij computernetwerken gebruik gemaakt van een horizontale en verticale structurering. Bij netwerktopologieën is al duidelijk naar voren gekomen dat bij computernetwerken sprake is van geografisch gedistribueerde systemen.

De *verticale structuur* ontstaat door in het netwerk substructuren te onderscheiden met gelijke of overeenkomstige interactiepatronen. Concreet zijn dit computersystemen zoals routers, switches, hubs, gateways, servers, printers en PC's. Hierdoor komt de verticale structuur overeen met de geografische scheiding van de computersystemen.

De *horizontale structuur* ontstaat door binnen ieder verticaal element, de functies die de toepassing direct(er) ondersteunen dicht(er) bij de toepassing te plaatsen, en de middelen waarop deze functies steunen daar hiërarchisch onder te plaatsen.

Door deze benadering herhaaldelijk toe te passen ontstaat een horizontale structuur van *hiërarchisch gerangschikte lagen* van functies. Binnen ieder systeem zijn dezelfde functies op hetzelfde niveau in de hiërarchie, d.w.z. in dezelfde laag, geplaatst.

Beschrijvingsconcepten

service

De toepassing van het horizontale structuringsprincipe van computernetwerkfunctionaliteiten geeft aanleiding tot een belangrijk concept, namelijk die van service. Om niet alle mogelijke horizontale lagen in een keer te hoeven beschouwen, is het noodzakelijk om te kunnen abstraheren van die (horizontale) gelaagdheid. Het concept service doet dit met betrekking tot de geleverde functionaliteit: het adresseert het "wat" (datgene waar de omgeving gebruikt van kan maken), en niet het "hoe" (de interne structuur, opbouw, samenhang en distributie). Een service wordt beschreven door zijn structuur en gedrag.

De structuur van een service wordt beschreven door de betrokken entiteiten, dit zijn: een *service provider* - de entiteit die de service levert; en één of meerdere *service users* die de service gebruiken. Interacties tussen service users en service provider wordt mogelijk gemaakt door zogenaamde *service acccess points*. Een voorbeeld van een service structuur is in Figuur 1.a gegeven, met daarin een service provider TS Provider, en twee service users TS User A en TS User B. Interacties vinden plaats via de service access points TS-A en TS-B.

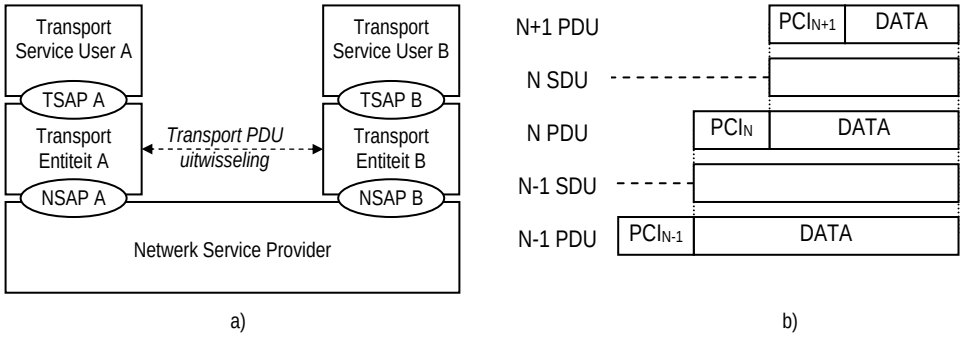
Het gedrag van een service wordt beschreven met behulp van een interactie diagram. Interactie vinden plaats via de service access points, en het interactie diagram geeft de tijdsvolgorde weer van de interacties. De eenheid van interactie wordt *service primitieve* genoemd. Een voorbeeld is in Figuur 1.b gegeven. In het diagram zijn de service access points opgenomen, de verticale lijnen geeft de tijd weer, en de horizontale pijlen met de annotaties dataRequest(.), dataIndicatie(.) etc., zijn de optredende service primitieven. Tot slot is d.m.v. stippellijnen de causale relatie tussen de optredende service primitieven aangegeven.

Figuur 2: Transport service: (a) service structuur; (b) service gedrag.

Protocol

Een protocol definieert hoe functies van een laag bijdragen aan de service die aan de direct daarboven liggende laag wordt geleverd. Anders dan het serviceconcept is het protocolconcept bedoeld om de functionele structuur en inhoud van een specifieke laag te definiëren. Het protocolconcept is niet gericht op de gebruiker van een laag, maar op de ontwerper die de functies van de laag moet implementeren, en is dus van belang voor de fabrikant.

N-protocol - Een N-protocol definieert de functies van laag N en de manier waarop de interactie van deze functies, via de onderliggende N-1-service, de N-service leveren. Een protocol kan dus niet onafhankelijk gezien worden van de service waarop het steunt en van de service die het moet ondersteunen. Figuur 3.a geeft een voorbeeld van het *transport protocol* dat steunt op de *netwerk service* om de *transport service* te leveren.



Figuur 3: Transport Service: (a) Transport protocol en netwerk service; (b) Opbouw van Protocol Data Units.

N-laag subsystemen - De functies die zich binnen een laag en een systeem bevinden worden *N-laag subsystemen* genoemd. In Figuur 3 zijn twee transportlaag subsystemen getekend en aangeduid met *transport entiteit.* Een N-laag subsysteem wordt voorts onderverdeeld in één of meerdere zgn. *protocol entiteiten,* afhankelijk of de functies van een laag door één of meerdere protocollen zijn gedefinieerd. In een protocolspecificatie wordt een protocol entiteit zodanig beschreven dat maximale vrijheid ontstaat voor de implementatie van het protocol, maar zodanig ingeperkt is dat correcte interacties met de andere entiteiten in dezelfde laag (*peer entiteiten*) ondubbelzinnig is gegarandeerd.

Protocol data unit - De interactie tussen peer protocol entiteiten geschiedt op basis van zgn. *Protocol Data Units* (PDUs). Deze PDUs worden afgebeeld op de Service Data Units (SDUs) van de onderliggende service. De PDUs worden ‘verpakt als

data' vervoerd naar de peer entiteit. Bovendien worden de SDUs weer afgebeeld op de lager liggende PDUs. Deze scheiding is nodig om in iedere laag een andersoortige problematiek te kunnen oplossen. Door deze benadering ontstaat de (zeer schematische) afbeelding van headers in opvolgende PDUs (zie Figuur 3.b). Headers bevatten (controle) informatie die protocol entiteiten met elkaar uitwisselen om hun functies te coördineren. Headers zijn in Figuur 3.b als PCI (*Protocol Control Information*) aangegeven.

1.4 Standaardisatie en Referentiemodellen

Standaardisatie, of *normering*, speelt een essentiële rol in de ontwikkeling en acceptatie van computernetwerken. Om verschillende systemen te verbinden via een computernetwerk is het nodig dat er gemeenschappelijke protocollen worden gebruikt. Elke gebruiker wil echter zijn protocolimplementaties betrekken van leveranciers en fabrikanten die de beste prijs/prestatie kunnen leveren voor het (specifieke) computerplatform van de gebruiker. Er zijn daarom protocolstandaarden nodig die precies voorschrijven wat nodig is om bepaalde interacties tussen systemen mogelijk te maken, maar geen onnodige beperkingen opleggen aan de fabrikant die de protocollen implementeert.

Behalve protocollen worden om dezelfde reden ook services, (abstracte) *interfaces*, *informatiestructuren* (bijv. voor gebruikersgedefinieerde documenten) en *informatieobjecten* (bijv. voor managementdoeleinden) gestandaardiseerd.

Standaardisatie wordt noodzakelijkerwijs in internationaal verband gedaan, met deelname van fabrikanten, leveranciers, gebruikersgroepen, academia en (soms) overheden. Behalve standaarden voor concrete systemen kunnen standaardisatieorganisaties ook richtlijnen ontwikkelen die systeemstructuren vastleggen. Dergelijke richtlijnen worden *referentiemodellen* genoemd, en hebben als belangrijkste doel om verschillende standaardisatieactiviteiten te coördineren en om de ontwerpcomplexiteit beheersbaar te houden. In de referentielijst is een aantal van de belangrijkste standaardisatie organisaties opgenomen.

Het referentiemodel dat tegenwoordig meestal wordt gebruikt voor computernetwerken is de Internet Protocol Suite. In dit referentiemodel worden de volgende vier lagen onderscheiden:

- *Applicatielaag*, deze bestaat uit de applicatieprotocollen die over een TCP/IP netwerk worden aangeboden, zoals DNS, SNMP, FTP, SMTP, NEWS, HTTP, HTML;
- *Transportlaag*, deze levert een end-to-end gegevensoverdracht service tussen applicatieprocessen (applicatieprogramma's). Meerdere

applicatieprocessen kunnen tegelijkertijd binnen een computersysteem draaien. Deze laag bevat de protocollen TCP en UDP;

- *Netwerklaag*, deze levert een end-to-end gegevensoverdracht service tussen computersystemen (zgn. hosts). Deze laag bestaat o.a. uit de protocollen IP, ICMP en routeringprotocollen zoals OSPF en BGP;
- *Subnetwerklaag*, deze bevat de nodige functies voor het versturen en ontvangen van netwerk laag pakketten via het lokale subnetwerk waarop een computersysteem is aangesloten. Voorbeelden van protocollen in deze laag zijn, ADSL, Ethernet, WDM, WLAN. Soms wordt binnen deze laag onderscheid gemaakt tussen de datalinklaag (waarbij het doel is om dataframes betrouwbaar uit te wisselen tussen twee systemen die direct met elkaar zijn verbonden) en de physiekelaag (waarbij het gaat om the mechanieken die nodig zijn om bits over een medium te versturen).

In het volgende hoofdstuk wordt volgens deze lagen indeling nader ingegaan op diverse protocollen en de functies die deze vervullen.

2 Computernetwerkfuncties

Functies binnen computernetwerken zijn laagsgewijs gedefinieerd. Een veel gebruikte lagenstructuur is die van het Internet, die van boven naar beneden bestaat uit een applicatielaag, transportlaag, netwerklaag en sub-netwerklaag.

2.1. Functies van de applicatielaag

Binnen de applicatielaag worden een groot aantal functies gebruikt. Omdat het onmogelijk is deze allen hier te behandelen, zullen in onderstaande slechts de bekendste de revue passeren.

Domain Name System (DNS)

Om communicatie tussen hosts te bewerkstelligen, moet ieder IP-pakket van adres informatie worden voorzien. IP-adressen zijn nummers met een lengte van 32 bits, die voor gebruikers weinig structuur vertonen waardoor er een grote kans op fouten ontstaat. Om het leven voor Internet gebruikers te veraangenamen, zijn er daarom eenvoudig te onthouden domeinnamen geïntroduceerd. Deze namen moeten door applicatiesystemen echter op IP-adressen worden afgebeeld; het Domain Name System (DNS) is hiervoor verantwoordelijk.

Domeinnamen zijn hiërarchisch opgebouwd volgens een bepaalde boomstructuur. De wortel van de boom is de ‘root’. Op het eerste hiërarchische niveau bestaan een beperkt aantal generieke domeinen (zoals ’com’ voor commerciële organisaties en ‘edu’ voor Amerikaanse onderwijsinstellingen), en een groot aantal land domeinen

waaronder: ‘nl’ en ‘be’ voor respectievelijk Nederland en België. Verdere opsplitsing van de domeinnamen gebeurt op opeenvolgende hiërarchische niveaus, bijvoorbeeld ‘utwente’ voor de Universiteit Twente en ‘ewi’ voor de Faculteit Elektrotechniek, Wiskunde en Informatica. Zo is er bijvoorbeeld een computer binnen de Faculteit EWI met de naam ‘demeter’, de domeinnaam van deze host is: demeter.ewi.utwente.nl. Het bijbehorende IP-adres is 130.89.10.21.

Om naam-adres transformaties te kunnen uitvoeren, is een gegevensbank nodig waarin naam-adres paren zijn opgeslagen. In het geval van het DNS is dit een gedistribueerde gegevensbank, die gegevens verspreid over een groot aantal zogenaamde DNS servers. De transformatie van hostnaam naar IP-adres (of omgekeerd) wordt op gang gezet door een DNS-request naar een DNS-server te versturen, de daarop verkregen DNS-response bevat het resultaat van de transformatie. Wanneer een DNS server een verzoek krijgt voor een domeinnaam waarover het geen adres informatie bezit, dan wordt het verzoek doorgestuurd naar een DNS server verderop in de boomstructuur.

HyperText Transfer Protocol (HTTP)

Het HyperText Transfer Protocol (HTTP) behoort bij de meest gebruikte Internet protocollen en wordt toegepast voor het uitwisselen van webpagina’s binnen het World Wide Web (WWW). Webpagina’s worden beschreven in de HyperText Markup Language (HTML); dit is een opmaaktaal waarin kan worden verwezen naar andere webpagina’s en naast tekst ook beeld, audio en video informatie kan worden opgenomen.

Bestanden waar naar verwezen wordt kunnen zich op willekeurige servers binnen het Internet bevinden. Om dergelijk bestanden te kunnen identificeren, wordt gebruik gemaakt van zogeheten Uniform Resource Locators (URLs). Deze beginnen met de domeinnaam van de server waarop de informatie ter beschikking wordt gesteld, gevolgd door een pad binnen het file systeem van deze server en de filenaam van het bestand.

Essentieel voor een gebruiker is dat het ophalen van informatie snel gebeurt, met dit doel voor ogen is HTTP ontworpen. Een enkele transactie verloopt als volgt:

- eerst wordt een TCP verbinding opgezet tussen de host en server;
- vervolgens wordt een HTTP request van de host naar de server verstuurd;
- daarna volgt een HTTP response van de server naar de host; deze response bevat het gevraagde HTML document;
- de transactie wordt afgesloten door het verbreken van de TCP verbinding.

File Transfer Protocol (FTP)

Het File Transport Protocol (FTP) is een van de oudste Internet protocollen voor het uitwisselen van bestanden tussen systemen. Het werkt onafhankelijk van de soort host, besturingssysteem, filestructuur of karakterset. Alhoewel het in vergelijking tot HTTP moeilijker is in gebruik, ondersteunt het de uitwisseling van bestanden in twee richtingen.

Om FTP te kunnen gebruiken, moet de gebruiker een account op de remote host hebben of de remote host moet anonymous FTP toestaan. In dit laatste geval kan doorgaans worden ingelogd met username ‘anonymous’ en het eigen e-mailadres als password.

FTP maakt gebruik van het onderliggende TCP protocol. Wanneer een FTP sessie wordt gestart, wordt eerst een TCP controleverbinding opgezet. Deze verbinding wordt gebruikt voor alle commando’s en de antwoorden hierop. Voorts zijn er drie situaties waarvoor een tweede FTP verbinding wordt opgezet:

- versturen van een bestand naar de remote host;
- versturen van een bestand van de remote host;
- versturen van de directory inhoud van remote naar local host.

E-mail protocollen

Een van de populairste Internet toepassingen is electronic mail (e-mail). Een e-mail bericht bestaat uit drie componenten:

- Envelope: Dit zijn de e-mail adressen van de zender en ontvanger, ze worden gebruikt om het bericht via de onderliggende protocollen te verzenden;
- Header: Dit zijn de velden die toegevoegde informatie over het e-mail bericht bevatten, zoals: tijdstip waarop het is verstuurd, tijdstip waarop het is aangekomen, onderwerp van het bericht;
- Body: dit is de inhoud van het e-mail bericht.

E-mail berichten bestaan volledig uit ASCII karakters. Om de hieraan inherente beperkingen weg te nemen, kan met behulp van MIME (Multipurpose Internet Mail Extensions) de body van een bericht zodanig worden ingericht dat deze gecodeerde, niet-ASCII bestanden bevat.

Iedere e-mail gebruiker heeft een eigen postbus (mailbox). Omdat deze postbus continue bereikbaar moet zijn, wordt deze doorgaans niet op het gebruikerssysteem ingericht, omdat de gebruiker dit systeem kan uitschakelen. Het is beter de postbussen van een groot aantal gebruikers op een centraal systeem te installeren; dit systeem is dag en nacht bereikbaar en wordt wel Message Transfer Agent (MTA) genoemd. Op dit systeem draait ook vaak een scanner die onderzoekt of e-

mails geen virussen bevatten. Wanneer een gebruiker een e-mail bericht heeft samengesteld en wil versturen, wordt het bericht eerst van de host naar de MTA getransporteerd, vervolgens door deze MTA doorgestuurd naar de MTA van de ontvanger, die het bericht in de juiste postbus opslaat. De ontvanger kan vervolgens het e-mail bericht ophalen uit deze postbus en overbrengen naar de eigen host.

Voor de communicatie tussen het systeem van de gebruikers en de MTA wordt meestal. het POP of IMAP protocol gebruikt, het SMTP protocol wordt gebruikt voor de communicatie tussen MTAs.

Post Office Protocol (POP)

POP is een relatief oud protocol en in verhouding tot IMAP vrij eenvoudig. De functionaliteit van POP beperkt zich tot:

- vragen of er nieuwe e-mail berichten zijn aangekomen;
- ophalen van e-mail berichten, waarna ze op de MTA worden verwijderd;
- ophalen van e-mail berichten, waarna ze op de MTA blijven staan.

Deze functionaliteit blijkt voor veel gebruikers toch voldoende. Vaak wordt vanaf de eigen werkplek de tweede functie gebruikt; dit heeft als voordeel dat de MTA geen berichten hoeft te bewaren en daarom relatief weinig schijfruimte nodig heeft. Wanneer een gebruiker (tijdelijk) vanaf een andere werkplek e-mail wil lezen, wordt meestal de laatste functie gebruikt. Om te voorkomen dat onbevoegden e-mail berichten van anderen lezen, wordt het ophalen van berichten voorafgegaan door een autorisatiefase, waarin om een gebruikersnaam en wachtwoord wordt gevraagd.

Internet Message Access Protocol (IMAP)

Indien meer functionaliteit vereist is dan POP kan bieden, kan IMAP worden toegepast. In tegenstelling tot POP biedt IMAP o.a. de mogelijk om:

- alleen de headers van berichten op te halen;
- alleen specifieke berichten op te halen;
- alleen e-mail berichten op te halen die aan een bepaald selectiecriterium voldoen;
- e-mail berichten op de MTA te markeren (bv. als ‘deleted’ of ‘unseen’).

Simple Mail Transfer Protocol (SMTP)

SMTP voorziet in betrouwbare communicatie tussen twee MTAs onder gebruikmaking van een TCP verbinding. Bij normaal (correct) verlopende e-mail uitwisseling worden achtereenvolgens de volgende commando’s uitgewisseld:

- HELO: identificatie de zendende MTA;
- MAIL: identificatie van de verzender van het e-mail bericht;

- RCPT: identificatie van de ontvanger van het e-mail bericht;
- DATA: verzenden van de inhoud van het e-mail bericht;
- QUIT: beëindigen de e-mail uitwisseling tussen de twee MTAs.

2.2. Functies in de transportlaag

De belangrijkste transport protocollen voor het Internet zijn het *User Datagram Protocol* (UDP) en het *Transmission Control Protocol* (TCP). Om te kunnen bepalen bij welk applicatielaag protocol de data die door het transport protocol wordt verstuurd behoord, maken zowel UDP als TCP gebruik van zogenaamde '*port-numbers*'. Voorbeelden van enkele bekende port-numbers zijn: 80 voor HTTP, 25 voor SMTP, en 110 voor POP.

UDP

Het *User Datagram Protocol* (UDP) is een eenvoudig protocol dat geen garanties biedt dat aangeboden berichten daadwerkelijk worden afgeleverd. De belangrijkste functie van UDP is het identificeren van de applicatielaag entiteiten waarvoor de UDP data is bestemd; om deze te kunnen identificeren bevat het UDP-PDU velden voor de *port-numbers* behorende bij de bron- en bestemmingsentiteiten. Verder bevat UDP nog een *checksum*-veld, waarmee fouten in het UDP bericht kunnen worden gedetecteerd. Omdat transmissiefouten vaak al op subnetwerk-niveau worden gedetecteerd, is de *checksum* vooral nuttig voor het detecteren van IP-reassembly-fouten. Indien een fout wordt gevonden, wordt het bijbehorende PDU weggegooid.

TCP

Het *Transmission Control Protocol* (TCP) is een betrouwbaar, en daardoor complex protocol. Het is, in tegenstelling tot de meeste andere protocollen, *stroom-georiënteerd*. Dit betekent dat de TCP gebruiker een stroom van data octetten aanlevert, in plaats van pakketten met een beperkte lengte. De TCP entiteit slaat deze stroom van octetten op in een buffer, en bepaalt in principe zelf wanneer de data wordt verstuurd. Door het zetten van een speciale *push flag*, kan de gebruiker echter ook aangeven dat de data direct verstuurd moet worden. Deze optie is vooral nuttig bij interactieve toepassingen.

TCP kent drie fases: verbindingsopbouw, data-uitwisseling en verbindingsbeëindigen.

De verbindingopbouw kan op twee manieren plaatsvinden:

- De TCP gebruiker geeft aan dat hij bereid is data te ontvangen. De bijbehorende primitieve heet '*passive open*' en wordt vooral gebruikt door

servers. Indien gewenst, kan de gebruiker aangeven dat de bereidheid alleen bestaat voor data vanuit een specifieke bron.

- De TCP gebruiker geeft aan dat hij van plan is data te versturen naar een specifieke bestemming. De bijbehorende primitieve heet '*active open*' en wordt vooral gebruikt aan de client zijde van de verbinding.

Nadat de verbinding is opgebouwd, kan met behulp van de *send*-primitieve data worden verstuurd. Net als bij UDP, bevat het TCP-PDU voor het detecteren van fouten een *checksum*-veld. Omdat TCP is voorzien van hertransmissie-functies, kunnen PDUs die niet (correct) zijn aangekomen opnieuw worden verstuurd. De hertransmissie-functie maakt gebruik van timers en een tweetal PDU velden: het *sequence number*-veld en het *acknowledgement number*-veld. Samen met het *window*-veld worden deze velden ook gebruikt voor TCP's flow control-functie. Met behulp van deze functie kan de ontvanger aangeven hoeveel data hij in staat is te verwerken.

De verbinding wordt gewoonlijk afgebroken door middel van de *close*-primitieve. Deze zorgt er voor dat alle nog in de buffers aanwezige data alsnog wordt verstuurd. Indien nodig kan de verbinding ook worden afgebroken met behulp van de *abort*-primitieve; eventueel in de buffers aanwezige data wordt dan niet meer verstuurd maar weggegooid

2.3. Functies in de netwerklaag

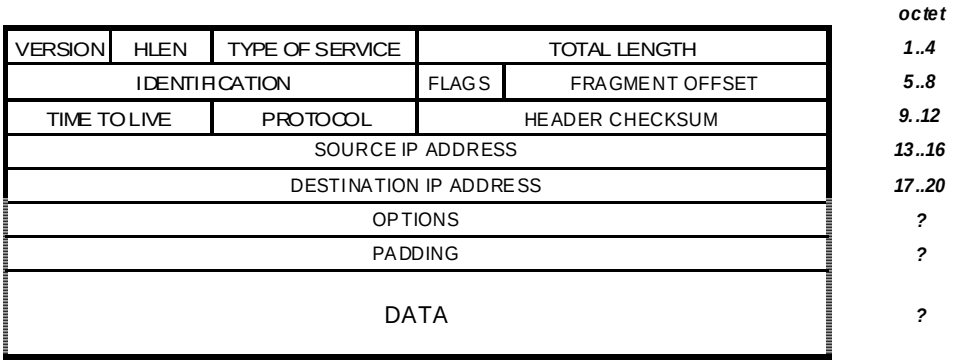
De netwerklaag levert 'end-to-end connectiviteit' aan haar gebruikers, de transport entiteiten. Deze end-to-end connectiviteit wordt gerealiseerd door verschillende soorten subnetwerken met behulp van routers zodanig met elkaar te verbinden, dat een rechtreeks communicatiepad ontstaat tussen eindsystemen. Alle routers en alle eindsystemen moeten hetzelfde netwerkprotocol ondersteunen; in de praktijk is dit het *Internet Protocol* (IP).

IP is een zogeheten 'connectionless' protocol, dus een protocol waarbij niet eerst een verbinding wordt opgebouwd voordat gebruikersdata wordt verstuurd. Het voordeel van een connectionless netwerkprotocol is dat routers geen status informatie omtrent verbindingen hoeven te bewaren en daardoor relatief eenvoudig zijn te bouwen. Een nadeel van een connectionless netwerkprotocol is dat ieder PDU het complete bron- en bestemmingsadres moet bevatten, waardoor de PDU header relatief groot wordt.

IP-PDU structuur

De structuur van een IP-PDU, ook wel datagram genoemd, is weergegeven in Figuur 4. De header begint met een veld voor het versienummer (de huidige versie van IP is 4), en heeft daarna een veld waarin de header-lengte wordt aangegeven.

Deze is minimaal 20 octetten (bytes), maar kan groter worden als de header ‘options’ bevat voor b.v. ‘route-recording’ of ‘source-routing’. Voor het aangeven van de totale PDU lengte zijn 2 octetten gereserveerd, zodat een IP PDU nooit groter kan worden dan 65535 octetten. Het ‘identification’ veld bevat een uniek volgnummer, en wordt evenals de twee volgende octetten gebruikt ten behoeve van ‘fragmentatie’ en ‘reassembly’. Het ‘Time to Live’ veld is nodig om PDUs te verwijderen als ze, ten gevolge van inconsistente routeringstabellen, in het netwerk blijven circuleren en de bestemming niet bereiken. Het veld wordt door de bron op één of andere waarde gezet (meestal 32, 64 of 128), en vervolgens door iedere router die wordt gepasseerd verlaagd. Als de waarde nul is bereikt, wordt het PDU weggegooid. Om fouten te kunnen detecteren bevat de header ook een checksum veld; merk op dat deze checksum alleen wordt berekend over de header, en niet over de data.



Figuur 4: Structuur van het IP-PDU.

Adressering

IP is oorspronkelijk ontworpen om netwerken van verschillende gebruikers door middel van één backbone met elkaar te verbinden. Om systemen wereldwijd uniek te kunnen identificeren, heeft ieder systeem (of preciezer gezegd: ieder netwerk-interface) een eigen 32 bits adres. Dit adres bestaat uit twee delen: een NETID die het gebruikersnet wereldwijd uniek identificeert, en een HOSTID die het systeem binnen het gebruikersnet uniek identificeert. NETIDs worden uitgegeven door de Internet Corporation for Assigned Names and Numbers (ICANN), de opvolger van de Internet Assigned Numbers Autority (IANA). HOSTIDs worden beheerd door de locale netwerkbeheerder.

Omdat IP PDUs een source adres veld bevatten, moet een systeem voordat het gaat communiceren zijn eigen netwerkadres kennen. In principe kan de netwerkbeheerder dit adres in de configuratie fase aan het systeem kenbaar maken, maar deze oplossing heeft als nadeel dat de beheerder ieder systeem fysiek moet

benaderen en ieder systeem permanent geheugen moet bezitten om het adres op te slaan. Er is daarom een speciaal protocol ontwikkeld dat door systemen in een LAN omgeving kan worden gebruikt om tijdens de start-up fase het eigen IP adres op te vragen. Dit protocol heet het Reverse Address Resolution Protocol (RARP), en maakt gebruik van een LAN-broadcast bericht.

Fragmentatie en reassembly

Het IP protocol kan gebruikt worden om verschillende soorten subnetwerken met elkaar te verbinden. Ieder type subnetwerk heeft echter zijn eigen beperkingen voor wat betreft de maximale PDU lengte. Indien het IP pakket groter is dan de maximale PDU lengte van het onderliggende subnetwerk, moet het IP PDU in kleine fragmenten worden opgedeeld. Deze functie heet fragmentatie.

IP fragmenten worden net zo behandeld als niet gefragmenteerde IP PDUs. Het is dus mogelijk dat fragmenten die bij hetzelfde bericht behoren verschillende routes door het netwerk nemen. Het weer samenvoegen van de fragmenten om het oorspronkelijke bericht te reconstrueren (reassembly) kan dan ook niet door een router in het netwerk plaatsvinden, maar alleen door de bestemming.

Foutafhandeling

Voor het melden van fouten heeft IP een eigen protocol: het Internet Control Message Protocol (ICMP). ICMP berichten worden verstuurd in het data veld van het IP PDU. ICMP berichten worden vaak gegenereerd door routers en eindsystemen nadat een fout in het IP protocol is gedetecteerd, het is echter ook mogelijk dat ICMP berichten worden verstuurd als een bepaalde vraag moet worden beantwoord. Ook kunnen tools zoals ping en traceroute ICMP berichten genereren. De onderstaande tabel geeft een overzicht van mogelijke ICMP berichten.

ICMP bericht	Foutmelding	Vraag
Destination unreachable	X	
Source quench	X	
Redirect	X	
Time exceeded	X	
IP parameter problem	X	
Echo request / reply		X
Timestamp request / reply		X
Address mask request / reply		X

Routering

Omdat IP volgens het ‘connectionless’ principe werkt, moet een router voor iedere PDU opnieuw bepalen in welke richting deze moet worden doorgestuurd. De router haalt hiertoe het IP bestemmingsadres uit het IP-PDU, en gebruikt dit om in de

routeringstabel het IP adres van het volgende systeem op het pad naar de bestemming te vinden. Indien dit systeem via een LAN bereikbaar is, moet ook het LAN adres van dit systeem worden bepaald. Hiertoe kan het Address Resolution Protocol (ARP) worden gebruikt.

Om de routeringstabel te vullen en te wijzigen nadat een verandering in de netwerk topologie is opgetreden, zijn een aantal routeringprotocollen gedefinieerd. Deze protocollen kunnen in twee categorieën worden ingedeeld: intra-domein (interior gateway) protocollen en inter-domein (exterior gateway) protocollen. De eerste soort wordt gebruikt binnen het domein van een enkele operator; inter-domein protocollen worden gebruikt voor het uitwisselen van routeringinformatie tussen operators. Een voorbeeld van een intra-domein protocol is Open Shortest Path First (OSPF); een voorbeeld van een inter-domain protocol is het Border Gateway Protocol (BGP). Een belangrijk verschil tussen beide protocollen is dat OSPF van het zogeheten link-state type is, en BGP van het distance vector type. Bij link state protocollen kent iedere router de totale netwerktopologie en is het detecteren en voorkomen van routeringfouten relatief eenvoudig. Een nadeel van link state protocollen is dat er veel informatie moet worden opgeslagen en dat het berekenen van routes relatief veel processing power kost. Deze problemen treden niet op bij distance vector protocollen, omdat routers hierbij slechts een deel van de netwerktopologie hoeven op te slaan. Deze protocollen hebben echter weer andere problemen, zoals trage aanpassing na veranderingen in de netwerktopologie en het gevaar dat door een al dan niet bewuste fout al het netwerkverkeer de verkeerde kant wordt opgestuurd zodat het verloren gaat (black holes).

IPv6

Om ook in de toekomst verdere groei van het Internet mogelijk te maken is een nieuwe versie van het IP protocol ontwikkeld: IP versie 6. IPv6 adressen hebben een lengte van 128 bits, en zijn dus vier keer groter dan de oorspronkelijke IPv4 adressen. Een interessante vernieuwing is het zogeheten anycast adres. Dit adres kan worden gebruikt voor het identificeren van een groep van systemen; een router die een PDU met een anycast adres ontvangt, zal het PDU doorsturen naar het systeem dat binnen deze groep het best bereikt kan worden. Anycast adressen zijn vooral nuttig voor bedrijven met meerdere identieke servers, die de belasting willen verdelen over de verschillende servers.

2.4. Functies in the subnetwerklaag

De subnetwerk laag heeft tot taak connectiviteit te leveren tussen systemen die rechtstreeks met elkaar verbonden zijn via een fysiek medium, zoals een koper kabel of glasvezel. Er zijn veel mogelijkheden om deze connectiviteit te realiseren; deze mogelijkheden worden vastgelegd in standaarden door organisaties zoals het

Institute of Electrical and Electronics Engineers (IEEE) en de International Telecommunication Union (ITU-T). De belangrijkste standaarden op subnetwerk niveau zijn Ethernet, Asymmetric Digital Subscriber Line (ADSL) en Wave Division Multiplexing (WDM).

Ethernet

De werking van Ethernet is vastgelegd in de IEEE 802.3 standaarden. Er zijn inmiddels een groot aantal van dergelijke standaarden, voor snelheden variërend van 10 Mb/s tot 10 Gb/s.

De eerste versies van Ethernet werkten op 10 Mb/s volgens de CSMA/CD (Carrier Sense Multiple Access/Collision Detect) methode. Bij deze methode zijn alle systemen op hetzelfde fysieke medium aangesloten (multiple access). Als een systeem een bericht wil versturen, kijkt het eerst of een ander systeem al aan het zenden is (carrier sense). Is het medium nog niet bezet, dan begint het systeem met het versturen van het bericht over het medium. Indien meerdere systemen gelijktijdig detecteren dat het medium vrij is en beginnen met het versturen van een bericht, treedt een botsing (collisions) op. Dergelijke botsingen verstoren de communicatie en worden door alle zendende systemen gedetecteerd, waarna deze het versturen van de berichten stopzetten. Iedere zender gaat vervolgens een willekeurig lange periode wachten, om het daarna nog eens te proberen. Indien een bericht te vaak (meer dan 16 maal) collisions veroorzaakt, zal de zender geen verdere pogingen meer ondernemen dit bericht te versturen.

In moderne versies van Ethernet zijn de systemen niet meer op hetzelfde fysieke medium aangesloten, maar via switches met elkaar verbonden. Er wordt dus geen gebruik meer gemaakt van CSMA/CD. Indien meerdere systemen gelijktijdig beginnen met het versturen van berichten, zal de switch deze berichten even opslaan en pas doorsturen als het volgende medium weer vrij is. Alle Ethernet versies hebben dezelfde berichtstructuur en kunnen door middel van switches eenvoudig onderling gekoppeld worden. Er kan gebruik gemaakt worden van verschillende soorten media, variërend van "telefoon kwaliteit" (cat 3) unshielded twisted pair (UTP), "hoge kwaliteit" (cat5) UTP, Shielded Twisted Pair (STP) of glasfiber.

ADSL

Asymmetric Digital Subscriber Line (ADSL) is een hoge snelheid transmissietechnologie ontwikkeld voor gebruik over bestaande koperen telefoonverbindingen. Deze verbindingen, die lopen tussen de abonnee (subscriber) en de telefooncentrale, kunnen meerdere kilometers lang zijn. Het versturen en ontvangen van data gaat in principe op verschillende snelheden (asymmetric); de ontwerpers gingen er immers vanuit dat abonnees vooral data ontvangen, en weinig

versturen. Of deze aanname ook nog in de toekomst geldt, als er op grote schaal gebruik gemaakt wordt van Peer to Peer (P2P) toepassingen, zal moeten blijken. Bij de oorspronkelijke versie van ADSL zijn downstream (van de telefooncentrale naar de abonnee) snelheden mogelijk tot 8Mb/s en upstream tot 1Mb/s. Bij nieuwe, ADSL2+ systemen zijn snelheden mogelijk tot 20Mb/s, afhankelijk van de lengte en kwaliteit van de telefoonleiding.

WDM

Wave Division Multiplexing (WDM) is een methode die in de kern van het netwerk (de back-bone) wordt gebruikt om meerdere optische signalen via één glasvezel (fiber) te versturen. Ieder optisch signaal heeft een eigen golflengte (kleur). Het voordeel van WDM is dat er over een enkele fiber parallelle communicatiekanalen ontstaan, waardoor de capaciteit van de fiber wordt verhoogd. De capaciteit van een kanaal (kleur) ligt tussen de tien en veertig Gb/s; omdat er honderden kanalen over een enkele fiber kunnen lopen, ligt de capaciteit van een fiber in de orde grootte van Terabits/s. Merk op dat een enkele kabel weer een groot aantal fibers kan bevatten, zodat de capaciteit van de totale kabel nog veel hoger is.

Sinds kort bestaan er WDM schakelaars, waarmee een optisch signaal op een bepaalde fiber geschakeld kan worden naar een optisch signaal op een andere fiber. Bij bepaalde uitvoeringen van de schakelaar kunnen de golflengtes op beide fibers van elkaar verschillen. Met behulp van WDM schakelaars is het in principe mogelijk volledig optische verbindingen tussen eindgebruikers te realiseren.

3 Computernetwerk thema's

In het voorgaande hoofdstuk is per laag een overzicht gegeven van de belangrijkste functies en mechanismen die nodig zijn om de diensten van de betreffende laag te bewerkstelligen onder gebruikmaking van de diensten die door de ondersteunende laag worden geboden. Naast deze laagsgewijze opbouw in termen van diensten en protocolfuncties is het ook mogelijk op een andere wijze naar computernetwerken te kijken. In de zogenaamde verticale zienswijze is de focus meer op aspecten en thema's die een rol spelen dwars door de hiërarchische lagen heen. Een aantal van deze thema's gaan we hier behandelen. Aangezien er potentieel veel thema's zijn beperken we ons hier tot de behandeling van: multimedia, mobiliteit, beveiliging en operationeel beheer.

3.1 Multimediatoepassingen

Zoals in paragraaf 2.1 al is aangegeven, zijn er zeer veel applicatieprotocollen, vervolgens zijn daar een aantal veel gebruikte applicatieprotocollen besproken. Nu

wordt nader ingegaan op de classificatie en karakteristieken van multimediatoepassingen, en wordt in algemene termen ingegaan op de daarbij gebruikte applicatieprotocollen en hun onderlinge samenhang.

Classificatie en Karakteristieken

Multimediatoepassingen kenmerken zich door het gebruik (i.e. communicatie) van meerdere media, zoals tekst, beeld (bijvoorbeeld foto's en figuren), spraak, audio en video. Afhankelijk van de toepassingen worden verschillende kwaliteitseisen gesteld aan het computernetwerk. Drie belangrijke kwaliteitscriteria hierbij zijn: tolerantie voor informatieverlies; benodigde bandbreedte; toelaatbare vertraging (of variaties daarin).

Toepassingen zoals email, web informatie diensten, file transfers zijn intolerant voor data verlies, daarentegen zijn ze bestand tegen grote fluctuaties in beschikbare bandbreedte en ongevoelig voor tijdsvertragingen. Deze klasse van multimediatoepassingen worden doorgaans aangeduid met de term *elastische toepassingen*.

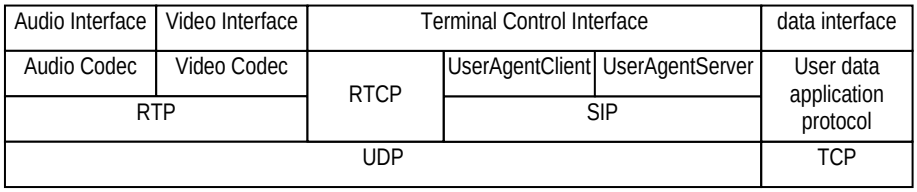
In toepassingen zoals video-conferencing en IP-telefonie wordt doorgaans gebruik gemaakt van een of meerdere van de volgende media typen: spraak, video, beeld en tekst. Hierbij gaat het om real-time communicatie tussen twee of meerdere personen. Allereerst stellen de hiervoor gebruikte applicaties minimum eisen aan de beschikbare bandbreedte, dit in verband met de grote hoeveelheden data die via het computernetwerk moet worden vervoerd. Aangezien de communicatie real-time is worden strenge eisen gesteld aan de tijdsvertragingen (maximaal een paar honderd milliseconden). Wellicht vreemd genoeg zijn deze applicaties in enige mate tolerant t.a.v. het verlies van informatie (enkele procenten data verlies is geen probleem). Deze klasse van multimediatoepassingen wordt meestal aangeduid met de term *interactieve real-time toepassingen*.

Een derde klasse van toepassingen wordt soms aangeduid met de term *entertainment toepassingen* of *interactieve non realtime toepassingen*. Een voorbeeld is Video-on-Demand. Dit type toepassingen verschilt met interactieve toepassingen wat betreft de eisen t.a.v. tijdsvertragingen, vertragingen van enkele seconden zijn geen bezwaar, eisen ten aanzien van verlies en bandbreedte zijn hetzelfde als die voor interactieve real-time toepassingen.

Functies en communicatieprotocollen voor multimediatoepassingen

Multimediatoepassingen bevatten doorgaans vele functies en maken meestal van meerdere communicatieprotocollen gebruik. Deze functies en protocollen moeten door de eindsystemen worden ondersteund. Aan de hand van de protocol

architectuur voor multimedia Internet telefonie (zie Figuur 5) zullen de belangrijkste functies en communicatieprotocollen besproken worden.



Figuur 5: Voorbeeld Protocol Architectuur voor Multimedia Internet Telefonie.

- A/D & D/A Conversie - Bij veel media gaat het om tijdcontinue signalen. Aan de zendende kant zal dus een analoog/digitaal conversie gedaan moeten worden teneinde, aan de ontvangende zijde zal de inverse bewerking uitgevoerd moeten worden (niet expliciet in Figuur 5 aangegeven).
- Compressie en Decompressie - Het resultaat van A/D conversie levert een datastroom op. Voor multimedia gaat het hierbij om enorme datavolumes. Bijvoorbeeld HiFi kwaliteit muziek heeft een bandbreedte van ca. 1,28 Mbps, en spraak circa 112 Kbps. Voor digitale TV is dit ongeveer 160 Mbps, en voor HDTV circa 640 Mbps. Daarom worden compressietechnieken toegepast aan de zendende zijde om zodoende de datavolumes te reduceren, in termen van real-time communicatie leidt dit tot een reductie van de benodigde bandbreedte. Aan de ontvangende zijde is de omgekeerde bewerking, decompressie, nodig. Compressietechnieken worden ook gebruikt voor beelden. Voor ieder type media bestaan vele verschillende compressietechnieken. Video-compressiefactoren van 20 tot 50 zijn zeer gewoon. (Codec - Compressie / Decompressie in Figuur 5).
- Streaming protocol - Voor het transport van een multimediastroom over een computernetwerk wordt gebruikt gemaakt van een streaming protocol. Zo'n protocol is specifiek ontworpen om, gegeven het computernetwerk, zo goed mogelijk tegemoet aan de kwaliteitseisen van de applicatie (bijvoorbeeld RTP - Real-time Transport Protocol in Figuur 5).
- Stream Control protocol - In toepassingen waar sprake is van meerdere datastromen, bijvoorbeeld video en spraak, kan synchronisatie van de stromen nodig zijn. Ook kan het nodig zijn om, als gevolg van veranderde netwerk omstandigheden, van compressietechniek te veranderen of om anderszins de datastroom te verkleinen. De hieraan gerelateerde informatie die tussen eindsystemen moet worden uitgewisseld maken gebruik van een

Stream Control protocol (bijvoorbeeld RTCP - Real-time Transport Control Protocol in Figuur 5).

- Signaleringprotocol - Een multimedia service sessie kent doorgaans een levenscyclus, bestaande uit het opzetten van de sessie (bijvoorbeeld een gebruiker nodigt een andere gebruiker uit voor een IP-telefonie sessie), het gedurende de sessie wijzigen (bijvoorbeeld een derde persoon wordt uitgenodigd om deel te nemen aan de bestaande sessie), en ten slotte het beeindigen van de sessie. De uitwisseling van informatie die hierbij nodig is wordt verzorgd door een zogenaamd signaleringprotocol (bijvoorbeeld SIP - Session Initiation Protocol in Figuur 5).
- Gebruikersinterfaces - Een multimedia-applicatie bevat doorgaans meerdere gebruikersinterfaces t.b.v. beeld, geluid en data. Uiteraard ook voor interacties met de gebruiker t.b.v. de besturing van de multimedia service sessie. (zie de diverse interfaces in Figuur 5)

3.2 Mobiliteit

In het dagelijkse taalgebruik worden mobiliteit en draadloze communicatie vaak door elkaar gebruikt, in een detail beschouwing is dit echte niet correct. Met draadloze communicatie wordt in feite gerefereerd aan draadloze datalink verbindingen tussen twee systemen. Als gevolg van het feit dat hierbij dus niet langer een kabel nodig is tussen twee of meerder netwerk systemen om gegevens (bijvoorbeeld datagrammen) uit te wisselen, worden hierdoor bepaalde vormen van mobiliteit mogelijk gemaakt. Er bestaan echter ook vormen van mobiliteit die strikt genomen geen draadloze communicatie vergen. In het navolgende zal allereerst ingegaan worden op de diverse vormen van mobiliteit. Er zal een korte inventarisatie gemaakt worden van een aantal generieke problemen die verbonden zijn aan mobiliteit. Vervolgens worden de principes van een netwerklaag oplossing en een applicatielaag oplossing besproken.

Vormen van Mobiliteit.

Er kunnen diverse, verschillende vormen van mobiliteit worden onderscheiden, t.w.:

- Gebruikers / Terminal mobiliteit - Deze vorm van mobiliteit houdt in dat het toestel / apparaat van de eindgebruiker van plaats verandert, terwijl nog steeds gebruik gemaakt kan worden van (dezelfde) communicatie en informatie diensten. Binnen deze vorm van mobiliteit zijn twee subvormen te onderscheiden.

  - Pre-call mobiliteit - hierbij wordt netwerk connectiviteit gerealiseerd voordat er een communicatiedienst wordt geïnitieerd of afgenomen.
  - Mid-call mobiliteit - hierbij wordt netwerk connectiviteit gehandhaafd terwijl er reeds een dienst is geïnitieerd of reeds wordt afgenomen.

  Pre-call mobiliteit is in het algemeen eenvoudiger te realiseren dan mid-call mobiliteit. Dit heeft ondermeer te maken met het feit dat voor pre-call mobiliteit meer tijd beschikbaar is om netwerk connectiviteit tot stand te brengen, terwijl bij mid-call mobiliteit de handhaving van netwerk connectiviteit aan strengere eisen moet voldoen, de mate waarin wordt ondermeer bepaald door de soort dienst.

- Sessiemobiliteit - Wanneer een dienst gaande is, duiden we dit aan met een sessie. Met sessie mobiliteit wordt dan de situatie bedoeld waarbij de sessie op een andere terminal doorgaat. Zo zou in het geval van sessie mobiliteit een sessie die gestart is om een mobiele PDA over kunnen gaan naar een desktop PC in het geval de gebruiker bij zijn werkplek aankomt. Of bijvoorbeeld een MP3 die on-line beluisterd wordt gaat verder op de stereo installatie wanneer de gebruiker thuis is aangekomen.
- Persoonlijke mobiliteit - Bij persoonlijke mobiliteit wordt in feite de mobiliteit tussen eind-gebruiker en eindsysteem mobiel gemaakt. Hierbij hebben we te maken met een enkele gebruiker met meerdere eindsystemen. De gebruiker wordt geïdentificeerd met een uniek logisch adres, afhankelijk van gebruikerspreferenties en configuratie worden informatie en communicatie diensten opgezet met een van de eindsystemen, of wordt tijdens een sessie overgaan van het ene eindsysteem naar een ander eindsysteem. Op deze wijze wordt de keuze van het eindsysteem transparant gemaakt van andere partijen.
- Dienstenmobiliteit - Bij dienstenmobiliteit heeft een eindgebruiker toegang tot een dienst onafhankelijk van het gebruikte eindsysteem. Voor bijvoorbeeld een persoonlijk telefoonboek of adressenboek is onafhankelijkheid van het eindsysteem een gemak voor de eindgebruiker.

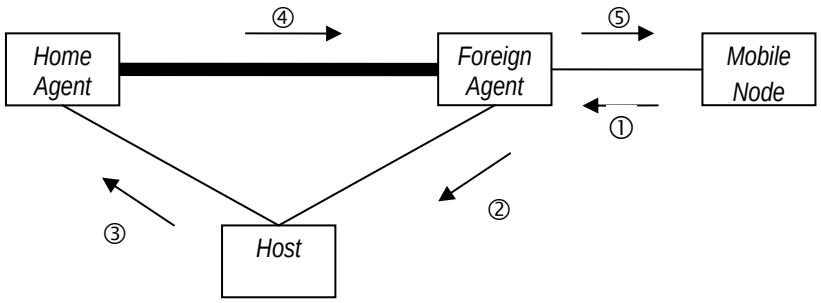
Probleem om mobiliteit te realiseren

Problemen van mobiliteit hebben vooral te maken met adresproblemen. Bijvoorbeeld wanneer we kijken naar gebruikersmobiliteit voor op IP gebaseerde diensten, dan betekent dit dat het point-of-attachment veranderd. Vanuit de netwerklaag bezien, betekent dit dat: 1) onder gelijkblijvend IP-address de routeringtabellen in het netwerk moeten worden aangepast, of 2) het IP adres van het eindsysteem moet veranderen. De eerste optie betekent zeer ingrijpende

veranderingen in het IP netwerk, dit is niet alleen zeer onpraktisch (bijvoorbeeld vanuit economisch perspectief) maar schaalt ook niet. De tweede oplossing is daarom meer voor de hand liggend: alleen de eindsystemen moeten zich aanpassen. Deze methode kan goed werken voor pre-call mobiliteit. Voor mid-call mobiliteit levert dit echter problemen op voor de hoger liggende lagen, en met name de TCP transport laag. Verandering van IP adres houdt namelijk in dat alle openstaande TCP verbindingen verbroken worden en dus alle lopende diensten die gebruik maken van TCP zullen beëindigd worden.

Netwerklaag oplossing

De oplossing voor gebruikers / eindsysteem mobiliteit op de netwerklaag is Mobile-IP. Deze oplossing is voor zowel de transportlaag als the applicatielaag volledig transparant is, d.w.z. wanneer deze oplossing gebruikt wordt zijn er geen aanpassingen nodig in de transportprotocollen noch in de applicaties and applicatieprotocollen. In het volgende wordt Mobile-IP voor IP versie 4 besproken. Alhoewel, IP versie 6 standaard ondersteuning biedt voor Mobile IP, feit is dat het overgrote deel van het huidige Internet nog steeds IPv4 is.



Figuur 6: Host Mobiliteit met Mobile-IP

De werking van Mobile-IP is, in grote lijnen, als volgt:

- Home agents en foreign agent adverteren hun aanwezigheid door het uitzenden van "advertentieberichten".
- een mobile node ontvangt "advertentieberichten" en bepaalt aan de hand hiervan of deze in het home network of in een foreign network aanwezig is.
- indien de mobile node in een foreign network is, ontvangt deze van het foreign network een care-of-address (dit kan gebeuren door de foreign agent zelf, of door aan ander mechanisme, bijvoorbeeld DHCP).

- de mobile node registreert zijn care-of-address bij de home-agent
- de uitwisseling van datagrammen tussen een mobile node en een willekeurige andere host (bijvoorbeeld een server) verloopt nu als volgt (zie Figuur 6) de mobile node verstuurd een request naar de host met zijn eigen home-address (de datagrammen op de gebruikelijke wijze gerouteerd via het foreign netwerk naar de host; de host verstuurd een response bericht (naar het home-address van de mobile-node), de datagrammen worden in het home-netwerk door de home-agent afgevangen (3); de home-agent verpakt de gehele ontvangen datagrammen in een nieuw datagram met als header o.a. het foreign-address van de mobile node, i.e. de orginale datagrammen worden via een tunnel doorgestuurd); in het foreign-network worden de datagrammen afgevangen door de foreign-agent (4); de datagram wordt uitgepakt en afgeleverd bij de mobile node (5).

Opgemerkt moet worden dat er diverse variatie op het hier geschetste gedrag mogelijk zijn, meer details hierover zijn te vinden in bijvoorbeeld [RFC 3344]

Applicatielaag oplossing

Een alternatief voor de netwerklaag oplossing van gebruikers mobiliteit is de applicatielaag oplossing voor gebruikersmobiliteit. Een mogelijk applicatielaag protocol dat hiervoor gebruikt kan worden is SIP (Session Initiation Protocol). Met behulp van SIP wordt er een tijdelijke relatie gelegd tussen een permanent gebruikeradres en een tijdelijk IP-adres. Wanneer het IP adres verandert (als gevolg van de mobiliteit), dan wordt de relatie vernieuwd met dit nieuwe IP adres. De gebruikersidentifier hebben een format dat sterk doet denken aan een email adres, bijvoorbeeld sip:jim@myprovider.com.

Opgemerkt moet worden dat deze oplossing geschikt is voor (UDP gebaseerde) multimediadiensten, en minder geschikt is voor TCP gebaseerde diensten (zoals de meeste informatiediensten).

Het pre-call scenario verloopt, in grote lijnen, als volgt (zie Figuur 7.a):

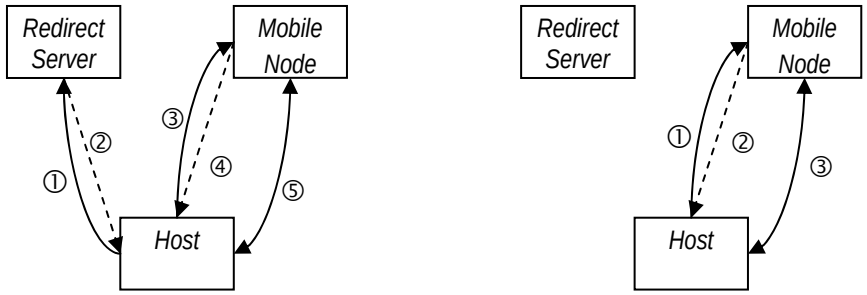
- Wanneer een Mobile node een nieuw IP adres krijgt toegewezen dan registreert deze zich (eventueel opnieuw) bij zijn thuis-registrar.
- Wanneer een andere host wil communiceren met de Mobile Node, dan verstuurd deze een SIP INVITE bericht naar de thuis registrar van de Mobile Node, (1). Deze stuurt een SIP 302 Moved Temporary bericht terug met daarin het huidige IP adres van de Mobile Node, (2).

- Nu verstuurt de host een SIP INVITE direct naar de Mobile Node, (3). Wanneer deze een SIP OK teruggestuurd (4) dan kan de uitwisseling van data plaatsvinden (5).

Als gedurende de sessie het IP adres van de Mobile Node verandert (zie figuur ?.b), dan:

- Verstuurt de Mobile Host simpelweg opnieuw een SIP INVITE naar de host met daarin een update van de sessie gegevens waaronder het nieuwe IP adres, (1).
- Indien de Host een SIP OK teruggestuurd, (2), dan gaat de data-uitwisseling verder (3).

Uit bovenstaande is te zien dat er meerdere oplossingen bestaan op verschillende protocollagen voor een probleem. In bovenstaande zijn de principes belicht en is niet ingegaan op de voor- en nadelen van iedere oplossing.



Figuur 7: Gebruikersmobiliteit met SIP: a) pre-call mobiliteit, b) mid-call mobiliteit.

3.3 Beveiliging

Bij elke computernetwerktoepassing wordt informatie uitgewisseld tussen computers. Het openstellen van computers voor communicatie brengt risico's met zich mee: ongeautoriseerde entiteiten, hierna *aanvallers* genoemd, kunnen proberen gecommuniceerde informatie af te luisteren of te wijzigen, de communicatie te blokkeren, of zich via de beschikbare communicatiemiddelen toegang te verschaffen tot computers en de daarop aanwezige informatie en programmatuur. De behoefte aan beveiliging groeit naarmate toepassingen meer communiceren via netwerken, in het bijzonder publieke netwerken zoals het internet. De noodzaak van beveiliging is evident bij toepassingen die 'kritisch' zijn voor bedrijfsprocessen of bij toepassingen die 'gevoelige' informatie gebruiken.

Echter, ook de gebruikers van ‘gewone’ computernetwerktoepassingen, zoals email, ervaren in toenemende mate het belang van een goede beveiliging.

Eindgebruikers en dienstenaanbieders moeten zich bewust zijn van de risico’s van computernetwerktoepassingen en zij moeten de nadelen van extra beveiliging (bijvoorbeeld additionele kosten en complexiteit) afwegen tegen de voordelen (bijvoorbeeld het voorkomen van verlies en misbruik van informatie).

Beveiliging onderscheidt zich van betrouwbaarheid doordat bij beveiliging gestreefd wordt naar het beschermen van informatie tegen doelgerichte aanvallen van mensen en organisaties, terwijl bij betrouwbaarheid informatie wordt beschermd tegen de feilbaarheid van implementaties en media.

Beveiligingsaspecten

We onderscheiden hier de volgende aspecten van beveiliging:

- *Aanval*: elke actie die tot doel heeft om informatie te compromitteren (te manipuleren zonder medeweten en toestemming van de eigenaar).
- *Mechanisme*: een stelsel van acties gericht op het detecteren, voorkomen or herstellen van een aanval.
- *Dienst*: verzameling functies die de beveiliging verbeteren, geïmplementeerd met een of meer mechanismen.

Beveiligingsaanvallen worden onderverdeeld in passieve en actieve aanvallen. Een *passieve aanval* kan ertoe leiden dat een aanvaller informatie achterhaalt, zonder dat dit effect heeft op de toestand of werking van de onderdelen van een computernetwerk. De informatie kan de inhoud van uitgewisselde berichten in een communicatie zijn, of betrekking hebben op de aard van de communicatie, zoals af te leiden uit de locatie en identiteit van de betrokken entiteiten en de lengte of frequentie van berichten. Deze laatste vorm van passieve aanval wordt *verkeersanalyse* genoemd. Omdat passieve aanvallen geen data wijzigen, zijn ze moeilijk te detecteren. De nadruk van beveiliging ligt daarom bij passieve aanvallen op het voorkomen van hun succes.

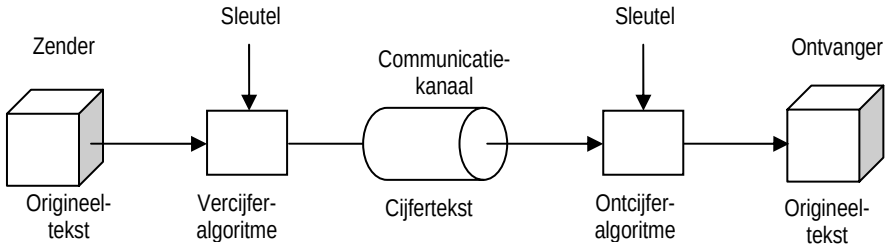
Een *actieve aanval* probeert de toestand of werking van onderdelen van een computernetwerk te wijzigen, door data in een communicatie te veranderen of valse data te injecteren. De volgende soorten worden onderscheiden:

- *Maskerade*: een indringer doet zich voor als een geautoriseerde entiteit.
- *Overspelen*: data of berichten die gekopieerd zijn uit een eerdere communicatie worden gebruikt om een valse communicatie te creëren.

- *Wijzigen*: data in berichten of de volgorde van berichten in een communicatie worden gewijzigd.
- *Obstructie* ('denial of service'): normaal gebruik of beheer van communicatie, applicaties of informatie wordt onmogelijk gemaakt.

In tegenstelling tot de aanpak bij passieve aanvallen, is bij actieve aanvallen beveiliging vooral gericht op detectie, en op herstel van ongewenste effecten die door de aanvallen gerealiseerd zijn.

Beveiligingsmechanismen vormen de bouwstenen voor beveiligingsdiensten. Vrijwel alle mechanismen zijn gebaseerd op cryptografische technieken. Het basismodel voor de toepassing van cryptografie is geïllustreerd in Figuur 8.



Figuur 8: Toepassing van cryptografie.

Aan de zenderkant wordt een bericht in originele vorm, de *origineeltekst*, getransformeerd naar een vercijferd bericht, of *cijfertekst*, met behulp van een *vercijferingsalgoritme*. Aan de ontvangerkant wordt de cijfertekst weer omgezet in de origineeltekst met behulp van een *ontcijferingsalgoritme*. Beide algoritmen maken gebruik van een *sleutel*. Het algoritme produceert een andere cijfertekst afhankelijk van de waarde van de sleutel. De meest gebruikte vorm van cryptografie in communicatiebeveiliging is *symmetrische cryptografie*, of geheime-sleutel vercijfering, waarbij de vercijferingssleutel en de ontcijferingssleutel identiek zijn. Ontvanger en zender krijgen een kopie van de sleutel, en moeten deze sleutel geheim houden om te voorkomen dat derden de cijfertekst kunnen ontcijferen. Meer recent is de toepassing van *asymmetrische cryptografie*, of publieke-sleutel vercijfering, waarbij een sleutelpaar worden gebruikt. Eén van de sleutels is geheim en slechts bekend bij een van de entiteiten (zender of ontvanger) in de communicatie; de andere sleutel is openbaar, en bekend bij beide entiteiten (en de rest van de wereld).

De toepassing van cryptografie resulteert in een beveiligd communicatiekanaal, mits: (1) de origineeltekst zonder de juiste sleutel niet uit de cijfertekst afgeleid kan worden, en (2) de geheime sleutel op een veilige manier bij de juiste entiteit wordt afgeleverd, en deze entiteit de sleutel geheim houdt. Gelukkig bestaan er oplossingen die praktisch voldoen aan deze eisen. De bekendste symmetrische

techniek is DES (Data Encryption Standard) en zijn opvolger AES (Advanced Encryption Standard). De meest gebruikte asymmetrische techniek is RSA (vernoemd naar de ontdekkers, Rivest, Shamir en Adleman).

Beveiligingsdiensten voor computernetwerken richten zich op de volgende eigenschappen:

- *Authenticatie*: aantonen dat een communicatie authentitiek is. Hiertoe moet de identiteit van de betrokken entiteit (zender of ontvanger) en de bron van de data in de communicatie gevalideerd worden.
- *Toegangscontrole*: controleren en beperken van de toegang tot applicaties en informatie via communicatiekanalen. Alleen geautoriseerde entiteiten mogen toegang krijgen.
- *Vertrouwelijkheid*: bescherming tegen het zonder toestemming openbaar maken van informatie. Vertrouwelijkheid kan betrekking hebben op alle data in een communicatie, of op geselecteerde onderdelen van de data.
- *Integriteit*: aantonen dat de ontvangen data in een communicatie identiek is aan de data die verzonden is door de zender. Net als bij vertrouwelijkheid, kan integriteit betrekking hebben op alle data of op geselecteerde onderdelen van de data in de communicatie.
- *Onlochenbaarheid* (‘nonrepudiation’): bescherming tegen het kunnen ontkennen dat een bericht is verzonden of ontvangen. Hiertoe moet een ontvanger kunnen bewijzen dat een bericht is verzonden door de vermeende zender, en moet een zender kunnen bewijzen dat een bericht is ontvangen door de vermeende ontvanger.
- *Beschikbaarheid*: voorkomen dat applicaties of informatie ontoegankelijk of onbruikbaar worden voor geautoriseerde entiteiten. Toegang via communicatiekanalen moet mogelijk zijn overeenkomstig de prestatiespecificaties van het systeem.

Beveiligingsoplossingen

De mogelijkheid om een aantal eigenschappen van beveiligingsdiensten met behulp van cryptografische technieken te realiseren volgt direct uit:

- de beschikbaarheid van een beveiligd communicatiekanaal (vertrouwelijkheid).
- de unieke relatie tussen cijfertekst en origineeltekst (integriteit).

- de unieke eigenschap van een geheime-sleutelbezitter om cijfertekst te genereren die met een corresponderende (geheime of publieke) sleutel te ontcijferen is (authenticatie, onlochenbaarheid).

Dit kan in principe op elk niveau in de protocolhiërarchie. Wanneer beveiligingsmechanismen gecombineerd worden met een specifiek applicatielaag protocol, dan kan de applicatie die dit protocol gebruikt tevens de geleverde beveiligingsdiensten gebruiken. De applicatielaag (gebruikers- en besturings-) data is dan van bron tot bestemming beveiligd, maar andere applicaties, met een ander applicatielaag protocol, kunnen niet van deze diensten gebruik maken. Bovendien wordt de besturingsdata die wordt toegevoegd in de lagere lagen niet beschermd. Wanneer beveiliging plaatsvindt in een transportlaag protocol, dan zijn de beveiligingsdiensten beschikbaar voor alle applicaties die dit transportprotocol gebruiken. Echter, met beveiligingsmechanismen uitsluitend op dit niveau wordt geen bescherming geboden tegen aanvallen die gebeuren op een hoger niveau in de protocolhiërarchie. Hetzelfde geldt voor beveiliging op nog lagere niveaus. Er is dus een behoefte aan beveiliging op zowel hogere als lagere protocolniveaus. De volgende standaarden illustreren dit:

- *IPsec* (IP security): IETF netwerklaag beveiligingsstandaard met diensten voor vertrouwelijkheid, integriteit, en bescherming tegen overspelen.
- *SSL* (Secure Socket Layer): oorspronkelijk door Netscape ontwikkelde oplossing voor beveiligde communicatie en authenticatie tussen een web client en een web server. HTTP kan gebruik maken van SSL, en wordt dan HTTPS (Secure HTTP) genoemd. SSL maakt gebruik van TCP.
- *TLS* (Transport Layer Security): IETF versie van SSL.
- *PGP* (Pretty Good Privacy): de facto beveiligingsstandaard voor email.

Een andere manier om een computernetwerk te beveiligen is door een beveiligingsmuur, of *'firewall'*, te plaatsen tussen het internet en het computersysteem of bedrijfsnetwerk dat aangesloten is op het internet. Al het verkeer van en naar het internet moet de firewall passeren, en kan daardoor onderworpen worden aan een lokaal gedefinieerd beveiligingsbeleid. Het belangrijkste voordeel van een firewall is gelegen in de concentratie van de beveiliging in een punt, wat leidt tot een vereenvoudigd management en monitoring van beveiligingsfuncties (met name voor toegangscontrole en beschikbaarheid). We onderscheiden twee soorten firewall-functies:

- *netwerklaag firewall*: filtert berichten door informatie in de berichten te inspecteren, bijvoorbeeld IP bron- en bestemmingsadres, transport poortnummer en IP protocolveld.

- *applicatielaag firewall*: laat alleen verkeer van geselecteerde applicaties door, nadat de gebruiker de juiste identificatie- en authenticatie-informatie heeft kunnen overleggen.

3.4 Operationeel Beheer

Tot operationeel beheer van computernetwerken worden al die taken gerekend die betrekking hebben op de dagelijkse levering van ICT diensten aan eindgebruikers. Naast operationeel beheer kunnen ook nog andere beheerstaken worden geïdentificeerd, zoals de (strategische) planning van de ICT infrastructuur (bijvoorbeeld netwerk en ICT applicaties), en de bedrijfsmatige aspecten betreffende de ICT voorziening (zoals bijvoorbeeld human resource management en financieel management).

Het doel van operationeel beheer is om er voor te zorgen dat het computernetwerk functioneert en blijft functioneren zodanig dat de diensten die geleverd worden voldoen aan de verwachtingen van de gebruikers, of zoals contractueel vastgelegd is met de gebruikers. Het geheel van verantwoordelijkheden van beide partijen (gebruiker en diensten leveraar) wordt doorgaans vastgelegd in een Service Level Agreement (SLA). Operationeel beheer betreft dus het beheer over alle systemen, hun verbindingen, alsook alle protocollagen en protocollen die in de infrastructuur voorkomen.

In het navolgende wordt op algemeen niveau ingegaan op de taakgebieden die tot operationeel beheer worden gerekend. Voorts zal slechts een klein deelgebied worden bekeken, te weten de aspecten en principes die ontwikkeld zijn voor het observeren en controleren van de bouwblokken die gebruikt worden voor het leveren van gebruikersdiensten.

Taakgebieden van operationeel beheer

Het operationele beheer van computernetwerken omvat een groot aantal taken. Er bestaan diverse raamwerken voor het categoriseren van deze taken, het meest gebruikte is ontwikkeld door ISO. Dit raamwerk bestaat uit de volgende vijf taakgebieden:

- Foutenbeheer - de verzameling van functies en processen die nodig is voor het detecteren, analyseren, identificeren, isoleren en verhelpen van fouten die optreden in de computernetwerkinfrastructuur. Het optreden van fouten heeft tot gevolg dat het computernetwerk niet meer voldoet aan een of meerdere operationele doelen die aan de infrastructuur gesteld zijn. Vaak kunnen fouten niet direct worden waargenomen maar slechts indirect door de symptomen die zij veroorzaken. Een van de concrete functies behorend

tot dit taakgebied is foutlokalisatie, d.w.z. een functie die op basis van geobserveerde symptomen, de foutbron(nen) identificeert.

- Configuratiebeheer - dit functiegebied heeft tot doel om de elementen waaruit het netwerk en de netwerksystemen zijn opgebouwd, en hun onderlinge samenhang te bewaken en waar nodig te veranderen. Configuratiebeheer is verantwoordelijk voor het monitoren van de configuratie (i.e. parameter settings) van de elementen, en waar nodig het veranderen de configuratie.
- Accountingbeheer - onder accounting management wordt verstaan het verzamelen, opslaan en verwerken van gegevens over het gebruik van geleverde diensten (door wie, is wanneer, welke dienst gebruikt, voor hoelang c.q. hoeveel). Dit kan onder meer tot doel hebben een rekening op te stellen voor de eindgebruikers.
- Prestatiebeheer - dit functiegebied heeft tot doel om de effectiviteit van de computernetwerk infrastructuur en het gedrag van de resources te evalueren. Voorbeelden van functies in dit managementgebied zijn: verzamelen, verwerken en rapporteren van statistische informatie over prestatie van de ICT infrastructuur en mogelijk individuele elementen in de infrastructuur.
- Beveiligingbeheer - dit functiegebied heeft tot doel om beveiligingsdiensten te ondersteunen (bijvoorbeeld distributie van sleutels t.b.v. encryptie en decryptie), detectie en ingrijpen in geval van oneigenlijk resource gebruik. Onder dit functiegebied valt ook het beheer van beveiligingsmaatregelen ten behoeve van de management infrastructuur zelf.

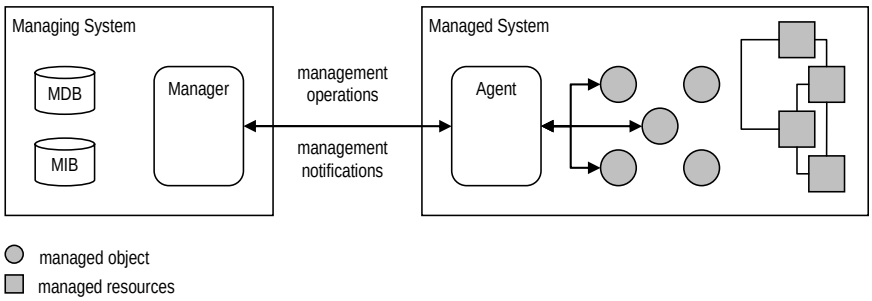
De taakgebieden van operationeel management kunnen opgevat worden als een functioneel model van beheer, daarnaast omvat een management architectuur nog drie andere typen modellen: organisatiemodel, informatiemodel en communicatiemodel. Deze worden in het navolgende kort besproken.

Organisatie model

Een organisatiemodel definieert de elementen van een management architectuur en hun samenhang. De elementen zijn (zie Figuur 9 ter illustratie):

- Managed System - dit is het systeem dat beheerd wordt, d.w.z. het systeem dat ten behoeve van operationeel management gemonitored en bestuurd wordt. Voorbeelden zijn: routers, switches, firewalls, base-stations, servers, desktops.

- Managing System - dit is het system dat primair verantwoordelijk is voor de uitvoering van management taken en functies behorend tot de functionele management gebieden. Deze taken worden uitgevoerd door de Manager die aanwezig.
- Managed Object - Een managed object is een projectie van een resource ten behoeve van management. Anders gezegd, een managed object is een (abstracte) representatie van een resource ten behoeve van het beheer van die resource. De drie basis abstracties zijn: attribuut (een eigenschap van een resource, bijvoorbeeld het aantal door een router verwerkte IP paketten)); operaties (functies die door een resource kunnen worden uitgoerd t.b.v. beheer, bijvoorbeeld het stoppen van een server process); en, notificaties (een berichtgeving over een bepaald event of bereikte toestand, bijvoorbeeld een volle buffer).
- Agent - Het managed systeem heeft een agent. Dit is een lokaal process dat toegang verschaft tot managed objects, en verantwoordelijk is de communicatie met manager.
- Manager - De manager bestaat uit een proces, of processen, die op basis van informatie verkregen via een of meerdere agents betreffende managed objects, een of meerdere beheertaken uitvoert. En, indien nodig dan wel gewenst, wijzigingen in attributen initieert of operaties op managed objects initieert.
- Management Database (MDB) - De Management Database wordt door de manager gebruikt om gegevens over managed objects op te slaan.
- Management Information Base (MIB) - Specificaties van Managed Objects zijn beschikbaar in de Management Information Base. Via de MIB heeft de Manager toegang tot informatie over de syntax en semantiek van managed objects.



Figuur 9: Organisatiemodel

Management Informatie model

Essentieel voor iedere management infrastructuur is de specificatie van managed objects. Enerzijds voor de manager om toegang te hebben tot de syntaxis en semantiek van managed objects (nodig voor zinvolle interacties met managed systems), anderzijds vormen deze specificaties het vertrekpunt voor het implementatie (nodig in een managed system). Het gevolg hiervan is dat er een 'taal' nodig is waarmee managed objects kunnen worden gespecificeerd. Binnen een specifieke management architectuur vinden we daarom doorgaans een specificatie taal voor managed objects, en een verzameling van specificaties waarin managed objects zijn gespecificeerd.

Communicatiemodel

Een communicatiemodel is noodzakelijk zodat een managing system management informatie kan opvragen en ontvangen van een of meerdere managed systems. In computernetwerken wordt, doorgaans gebruik gemaakt van dezelfde netwerkinfrastructuur als die waarover gebruikersverkeer gaat.

Een aantal essentiële aspecten van het communicatiemodel is:

- adressering / identificatie van managed objects: de manager zal, voor het monitoren en het uitoefenen van controle op managed objects, de managed objects moeten kunnen identificeren en adresseren.
- authorisatie en authenticatie: wanneer een manager toegang probeert te krijgen tot een agent, zal een vorm van authorisatie en authenticatie nodig zijn. Met name wanneer control activiteiten op een resource uitgevoerd moeten gaan worden is het noodzakelijk om ervoor te zorgen dat dit door de daartoe aangewezen manager gebeurt.

Verder zal het communicatiemodel ondersteuning moeten geven voor het opvragen van attribuut waarden, eventueel veranderen van attribuut waarden, in voorkomende gevallen uitvoeren van operaties en uitwisseling van notificaties.

Concrete Architecturen voor Resource Management

Er bestaan diverse concrete architecturen voor operationeel beheer. Zonder in veel detail te treden zullen er drie worden toegelicht en hun belangrijkste karakteristieken worden gegeven.

- SNMP (Simple Network Management Protocol) - SNMP is wel het bekendste en meest gebruikte architectuur. SNMP ondersteund alleen attributen (in SNMP jargon scalar objects geheten) en notificaties (in SNMP jargon alarms genoemd). Operaties kunnen op indirecte wijze ondersteund worden als bedoeld en gespecifieerd zijeffect van het veranderen van

attribuut waarden. De 'taal' waarin Managed Object gespecificeerd worden is de SMI (Structure of Management Information). De SMI is gebaseerd op ITU-T's ASN.1 (Abstract Syntax Notation One). Er zijn vele gestandaardiseerde MIB Modules gespecificeerd, variërend van modules voor het beheer van routers (en aanwezige protocol entiteiten, en fysieke componenten) tot applicaties zoals Mail Transfer Agents en Web Servers. Ten behoeve van communicatie bestaan er drie verschillende versies van het SNMP communicatie protocol, de meest recente versie (SNMP versie 3) is alomvattend in de zin dat deze ook de oudere versies (SNMPv1 en v2c) ondersteund. Ook het communicatie protocol is gespecificeerd met behulp van ASN.1, de encoding regels voor de mapping naar de transport laag is BER (Basic Encoding Rules), dat onderdeel is van de ASN.1 suite. Standaard wordt UDP gebruikt voor het transport van management data tussen de manager en agent.

- WBEM (Web Based Enterprise Management) - WBEM wordt veel gebruikt voor het management van bedrijfsnetwerken. Het informatie model (Common Information Model, CIM) ondersteund naast attributen en notificatie ook operaties. CIM is gebaseerd of IDL (Interface Definition Language), en maakt gebruik van UML om de diverse modellen weer te geven. CIM maakt gebruikt van Object Oriented technieken, en biedt daardoor betere ondersteuning voor model uitbreidingen. Ten behoeve van de communicatie wordt http gebruikt, hiertoe worden de management operaties (attribuut waarden ophalen, veranderen, uitvoeren van operaties en notificatie) afgebeeld naar http berichten.
- WSDM (Web Services Distributed Management) - WSDM is een zeer recente ontwikkeling voor het operationeel beheer van resources. Hierin wordt gebruikt gemaakt van XML Schema's om management informatie te specificeren. Voor de communicatie wordt gebruik gemaakt van Web Services, WSDM communicatie is gespecificeerd in de Web Services Description Language. WSDM maakt onderscheid tussen Management using Web Services (MuWS) en Management of Web Services (MoWS). Web Services zijn namelijk zelf ook resources en dus onderwerp voor management.

Literatuur

F. Halsall. Multimedia Communications - Applications, Networks, Protocols and Standards; Addison-Wesley, 2001.

James F. Kurose & Keith W. Ross. Computer networking – A top-down approach featuring the Internet. Third edition, Addison-Wesley, 2005.

William Stallings. Cryptography and network security – Principles and practice. Third edition, Prentice Hall, 2003.

M. Subramanian; Network Management, Principles and Practice; Addison-Wesley, 2000.

H. Schulzrinne, E. Wedlund. Application-Layer Mobility Using SIP, ACM SIGMOBILE Mobile Computing and Communications Review, Volume 4, Number 3, (July) 2000, pp. 47-57.

Internetsites:

IEEE http://www.ieee.org/

IETF http://www.ietf.org/

ISO http://www.iso.org/

ITU http://www.itu.int/

OMG http://www.omg.org/

W3C http://www.w3c.org/

DMTF http://www.dmtf.org/

OASIS http://www.oasis-open.org/