

ATARI Trainingen

**ST(E)/TT
NETWERKEN**

Inhoud (ochtend)

- Wat is een L.A.N.
- Waarom een netwerk
- Geschiedenis van netwerken
- Begrippen en definities
- Overzicht LAN transport media
- Netwerk topologiën
- Netwerk standaards
- Medium toegangsprotocollen
- Netwerk besturings software
- Samenvatting
- Applicaties en het netwerk

Wat is een L.A.N.

Local Area Network

Kenmerken:

- Beperkte geografische spreiding (kamer, afdeling, gebouw)
- Het medium is in bezit van de gebruiker
- Hoge transmissie snelheid (> 1 Mbit/s)

Wetenswaardigheden

- Meestal 1 groep gebruikers (afdeling) met toegang tot beperkte hoeveelheid gegevens (boekhouding, database)
- Veel LANs worden gebruikt door hele afdeling
- Trend in richting van gehele onderneming met name communicatie

Waarom een netwerk

Data Sharing	Gezamenlijk I bestand, dus up-to-date
Program Sharing	Voor grote netwerken Vereenvoudigd prog- ramma updates Licentie vaak voor gelijktijdig gebruik
Device Sharing	Doorgaans voor kleine groepen
Communicatie	Email
Centrale backup	Overzichtelijker, door gespecialiseerd persoon

Geschiedenis van netwerken

Ethernet (amerika)

- Eind jaren 60 door Universiteit hawai (ALOHANET)
- Begin jaren 70 door Xerox (1 mbit/s), eind jaren 70 commercieel
- Begin 80 ethernet Release 1.0, met Digital, Intel en Xerox (10 Mbit/s)

Token Passing (europa)

- Oorspronkelijk idee van Olaf Söderblum
- Ontwikkeld als RING door IBM laboratoria te Zurich
- Eerst op de markt gebracht door Proteon
- Daarna door IBM (1984, 4 Mbit/s)
- Hetzelfde concept uitgewerkt voor een BUS door Datapoint en uitgebracht als ARCnet (begin jaren 80, 2,5 Mbit/s)
- Eind jaren 80 kwam 16 Mbit/s versie beschikbaar

Begrippen en definities

node	knooppunt, aansluiting in netwerk, gebruiker
server	1) centrale computer in netwerk die de totale netwerk besturing voor rekening neemt alsmede de opslag van gezamenlijke data 2) proces dat een ander proces bediend
client	1) zie node 2) proces dat door een ander proces bediend wordt
bridge	apparaat dat interconnectie verzorgt tussen twee netwerken ONAFHANKELIJK van de in de netwerken gebruikte HOGER NIVEAU protocollen
gateway	apparaat dat interconnectie verzorgt tussen twee netwerken waarbij TOTALE protocol conversie plaatsvind, bv TCP/IP naar SNA.
router	apparaat dat interconnectie verzorgt tussen twee netwerken met gezamenlijk protocol (heeft ingebouwde intelligentie met de adressen van beide netwerken)

repeater	apparaat(je) dat lengte van netwerk vergroot door signaal te versterken
transceiver	verbind node met baseband kabel
transparant	een netwerk/verbinding dat zich dusdanig natuurlijk gedraagt dat de gebruiker niet door heeft dat het om een netwerk gaat
segment	een deel in het totale netwerk dat niet uitgerust is met een bridge, router en/of repeater. Achter een dergelijk apparaat begint het volgende segment

Let OP !! Ethernet zegt wat van bekabeling, low level transport, maar NIETS van besturingssoftware. Ethernet is dus geen garantie voor connectivity.

Overzicht LAN transport media

Snelheden van netwerken

Bell 103 Modem	300 bit/s
Bell 212/V.22 Modem	1200 bit/s
V.22bis Modem	2400 bit/s
V.29/V.32 Modem	9600 bit/s
Snelste RS-232	19.200 bit/s
Starlan/10-Net/Omninet etc.	1.000.000 bit/s
Telefoon T1-Kanaal	2.000.000 bit/s
ArcNet	2.500.000 bit/s
Token Ring (huidig)	4.000.000 bit/s
Ethernet/Pronet-10	10.000.000 bit/s
Token Ring (nieuwste versie)	16.000.000 bit/s
Pronet-80	80.000.000 bit/s
FDDI (Fiberoptics Distributed Data Interchange)	100.000.000 bit/s

Wij behandelen:

Ethernet, ARCnet, Token Ring en FDDI

Netwerk topologiën

Topologie

geografische structuur van communicatieverbindingen en computers die een netwerk vormen

We onderscheiden elektrische- en fysieke topologie.

We behandelen:

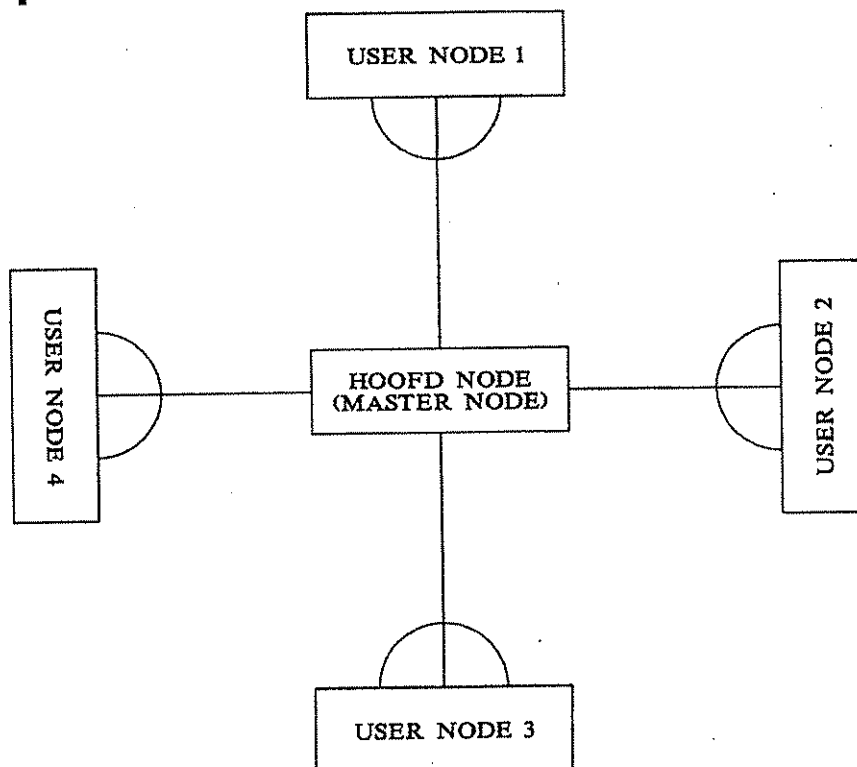
electrisch STAR, BUS, RING en combinatie's daarna de fysieke uitvoering

STER

Voorbeeld:

het openbare telefonie systeem

- Zeer snelle verwerkingstijden
- Moeilijk uit te breiden
- Capaciteit wordt beperkt door centrale eenheid
- Moeilijk te beheersen
- Meer dan 1 verbinding op hetzelfde tijdstip

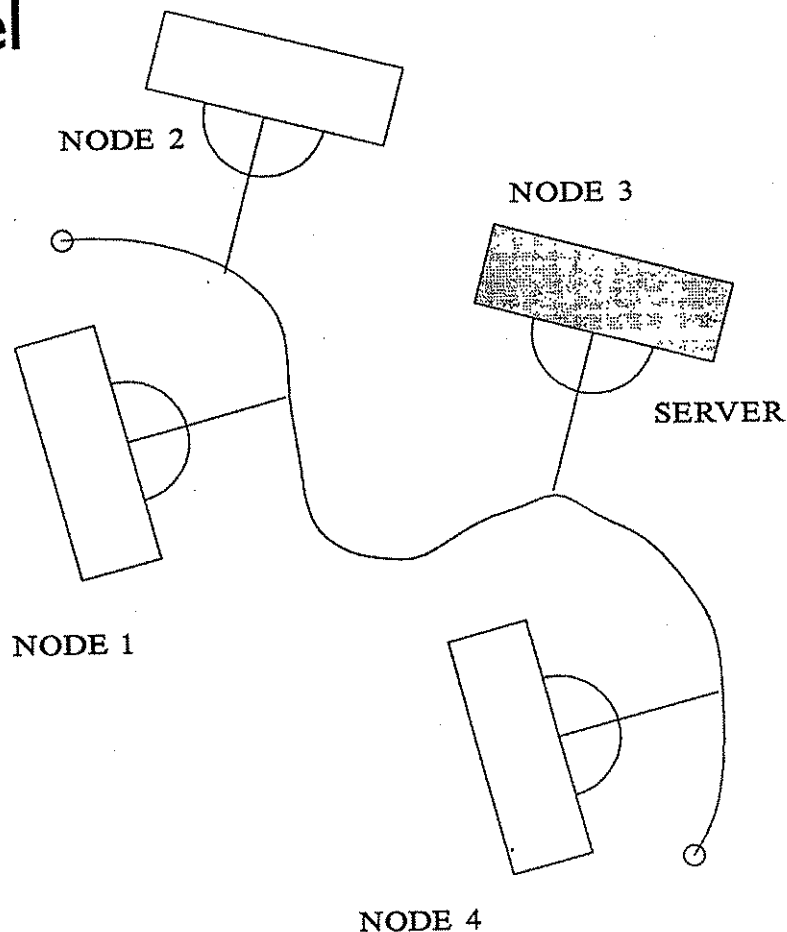


BUS

Voorbeeld:

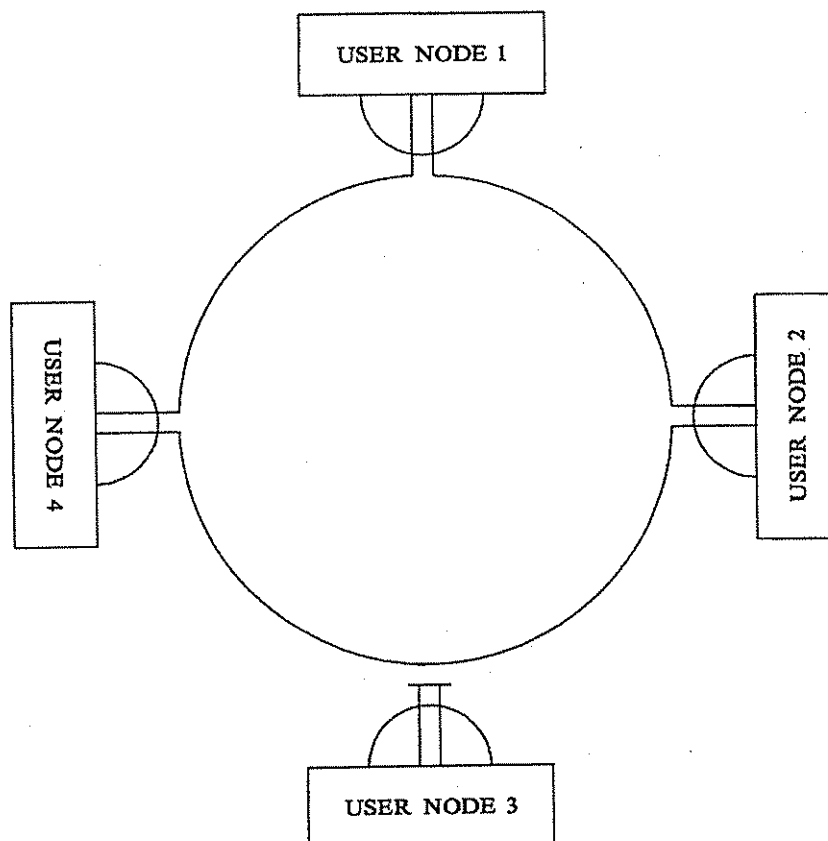
het openbare elektriciteits net

- Alle boodschappen gaan naar elke node
- Berichten worden als omroep uitgezonden (radio)
- Gemakkelijk uit te breiden
- Problemen moeilijk te localiseren
- Capaciteit beperkt door bandbreedte van kabel

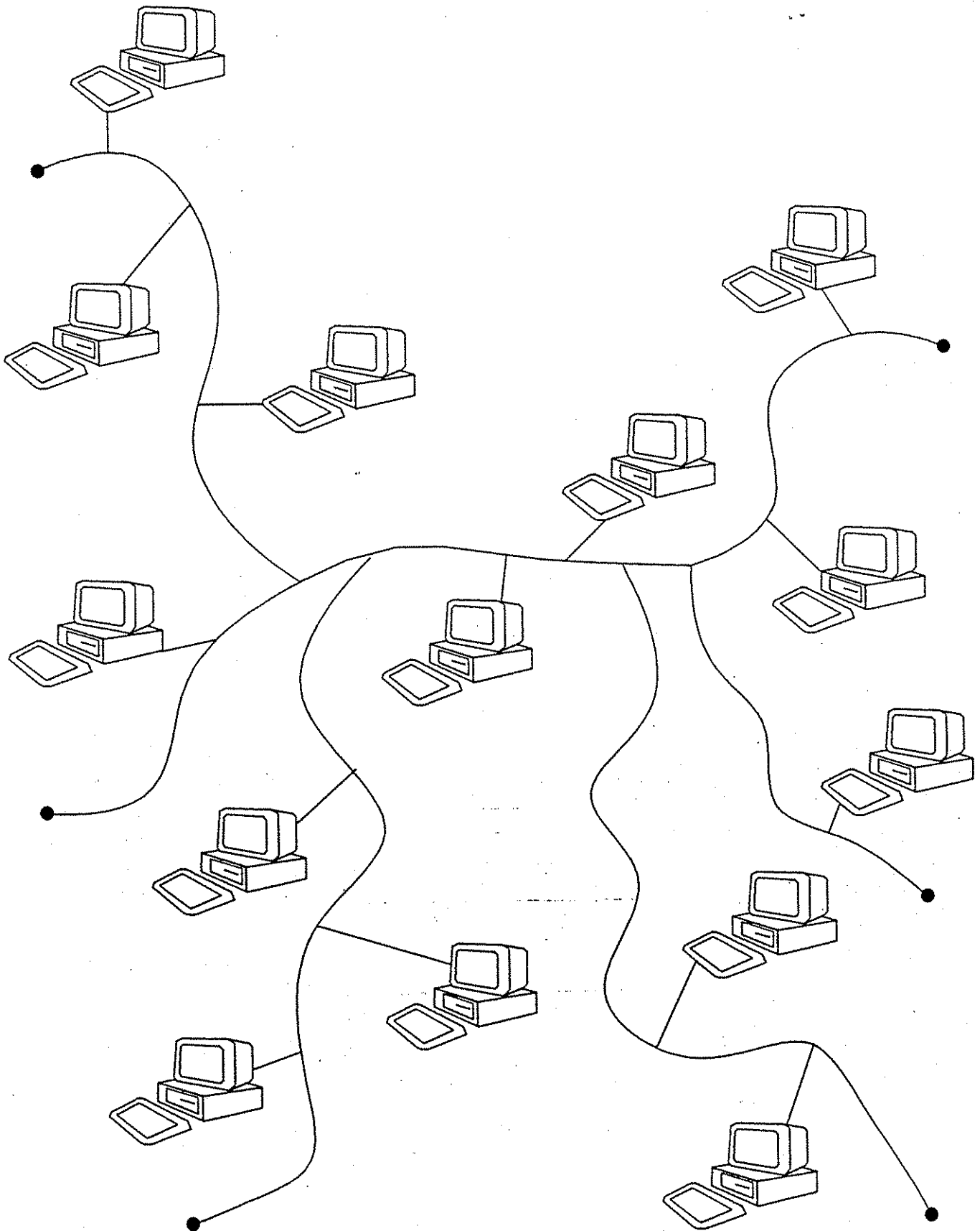


RING

- Transmissies worden in volgorde doorgegeven aan volgende node
- Vrij eenvouding uit te breiden
- Door ringvorm wordt betrouwbaarheid vergroot
- Capaciteit wordt beperkt door aangesloten nodes

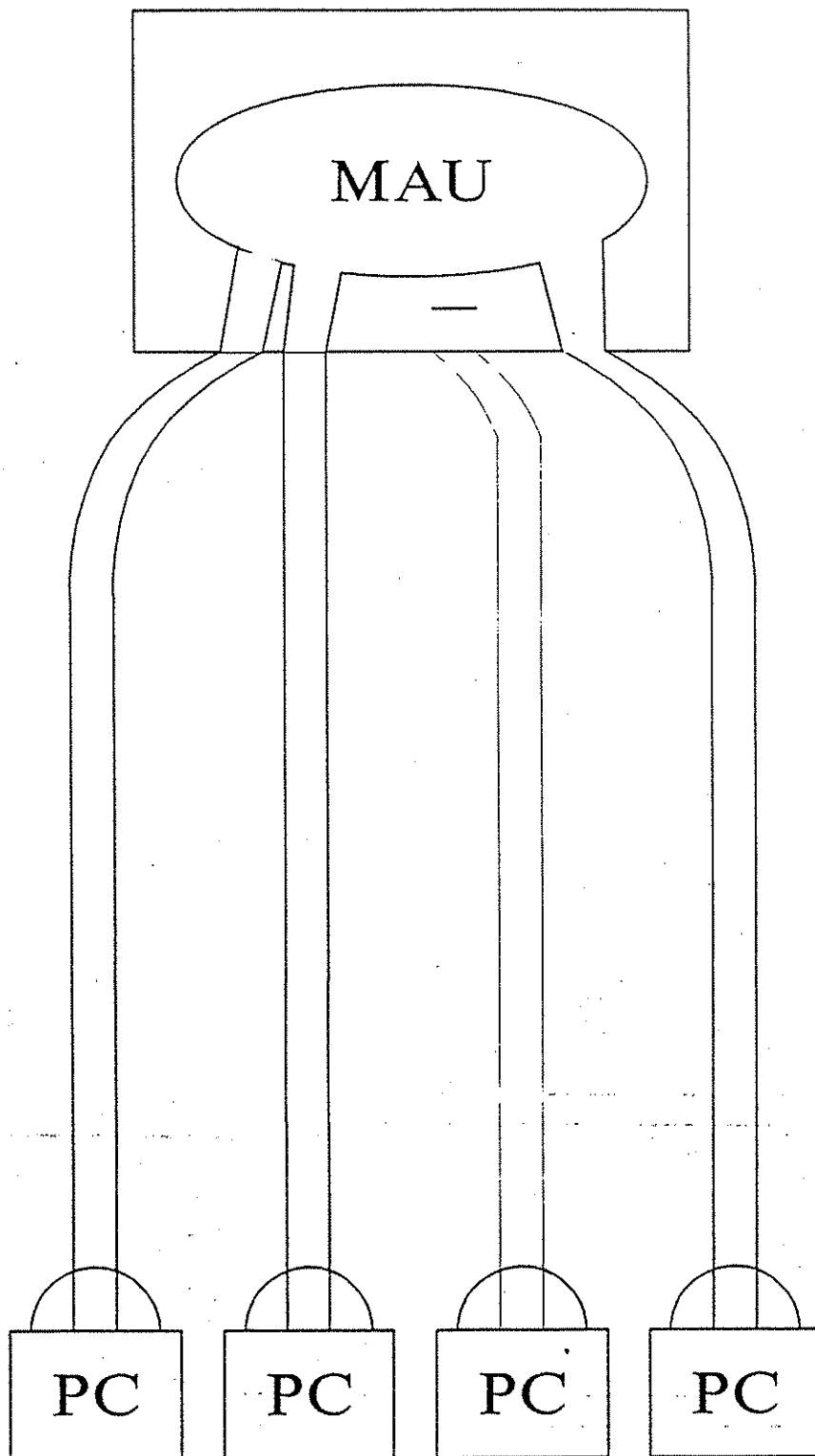


BOOMVORMIG NETWERK

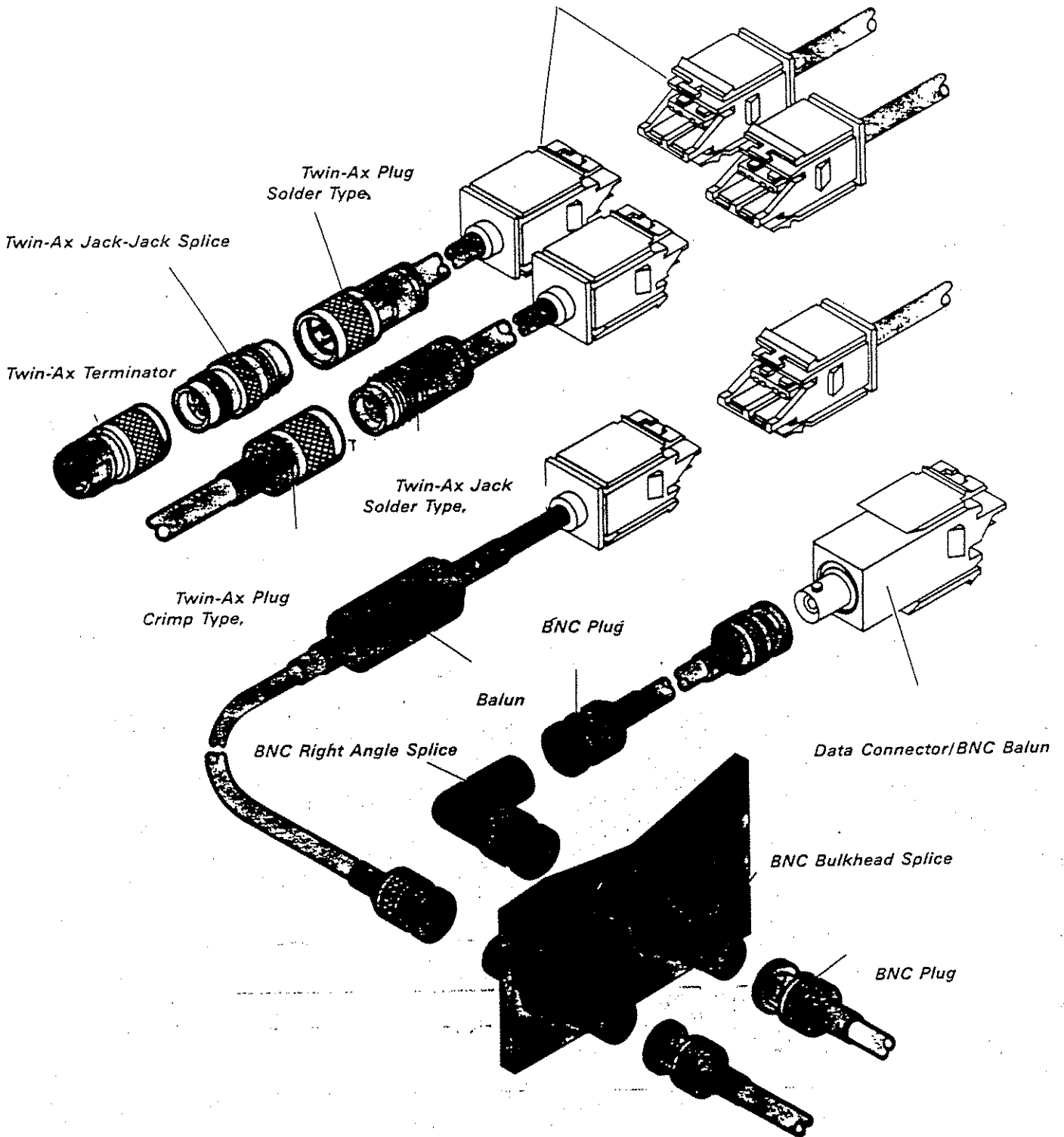


Fysieke Topologie

- Een fysieke STER-vorm is mogelijk voor ALLE elektrische vormen
- Ringen zijn meestal STERvormig bekabeld
- Centraal in deze STERvorm staat een schakelkast;
- Concentrator voor ethernet
- MAU voor Token Ring
- HUB voor ARCnet



4 Position Data Connector



Connectors Compatible with IBM Alternative Cabling System

Netwerk standaards

IEEE 802.3 CSMA/CD

Standaard voor Ethernet, Starlan ed

Onderverdeeld in substandaarden,
genoemd; x Base/Broad y

x	Transmissiesnelheid in Mbit/s
Base/Broad	type transmissie techniek
y	maximale lengte van segmenten in meter x 100 (afgerond)
10 Base 5	Dik Ethernet 10 Base T
10 Base 2	Ethernet voor twisted pair Dun Ethernet 10 Broad 36 Breedband Ethernet

IEEE 802.5 Token Passing Ring

IBM's Token Ring

IEEE 802.8 FDDI

Fiberoptics Distributed Data Interchange
Glasvezel netwerk op 100 Mbit/s
Momenteel nog erg duur

Medium toegangsprotocollen

CSMA/CA

- Carrier Sence Multiple Access/Collision Avoidance
- Station controleert of de lijn vrij is aan het begin van een tijdsinterval
- Als de lijn vrij is wordt er gewacht op het toegekende tijdstip
- Als de lijn dan nog vrij is wordt er verzonden
- Vervolgens wordt er gewacht op bevestiging van ontvanger

Nadeel:

Er veel vertraging terwijl de lijn misschien wel direct vrij is

CSMA/CD

- Carrier Sense Multiple Access/Collision Detect
- Luister en wacht op vrije lijn
- Begin met verzenden

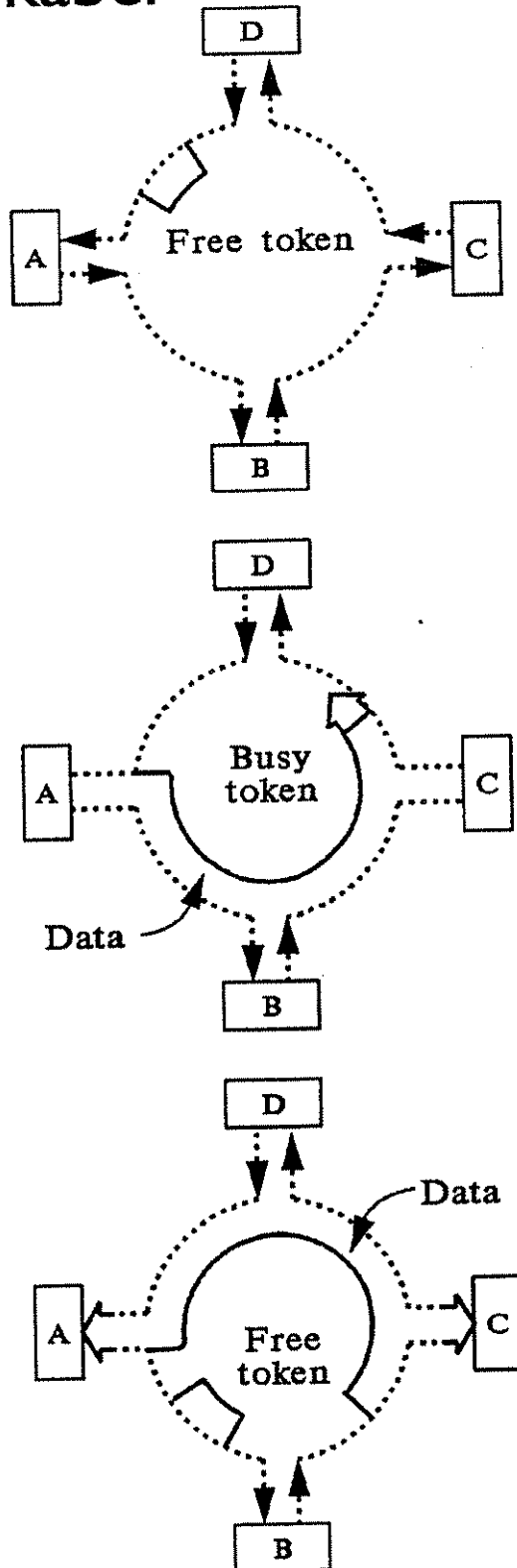
(Als een ander ook dan begon is er sprake van een botsing (collision), beide stations proberen het op een verschillende tijdsinterval nog eens)

Botsingen komen slechts nauwelijks voor, in praktijk +/- 10%

Token Passing

- Er circuleert een vrij token
- Het token wordt gepakt door een verzendende node. Deze stuurt een frame uit
- Elk token of frame wordt door elk station bekeken en zonodig doorgegeven aan de volgende node
- De ontvangende node markeert het frame als ontvangen

- De zender krijgt uiteindelijk het frame terug, controleert dat op bevestiging en zet een vrij token op de lijn
- De prestatie is in het slechste geval te berekenen uit het aantal nodes en de lengte van de kabel



Netwerk besturings software

We behandelen:

- Novell Netware (globaal)
- TCP/IP (diepgaand)
- NFS (globaal)

We behandelen niet:

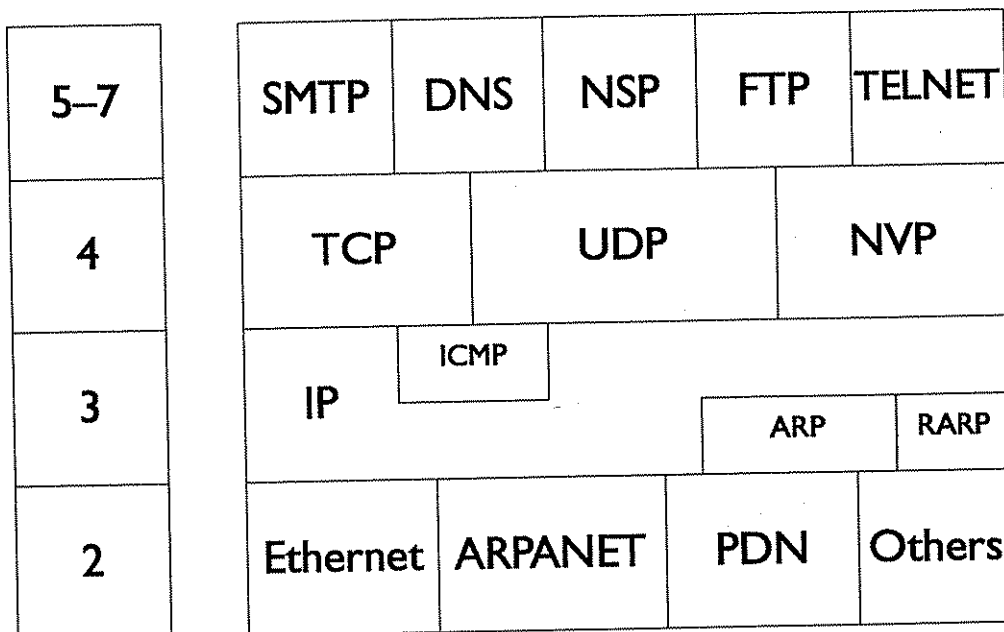
- diverse anderen zoals PC-Lan, LAN Manager

Novell Netware

- Beschikbaar op Ethernet, ARCnet en Token Ring
- HET netwerkbesturingssysteem, gaat zo ver dat het het operating system vervangt (DOS eruit, NETWARE erin).
- Goede protectie, biedt veel mogelijkheden voor beheerder.
- Eigen standaard, niet beschikbaar voor derden, hoge prijzen
- IPX Internetwork Packet eXchange, het protocol voor communicatie in een NetWare omgeving
- NLM Network Loadable Modules, modules voor koppeling met TCP/IP, NFS enz. Onderdeel in NetWare 3.1

TCP/IP

- TCP/IP is **GEEN** transparant netwerk besturingsysteem maar slechts een transmissieprotocol !!
- Een standaard die **NIET** merkgebonden is en open staat voor iedereen



- IP** Internet Protocol, zorgt voor netwerk transactie's en biedt functies voor bovenliggende lagen.
- ICMP** Internet Control Message Protocol, ICMP heeft als taak de IP-modules te waarschuwen wanneer iets abnormaals gebeurt bij de verzender.
- ARP** Address Resolution Protocol, zet een IP adres om in een ethernet adres.
- RARP** Reversed Address Resolution Protocol, zet een ethernet adres om in een IP adres.
- TCP** Transmission Control Protocol, TCP draagt zorg voor de transmissie van data dwz beheert de verbinding en controleert de gegevensstroom.
- UDP** User Datagram Protocol, UDP is vergelijkbaar met TCP en heeft minder overhead (controle) dan TCP.
- NVP** Network Voice Protocol, protocol voor overdracht van gedigitaliseerd/gecomprimeert geluid.
- SMTP** Simple Mail Transfer Protocol, biedt mogelijkheden voor het verzenden van post (teksten) tussen gebruikers onderling.
- DNS** Domain Service Protocol, DNS is een complexe service die een 'naam' toekent/vertaalt in een IP adres.
- NSP** Name Service Protocol, voorloper van DNS, minder complex van opzet.
- FTP** File Transfer Protocol, biedt mogelijkheden voor file uitwisseling tussen computers.
- TELNET** Virtueel terminal programma voor interactieve toegang tot hosts.

NFS

Network File System

- Ontwikkeld door SUN, toch voor derden beschikbaar
- Transparant netwerkbesturingssysteem om basis van filesystem

Samenvatting

	Ethernet	FDDI	Token Ring	ACRnet
Topologie				
electrisch fysiek	bus bus (coax) ster (utp)	bus bus	ring ster	bus ster
protocol	CSMA/CD	CSMA/CD	Token Passing	Token Passing
transmissie	baseband broadband	baseband	baseband	baseband broadband
kabel	Dun ethernet coax Dik ethernet coax	Fiber coax	STP: IBM Type 1 UTP: IBM Type 3	Coax: RG62
snelheid	10Mbit/s	100Mbit/s	4 of 16Mbit/s	2,5Mbit/s
aanbeveling	mixed vendor	mixed vendor	IBM world	Bijna alleen PC's

Applicaties en het netwerk

De reactie van applicatie software op het netwerk kan men als volgt indelen

NETWORK BLIND

- Herkennen niet het bestaan van het netwerk
- Spreken vaak direct de hardware aan

NETWORK TOLERANT

- De meeste 'netwerk-versies'
- Kunnen overweg met het filesysteem van het netwerk op dezelfde basis als een gewone floppy of harddisk

NETWORK USING

- Maakt nuttig gebruik van netwerk
- Houdt rekening met meer dan 1 gebruiker

- Ondersteund gezamenlijk gebruik van apparatuur

Bijvoorbeeld: database met record locking

NETWORK LOCKING

- Speciaal geschreven vanwege netwerk en multiuser gebruik, zijn zonder netwerk niet bruikbaar

Vormen vaak opzich al een reden om een netwerk te kopen

Inhoud (middag)

- Wat is A.N.S.
- A.N.S. en de rest van de wereld
- Installatie stap voor stap
- Wat kan er mis gaan?
- Demonstraties
- Onderhoud
- Overzicht andere ST/TT netwerken
- Achtergrond informatie

Wat is A.N.S.

Atari Network System

Bestaat uit:

- ethernet board voor MEGA-bus of VME bus
- A.F.S. Atari File System (netwerkbesturing)
- aanvullende utilities

Opbouw: zie schema

A N S



Atari Network System

Atari Gem Desktop

Menügesteuerte
netzwerkweite
Installation
aller Server
Clients, Dienst-
programme und
Netzwerkparameter

Server

- AFS
- FTP
- TFTP
- Netzdrucker Spooler

Applikation

- Telnet v2100
Tektronix 4010
- X11R4
- FTP
- TFTP
- Mail

A F S

Atari File System

Multitaskingkern - Netzwerkkern - Client des netzwerkweiten Atari Filesystems - Client des netzwerkweiten
Drucksystems - Client des Mailsystems - Management localer Server

TCP/IP

Industriestandard Protokollfamilie

◁ ARP ▷ IP ▷ ICMP ▷ UDP ▷ TCP ▷
Hochsprachenschnittstelle

repdev

Packetorientierter Treiber mit Hochsprachenschnittstelle

Riebl-Card plus (Mega ST)

16 Bit Ethernet-Controller LANCE
64 KB Dualported RAM
Mega ST Bus

Riebl-Card plus (TT, Mega STE)

16 Bit Ethernet-Controller LANCE
64 KB Dualported RAM
A24/D16 VME-Bus Slave-interface

Ethernet (IEEE 802.3 10 Base 5, IEEE 802.3 10 Base 2)

A.N.S. en de rest van de wereld

Momenteel:

uitsluitend koppeling MEGA ST(E) en TT

Toekomst:

via internet utilities koppeling met UNIX ed.

Voorlopig niet:

koppeling novell (TCP/IP NLM nog niet uitgeprobeert)

Installatie stap voor stap

1003.06 -TT2 = 00.00.36.04.01.21
1003.05 -TT1 = .04.01.72
SERV = .02.01.45

- Ethernet nummers van kaarten opschrijven
- Jumpers goed ? Kaarten installeren
- RCPDEV op elke machine opstarten
→ \AUTO\
- INSLIE opstarten, naam machine ingeven
- ANSINS opstarten Host Datei einrichten
INITD parameter einstellen
AFS-Server einrichten
AFS-Mount Datei einrichten
- xxSERVER, AUTOLOG, LOGIN.ACC installeren (lep op serie nummers)
- SERVER.TOS starten op server
- machines van gebruikers opstarten en inloggen

Wat kan er mis gaan

- RCPDEV vergeten, zie ook
\\ETC\INITD.LOG
Opl: alsnog opstarten
- kaart is ethernet nummer kwijt
Opl: alsnog installeren mbv
RCPCHECK, batterij vervangen?,
OLDCARD installeren in INITD.CNF
- ANSINS niet volledig doorlopen
Opl: alsnog doorlopen
- Gelijke serienummers in ANS software
Opl: andere diskette installeren
- Gelijke IP nummers
Opl: nog eens INCLIE en ANSINS
doorlopen
- Netwerk transmissie fouten, zie je vaak
al met ANSINS
Opl: Nodes ontkoppelen (T-stuk los),
werkt het dan ? Ja, ergens kaart of
machine niet goed. Nee, kabel voor
kabel aansluiten.

- Kaart defect ?
Opl: RCPCHECK opstarten en oa externe loopback testen.

Demonstraties

- Tracks Flexibase
- MegaSystems administratieve software
- XCOPY software
- TELNET (PC en UNIX)

Onderhoud

UPDATE

- Nieuwe software installeren in bestaand netwerk

Update functie ANSINS gebruiken, te updaten bestanden opnemen in \ANS\UPDATE\. Elke client MOET \ANSBIN\xxSERVER.xxx hebben !!

Netwerk uitbreiden

- Server stoppen, ANSINS en INSCLE draaien of

ANSINS vanaf terminal met copie van \ANS*.*, daarna terugzetten en alsnog de server opnieuw opstarten

Backup

- Lokaal naar netwerk → XCOPY
Netwerk mbv streamer of SB Backup

Achtergrond informatie:

- Alles over netwerken (START 3 I, sep/ okt 1991)
- TCP/IP en ISO lagen (Data Decisions, okt,nov,dec 1990)
- Terms in computer networking and network management (3Com)
- A.N.S. manual

Uit de studie boeken: (uitspraak ter overweging)

- Een netwerkbeheerder besteed 1 uur per node per week

Dit najaar komt het Atari Network System (ANS) beschikbaar. Na twee jaar ontwikkeling door een Europees team ziet ANS nu eindelijk het levenslicht. Het laatste half jaar stonden de ontwikkelingen zelfs onder Nederlandse leiding van Wilfred Kilwinger (Atari Benelux), daarbij gesteund door bèta-testers als Commedia te Amsterdam, Tracks te Haarlem en MegaSYSTEMS te Ede. Speciaal voor START vertelt Wilfred wat u van ANS kunt verwachten.

ALLES OVER NETWERKEN

Alvorens we u het nodige over ANS vertellen, geven we u een spoedkursus netwerken. Kenners kunnen direkt doorbladeren naar het tweede deel van dit artikel, of kunnen proberen ons op fouten in het eerste deel te betrappen.

In veel bedrijven en instellingen staan inmiddels volop (stand-alone) PC's. In een dergelijke omgeving groeit al snel de behoefte om gegevens uit te wisselen. Dit gebeurt dan ook vaak in een zogenaamd 'frisbee-netwerk'. Dat wil zeggen: de data wordt op diskette gezet, waarna deze met een ferme zwaai in de richting van de persoon die de informatie heeft aangevraagd verdwijnt. Een uiterst goedkoop, maar niet zo betrouwbaar netwerk.

Bij gebruik van stand-alone PC's heeft men snel te kampen met het feit dat iedere PC zijn eigen relatiebestand heeft en de diverse bestanden geenszins op elkaar lijken, met alle gevolgen van dien. ('Nee joh, die is allang verhuisd.' 'Waarom weet ik dat dan niet?') Ook hier is een netwerk in combinatie met een multi-user database een goede oplossing.

Een netwerk biedt de mogelijkheid belangrijke data centraal op te slaan. Voor het archiveren van deze gegevens hoeft de gebruiker dan uitsluitend een backup van de harddisk van de server te maken. De server is de hoofdcomputer die zorg draagt voor de netwerkkommunikatie. Aangezien de server meestal onderhouden wordt door iemand met kennis van zaken, is de kans dat de backup slaagt veel groter dan wanneer iedere gebruiker afzonderlijk zijn data moet zekerstellen. Hoewel een netwerk vaak relatief hoge aanschafkosten met zich meebrengt, kunnen grotere netwerken juist een ruime besparing opleveren, omdat men minder randapparatuur hoeft te kopen. Eén apparaat is namelijk door meerdere gebruikers te benutten.

POSTBODE

Als laatste facet (er zijn er vast nog veel meer) behandelen we de uitwisseling van elektronische berichten, in vaktermen 'email' geheten. Dit is, mits verbonden aan enige regels, een zeer nuttige toepassing. Het kan vele 'wandelingen' door het gebouw besparen (of interne telefoontjes). Elk idee dat je een collega wilt voorleggen, tik je in op je eigen toetsenbord en stuur je via het netwerk naar de computer van je kollega. Het is zelfs mogelijk om vragen te stellen aan mensen die er (nog) niet zijn: het netwerk houdt berichten vast tot de geadresseerde ze gelezen heeft. Dit werkt natuurlijk

niet voor spoedeisende zaken, maar voor de vele niet urgente berichten is het een prima oplossing. Er zijn mensen die denken dat dit ten koste gaat van de sociale kontakten, maar het één hoeft het ander niet uit te sluiten. Elektronisch berichtenverkeer is een welkome aanvulling op de dagelijkse communicatie.

Het uitwisselen van data en berichten wordt overigens volgens de laatste modegrillen in automatiseringsland Electronic Data Interchange, kortweg EDI genoemd.

Samengevat zijn er dus minimaal zes voordelen voor het gebruik van netwerken:

1. uitwisseling data
2. centraal onderhoud van bestanden
3. centrale backup van data
4. multi-user applicaties (programma's)
5. gezamenlijk gebruik randapparatuur
6. elektronische post

Natuurlijk zijn er ook nadelen. Men moet goed opletten bij de beveiliging van de verschillende

veelgebruikte en relatief eenvoudige netwerk-topologie. Het hele netwerk is opgebouwd rond één centrale kabel (bus) met aan het begin en eind zogenaamde 'terminators' die de bus afsluiten. Naar verhouding vraagt deze opzet weinig kabel. Bij een kabelbreuk is het hele netwerk onbruikbaar, omdat de bus niet meer op de juiste wijze is afgesloten.

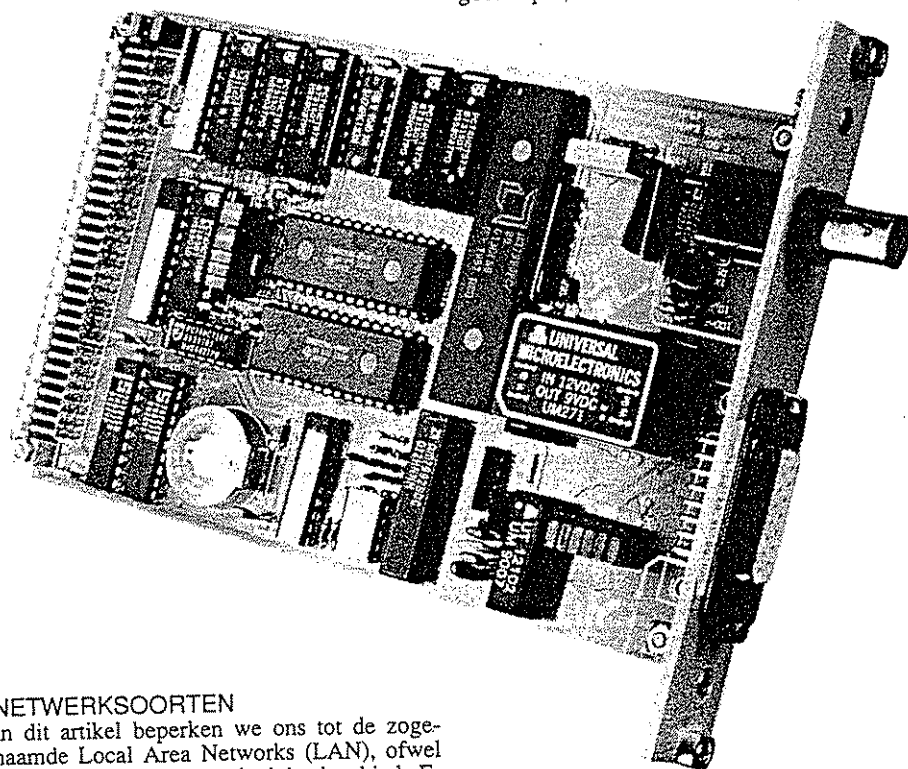
-STERSTRUKTUUR: Bij de sterstructuur heeft ieder station zijn eigen kabel naar de centraal opgestelde server. Dit vraagt natuurlijk om erg veel kabel, vooral als de stations ver weg staan. Het heeft echter als voordeel dat het netwerk operationeel blijft als er ergens een kabel breekt. Met name in militaire situaties is dit natuurlijk een vereiste.

-RINGSTRUKTUUR: Als de diverse servers en stations als het ware in een grote kring met elkaar verboden zijn (net zolang tot de uiteinden van de kabels weer bij elkaar komen), spreken we van een ringstructuur. Ook hier legt kabelbreuk het netwerk 'plat'.

TECHNIEKEN

Eén van de bekendste netwerktechnieken met een duidelijke busstructuur is Ethernet. Men maakt onderscheid tussen dik en dun Ethernet (ook wel Cheapernet genoemd). Dik Ethernet bestaat uit een zware (gele) kabel uit één stuk die door het gebouw loopt. De diverse stations worden aangesloten met behulp van een zogenaamde tranceiver, een kastje dat je op de kabel prikt. Bij elkaar een zeer dure aangelegenheid. Cheapernet bestaat uit een coaxkabel die langs elk station loopt en middels een t-stuk op het station wordt aangesloten. Hoewel beduidend goedkoper, heeft dit als nadeel dat je vaak met

bestanden (wie kan bij welke data?) Verder is een netwerk gevoelig voor virussen, maar daar kan de netwerkbeheerder gelukkig centraal iets aan doen. Daarnaast is de aanschafprijs, vooral bij kleine netwerken, relatief hoog.



NETWERKSOORTEN

In dit artikel beperken we ons tot de zogenaamde Local Area Networks (LAN), ofwel netwerken op een beperkt lokaal gebied. Er bestaan ook de Wide Area Networks (WAN) zoals Datanet 1 van de PTT, of de videotex-nummers 06-7x00.

Als twee computers met elkaar in een netwerk willen praten, moeten ze niet alleen over dezelfde bekabeling beschikken, maar ook over hetzelfde software-protocol. Voor we in detail gaan over de technieken, behandelen we eerst de fysieke vorm die een netwerk kan hebben. In vaktermen noemen we dit een topologie. Hoewel er minstens zeven topologieën bekend zijn, bespreken we slechts de belangrijkste drie:

-BUSSTRUKTUUR: De busstructuur is een

twee kabels per werkplek zit (aan- en afvoer) en moeilijk een station kunt verplaatsen. Verder is de maximale reikwijdte van Cheapernet beduidend lager dan bij dik Ethernet.

Ethernet werkt op een snelheid van 10Mhz (10 miljoen bits per seconde). Een station dat iets wil verzenden, zet de data direkt op de bus zonder te kijken of die vrij is. Door vervolgens de bus af te luisteren ziet de netwerkkaart of de data heel is overgekomen of mogelijk gebotst is op reeds aanwezige data. In dat laatste geval herhaalt de netwerkkaart zijn transport na enige milliseconden. Dit principe noemen we 'Carrier Sence Multiple Access/Collision Detect'

(CSMA/CD). Collision Detect betekent zoiets als botsingdetectie. Aangezien dit in enkele milliseconden gebeurt, merkt de gebruiker er niets van. Ethernet heeft als nadeel dat de performance (effektieve snelheid) enorm afneemt naarmate de netwerkbezetting toeneemt. Aan de andere kant is het toch heel snel: in 25,5 milliseconde kan men 32 Kb transporteren. Ethernet is door het Institute of Electrical and Electronic Engineers (IEEE) vastgelegd in stan-

leeg is, kan het station er data op laden. Een volle trein rijdt door. Op het juiste station lost de trein zijn gegevens en neemt mogelijk weer nieuwe data mee. Token Ring heeft het voordeel dat de performance ook bij een grote belasting hoog blijft: de token draait immers op een vaste snelheid rond. Een nadeel is de ingewikkelde en dure kabelstructuur. Token Ring is vastgelegd in de standaard IEEE 802.5.

betrouwbaarheid en een krachtige beveiliging. De prijs is dan ook navenant.

TCP/IP

Bij communicatie via netwerken zijn duidelijke afspraken nodig. Tenslotte moet van elk blokje data vastliggen wie de verzender is en wie de geadresseerde. Het Atari Network System maakt gebruik van TCP/IP (Transmission Control Protocol/Internet Protocol), een internet protocol dat niet afhankelijk is van één fabrikant. Eigenlijk is TCP/IP méér dan een netwerkprotocol, omdat ook de werking van diverse applicaties vastgelegd is (TELNET, FTP, SMTP). Het internet protocol is al heel oud en stamt af van het Amerikaanse defensienet ARPA. De ontwikkelingen begonnen in 1969, maar sinds 1983 is TCP/IP echt als standaard doorgevoerd.

Het internet protocol bestaat uit vier lagen:

- Network-layer: het fysieke netwerk (Ethernet-kabel en netwerkkaart)
- Internet-layer: bevat een aantal protocollen dat zorgdraagt voor een verstaanbare communicatie tussen de computers in één of meerdere netwerken. Een belangrijk aspect daarbij is de adressering van nodes (middels IP nummers).
- Service/Host-layer: De service/host-laag zorgt voor een intelligente communicatie tussen de zender (server) en de ontvanger (client). Begrippen als server en client worden vaak voor meerdere zaken gebruikt. Een server kan de computer zijn die het hele netwerk bestuurt, maar ook een zendproces. Andersom kan een client een gebruiker in het netwerk zijn, maar ook een ontvangstproces. In geval van netwerkaansluitingen kunnen we beter van een 'node' spreken.
- Het gebruik van servers en clients (zend- en ontvangstprocessen) is kenmerkend voor TCP/IP.
- Application-layer: Hierin bevinden zich programma's die zorgen voor de communicatie tussen de gebruiker en het netwerk. Voorbeelden zijn SMTP, DNS, NSP, FTP, TELNET, maar ook drivers voor TOS of Netbios. Door de laatste twee is het mogelijk dat programmeurs programma's maken voor gebruikers en netwerken.

NETWERK TERMINOLOGIE

IP	Internet Protocol; zorgt voor netwerktransacties en biedt functies voor bovenliggende lagen.
ICMP	Internet Control Message Protocol; ICMP heeft als taak de IP-modules te waarschuwen wanneer iets abnormaals gebeurt bij de verzender.
ARP	Address Resolution Protocol; zet een IP adres om in een ethernet adres.
RARP	Reversed Address Resolution Protocol; zet een ethernet adres om in een IP adres.
TCP	Transmission Control Protocol; TCP draagt zorg voor de transmissie van data (beheert de verbinding en controleert de gegevensstroom)
UDP	User Datagram Protocol; UDP is vergelijkbaar met TCP maar heeft minder overhead (controle).
NVP	Network Voice Protocol; protocol voor overdracht van gedigitaliseerd/ gekomprimeerd geluid.
SMTP	Simple Mail Transfer Protocol; biedt mogelijkheden voor het verzenden van post (teksten) tussen gebruikers onderling.
DNS	Domain Service Protocol; DNS is een complexe service die een 'naam' toekent/vertaalt in een IP adres.
NSP	Name Service Protocol; voorloper van DNS; minder complex van opzet.
FTP	File Transfer Protocol; biedt mogelijkheden voor file-uitwisseling tussen computers.
TELNET	Virtueel terminal programma voor interactieve toegang tot een host.
Hoewel niet afgebeeld in het schema (zie rechts) zijn er veel meer toepassingen op de vierde laag zoals:	
TFTP	Trivial File Transfer Protocol; wordt met name gebruikt voor de uitwisseling van data voor printers (spoolers)
NFS	Network File System; netwerk besturingssysteem ontwikkeld door SUN.

daard IEEE 802.3 10Base2 (dun ethernet) en IEEE 802.3 10Base5 (dik). Naast transmissiesnelheid en bekabeling is ook een transfer-protocol vastgelegd. Elke Ethernetkaart heeft een eigen identifikatienummer (adres) dat uit twaalf digits bestaat. Het Amerikaanse bedrijf Xerox beheert deze nummers. Voor één dollar kan een fabrikant van Ethernetkaarten een groep nummers kopen. Atari heeft 00.00.36.02.xx.xx en 00.00.36.04.xx.xx gekocht voor respectievelijk de Megabus en VME netwerkkaarten.

TOKEN RING

Token Ring is door IBM ontwikkeld en heeft een ringvormige topologie. Men maakt gebruik van speciale kabels en aansluitingen. Bij de speciale konnektoren bestaan geen 'mannetje' en 'vrouwje': ze zijn min of meer onzijdig. Dit wil zeggen dat konnektoren van hetzelfde type op elkaar aangesloten kunnen worden. Hoewel het Token Ring netwerk een ringvorm heeft, is het stervormig uitgevoerd doordat zowel de server als de stations aangesloten zijn op een Multi Access Unit (MAU). Deze zorgt er echter voor dat het netwerk een ring blijft (de kabel bezit een aan- en afvoer). Mocht de kabel breken, dan schakelt de MAU dat station uit en maakt de ring weer compleet.

Oorspronkelijk 'draaide' Token Ring op een snelheid van 4 Mhz, maar tegenwoordig is 16 Mhz mogelijk. Het netwerk werkt door middel van een 'token' die het netwerk rondgaat. Een token is te zien als een treintje dat de kring rondrijdt en langs elk station komt. Als de trein

ARCNET

ARCnet is eigenlijk een netwerk dat in STER-vorm werkt, hoewel het in de praktijk vaak een busstructuur heeft. Het werkt op basis van 'token passing' en dus op dezelfde manier als een token ring, ondanks het feit dat het niet ringvormig is. ARCnet werkt op een snelheid van 2,5 Mhz en is dus duidelijk de langzaamste van de drie.

BESTURINGSSYSTEMEN EN PROTOCOLLEN

De topologieën en netwerkkaarten kunnen niets zonder software (protocollen). Ook hier vinden we verschillende mogelijkheden:

PC LAN

Het PC LAN netwerkbesturingssysteem werd door IBM ontwikkeld. Naast data-overdracht ondersteunt PC LAN het gezamenlijk gebruik van randapparatuur en email. PC LAN heeft als voordeel dat het server-programma in de achtergrond (background) kan draaien, zodat de computer ook nog voor andere taken in te zetten is (non-dedicated server). Natuurlijk gaat dit ten koste van de snelheid, maar het houdt de aanschafprijs vooral bij kleine netwerken laag.

Voor grotere netwerken neemt men meestal wel een aparte (dedicated) server.

NOVELL NETWARE

Novell is absolute marktleider voor netwerken met MS-DOS compatibele computers. Het door Novell ontwikkelde netwerkprotocol heet IPX. Novell staat bekend om hoge prestaties, goede

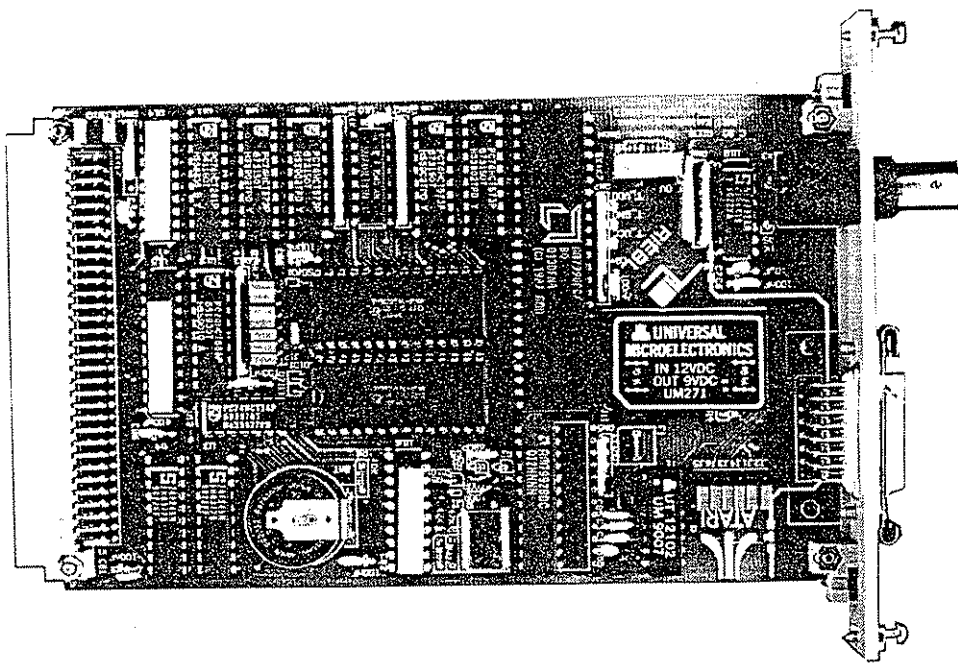
In het schema vindt u de diverse lagen afgebeeld, afgezet tegen het OSI (Open System Intergration) protocol dat uit zeven lagen bestaat. OSI is opgezet door het ISO (International Standards Organisation). Er zijn mensen die verwachten dat de OSI standaard eind jaren negentig TCP/IP zal vervangen.

5-7	SMTP	DNS	NSP	FTP	TELNET
4	TCP	UDP		NVP	
3	IP		ARP		RARP
2	Ethernet	ARPANET	PDN	Others	

X-PROTOCOL

Het X-protocol maakt gebruik van TCP/IP. Het biedt mogelijkheden om de uit- en invoer van een programma op de ene machine te laten plaatsvinden, terwijl het programma feitelijk op de andere machine werkt. Met name onder UNIX wordt dit veel toegepast. Je zou het kunnen zien als een grafische terminal.

ATARI NETWORK SYSTEEM



Het Atari Network Systeem, kortweg ANS, bestaat uit Ethernetkaarten voor zowel de MEGA ST (Megabus) als de MEGA STE en TT computers (VME-bus). Een netwerkkaart ondersteunt zowel dun als dik Ethernet. Middels jumpers kan men instellen welke van de twee soorten Ethernet gewenst is. Bij de VME-kaarten bepaalt men via jumpers of de kaart in een MEGA STE of een TT toegepast wordt. Dit is noodzakelijk in verband met het geheugenadres dat de kaart in gebruik neemt.

Met name de VME-kaarten zijn zeer eenvoudig te installeren: men hoeft zelfs de kast van de computer niet te openen. Kenmerkend voor de Atari netwerkkaarten is dat het Ethernet-adres niet vast in de hardware zit, maar met behulp van software in de chipset geschreven kan worden. Een batterij op de kaart houdt het nummer vast. Hierdoor zijn ontwikkelaars van netwerk-software beter in staat hun programma's te analyseren. De netwerkkaarten zijn voorzien van 64 Kb statisch RAM om netwerkdata te kunnen bufferen.

ANS maakt gebruik van het TCP/IP protocol, waardoor koppeling tussen (Atari) UNIX en de ST/TT mogelijk is. TCP/IP heeft verder het voordeel dat iedereen het als protocol mag gebruiken, terwijl Novell het IPX-protocol alleen voor zeer grote bedragen beschikbaar stelt. Het voor Atari ontwikkelde netwerkbesturingssysteem heet AFS (Atari File Server) en

lijkt sterk op het door SUN ontworpen NFS. Eén van de belangrijkste eigenschappen die AFS biedt, is het principe van de zogenaamde 'remote procedure calls'. Als een client (node) een functie van het besturingssysteem aanroept (call), wordt deze taak op de server uitgevoerd. De applicatie die de call doet, denkt dat de lokale machine hem uitvoert. In werkelijkheid gebeurt dat op afstand. AFS maakt gebruik van de volgende TCP/IP protocollen: IP, ICMP, ARP, RARP, TCP en UDP.

Omdat TCP/IP veelvuldig gebruik maakt van server/client processen (en er dus meerdere processen tegelijkertijd moeten draaien) heeft Atari een multitasking-omgeving voor AFS ontwikkeld. Deze is zo snel dat hij de overige taken van de computer niet hindert.

INSTALLATIE

ANS laat zich redelijk eenvoudig installeren door het programma ANSINS. Bij een eerste installatie moeten alle nodes aanstaan en de

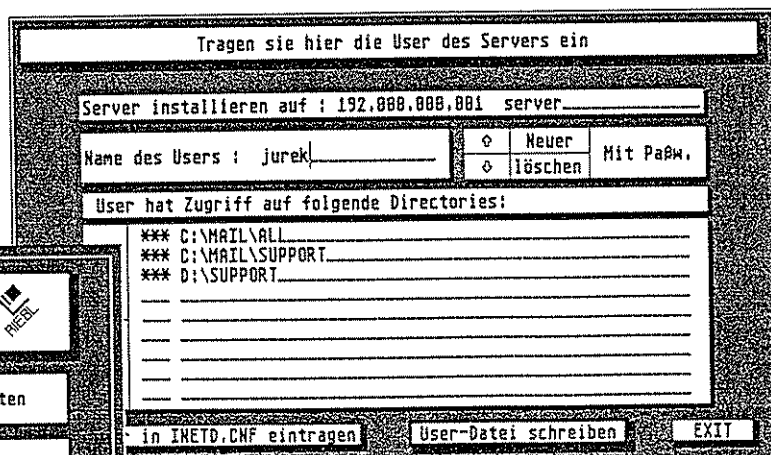
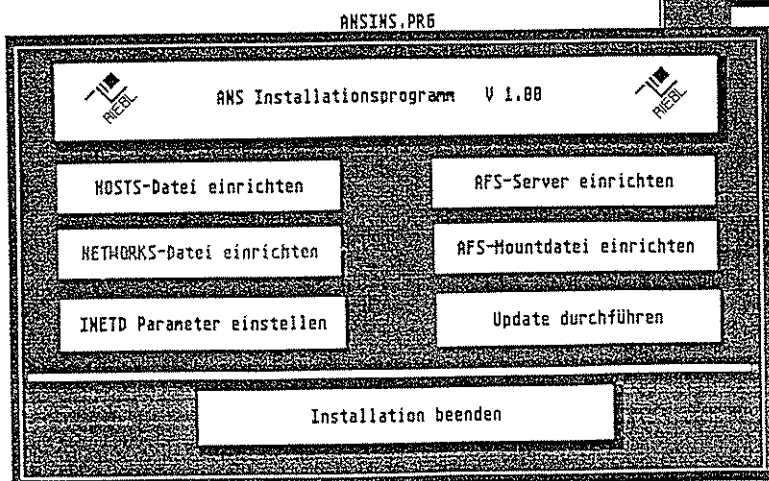
programma's RCPDEV (driver voor kaart) en INSCLIE actief hebben. INSCLIE vraagt eerst naar de naam van de node en leest vervolgens alle configuratiedata van het netwerk, om die op de bootdrive van de node te installeren. Het netwerk stopt na afloop alle INSCLIE programma's. De gebruiker heeft daarna de keuze de besturingsprogramma's in de AUTO-folder te plaatsen of vanuit de desktop te starten.

In een bestaand netwerk kan men volstaan met INSCLIE te draaien op de node die erbij gekomen is. Indien men ANSINS niet op de server-machine draait, maar op een client, kan de installatie van de nieuwe gebruiker zelfs in een draaiend netwerk plaatsvinden.

ANSINS vraagt via het netwerk welke ethernet-adressen (op de netwerkkaarten) aanwezig zijn en welke naam deze machines via INSCLIE gekregen hebben. Op elke node moet de gebruiker een INITD.CNF file aanmaken. Hierin staat welk IP-adres de node gekregen heeft, hoeveel geheugen de node beschikbaar stelt voor de netwerkcommunicatie en of de node extra programma's in de achtergrond wil laten meedraaien (bijvoorbeeld een printerspooler). Bij de volgende stap is het goed opletten. Hier bepaalt men welke machine(s) als server moeten gaan werken en welke toegangsprivileges de afzonderlijke gebruikers hebben. Een computer die aangesloten is op het netwerk krijgt er een paar drive-ikonen bij. In zogenaamde MOUNT-files staat aangegeven naar welke directory van de server deze extra ikonen wijzen. Een mount-file kan er als volgt uitzien:

```
H: C:\MAIL\ALL
I: C:\MAIL\SUPPORT
J: D:\
K: E:\DATABASES\SUPPORT
L: F:\
```

AFS staat toe dat er meerdere servers in het netwerk zijn waar de gebruikers toegang tot hebben. Voor het inloggen (contact leggen met de server) zijn twee programma's beschikbaar: AUTOLOG voor in de AUTO-folder en AFSLOGIN.ACC, een desktop accessoire. AUTOLOG heeft als nadeel dat het systeem van een gebruiker niet wil doorstarten zodra er iets mis is met het netwerk. Men moet AUTOLOG dus uitsluitend gebruiken in combinatie met een BOOT-programma zoals MOBZetup, Superboot en dergelijke. Het forceert in ieder geval dat iedere gebruiker altijd inlogt. AFSLOGIN geeft naast de mogelijkheid tot in-



en uitloggen ook toegang tot het mail-systeem. Hierdoor kan de gebruiker korte berichten naar collega's sturen. Mocht een gebruiker post ontvangen, dan wordt dit via een alertbox op het scherm kenbaar gemaakt. Deze verschijnt overigens niet direct. Het mailsysteem kijkt na een bepaalde tijdseenheid en bij het starten of verlaten van programma's of er post is. De mail

wordt altijd opgeslagen op de harddisk van een server. Mocht de geadresseerde niet aanwezig zijn, dan kan hij later zijn post (mail) lezen. De netwerkbesturingssoftware (AFS) ondersteunt zowel dedicated als non-dedicated servers. In kleine netwerken met een TT als non-dedicated server valt goed te werken. Voor grotere netwerken moet men om redelijke performance te halen een dedicated server nemen. Ook hier is de TT weer uitermate geschikt.

RANDAPPARATUUR

Eén van de voordelen van een netwerk is het gezamenlijk gebruik van randapparatuur zoals printers. Iedere node kan uitdraaipunt worden door een printerspooier in de achtergrond actief te hebben. Via het meegeleverde programma ANSPRINT kan de gebruiker aangeven naar welk station hij wil printen. Voorwaarde is dat het programma dat wil printen gebruik maakt van het Atari Operating System (TOS) en niet

rechtstreek de hardware aanspreekt. Output van Calamus naar de laserprinter laat zich dus niet omleiden. Met de Atari laserprinter komt er nog een ander probleem om de hoek kijken. Deze printer bevriest de ST als hij gaat printen, waardoor de netwerkcommunicatie stil komt te liggen. De netwerkversie van Calamus omzeilt dat door een station als server in te richten die het te printen document zelf uit een vastgestelde directory haalt en in eigen beheer afdrukt.

Wil men met Wordplus op de laser van een andere gebruiker printen, dan kan dat omdat in dat geval de diablo driver op het andere systeem voor de buffering zorgt. Om praktische redenen is het in dat geval het beste om één machine met laser voor dat doel te reserveren, daar een gebruiker het niet leuk zal vinden als het systeem waarop hij werkt telkens bevriest omdat collega's printen. Doordat bij het printen gebruik gemaakt wordt van het TFTP protocol, is het mogelijk dat UNIX of andere TCP/IP machines

op de ST/TT printen of dat de ST/TT op die andere machines afdrukt.

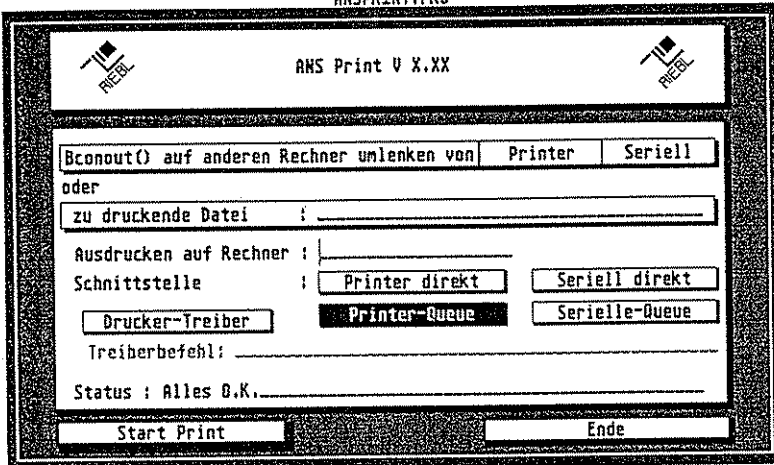
PRIJZEN

ANS bestaat uit een ethernet kaart, AFS software en een handleiding. Een set voor de megabus kost f 1.199,- ex. BTW, een set voor de VME bus f 1.399,- ex. BTW. De software bestaat uit installatieprogrammatuur voor het netwerk, printerspooiers, de netwerk-software (AFS), server programmatuur, login en password utilities en het AFS-login accessoire met het mail systeem.

UITBREIDINGEN

Verderop in het jaar komen de 'Internet tools' (TELNET, FTP, SMTP) en 'ANS advanced mail' (SMTP geïntegreerd in ANS) optioneel beschikbaar. Daarnaast heeft Atari Duitsland X/windows ST aangekocht dat op hetzelfde ethernet board werkt. Dit is X/client software voor de ST, zodat de MEGA ST(E) als X-terminal gebruikt kan worden. Prijzen en release data voor deze uitbreidingen zijn nog niet bekend. Daarnaast zal het Atari File System (AFS) ook onder UNIX beschikbaar komen. Op dit moment is het slechts mogelijk om via de optionele TELNET-software met een UNIX-server te communiceren. Dit is echter niet meer dan een terminal verbinding: het versturen van bestanden moet met behulp van communicatie-software (FTP). Beter zou zijn als de UNIX-machine een drive-ikoon op de desktop is en we daar vanaf kunnen kopiëren. In dat geval is het netwerk transparant voor de gebruiker: hij of zij heeft niet door dat er een netwerk is. Een UNIX-machine kan alleen transparant zijn als er een AFS-server onder UNIX beschikbaar komt. Daar wordt hard aan gewerkt.

ANSPRINT.PRG



• Wilfred Kilwinger

EUROFONDS

EUROFONDS bestaat uit twee programma's: "Download" waarmee u automatisch koersen van aandelen uit externe bestanden kunt laden en "Beurs" waarmee u deze koersen kunt verwerken in talloze grafieken.

EUROFONDS helpt u om de meer dan 20 verschillende grafieken te kunnen interpreteren via een beleggerscursus, die u in staat stelt om op de beurs een zo goed mogelijk resultaat te behalen. Door middel van een handboek met meer dan 130 pagina's en 100 verschillende grafieken worden u een aantal analyse methodes uitgelegd om te komen tot de koop of verkoop van aandelen, niet alleen Nederlandse maar ook buitenlandse aandelen.

Naast de mogelijkheid van externe gegevens bestanden kunt u ook handmatig aandelen invoeren en ook houdt het programma via portefeuille beheer bij wat de waarden van uw beleggingen zijn.

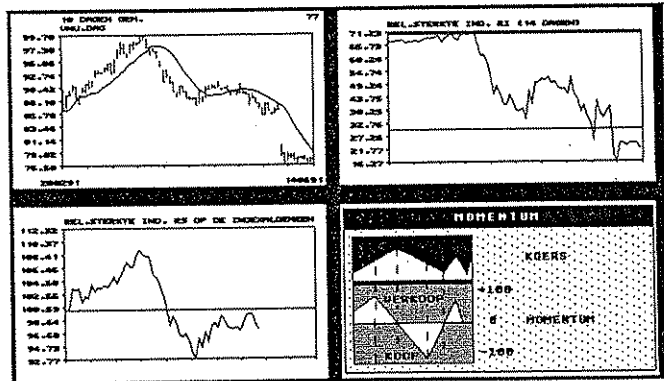
EUROFONDS biedt de mogelijkheid aan geïnteresseerden om zonder daadwerkelijk aandelen te kopen, uw vaardigheden te vergroten. Daarnaast aan beleggers om professioneel gereedschap te hebben voor betere resultaten.

Wat kunt u verwachten?

- Handboek met meer dan 130 pagina's en 100 grafieken
- 2 programma's: Beurs en Download
- Beleggerscursus!!
- 500 koersen om snel te kunnen oefenen
- Uitleg van beide programma's

Een voorbeeld uit het handboek

INFORMATIE BESTANDEN KOERSEN ANALYSE PORTFOLIO MODEM



Welke indicatoren worden o.a. uitgelegd

- Trendlijnen
- Trading bands
- Rel. sterkte (RS)
- Neg. volume indicator
- Pos. volume indicator
- Meer dan 1000 verschillende aandelen
- Tijdreeksen
- Moving Averages
- Oscillators
- Relatieve sterkte (RI)
- Dagelijkse Vol. Indicator
- Momentum
- Fundamentele Analyse
- 7 verschillende Analyses
- 10 Koop/Verkoop adviezen

FL. 149,- Incl. B.T.W.

Hoe kunt u het handboek en de programma's bestellen?

Door overmaking van bovenstaand bedrag op giro 21 72207 t.n.v. EUROSYS, Boomstede 158, 3608 AH Maarssen of door een bank- of girocheque op te sturen, ontvangt u per omgaande het pakket EUROFONDS.

TCP/IP en ISO-lagen (1)

Met deze artikelenreeks over TCP/IP wordt gepoogd dit protocol te toetsen aan de lagen uit het OSI-model.

Daarom wordt ditmaal meer speciaal aandacht besteed aan de data link- en network layers.

We «vergeten» bewust even laag-1, namelijk de physical layer, en gaan dus over naar de tweede laag uit het OSI-model, de data link layer.

NIVEAU 2 - DATA LINK LAYER

Data link types: LAN en WAN

De data link of gegevensverbinding in lokale netwerken die TCP/IP ondersteunen, bestaat uit informatiesegmenten of frames. Gewoonlijk nemen alle op het LAN aangesloten stations kennis van de frames die over de netwerkdrager circuleren.

Aangezien bij de transmissie steeds fouten kunnen voorkomen, worden de gegevens die in deze frames circuleren, beschermd door een «checksum». Deze wordt gegenereerd door de hardware, en dus niet meer berekend door de transmissiesoftware zelf.

Verbinding in wide area networks (het kan dan gaan om netwerken van het type ARPANET, om publieke X.25 netwerken of andere) verloopt enigszins verschillend. In een dergelijke situatie worden de computers aangesloten op apparatuur die zorgt voor een «store-and-forward» verwerking van de uitgezonden gegevenspakketten.

Hieruit blijkt dus dat de verwerking binnen de data link layer in LAN's en WAN's reeds verschillend is. Men zou dus TCP/IP kunnen onderzoeken -en dat gebeurt ook- los van deze laag van niveau-2, en de verwerking beperken tot de hogere niveaus. Om de lezer echter een maximum aan nuttige informatie te bezorgen, volgt hier een korte beschrijving van de data link layer voor wat betreft Ethernet lokale netwerken. Om te beginnen herinneren we eraan dat het vooral Ethernet is, dat gebruik maakt van TCP/IP, en ook dat TCP werd ontwikkeld vóór de Ethernet standaardisering. Daarom werden bijzondere protocollen opgesteld bovenaan in laag-2, om IP te kunnen gebruiken en verwerken. Mocht u het vergeten zijn, dan vermelden we ook nog dat elke laag uit het OSI-model bestaat uit twee sub-lagen: een hogere en een lagere. Ten onrechte gaat men er soms van uit dat elke laag direct met de nabijgelegen laag kan communiceren: alleen de sub-lagen kunnen dat met de onmiddellijk aansluitende sub-laag. Elke dialoog verloopt (uiteeraard) verticaal, naar boven of onder binnen eenzelfde laag, of naar boven en onder over de grens van de laag (n) naar laag (n-1) of (n+1), al naargelang de sub-laag van vertrek hoger of lager ligt dan (n).

De data link layer vormt geen uitzondering op deze regel, en dat gaan we hierna onderzoeken.

De sub-lagen van de data link layer

Deze laag bestaat uit twee delen: de lagere sub-laag heet «Media Access Control» (MAC), de hogere sub-laag is de «Logical Link Control» (LLC).

De MAC sub-laag beheert het gebruik dat de vele aangesloten stations maken van het medium; de LLC laag voert verwerkingen uit die men gewoonlijk associeert met de data link layer, namelijk: adressering en foutencontrole (checksum, CRC, BCC en andere).

Het is ook deze laag -en dat is van groot belang bij lokale netwerken- die het een station mogelijk maakt een N aantal relaties aan te knopen met N andere stations in het netwerk. Men zou in zekere zin kunnen spreken over logische multiplexing van informatie tussen stations. Voor zover nodig, wijzen we er hier nogmaals op dat een lokaal netwerk het best presteert wanneer het erin slaagt een «peer-to-peer communication» tot stand te brengen, dat wil zeggen communicatie tussen twee bepaalde stations die uitsluitend via de

verbindingskabel gebeurt, zonder tussenkomst van apparaten zoals de server of andere elementen uit het LAN.

Data link layer, Ethernet en TCP/IP

Technieken voor het koppelen van Ethernet en TCP/IP bestaan reeds geruime tijd, meer bepaald bij informatie die via de kabel wordt verzonden. Een schema daarvan vindt u in figuur 1.

Zoals u ziet hebben de Ethernet frames een adres van verzending en een van bestemming. Elk van deze gegevens staat in co-devorm in 6 bytes, of 48 bits.

Op 2 bytes vindt men ook een «Type» veld. Hierin wordt het formaat van de via kabel verzonden

niet. Ook andere elementen zijn noodzakelijk, meer bepaald wanneer informatie dient uitgewisseld te worden tussen netwerken, of binnen eenzelfde netwerk voor datatransmissie.

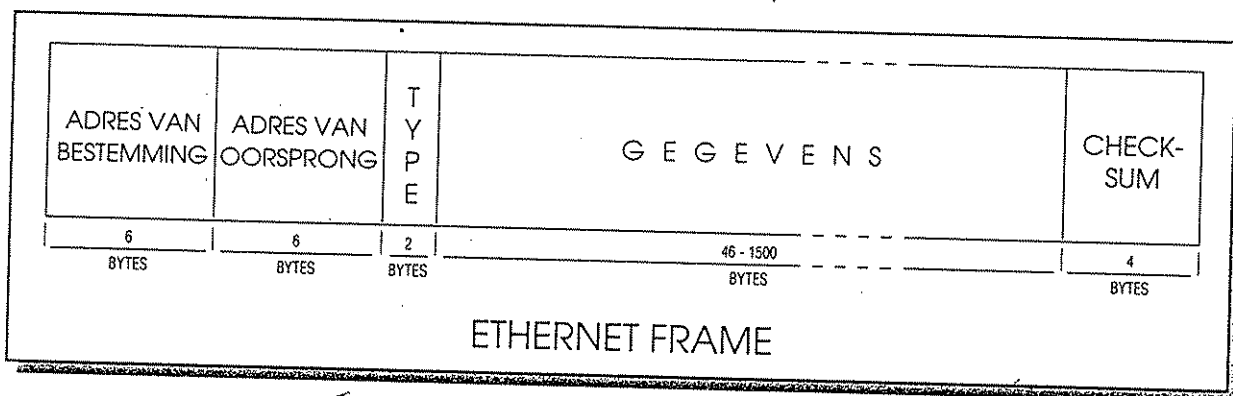
Aanvullende services die in laag-3 worden geboden, maken het mogelijk -naast het leveren van pakketten- adressen te manipuleren en dus verzender en ontvanger te kennen. Een ander element uit laag-3 is de segmentatie en samenvoeging van gegevens.

Deze segmentatie en samenvoeging van gegevens hebben tot doel laag-2 te «misleiden» omtrent de lengte van de frames, zodat men over het netwerk een hoeveelheid gegevens kan versuren die groter is dan wat laag-2 zou toelaten. In die laag-2 is

datatransmissie onderling te koppelen, en er een «internet» van te maken. IP is een element dat services verleent aan een hele reeks ULP's (Upper Layer Protocol, bijvoorbeeld 3270, VIP, VT100,...).

Deze services staan in voor het verkeer van gegevens, die door deze protocollen van hoog niveau (ULP's) via een of meer datagrammen worden gegenereerd. Gaat het om XNS, dan is deze service ook bekend onder de naam Internet Datagram Protocol (of IDP).

IP staat dus in voor een belangrijke basisfunctie, namelijk het afleveren van een datagram (of gegevensblok) doorheen het «internet». IP beschouwt alle via de lijn verzonden bytes als gegevens, dus ook de «dienstmede-



den informatie vastgelegd. Het is deze «Type» informatie die in laag 2 wordt gebruikt om pakketten te scheiden naargelang de laag van bestemming. Zo krijgen bijvoorbeeld alle gegevens met betrekking tot IP de waarde 800H in het veld «Type», en wordt met een waarde 600H bedoeld dat het om het XNS (Xerox Network System) protocol gaat.

NIVEAU 3 - NETWORK LAYER

Voor telecommunicatie volstaan de services van laag-2 natuurlijk

immers een beperking ingebouwd van het aantal via de lijn verzonden bytes, en laag-3 kan dit omzeilen via het procédé van segmentatie/samenvoeging.

Binnen deze netwerklaag functioneren 4 verschillende en vrij belangrijke protocollen. Dat zijn IP, ICMP, ARP en RARP. We laten ze even de revue passeren.

IP, of Internet Protocol

IP is het belangrijkste protocol («statistisch» gesproken) dat we terugvinden binnen laag-3.

De «opdracht» van IP bestaat erin een of meer netwerken voor

delingen» van het ULP dat van IP gebruik maakt. Elk datagram uit dit internet is volledig onafhankelijk, en heeft dus niet de minste relatie met andere datagrammen. De IP-laag (voor zover men van een «laag» kan spreken) biedt services aan de transportlaag (ULP), uitgaande van informatie die verkregen en doorgegeven worden vanuit de data link layer. Zodra men echter het internet concept hanteert, en men de relaties tussen IP en een protocol van hoger niveau bekijkt, duikt een essentieel begrip op. En dat is het gateway of de communicatiepoort.

- IP, ULP en gateway: wie doet wat?

De transmissie begint met een protocol van hoger niveau dat gegevens wil uitwisselen met een ander systeem, door gebruik te maken van de services van IP. IP neemt de te verzenden gegevens in ontvangst (binnen eenzelfde systeem) en ordent die in een handelbare vorm, waarbij het bekende datagram wordt opgebouwd. Dit datagram wordt dan doorgestuurd naar laag-2 voor verzending in het netwerk.

Bevindt het systeem van bestemming zich in hetzelfde netwerk, dan zendt IP dit datagram rechtstreeks door. In het andere geval stuurt IP de informatie naar een -in dit geval- lokaal-gateway. Zodra het lokale gateway de gegevens ontvangt, kan het twee kanten op: ofwel het datagram verzenden naar de betrokken computer, ofwel het datagram doorsturen naar een ander gateway, dat op zijn beurt enz., enz. Deze gateways zijn dus, zoals men kon vermoeden, netwerkelementen die als relais optreden bij de transmissie van datagrammen. Deze relais zijn enkel noodzakelijk voor de verbinding tussen minstens twee netwerken, of sub-netwerken. Elk gateway beschikt over een IP-module waarmee het de IP «dienstmedelingen» herkent die door de verzender werden aangebracht. Deze IP-module bevindt zich uiteraard boven de data link layers, waarvan er minstens twee moeten zijn (men kan immers niet van verschillende netwerken spreken indien het beheer op het niveau van laag-2 vanuit één punt zou geschieden: hier ziet men dan ook duidelijk het verschil tussen een bridge en een gateway, in het kader van LAN's).

De via de lijn verzonden gegevens kan men best vergelijken met passagiers die overstappen tussen twee (N) treinen of vlieg-

tuigen. Het gaat dus om doorvoer. Het beheer van deze gegevensdoorvoer gebeurt via een routing die plaatsvindt binnen de gateways. Deze routing verloopt verschillend naargelang het gaat om lokale of om wide area netwerken, maar het gateway neemt steeds een beslissing op grond van de gegevens in het ontvangen datagram.

Een gateway dat aan twee of meer netwerken is gekoppeld, moet immers uitmaken voor welk netwerk het bericht bestemd is. Daarom bevatten IP-berichten steeds een «header» waarmee (onder meer) het gateway de juiste beslissing kan treffen.

- de IP-header

In figuur 2 wordt de structuur van de IP-header weergegeven. Het zou ons te ver voeren alle velden van deze header in detail te bespreken. We beperken ons daarom tot de meest interessante topics, en vermelden de overige slechts terloops. We hopen dat de lezer hiervoor begrip opbrengt (en de redactie verwittigt, mocht hij of zij toch meer details willen vernemen).

VER: afkorting van Version

Dit veld, gecodeerd in 4 bits, duidt het formaat van de IP-header zelf aan. Dit veld is interessant indien men nieuwere versies van het protocol wil ontwikkelen wanneer het netwerk reeds in gebruik is,

en dit zonder de werking ervan te verstoren.

IHL: afkorting van Internet Header Length

Dit veld, gecodeerd in 4 bits, geeft de lengte van de header aan in eenheden van 32 bits.

TOS: afkorting van Type of Service

Dit veld is gecodeerd in 8 bits, en bevat eigen parameters van IP waarmee de aard van de gevraagde service bij de verwerking van dit datagram wordt aangegeven.

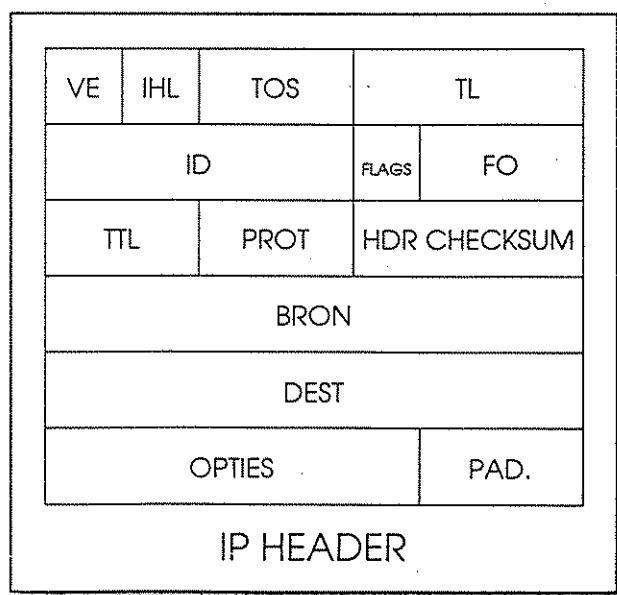
In dit veld kan bijvoorbeeld het prioriteitsniveau van het datagram aangegeven worden, of de resources die ervoor nodig zijn. Het TOS veld heeft alleen een informatieve betekenis. De netwerken waarlangs dit datagram gaat passeren, zijn soms niet -of slechts gedeeltelijk- in staat de gevraagde services te leveren.

TL: afkorting van Total Length

Dit veld van 16 bits geeft de lengte in bytes aan van het datagram, header inbegrepen.

ID: afkorting van Identification

Dit veld van 16 bits wordt gebruikt



in geval van segmentatie van datagrammen. Een protocol van hoog niveau gebruikt ID om aan zijn correspondent te laten weten dat het ontvangen datagram deel uitmaakt van een in ID omschreven informatiepakket.

ments», die respectievelijk de segmentatie verhinderen, of helpen de positie van het segment te bepalen binnen het gehele bericht. Helaas wordt deze segmentatie niet ondersteund op een groot aantal TCP/IP toepassingen.

gegevens binnen het ontvangen segment. Een enkel datagram, of het eerste van een reeks, krijgt een nul in dit vak.

FLAGS: afkorting van... niets
Dit veld, gecodeerd in 3 bits, bevat meer bepaald de commando's «Don't fragment» en «More frag-

FO: afkorting van Fragment Offset
Dit veld, gecodeerd in 13 bits, duidt de positie aan van de

FO definieert de gegevensadressen in veelvoud van 8 bytes. Aangezien 13 bits beschikbaar zijn, bedraagt het maximum aantal 8.192 segmenten per datagram. Deze 8.192 segmenten stemmen overeen met een totale datagram-lengte van 65.536 bytes.



Het stormt behoorlijk aan het modemfront. Nu zelfs met de kracht van een Tornado. De Tornado 2400 bps modemkaart is geschikt voor inbouw in iedere IBM compatibele PC. Volledig Hayes compatible. Eenvoudig te monteren. 300-1200-2400 en 75/1200 baud (Videotex en Minitel France). Natuurlijk zijn ze uitgerust met auto-dial, auto-answer, full- en half duplex, auto fall-back, test modes, audio-monitor voor foutmeldingen, enz. Foutcorrectie en datacompressie (MNP5) in optie. Kompleet met Nederlandstalige handleiding en RTT-aansluitkabel, voor een windstil prijsje. Eén jaar gratis aansluiting op Tornado BBS.

* RTT goedgekeurd, prijs BTW niet inbegrepen.



TORNADO BELGIUM
Molenstraat, 7 3202 Rillaar
Tel.: 016/ 50.04.60
Fax.: 016/ 50.04.59
Tornado BBS: 016/ 44.77.57

Voor Nederland
G&B COMPUTERS
Hoeksteen, 119
2132 MX HOOFFDORP
Tel.: 02503 - 21709
Fax.: 02503 - 21618

TTL: afkorting van Time-To-Live
Dit veld bepaalt de maximale levensduur van een datagram binnen het internet. Bereikt de TTL waarde 0, dan wordt het datagram gewist. Maateenheid is de seconde: voor het doorvoeren van een datagram wordt dus tot 255 seconden voorzien. TTL wordt minstens met 1 verminderd telkens het een gateway passeert.

PROT: afkorting van Protocol
Dit veld duidt in 8 bits aan voor welk ULP de uitgezonden gegevens bestemd zijn.

Header Checksum: bevat de checksum voor de header alleen.

SOURCE: afkorting van Source Address
Dit veld van 32 bits bevat het internet-adres van het systeem dat het datagram verzendt.

DEST: afkorting van Destination Address
Dit veld van 32 bits bevat het adres van het ontvangende systeem. Het gedeelte «netwerkidentificatie» beslaat 8 à 24 bits, en de rest is voor het apparaat van bestemming binnen dit netwerk.

OPT: afkorting van Options
Dit veld (onbepaalde lengte) dient vooral voor het uitvoeren van tests zonder dat een nieuwe header moet gedefinieerd worden.

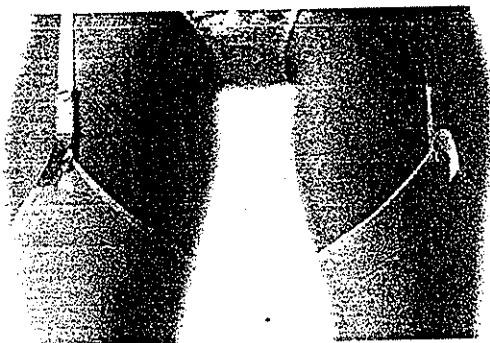
- IP en netwerk-adressering
Een van de uitdrukkelijke doeltellingen van IP is services te verlenen aan de meest uiteenlopende categorieën netwerken, en tevens aan omgevingen met meerdere netwerken. Om dit te bereiken werden de adressering-smechanismen zodanig bepaald dat IP zich kan aanpassen (of

aangepast worden?) aan drie verschillende groepen configuraties. Bij elk van deze drie groepen, zeer poëtisch A, B en C genoemd, hoort een type adressering.

Groep A met bijbehorende adressering stemt overeen met: vele systemen binnen weinig netwerken.

Groep B met bijbehorende adressering stemt overeen met: een normale distributie van netwerken en systemen (met normaal wordt hier telkens een «normaal aantal» bedoeld).

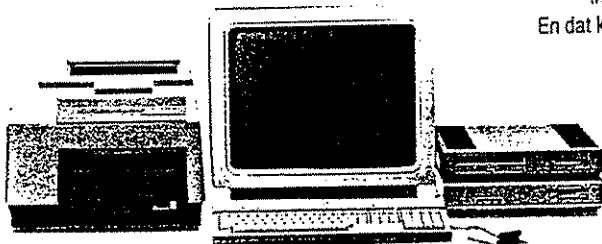
Groep C met bijbehorende adressering stemt overeen met het omgekeerde van A, met andere woorden weinig systemen in een



ATARI DTP LAAT U HET HELE BEELD ZIEN.

We hoeven u niet meer uit te leggen wat het verschil is tussen knippen en kleven en Desk Top Publishing. Maar misschien is het wel nuttig dat we u wijzen op het Desk Top Publishing-systeem van ATARI.

In tegenstelling tot de meeste concurrenten laat ATARI namelijk vooraf het totale beeld zien dat geprint gaat worden. Dat is nogal bijzonder.



Mega ST 4: 68000 processor, 4 Mb RAM, 3,5" disk drive - Megafille 30: 30 Mb hard disk - Megafille 44: 44 Mb verwisselbare hard disk - Megafille 60: 60 Mb hard disk - Laserprinter SLM 804: halfgeleiderlaser, 8 x A4 per minuut, 300 dpi - Monitor SM 194: 19", ontspiegeld.

Het beeld op de monitor is namelijk scherp gedetailleerd en vooral volledig op het scherm te brengen. Dit komt omdat ons DTP-systeem van vectoriële beeldopbouw gebruik maakt.

Wij noemen dit systeem: What You See Is What You Get. Hoe handig dat is, merkt u vooral als u vooraf niet weet waar u met de lay-out naartoe wil.

Daarnaast blijkt de befaamde ATARI-muis een onnavolgbare manipulator op het gebied van speciale effecten, typografie, tekstredactie en beeldvorming.

Het geheim van ATARI (dat mag iedereen weten) is een snelle 68000 microprocessor (8 MHz) die wordt ondersteund door een stel vernuftige chips. Eén ervan is bijvoorbeeld een zogenaamde "Blitter Chip" die voor een razendsnelle beeldopbouw zorgt.

Verder is dit ATARI DTP-systeem, Calamus genoemd, zeer gebruiksvriendelijk. De menu's op het scherm zijn overzichtelijk en de symbolen gemakkelijk te begrijpen.

Maar de grootste verrassing is van financiële aard, want met ons DTP-systeem kunt u een Linotronic 300 belichter aansturen zonder dat u zich zo'n peperdure Raster Image processor hoeft aan te schaffen. In plaats daarvan werkt hij met een extra interface. Het resultaat is hetzelfde, en het bespaart u het bedrag van een knappe middenklasser bolide. Ook kunt u een "gewone" ATARI-laserprinter aansluiten op deze Desk Top Publisher van ATARI.

Beide garanderen printwerk van sublieme kwaliteit.

Wilt u de Desk Top Publisher van ATARI aan het werk zien, dan kunt u het beste één van de demonstratiecentra bezoeken. Voor meer informatie mag u ons ook bellen.

Tenslotte bent u zeker geïnteresseerd in de prijs. Welnu, het ATARI DTP-systeem is al verkrijgbaar vanaf zo'n 180.000,- Bfr.

In alle gevallen ziet u gegarandeerd het hele beeld. En dat kan u van deze advertentie niet zeggen ...

ATARI
WE MAKE TECHNOLOGY EXCITING.

Voor meer informatie, bel ATARI:
03-326.34.62
Industriezone, Vosveld 17, 2110 Wijnegem

(zeer) groot aantal netwerken. Zoals hierboven uiteengezet, worden de adressen gecodeerd over 32 bits, waarin de identificatie voorkomt van zowel netwerk als apparaat van bestemming.

Een internet bestaande uit een klein aantal netwerken heeft een geringer aantal bits nodig om het netwerk van bestemming aan te duiden. Voor Groep C, waar het aantal netwerken het hoogst is, zullen echter meer bits nodig zijn. De regel is dat bits die het netwerk-adres aangeven, het meeste gewicht krijgen.

Zo zal voor Groep A (7 bits netwerk-adres, 24 voor adres binnen het netwerk) het IP-adres beginnen met de bits 0XX; voor Groep B (14 bits netwerk, 16 voor systeem-adres) begint dit adres met 10X; en voor Groep C (21 bits netwerk en 8 bits systemen), begint het met 110.

Binnen een netwerk kunnen systemen «gegroepeerd» worden in afzonderlijk benoemde «sub-netwerken». In de 32 bits structuur van de adressering door IP binnen een netwerk wordt hiermee rekening gehouden. Men kan inderdaad sommige van deze 32 bits maskeren, en dit kan dienen als identificatie van het sub-netwerk.

Een voorbeeld?

Laten we ons even een bedrijf voorstellen, of een universitaire campus, of (waarom niet?) een aantal parlementairen, aangesloten op een netwerk. Dit netwerk zou van het type B zijn, wat grosso modo neerkomt op 2 bytes voor het netwerkgedeelte, en 2 bytes voor het «intelligent» (elektronisch, wel te verstaan!) gedeelte.

Hiermee kunnen we dus 65.536 adressen van intelligente units opgeven. Voor de parlementairen van sommige landen kan dit misschien wat weinig lijken, maar voor bedrijven waar hoe dan ook de kostenfactor doorweegt, is het

beslist meer dan genoeg. Wat de campus betreft...

In plaats van dus 65.536 verschillende adressen op te stellen, zou men evengoed de 2 bytes voor intelligente units kunnen splitsen in 2 sub-velden: het eerste voor het sub-netwerk en het tweede voor het eigenlijke systeemadres.

In die hypothese zouden dan 254 sub-netwerken en 254 systeemadressen aangesloten zijn.

Een IP-adres wordt vaak gevormd door 4 velden, gescheiden door een punt: elk veld bestaat uit een byte, en kan een waarde aannemen van 0 tot 255.

Zo bedragen de initiële waarden naargelang de Groepen:

Initiële waarde	Groep
000 - 127	A
128 - 191	B
192 - 223	C
224 - 255	D

(Opmerking: momenteel wordt aan een vierde groep D gedacht, maar die wordt nog niet gebruikt. Voor deze Groep D is de configuratie van de eerste bits in het IP-adres 111)

Daaruit kan men afleiden dat een adres 11.1.12.1 overeenstemt met een adres van type A, dat een adres 129.203.35.18 overeenstemt met Groep B, en een adres 192.1.2.3 met Groep C.

ICMP of Internetwork Control Message Protocol

Het ICMP protocol wordt op grote schaal toegepast bij datatransmissie. De belangrijkste taak van ICMP is de IP-modules te waarschuwen wanneer «iets» abnormaals gebeurt bij de verzender. Dit abnormale karakter wordt doorgaans vastgesteld wanneer de informatie vanuit de verzen-

der niet overeenstemt met hetgeen men verwachtte.

Dit afwijkend gedrag kan om het even waar en door gelijk welk element vastgesteld worden: doel-computer of gewoon het gateway. Deze fouten worden dan doorgegeven aan het ICMP, dat daarop de nodige schikkingen treft om de verzender ervan te verwittigen dat een element in de datatransmissie (verzender zelf, het netwerk, de toegangspoort, enz.) het laat afweten.

Officieel maakt ICMP deel uit van IP. De datagrammen die door ICMP worden uitgezonden, passeren inderdaad via IP. Toch geniet ICMP een bijzonder statuut, aangezien het tegelijk een protocol is van laag-3 en van laag-4.

ARP of Address Resolution Protocol

Aan het begin van dit artikel werd gesteld dat vooral Ethernet gebruik maakt van TCP/IP. Daarnaast hebben we bij het onderzoek van de IP-header gezien dat 32 bits beschikbaar waren voor adressering.

Helaas beslaat de adressering in Ethernet 48 bits... enkel voor de identificatie van het Ethernet adres van bestemming, of dat van het volgende gateway.

Uiteraard is het volstrekt onmogelijk te «doen alsof» 32 = 48 zou kloppen. Men kan evenmin links en rechts bits «opraperen» om een waarde 48 te bereiken, en men kan er ook geen «bijmaken».

Bijgevolg moet worden ingegrepen op het niveau van de network layer om te zorgen voor het «samenvallen» van het standaard IP-adres en het normale Ethernet-adres. Met dat doel werd ARP ontwikkeld.

Toch liggen de zaken niet zo simpel. Vooral niet in een omgeving met meerdere netwerken. De kans is groot dat op een

gegeven ogenblik een systeem A het Ethernet station XYZ wil bereiken, maar de waarde XYZ zelfs niet kent. En dan arriveert er op het XYZ-netwerk een pakket waarvan het IP-adres is opgegeven, maar niet het Ethernet-adres. Met als gevolg...

Dit nu, is een opdracht voor de ARP functie.

In deze situatie gaat het netwerk aan «broadcasting» doen, om uit geloofwaardige bron binnen het netwerk het betrokken Ethernet-adres te vernemen. Deze broadcast is bestemd voor de ARP servers in het netwerk.

Loopt het antwoord binnen, dan worden de 48 bits van het Ethernet-adres in tabellen in het geheugen opgeslagen, zodat geen

nieuwe ARP bewerking nodig is wanneer een volgend bericht met hetzelfde IP-adres verzonden wordt. Niettemin kan het gebruik van ARP definitief uitgeschakeld worden, indien de tabellen met de relaties tussen IP- en Ethernet-adressen tot de configuratie behoren, en van bij de start beschikbaar zijn.

RARP of Reverse Address Resolution Protocol

Laten we nu het probleem van ARP eens in omgekeerde richting bekijken: een station zou bijvoorbeeld enkel zijn eigen Ethernet-adres kennen, hoewel het aangesloten is op een net-

werk waar IP de scepter zwaait. In dat geval gaat het Ethernet-station een beroep doen op de functionaliteiten van RARP door op het netwerk een «Wie ben ik?» bericht te sturen, met andere woorden: «Welk is mijn IP-adres?»

Evenals bij ARP wordt ook dit adres slechts één keer naar het vragende station doorgestuurd.

Tot besluit dient erop gewezen dat in elk Ethernet segment een RARP server noodzakelijk is.

Volgende maand komt de transport layer van TCP/IP aan de beurt, en indien het volume niet te hoog oploopt, ook de hogere lagen.

Pierre Ausloos,
Consultant.

A G E N D A

Van 15 tot 20 oktober 90
Inter/Elec'90 te Gent
Inlicht.: tel. 02/217 28 75

Van 22 tot 26 oktober 90
Systemec 90 te München
Inlicht.: tel. (89)5107-275

Van 24 tot 27 oktober 90
Data Show te Tokyo
Inlicht.: tel. (81)3-4334547

Van 24 tot 27 oktober 90
Laser-Asia'90 te Singapor
Inlicht.: Münchener Messe. Tel. (089)51 07-0

Van 25 tot 30 oktober 90
Orgatec 1990 te Keulen
Inlicht.: (0221)821-0

Van 30 oktober tot 1er november 90
Electronic Data Interchange te Londen
Inlicht.: Blenheim Exh. Tel. (44)625 879965

Van 5 tot 9 november 90
Int. Council for Comp. Communication te New Delhi
Inlicht.: tel. 6830087 - 6840052

Van 6 tot 8 november 90
EDI 90 te Parijs
Inlicht.: Blenheim Exh. Tel. (331)47 56 50 00

Van 6 tot 8 november 90
Computer Graphics te Londen
Inlicht.: Blenheim Exh. Tel. (44)625 879965

Van 6 tot 8 november 90
Desktop CAD te Londen
Inlicht.: Blenheim Exh. Tel. (44)625 879965

Van 6 tot 8 november 1990
Scan-Tech Europe'90 te Frankfurt
Inlicht.: tel. (44)422 359161

Van 7 tot 9 november 90
Open Systems te Londen
Inlicht.: tel. (44)1-4044844

Van 12 tot 16 november 90
Comdex Fall te Las Vegas
Inlicht.: tel. (1)617-4496600

Van 13 tot 15 november 90
Electronic Displays '90 te Londen
Inlicht.: Blenheim Exh. Tel. (44)625 879965

Van 13 tot 15 november 90
Computers in the city te Londen
Inlicht.: Blenheim Exh. Tel. (44)625 879965

Van 12 tot 16 november 1990
Comdex/Fall'90 te Las Vegas
Inlicht.: tel. (617)449-6600

INTERNETWERK-COMMUNICATIE

TCP/IP en de OSI-lagen (2)

In aansluiting op het artikel van vorige maand zetten we ons onderzoek van TCP/IP voort en daarbij behandelen we met name laag 4 van het OSI-model, de zogenoemde transportlaag.

In het communicatieproces, zowel tussen machines als tussen mensen, kunnen twee lagen worden onderscheiden: de eerste laag is die van de "verstaanbare communicatie", een tweede laag, die voortvloeit uit de eerste, is de "intelligente communicatie". Ook de lagen van het OSI-model maken geen uitzondering op deze regel.

De lagere lagen, die we vorige maand behandelden, zorgen voor een verstaanbare dialoog tussen twee machines in één of meerdere netwerken. De transportlaag brengt de intelligentie in de communicatie. Ze brengt een relatie tot stand tussen het zender-proces binnen machine X en een ontvangst-proces binnen machine Y.

Het mag dus duidelijk zijn dat eens de barrière van laag 4 is overschreden, de communicatie ook werkelijk is gelegd en dat de rest alleen nog maar een kwestie is van interne verwerking van de ontvangen informatie in de ontvangende machine.

Het is eveneens ter hoogte van de transportlaag dat er sprake is van een begrip waarvan gebruik wordt gemaakt in de X.25-netwerken: de **virtuele circuits**. Het virtuele circuit is een zuiver abstract begrip dat ervoor zorgt de diverse pakketten samen te nemen, waarbij dan gedaan wordt alsof deze pakketten via één

verbinding - een punt-tot-punt verbinding of een vaste lijn -transiteren.

Deze pseudo-vaste lijn moet gezien worden als een dienst die de dialogerende systemen wordt bewezen; deze dienst wordt geleverd door het **transportprotocol**. Dat zorgt voor het leveren van de informatie, verzorgt de transmissie (en de eventuele hertransmissie) van pakketten over de lijn en beheert deze pakketten. Er moet namelijk op toegezien worden dat pakket 2 niet na pakket 3 aankomt en verder mag een pakket evenmin twee of drie maal verzonden worden.

TCP/IP en de transportlaag

We hadden het net over het bestaan van een **transportprotocol** en ook TCP/IP maakt daar gebruik van.

TCP/IP* beschikt in laag 4 over twee protocollen:

- **TCP** of Transmission Control Protocol;
- **UDP** of User Datagram Protocol.

Het UDP zullen we hier niet behandelen, evenmin als de andere mogelijke protocollen die bijvoorbeeld worden ingezet voor de digitale stemtransmissie.

* De belangstellende lezer willen wijzen op het feit (en zonder dat dit als reclame moet worden opgevat) dat het High-Tech Institute van Telindus/Telinfo grondige cursussen organiseert over TCP/IP.

Het Transmission Control Protocol of TCP

Het TCP werd ontwikkeld om zich te kunnen aanpassen aan een groot aantal netwerken van diverse types en niettemin een betrouwbaar interface voor de gegevens van de gebruiker te blijven.

Vanwege die veiligheid zit het protocol relatief complex in mekaar. Dat kon ook niet anders: TCP moet namelijk blijf geven van een groot aanpassingsvermogen omdat het bestemd is voor de meest diverse omgevingen en de meest heterogene machines. TCP werd ontworpen om te worden uitgevoerd boven het IP, boven de netwerklaag dus en bijgevolg moet het de verbindingen tussen de netwerken kunnen ondersteunen.

TCP ondersteunt een aantal protocollen van een hogerniveau, de zogenoemde **ULP's** (Upper Level Protocols). Deze ULP's worden door de toepassingen gedwongen berichten uit te zenden naar een bepaald systeem binnen het netwerk.

Om een zo groot mogelijk aantal ULP's te kunnen beheren zal het TCP zich niet veeleisend tonen: de ULP's wordt niets opgelegd en de berichten kunnen in welke vorm of structuur ook worden doorgezonden.

Om dit resultaat te bereiken mag het TCP zich in geen geval bezighouden met de inhoud noch met

de betekenis van deze berichten. De gegevens die worden verzonden door een ULP worden door het TCP beschouwd als een reeks bits. TCP laat de zorg voor de structuur en/of het formaat van de gegevens die over zijn lijnen worden doorgestuurd dus over aan het hogere protocol. Het TCP van machine A moet echter begrepen worden door de tegenhanger van machine B. Daarom zal het TCP de gegevensstroom afkomstig van het zend-ULP discreet fragmenteren. Deze gegevensfragmenten worden **segmenten** genoemd: de gegevens worden immers gesegmenteerd.

TCP en X.25

Tot nu toe week onze beschrijving niet af van wat er zich in een X.25-netwerk afspeelt, zelfs het gehanteerde jargon is hetzelfde. Maar vanaf nu komt daar verandering in.

Want het X.25-protocol werd immers niet ontworpen om **netwerkonafhankelijk** te zijn. Iedereen weet dat een X.25-protocol dient voor een X.25-netwerk.

Dat geldt niet voor TCP.

Terwijl de X.25-norm (in zekere mate) de omvang van de pakketten zal bepalen, zal TCP daarentegen werken met een onbepaalde omvang. TCP kan pakketten aan met een omvang tot 65 KB. Het zend-TCP kan gegevens van welke lengte ook verzenden, op voorwaarde althans dat die lengte niet groter is dan de netvernoemde grens van 65 KB. Dat is natuurlijk theorie. Want de 65 KB in kwestie zal gefragmenteerd worden in overeenstemming met de specificaties van het netwerk waarop het systeem, waarin dan TCP wordt uitgevoerd, is aangesloten. We stellen dus vast (we vergeten de theorie even) dat in de praktijk de omvang van de door het netwerk verzonden informatie exact zal overeenstem-

men met de omvang die het netwerk eist.

Segmentnummering

Om bij een fout te kunnen optreden gaat TCP als volgt te werk: de gegevens uit de ILP's worden altijd beschouwd als een onafgebroken gegevensstroom. Voor het TCP ziet deze stroom eruit als een oneindig aantal gegevens.

Wanneer deze gegevens het TCP bereiken, krijgen ze van het protocol een soort reeksnummer of een 'offset'; dit reeksnummer zorgt ervoor dat exact de gewenste byte in de oneindige gegevensstroom die door het TCP wordt beheerd wordt opgehaald. Wanneer de informatie in de vorm van segmenten wordt uitgewisseld, nummert TCP het segment. Deze nummering gebeurt op een speciale manier, in die zin dat het segmentnummer gelijk is aan het reeksnummer van het eerste gegeven dat dit segment bevat. Naast dit segment/reeksnummer geeft TCP ook het aantal bytes aan in het segment.

Compressie van segmenten

Met deze twee service-gegevens kan het TCP de over de lijn verzonden segmenten dynamisch beheren en onverwachte prestaties leveren. Zo kan het bij foutdetectie twee segmenten samenvoegen tot een groter segment. Op het eerste gezicht lijkt deze techniek van segmentcompressie geen zin te hebben, het lijkt wel of men het gewoon moeilijker wil maken, maar dat is niet het geval. In lange-afstandsnetwerken zal het verzenden van informatie met een lengte 2.n. duidelijk minder tijd in beslag nemen dan twee transmissies van gegevens met een lengte van 1.n. Dat heeft te maken met het modembeheer, nl. met het wachten op de nodige signalen (Request to Send/Clear to Send). Bij

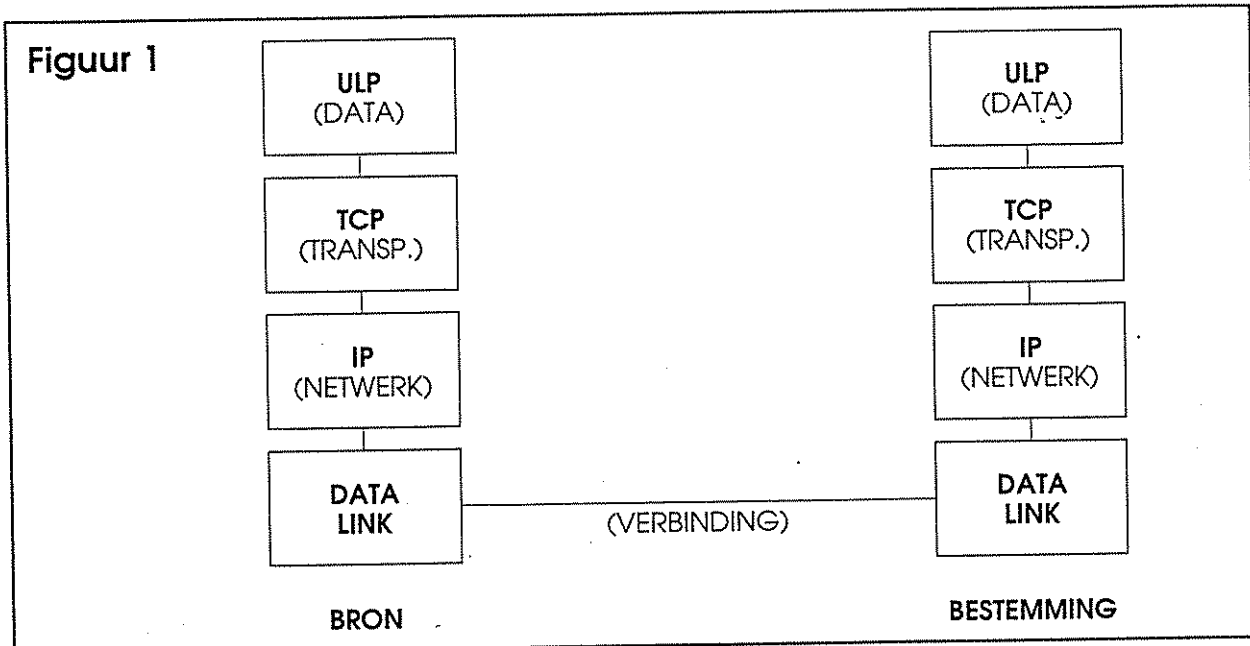
twee transmissies moet twee keer op de signalen worden gewacht, terwijl men bij de verzending van één informatiereeks die twee keer zo lang is natuurlijk maar 1 maal op de signalen moet wachten. De bedoeling van zo'n compressie is dus het lijnbeheer zo efficiënt mogelijk maken.

Vanwege deze techniek is TCP eigenlijk een veel complexer protocol dan de meeste andere transportprotocollen. Want er kunnen zich twee situaties voordoen:

- ofwel bevat het dubbele segment al segmenten die de correspondent al onder ogen kreeg;
- ofwel bevat het dubbele segment al gegevens die de correspondent al eens heeft ontvangen, maar ook nieuwe gegevens. Het beheer van deze twee gevallen is dan ook totaal verschillend bij ontvangst van het dubbele segment.

Schema illustreert het volledige transmissieproces tussen twee systemen: vanaf het ULP dat verzendt tot de ULP-bestemming.

- 1. De zend-ULP stuurt de gegevens naar de transportlaag om door het TCP verwerkt te worden.
- 2. Het TCP fragmenteert de gegevensstroom van de ULP in segmenten. De transmissie kan al dan niet in full duplex geschieden en TCP houdt onder meer rekening met de volgende communicatie-aspecten:
 - hertransmissies beheerd door de klok: wanneer die worden verwacht en de time-out bereikt is, zal het TCP het ULP melden dat er een probleem is. Het ULP kan dan de nodige maatregelen nemen;
 - ordenen van de gegevens (pakket 1 wordt verwerkt voor pakket 2);
 - prioriteit en veiligheid van de verzonden gegevens. TCP verleent het ULP en de berichten die



Compleet datatransmissieproces tussen twee systemen en van een bron-ULP naar een bestemming-ULP

het verzendt een veiligheids- en prioriteitsniveau. Deze niveaus worden in principe bepaald bij het tot stand brengen van de verbinding door het ULP. Het komt ook voor dat het ULP niets meldt aan het TCP; TCP zal dan bij-verstek prioriteits- en veiligheidsniveaus definiëren.

Bij de gegevensuitwisseling eist TCP dat de waarden van de prioriteits- en veiligheidsinformatie dezelfde zijn bij verzending en ontvangst. Mocht dat niet het geval zijn, dan zal verklaard worden dat er een probleem is bij de verbinding en wordt de lijn verlaten;

- controle van de gegevensstroom: het regelen van de gegevensstroom doorheen het netwerk om te voorkomen dat ze vast raakt en dat de service aan het ULP (en ook aan de gebruikers...) niet behoorlijk is;
- foutenbeheer, zowel bij het verzenden (berekening van de checksum) als bij de ontvangst (berekening en controle na transit doorheen het netwerk).

Na deze verwerkingen geeft TCP

de segmenten door aan de hogere laag, het IP;

- 3. IP voert de transmissieverwerking daadwerkelijk uit: het verzendt de gegevens doorheen de lagen 2 en 1 en doorheen het hele netwerk naar het IP dat bestemming is;
- 4. Dit bestemming-IP voert de nodige controleverrichtingen uit. Het reconstrueert de gegevens die door het bestemming-TCP in verstaanbare segmenten zijn ontvangen en geeft ze door aan het TCP;
- 5. Het bestemming-TCP voert het werk van de oorspronkelijke TCP in omgekeerde zin uit vooraleer de gereconstrueerde gegevens aan de ULP's door te geven.

De aanhef van het TCP

Net zoals het IP bezit het TCP ook service-gegevens die samengebracht zijn in een aanhef of 'header'. In schema 2 staat afgebeeld hoe dat in zijn werk gaat.

- Source Port, afgekort **SRC PORT**

Deze zone wijst op een adres aan de verzenderszijde, dat van een **service** of van een **proces** kan zijn. Men mag dit adres niet verwarren met de SOURCE en DEST gegevens van de IP-aanhef die direct te maken hebben met het netwerk.

Uit de combinatie van elementen (netwerkadres + procesadres) kan worden afgeleid wie zich tot wie richt (het who's who van het TCP/IP in zekere zin).

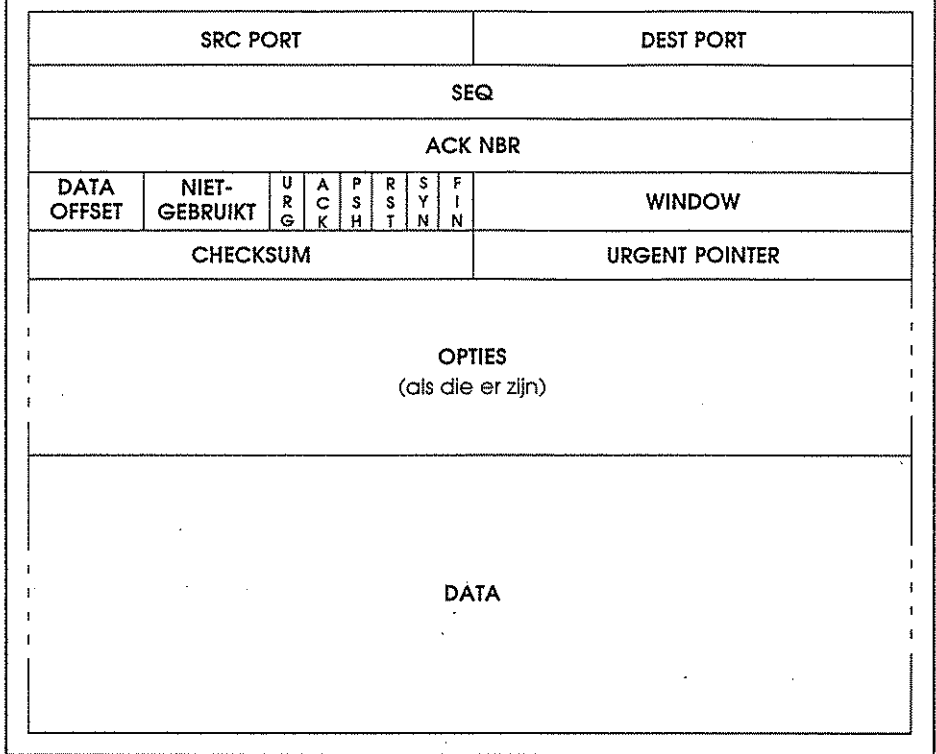
Met deze beide gegevens kan men een **socket** definiëren. Sockets zijn technieken die men onder meer onder het Unix van Berkeley hanteert om een enig toegangspunt binnen een proces te bepalen.

- Destination Port of DEST PORT

Deze zone is te vergelijken met SRC PORT maar dan wel aan de ontvangtzijde. Op te merken valt dat de SRC en DEST PORT's onder de controle staan van elk van beide systemen en dat deze hen waarden kunnen toewijzen.

- Sequence Number of **SEQ**
Dit gebied, gecodeerd over 32

Figure 2 - HEADER TCP



SYN: wordt gebruikt om de verbinding tot stand te brengen wanneer hij een waarde 1 heeft;
 ACK: wanneer ACK=1 dan betekent dit dat het ACK-veld een bepaalde betekenis heeft;
 RST: bij RST=1 moet de verbinding worden opgegeven, en dit om diverse redenen. Die redenen hebben niet altijd te maken met de telecommunicatie zelf, het kan ook gaan om een probleem in een van de partnersystemen;
 PSH: wanneer flag PSH=1 informeert deze waarde het partner-TCP dat de gegevens van dit segment onmiddellijk naar het betrokken ULP kunnen worden verstuurd. Doorgaans wordt deze PSH-functie (PUSH) gebruikt om het einde van de verzending aan te geven: bijkomende gegevens moeten dan niet meer verwacht worden voor een bepaalde tijd;
 FIN: wanneer FIN=1 informeert de verzender de ontvanger dat er geen gegevens naar het ULP moeten verstuurd worden.

bits, kan een waarde opleveren gelijk aan $2^{*32} - 1$. Deze waarde is het sequentienummer van de eerste 'bruikbare' byte in een segment: we zeggen "bruikbaar" want de synchronisatietekens (SYN) worden niet in aanmerking genomen.
 De 32 bits zijn nodig uit overwegingen die te maken hebben met de lengte van de berichten en de veiligheid.
 Wat de **lengte van de berichten** betreft, heeft men uitgerekend dat wanneer om de seconde een bericht van 1.000 bytes wordt verzonden, men 50 dagen lang zou kunnen verzenden om de maximale SEQ-waarde te bereiken. Deze 32 bits zijn ook een uiting van de **voorzichtigheid** van de ontwerpers van TCP/IP. Met zo'n groot aantal is het namelijk bijna onmogelijk dat een pakket dat wat tijd verloren heeft op het netwerk bij het tot bestemming komen beschouwd wordt als het verzonden pakket.

- Acknowledgement Number of ACK
 Als de ACK Control Bit op waarde 1 staat, bevat dit gebied de waarde van het volgende sequentienummer dat de verzender verwacht.

- Data Offset
 Dit gebied geeft het aantal 32 bitwoorden in de TCP-header; uit deze waarde kan worden afgeleid wanneer de eigenlijke gegevens beginnen. Deze informatie is vereist omdat het "opties"-veld van variabele lengte is.

- Flags
 Er zijn 6 controle-flags die de verbinding helpen leggen, behouden en voltooien. Deze flags zijn:
 URG: wanneer URG=1 dan betekent dit dat het veld "Urgentie Wijzer - URGPTR" gebruikt moet worden, omdat het bericht gegevens met een hoge prioriteit transporteert. Dit is tevens een onderbrekingspakket;

- Window, afgekort WNDW
 Deze waarde, gebruikt voor de controles van de gegevensstromen, staat voor het aantal bytes (die van ACK inbegrepen) dat de verzender zal aanvaarden bij antwoord van de ontvanger.

- Checksum
 Hiermee kan een eventuele fout in de header en de gegevens worden opgespoord. Wordt gevormd door het complement van 1 van de som van de complementen van 1 van de 16 bitwoorden van het bericht.

- Urgent Pointer of **URGPTR**
Dit veld verwijst naar de laatste byte van het dringende gegeven dat in het bericht zit.

- Opties of **OPT**
De opties bevinden zich in de staart van de TCP-header. Ze worden begrepen in de berekening van de checksum en kunnen op welke grens van een byte een aanvang nemen. De meest gebruikte optie is die bij het tot stand brengen van de communicatie en ze geeft de maximale omvang van een segment aan.

De TCP-functies

De functies zijn de volgende:

- functies voor het beheer van de verbinding;
- ontvangstberichten;
- controle van de gegevensstroom;
- multiplexing;
- synchronisatie;
- techniek van de afspraak.
- Beheer van de verbinding

Het beheer van de verbinding door TCP heeft te maken met het paar ULP's die met elkaar in communicatie moeten treden. Die verbinding kan worden bekeken vanuit drie aspecten:

- het leggen van de communicatie;
- het behoud van de communicatie;
- het afbreken van de communicatie.

We houden ons nu alleen bezig

met het leggen en het behoud van de communicatie tussen twee ULP's. Een verbinding wordt gedefinieerd door de combinatie van de twee sockets van de participanten en TCP legt de verbinding als volgt:

- * een verbinding kan worden gelegd als beide sockets al bestaan;
- * de interne TCP-resources moeten toereikend zijn;
- * de ULP's hebben tegelijk twee OPEN's uitgevoerd. Het ene is actief, het andere passief. Een actief OPEN is een verzending van een CALL, een passief OPEN is een ontvangst van een LISTEN;

De verbinding met de correspondenten kan door TCP op tweeërlei wijze worden opgevat: het ULP wacht op een lijn met een welbepaalde correspondent, ofwel met welke correspondent ook. Bijgevolg kunnen twee soorten van OPEN-instructies worden uitgevoerd: de **Fully Specified** of **Unspecified** OPEN's.

Bij de Fully Specified OPEN wordt een oproep vanuit een ULP alleen bepaald door zijn **socket**. Een binnenkomende oproep zal alleen dan worden geaccepteerd als hij van de juiste socket komt. Anders wordt hij verworpen.

Bij een Unspecified OPEN wordt de socket niet nader bepaald. Bijgevolg kan een verbinding worden gelegd met welke afgelegen ULP ook.

De technieken van de Specified en Unspecified OPEN's kunnen worden vergeleken (met enig

voorbehoud, maar de concepten liggen dicht bij elkaar) met de technieken van de Baseband en de Broadband die we al behandelden.

Is de verbinding tot stand gekomen, dan zal TCP ze zolangacyveren als de correspondenten dat wensen.

Natuurlijk kan het gebeuren dat een verbinding wordt aangehouden terwijl de twee correspondenten elkaar een tijd lang geen gegevens doorzenden. In dat geval zal TCP zelf lege pakketten genereren met niet-correcte sequentienummers. In deze situatie moet de ontvanger een pakket (datagram) terugzenden met het juiste sequentienummer. Volgt er geen antwoord, dan kan TCP beslissen om de lijn op te geven.

Een verbinding kan op twee manieren worden verlaten: ofwel door een vriendelijke CLOSE, ofwel door een brutale ABORT. Bij een CLOSE sluiten de twee ULP's de verbinding (ofwel simultaan ofwel na elkaar) bij afloop van de gegevensuitwisseling. TCP moet deze operatie coördineren en ervoor zorgen dat de laatste transit-informatie niet verloren gaat.

Bij een ABORT is de procedure heel wat agressiever. De beslissing tot een ABORT wordt genomen door één van beide ULP's en TCP is niet aansprakelijk voor eventueel verloren gegane gegevens op de lijnen op dat moment.

DATA
decisions
VOLGENDE DOSSIER:
HET MULTI-MEDIA
PUBLICITEIT: 02/332 24 26

- Ontvangstberichten

Om het verlies van informatie door de lagere lagen van het OSI-model te laten opvangen gebruikt TCP een techniek die PAR heet (Positive Acknowledgement with Retransmission). PAR geeft het TCP van het zendersysteem de mogelijkheid de gegevens met regelmatige tussenpozen terug te zenden totdat er eindelijk een reële ACK doorkomt.

Om onnodige transmissies en hertransmissies en dus een onverantwoorde overbelasting van het netwerk te vermijden beschikt TCP over een algoritme dat de time-out's op een dynamische manier kan regelen.

Op dit vlak wordt pas duidelijk hoe interessant TCP wel is in meervoudige netwerken. Werkt men in TCP/IP op de netwerken van het type Ethernet, worden de time-out's berekend in enkele duizendsten van een seconde; wordt dit protocol echter gebruikt voor satellietverbindingen dan is er geen sprake meer van milliseconden maar van seconden. TCP beschikt ook over adaptatieve tijdsbeheertechnieken opdat een station niet te snel of niet te traag gaat verzenden.

- Controle van de gegevensstroom

Deze controletechnieken geven een ontvangst-TCP de mogelijkheid de gegevensstroom die hem door het zend-TCP wordt doorgezonden beter te beheren. Deze techniek steunt op een window waarin een aanvaardbare gegevenssequentie wordt gedefinieerd; Dit venster kan vergroot of verkleind worden om te vermijden dat bij te grote window-waarden er te aanzienlijke overheads worden veroorzaakt. Te krappe waarden zullen een invloed hebben op het gebruik van het netwerk en de machinetijd, want in

dat geval zullen de ULP's een reeks datagrammen met een geringe inhoud over de lijn sturen in plaats van een groter aantal datagrammen met een hogere capaciteit.

- Multiplexing

Twee ULP's die van plan zijn met elkaar te communiceren moeten hun respectieve TCP's daarvan op de hoogte brengen; Die gaan dan een reeks initialiseringen uitvoeren en tussen beiden een virtueel circuit tot stand brengen. Dit virtueel circuit wordt verkregen na een fase van synchronisatie of **handshake** die de communicatie werkelijk opent (de term 'handshaking' werd ontleend aan de elektronica en meer bepaald aan de elektronica van de modems wanneer deze hun dialoog aanvatten).

Deze handshake met het oog op een synchronisatie steunt op de uitwisseling van drie segmenten. Deze procedure is bekend onder de naam "three-way handshake" en is opgebouwd rond het feit dat als twee machines willen dialogeren ze eerst SEQ en dan ACK doorzenden.

Deze procedure wordt beschreven in schema 3:

- Techniek van de afspraak

Elke ULP kan een verbinding

openen (OPEN) volgens twee manieren: de actieve of de passieve manier.

Wanneer het ULP een **ACTIEVE OPEN** uitvoert, geeft hij het TCP het bevel met de hoger beschreven synchronisatieprocedure te beginnen. Bij een **PASSIEVE OPEN** daarentegen zal het TCP wachten op een lijn die door een actieve oproeper is geïnitieerd;

Dit onderscheid tussen actief en passief blijkt zijn nut te hebben in het kader van de cliënt/server toepassingen. Een beheersprogramma kan in deze optiek wachten (op de server en op een passieve manier) tot een werkstation het aanroept (actief). Vandaar de term afspraak.

Handshaking van het TCP zorgt ook voor de coördinatie van 2 gelijktijdige actieve OPEN's. Toch is het niet nodig dat een van beiden actief zou zijn en de andere passief opdat de communicatie wordt gelegd.

Volgende maand sluiten we deze reeks artikelen over TCP/IP af met een beschrijving van de bovenste lagen: de sessielaag, de presenatielaag en de applicatielaag.

P. Ausloos,
Consultant.

Schema 3 - Procedure van de three-way handshake

NIVEAU 1	NIVEAU 2	NIVEAU 3
BRON	BESTEMMING	BRON
Kan ik...?	Ja, natuurlijk.	
SEQ = X	SEQ = Y, ACK = X+1	SEQ = X+1+ DATALENGTE, ACK = Y+1
Begin van de transmissie.		Behoud van de transmissie.

INTER-NETWERKCOMMUNICATIE

TCP/IP en de ISO-lagen 5, 6 en 7

Zoals iedereen weet werken de netwerkdiensten van de lagere lagen in het OSI-model heel discreet. Zodanig zelfs dat de toepassingsprogrammeur er nauwelijks iets van merkt, en ook het programma "weet" niet hoe de dingen zich op het moment zelf afspeelen.

Bovendien zou men de lagen 5, 6 en 7 kunnen bestempelen als gemengde lagen. We zagen al dat elke laag van het OSI-model bestaat uit twee helften en dat elke halve laag kan dialogeren met de laag die daar net boven of onder ligt. Dat geldt echter niet voor de sessie-, presentatie- en applicatielaag. Netbios bijvoorbeeld is een element die gebruik maakt van de 3 lagen en aangezien TCP/IP in sommige gevallen met Netbios te maken heeft moet er een superstructuur worden gevormd die betrekking heeft op deze drie lagen.

Het Netbios vermelden we trouwens maar even terloops. De lagen 5, 6 en 7 leveren vier netwerkdiensten in het raam van TCP/IP:

- DNS (Domain Name Service);
- SMTP (Simple Mail Transport Protocol);
- FTP (File Transfer Protocol);
- TELNET.

We laten de vier even de revue passeren voordat we deze reeks artikelen over TCP/IP afsluiten, maar eerst bekijken we nog even de functie van de sessie-, presentatie- en applicatielaag.

Functies van de lagen

Laag 5 of sessielaag zorgt voor de administratie van de dialoog (of sessie) tussen de twee gesprekspartners. Wat hier sessie wordt genoemd is eigenlijk gewoon een verbinding tussen twee presentatielagen. Dank zij deze sessielaag kan een programma die een verbinding met de buitenwereld vraagt die verkrijgen, behouden en zo nodig ook opgeven.

De verbinding wordt tot stand gebracht aan de hand van namen die daarna in netwerkadressen worden omgezet (sockets). De sessielaag beheert ook de hernemingen tussen de correspondenten. Met die hernemingen bedoelen we begrippen zoals checkpoint of restart: begrippen die de meesten onder ons als elementair zullen voorkomen, maar waar toch voor moet worden gezorgd...

Voor de sessieverwerking die door TCP/IP wordt uitgevoerd zijn geen speciale protocollen nodig.

Laag 6 is de presentatielaag. Die bepaalt de manier waarop de gegevens moeten worden begrepen (geïnterpreteerd) tussen

twee correspondenten. Zij gaat bijvoorbeeld de compressie/decompressie van de spaties uitvoeren, wat eventueel het ontvangen bericht zal wijzigen om het compatibel te maken met het geadresseerde randapparaat (het beste voorbeeld is de toevoeging of verwijdering van CR/LF data aan het einde van de lijn wanneer men zich wendt tot een of ander printertype), die het bericht van ASCII in EBCDIC en omgekeerd gaat omzetten.

Deze presentatielaag is van uitzonderlijk belang. Want zij zorgt ervoor dat een bericht beschouwd wordt als een immaterieel element, als een soort concept en bovendien wordt dat immaterieel element plots realiteit: het bericht komt op de juiste plaats terecht op het beeldscherm omdat de cursor juist werd geplaatst, het bericht wordt correct afgedrukt zonder dat een regel wit bleef, enz.

Kortom, het is de 'mirakellaag' ! Laag 7 is de applicatielaag. Die laag zorgt voor de eigenlijke gegevensverwerking. Bijgedistribueerde informatica (en kunnen we die eigenlijk over het hoofd zien in de context van de tele-

communicatie?) moeten deze verwerkingen volstrekt synchroon zijn opdat de gegevens die door de ene wordt uitgezonden door de andere begrepen en verwerkt kunnen worden. Daarom is het idee dat een programmeur in zijn eentje aan de applicatielaag zit te werken onzin. Het gedistribueerde informatiemodel wint overigens steeds meer veld.

Het File Transfer Protocol (FTP)

Het FTP controleert en beheert de bestandsuitwisselingen tussen twee systemen. FTP voert de verwerking uit via twee aparte TCP/IP kanalen: de eerste verbinding zorgt ervoor dat beide systemen service-informatie, commando's, antwoorden enz. kunnen uitwisselen; de tweede verbinding wordt gebruikt voor de uitwisseling van de eigenlijke gegevensbestanden.

FTP kan worden vergeleken met de (hardware)-techniek van modems met feedback. Via een hoge-snelheidslijn worden de data uitgewisseld en via een lijn met lage snelheid loopt de service-informatie...

1 - De service-lijnen

FTP maakt gebruik van een cliënt/server-model. Onvermijdelijk treffen we hier dus twee hoofdcomponenten aan: de FTP-client en de FTP-server.

De FTP-client zet het transferproces in gang, terwijl de server op een passende wijze antwoordt op de verzoeken van de cliënt.

Dit model is natuurlijk interessant voor de transactionele systemen: de FTP-client is niet meer dan de

antenne van de eindgebruiker; deze antenne kan dan naar een of ander afgelegen systeem worden gericht om er de gewenste gegevens uit te halen.

Om gegevens met een partner uit te wisselen opent de FTP-client eerst een controleverbinding met de FTP-server. Die is zo geprogrammeerd (of geparametreerd) dat een uitvoering volgt bij een welbepaalde poort van het afgelegen systeem.

Eens de verbinding is gelegd (de cliënt is geïdentificeerd, het bestand een naam heeft), kan de cliënt zijn bevelen geven aan de server. Deze bevelen hebben betrekking op het type van verwerking dat men op dat bestand wil uitvoeren, bijvoorbeeld: RETRIEVE, STORE, DELETE, enz.

2 - De lijnen

voor de gegevensuitwisseling
Wanneer een transfer moet worden uitgevoerd leggen de FTP-client en -server een tweede TCP/IP verbinding dat als substraat dienst doet.

Aan de hand van de service-lijn worden de gegevens die verbonden zijn met de data-lijn uitgewisseld. Deze gegevens zijn bijvoorbeeld het poortnummer, het soort van transfer (binair, ASCII,...) en alle andere parameters die nodig zijn bij een goede transmissie.

De FTP-client is dan klaar om te luisteren bij de vooraf gedefinieerde poort van de lijn en de server begint de gegevens over te brengen; deze transfer zal zich volgens alle afspraken afspelen die eerder in de dialoog werden vastgelegd.

We moeten erop wijzen dat de data- en service-lijnen niet altijd twee dezelfde machines met

elkaar verbinden. Ook een driehoeksmodel is mogelijk.

Als machine A cliënt is kan ze een service-verbinding maken met machine B en een datatransfer-verbinding met machine C; daarbij is alleen het poortnummer waarnaar geluisterd moet worden belangrijk.

Men kan nog een stap verder gaan: als machine A in een driehoeksverhouding werkt dan kan ze een service-verbinding tot stand brengen met B en C, op zo'n manier dat B en C onbewust met elkaar gegevens uitwisselen.

Dat brengt natuurlijk gevaren met zich mee maar het biedt ook voordelen voor het onderhoud op afstand van de netwerken.

TELNET

TELNET is een standaardprotocol dat in beide richtingen zorgt voor communicatie tussen twee systemen. TELNET kan zowel tussen terminals als tussen processen verbindingen tot stand brengen.

Een TELNET-verbinding is een TCP-verbinding die gebruikt wordt om gegevens over te brengen die specifieke TELNET-gegevens bevatten. Dit protocol werd opgebouwd volgens twee basisideeën: de virtuele terminal (NVT: Network Virtual Terminal) en de onderhandeling.

1 - De virtuele netwerkterminal

Een TELNET-verbinding brengt gewoonlijk een relatie tot stand tussen een terminal en een centrale machine. Elk van deze beide polen kan echter bekeken worden door een soort vervor-

mende lens die aan beide zijden dezelfde specifieke kenmerken, dezelfde standaard teweegbrengt. Dat is de virtuele terminal.

Een virtuele terminal is een denkbeeldig netwerkobject dat op een bepaalde manier reageert.

Zowel de client als de server hoeft dan niet meer de 'who is who' van het netwerk in zijn geheugen op te slaan, want per definitie reageren ze allemaal op dezelfde wijze. Alle netwerkobjecten zijn uitgerust met een TELNET-converter. Deze converter is een programma dat de overeenstemming gaat realiseren tussen de specificaties van de virtuele terminal en van de reële terminal;

Het is een filter waardoor herkenning van de typische tekens en commando's van de beschouwde terminal mogelijk wordt.

2 - De onderhandeling

Met TELNET kunnen de leden van een netwerk kiezen uit de diensten die bepaald zijn door de virtuele terminal. Deze service-selecties vinden plaats via een bepaald aantal opties die bepaald worden binnen TELNET zelf, maar die nochtans onafhankelijk zijn van elkaar.

De verwerking van deze gespreksopties gebeurt in de vorm van alles of niets. Zo kunnen de gesprekspartners - cliënten en servers - het eens worden over de TELNET-verbinding die later bij de verbinding zal worden gebruikt.

Tijdens de onderhandeling gaat de verzender gegevens verzenden waarmee hij de ontvanger inlicht of hij een bepaalde functie al dan niet kan uitvoeren of waarmee hij zijn partner vraagt een bepaalde optie al dan niet te

'setten'. De ontvanger gaat dan een rapport terugzenden waarin staat of de gevraagde opties al dan niet aanvaard worden.

De frontale Datanet processoren van de fabrikant Bull werken op deze manier, alsook de X.3 modus wanneer een asynchrone terminal via een PAD in communicatie wil treden met een X.25-computer. De beschouwde opties zijn bijvoorbeeld het gebruik van een bepaald type van teken, de echo modus ON of OFF, enz. Een vande gesprekspartners heeft altijd het recht NEE te antwoorden op een optie die de transmissie complexer maakt, maar kan nooit een optie weigeren die de transmissie eenvoudiger maakt.

Nemen we bijvoorbeeld aan de ene kant een systeem A met een modem met 1.200 baud en aan de andere kant een systeem B met een modem die een bereik van 1.200 tot 9.600 baud kan aftasten. Elke aanvraag van B om een snelheid te eisen van 9.600 baud zal worden geweigerd door A dat zal aangeven dat de optie 1.200 baud moet bedragen. B zal niet kunnen weigeren onder deze snelheid te gaan, terwijl A het recht heeft de hogere snelheid van 9.600 baud, die dus voor hem te hoog ligt, te weigeren.

Printers werken volgens hetzelfde mechanisme - één printer zal dan 132 tekens per regel hebben en de andere bvb. 132 - en dat geldt ook voor gelijk welk netwerkelement.

Domain Name Service (DNS)

DNS is een voorbeeld van een protocol dat gebaseerd is op de

naam. Het zal een relatie leggen tussen de objectnaam in een netwerk en het adres van dit object. DNS zorgt eveneens voor een volledig gedecentraliseerd gebruik van de resources en van de servers.

Het aanvankelijk doel van DNS lag in de Electronic Mail.

Deze decentralisering van de namen wordt uitgevoerd door het gebruik van een aantal velden, waarbij elk veld overeenstemt met een sectie van het netwerk. Net zoals bij het MS-DOS waar de directories zorgen voor een fijnere schijfindexing.

Dit DNS lijkt een beetje op de "StreetTalk" van Banyan in het kader van de lokale netwerken.

Simple Mail Transport Protocol (SMTP)

Hpewel het gaat om transport heeft SMTP niets te maken met de laag van dezelfde naam. Deze dienst, ter hoogte van laag 7, gebruikt de TCP/IP verbindingen om berichten te transporteren via een netwerk. Hij kan ook worden gebruikt om berichten van een proces naar het andere over te brengen binen dezelfde machine.

Hiermee sluiten we deze artikelenreeks over TCP/IP* af, we hopen dat we een en ander hebben verduidelijkt.

Pierre Ausloos
Consultant.

* We bedanken de firma Ungermann-Bass voor de geleverde documentatie waarmee we dit thema hebben kunnen uitwerken.



X.25. The Consultative Committee for International Telephony and Telegraphy's (CCITT) designation for a standard interface for packet-switched data-communications networks. X.25 networks employ virtual circuits for end-to-end connections, in contrast to TCP/IP networks, which use datagrams. The X.25 standard is designed to let mainframes access a public or private packet switching network.

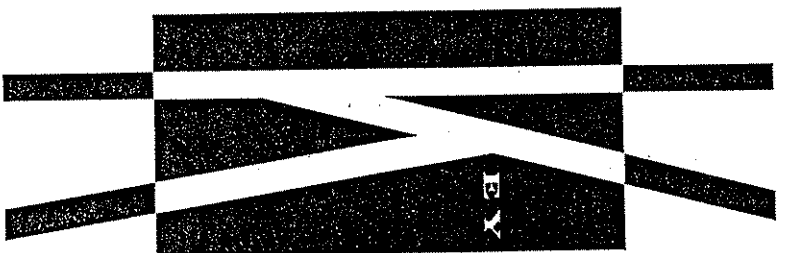
X.400. The CCITT designation for an international electronic mail distribution system.

X.500. The CCITT designation for a directory standard to coordinate the dispersed file directories of different systems.

XNS (Xerox Network Systems). A Xerox-developed set of communications protocols designed to run on Ethernet networks. The XNS internetwork datagram protocol provides standards for network layer communications, and the sequenced packet protocol provides standards for the transport layer. Contrast with *TCP/IP* and *OSI*.

X/Open. A consortium of computer industry vendors chartered to specify an open system platform based on the Unix operating system.

X Window. A network-based windowing system that provides a programmatic interface for graphic window displays. X Window permits graphics produced in one workstation in a network to be displayed on another.



BY
TERMS IN
COMPUTER
NETWORKING
AND
NETWORK
MANAGEMENT

Token ring. A network that uses a ring topology and the token passing access method. Contrast with *Ethernet*.

TOP (Technical and Office Protocol). An implementation of OSI standards in office and engineering environments. TOP, developed by Boeing® and other firms, employs Ethernet specifications.

Topology. The pattern of physical and logical links between nodes on a network. See *Bus topology*, *Ring topology*, and *Star topology*.

Transceiver. A device that functions as both a transmitter and a receiver. In an Ethernet network, a transceiver links a node with baseband cable.

Transport layer. Layer 4 of the Open Systems Interconnection (OSI) protocols. It structures messages for transmission over the network by splitting the messages for sending and reassembling them as they are received. The transport layer also provides recovery from transmission errors.

Twisted-pair wire. A cable composed of two 18 to 24 AWG (American Wire Gauge) solid copper strands twisted around each other. The twisting provides a measure of protection from electromagnetic and radio-frequency interference (EMI/RFI). Two types of twisted-pair wire are available: shielded and unshielded. The former is wrapped inside a metallic sheath that provides protection from EMI/RFI. The latter, also known as telephone wire, is covered with plastic and/or PVC, which does not provide protection from EMI/RFI.

Type 3 cable. An unshielded twisted-pair wire that meets IBM specifications for use in 4-Mbps token ring networks.

UDP (User Datagram Protocol). An Internet standard protocol that allows an application program on one machine to send a datagram to an application program on another machine.

Access method. The method used by networked stations to determine when they can transmit data on a shared transmission medium.

Accounting management. One of the five basic categories of network management defined by the International Standards Organization (ISO). Accounting management assigns costs to the use of network resources by users or groups of users.

ACF/NCP. See *Advanced Communications Function for the Network Control Program*.

ACF/VTAM. See *Advanced Communications Function for the Virtual Telecommunications Access Method*.

Address. The unique identity of a station or network.

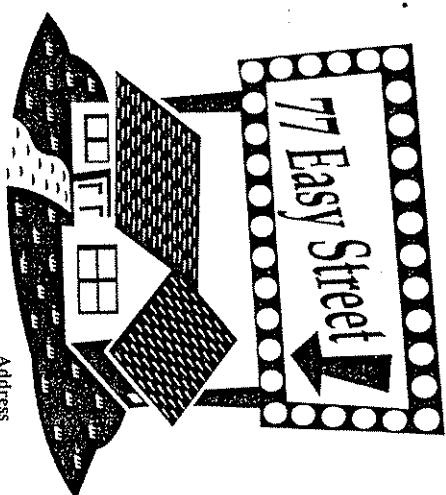
Address Resolution Protocol (ARP).

A protocol within the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite that "maps" IP addresses to Ethernet addresses; required by TCP/IP for use with Ethernet.

Advanced Communications Function for the Network Control Program (ACF/NCP). An IBM® product that controls the operation of a communications controller.

Advanced Communications Function for the Virtual Telecommunications Access Method (ACF/VTAM). An IBM program that controls communications and the flow of data in an SNA™ network. ACF/VTAM runs under several IBM operating systems.

Advanced Program-to-Program Communications (APPC). An implementation of SNA LU 6.2 sessions that permits personal computers in an SNA network to communicate in real time with the mainframe host and other networks.



Address Resolution Protocol





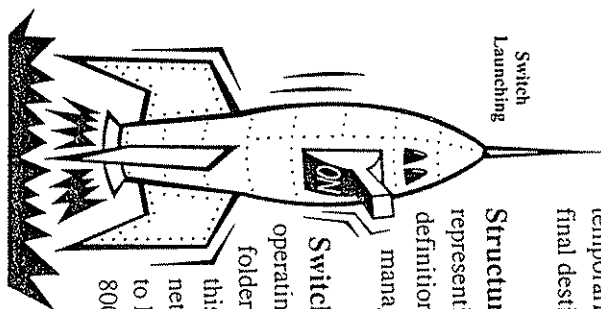
StarLAN. AT&T's proprietary networking protocol. It supports both 1- and 10-megabit-per-second data rates.

Star topology. A network configuration in which nodes are connected individually to a common device, such as a concentrator, which acts as a focal point for network cabling. Contrast with *Bus topology* and *Ring topology*.

Store-and-forward. A communications technique in which messages are received at intermediate routing points and stored temporarily, then retransmitted to an additional routing point or final destination.

Structure of Management Information (SMI). A way of representing network management information. SMI includes definitions of data types. It is used to specify models of network management information in OSI and IETF.

Switch launching. The facility within the Apple Macintosh operating system that allows a Macintosh to use a system folder located on a network disk. In Macintosh terminology, this is referred to as switching from a local disk to one on a network volume. Switch launching permits Macintosh users to have more fonts and desk accessories than will fit on an 800 Kb diskette.



Systems Application Architecture. See *SAA*.

Systems Network Architecture. See *SNA*.



3+Open™. A family of 3Com networking system products built around the LAN Manager file/print server. 3+Open includes connectivity, messaging, and network management services.

10BASE2. IEEE's specifications for running Ethernet over thin coaxial cable.

AppleTalk Filing Protocol (AFP). A protocol that lets workstations access files from remote file servers. The protocol corresponds to layer 6 of the Open Systems Interconnection (OSI) protocols. AppleShare® is Apple's implementation of an AFP server using a Macintosh as a server.

Application layer. Layer 7 of the Open Systems Interconnection (OSI) protocols. It serves as the window through which applications access communication services, including file-transfer functions, virtual-terminal functions, and electronic-mail functions.

ARP. See *Address Resolution Protocol*.

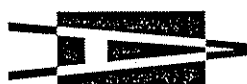
ARPAnet (Advanced Research Projects Agency Network). A network of computers located mainly at U.S. universities, but also at other sites in the U.S. and other nations. ARPAnet activities are now the responsibility of Internet. See *Internet*.

ASCII (American Standard Code for Information Interchange). A system for representing alphanumeric data using 7-bit data codes. It and EBCDIC are the two most widely used data codes. Contrast with *EBCDIC*.

Assembly language. A low-level programming language whose statements are similar in form to the machine language of a computer. Because programs written in assembly language "speak" directly to the hardware, they are extremely compact, efficient, and fast.

Asynchronous transmission. Data transmission in which the interval between transmitted characters may be of unequal length. Start and stop bits at the beginning and end of each character control data transmission and timing.

Attenuation. The decrease in magnitude of the power of a signal transmitted over a wire, measured in decibels per kilometer. As attenuation increases, signal power decreases.





RS-422/RS-423. EIA-specified standards that operate in conjunction with RS-449. They specify electrical characteristics for balanced/unbalanced circuits, respectively. (Balanced circuits have their own ground leads. Unbalanced circuits use a common or shared ground lead.)

RS-449. An EIA standard that applies to binary, serial synchronous, or asynchronous communications systems.



SAA (Systems Application Architecture). An IBM-developed set of standards that provides identical user interfaces for applications running on PCs, minicomputers, and mainframes.

SDLC (Synchronous Data Link Control). The primary data-link protocol in IBM SNA networks.

Security management. One of the five basic categories of network management defined by the International Standards Organization (ISO). Security management prevents the misuse of network resources by means of user authorization, access control, and data encryption.

SEF (Source Explicit Forwarding). A security feature that permits only packets from specified stations to be forwarded across a bridge. By using SEF, an administrator can control access to resources on a network segment.

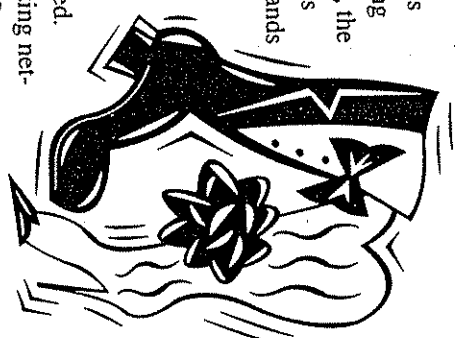
Server. A specialized computer that provides a particular service, such as file or print service, to a network.

Server Message Block (SMB). A file system protocol used to package data and exchange information with SMB-compatible systems.

Session. An active connection between two application programs on a network, allowing communication between them.



Boot PROM (Boot Programmable Read-Only Memory). A microprocessor that allows personal computers to retrieve and load operating system software over the network. For example, the boot PROM in a network adapter board provides the PC with start-up information and the commands to "look" to a specific file server for operating system files.



Boot PROM

Bridge. A device that interconnects local or remote networks no matter what higher level protocols (such as XNS[®] or TCP/IP) are involved. Bridges form a single logical network, centralizing network administration. They operate at the Open Systems Interconnection (OSI) physical and data link layers. See *Source Explicit Forwarding* and *Spanning Tree Algorithm*. Contrast with *Router*, *Brouter*, and *Gateway*.

Broadband. A data-transmission scheme in which multiple signals share the bandwidth, or data-carrying capacity, of a medium. This allows the transmission of voice, data, and video signals over a single medium, such as a coaxial cable. Cable television uses broadband techniques to deliver several dozen channels over one cable. Contrast with *Narrowband*.

Brouter. A device that combines the functions of a bridge and a router. Brouters can route one or more protocols, such as TCP/IP and/or XNS, and bridge all other traffic. Contrast with *Bridge*, *Router*, and *Gateway*.

Bus topology. The network pattern in which all nodes share a single channel. Contrast with *Ring topology* and *Star topology*.

Byte. A unit of consecutive binary digits (for example, an 8-bit or 16-bit byte).





Presentation layer. Layer 6 of the Open Systems Interconnection (OSI) protocols. It manages data formats, converting data from one format to another according to application requirements.

Presentation Manager. The portion of the OS/2 operating system that provides users with a graphical-based, rather than character-based, interface similar to that of Apple's Macintosh.

Printer spooler. The software that sends a file to a shared printer over a network even when the printer is busy. The file is saved in temporary storage and then printed when the printer is available.

PROFS (Professional Office System). Interactive productivity software that runs under the VM/CMS mainframe system. PROFS is frequently used for electronic mail.

Propagation delay. The time necessary for a signal to travel from one point on a circuit to another.



Query language. A programming language designed to make it easier to specify exactly what information a user wants to retrieve from a data base.

Queue. A list formed by items in a system waiting for service. An example is a print queue of documents to be printed in an electronic publishing system.



Repeater. A network component that regenerates digital signals, thus extending network length. A repeater can interconnect a variety of media such as thick and thin coax. It operates at the Open Systems Interconnection (OSI) physical layer.

Configuration management. One of the five basic categories of network management defined by the International Standards Organization (ISO). Configuration management monitors the physical and logical state of the network as well as applications and services. A function of configuration management is to keep an inventory of network resources and their operating parameters, which set the operating conditions for the network.

Corporation for Open Systems (COS). An industry-sponsored nonprofit research and development organization that promotes the adoption of international standards in data communications.

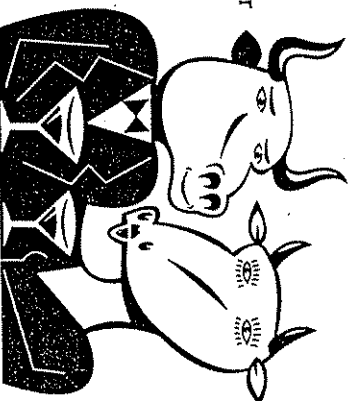
COS. See *Corporation for Open Systems*.

COW interface (Character-Oriented Windows interface). An SAA-compatible user interface for OS/2 applications.

CRC (Cyclical Redundancy Check).

A method of detecting errors in a message by performing a mathematical calculation on the bits in the message and then sending the results of the calculation with the message. The receiving station performs the same calculation on the message data it receives and then checks the results against those transmitted at the end of the message. If the results do not match, the receiving station asks the sending station to send the message again.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection). A network access method in which contention between two or more stations is resolved by collision detection. When two stations transmit at the same time, they both stop and send "jamming" signals that indicate a collision has occurred. Each then tries again after waiting a separate randomly determined time period, usually several microseconds. Contrast with *Token passing*.



COW Interface



Open View™. Hewlett-Packard's suite of network management applications, a server platform, and support services. Open View is based on HP-UX, which complies with AT&T's Unix system.

OS/2 (Operating System/2). An operating system developed by IBM and Microsoft for use with Intel's 80286 and 80386 microprocessors. Unlike its predecessor, DOS, OS/2 is a multi-tasking operating system.

OS/2 Extended Edition. IBM's proprietary version of OS/2. It includes built-in communications and database management facilities.

OSF (Open Software Foundation). A consortium of industry leaders working to standardize the Unix operating system.

OSI (Open Systems Interconnection). A seven-layer set of data communications protocols developed by the International Standards Organization (ISO). See *Physical layer*, *Data link layer*, *Network layer*, *Transport layer*, *Session layer*, *Presentation layer*, and *Application layer*. Contrast with *XNS* and *TCP/IP*.

Packet. A group of binary digits, including data and control information, sent in a well-defined format over a network.

Packet filter. A feature of a bridge that compares each packet received with specifications set by the network administrator. If the packet matches the specifications, the bridge can either forward or reject it. Packet filters let the administrator limit protocol-specific traffic to one network segment, isolate electronic mail domains, and perform many other traffic control functions.

Packet switching. The internal operation of a communications network that uses software to dynamically route packets from a source to a destination. Packet switching allows the sharing of a single communications channel among several connections. Contrast with *Circuit switching*.



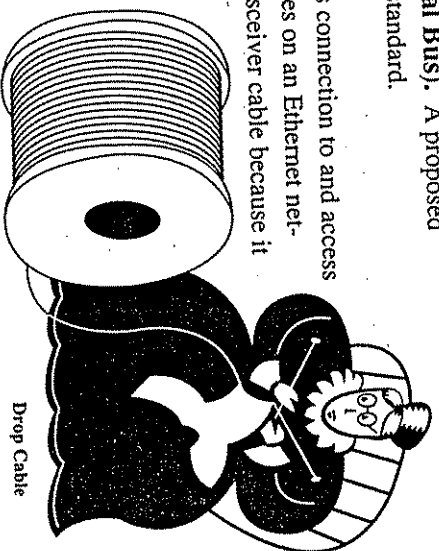
DLC. See *Data-link control*.

DNA. See *Digital Network Architecture*.

DQDB (Distributed Queue Dual Bus). A proposed metropolitan area network (MAN) standard.

Drop cable. The cable that allows connection to and access from the distribution and trunk cables on an Ethernet network. Drop cable is also called transceiver cable because it runs from the network node to a transceiver (a transmitter/receiver) attached to the trunk cable. Drop cables are made up of two pairs of shielded twisted-pair wiring.

DTE (Data Terminal Equipment). The end-user equipment, typically a terminal or computer, that can function as the source or destination point of communication on the network. Contrast with *DCE*.



EBCDIC (Extended Binary Coded Decimal Interchange Code). An 8-bit data-exchange code used in IBM mainframes, other computer systems, and associated communications equipment. It and ASCII are the two most widely used data codes. Contrast with *ASCII*.

ECMA (European Computer Manufacturer's Association). A trade association that provides input to international standards-forming organizations.

EDI (Electronic Data Interchange). The communication of orders, invoices, and similar transactions electronically between organizations.





NDIS (Network Driver Interface Specification). A device driver specification codeveloped by 3Com and Microsoft. Besides providing hardware and protocol independence for network drivers, NDIS supports both DOS and OS/2 and offers protocol multiplexing so that multiple protocol stacks can coexist in the same host.

NetBIOS (Network Basic Input/Output System). Software developed by IBM that provides the interface between a PC's operating system, its I/O bus, and the network. NetBIOS is a de facto network standard.

Netstation. A personal computer designed specifically for operation on a local area network. Typically, netstations contain built-in network connectors. They do not contain disk drives for local data storage and/or startup facilities.

NetView®. IBM's network management system. NetView is designed to run on mainframes in SNA environments and to manage both SNA and non-SNA devices on the network.

NetWare. A series of network operating systems and related products made by Novell®, Inc.

Network layer. Layer 3 of the Open Systems Interconnection (OSI) protocols. It establishes connections for communication between two nodes.

NFS (Network File System™). An extension of TCP/IP that allows files on remote nodes on a network to appear locally connected. NFS was developed by Sun Microsystems®.

NMP (Network Management Protocol). An AT&T-developed set of protocols designed to exchange information with and control the elemental managers that govern various components of a network, including modems and T1 multiplexers.

NNTP (Network News Transport Protocol). An extension of the TCP/IP protocol that provides network news transport service.

Fault management. One of the five basic categories of network management defined by the International Standards Organization (ISO). Fault management is used for the detection, isolation, and correction of faults on the network.

FDDI (Fiber-optic Data Distribution Interface). A LAN technology that permits 100-megabit-per-second (Mbps) data transfer. FDDI is proposed as American National Standards Institute (ANSI) standard X3T9.5.

FEP. See *Front end processor*.

Fiber-optic cable. A transmission medium that uses glass or plastic fibers, rather than copper wire, to transport data or voice signals. Information is imposed on the glass fiber via pulses (modulation) of light from a laser or a light-emitting diode (LED). Because of its high bandwidth and lack of susceptibility to interference, fiber-optic cable is employed in long-haul or noisy applications.

File server. A specialized computer that stores data and programs to be shared by users on a local area network. The server functions as a remote disk drive for users.

Filter. See *Packet filter*.

Flow control. A hardware or software mechanism employed in data communications to turn off the transmission when the receiving station is unable to store the data it is receiving.

Frame. A group of bits that make up an elementary block of data to be sent over a communications channel. Usually, a frame contains its own control information, including the transmission address and data for error detection.

