

# NETWERKBEHEER EN BEVEILIGING

Bedrijfsprocessen zijn afhankelijk van het goed functioneren van netwerken. In de exploitatiefase van het netwerk is beheer cruciaal. Onder beheer worden naast onverwachte gebeurtenissen zaken geregeld zoals:

- apparatuuronderhoud
- beheer van namen en adressen (te bereiken bestemmingen)
- beheer van congestie
- beheer van veiligheid

## 4.1 Netwerkbeheer

- Managementtaken en organisatie
- Netwerkmanagement en OSI
- Agents en element-management
- Managementstation
- System-management

### OSI-management-framework

Configuratiegegevens vormen de basis om het beheer van netwerken te kunnen uitvoeren. Je moet dus weten waar de netwerkapparatuur staat ! (switches, modems, verbindingen ... verspreid in gebouwen, over een land, continent of de hele wereld).

Aanvankelijk was hiervoor binnen OSI geen aandacht voor. Later is dit vastgelegd in een addendum onder de naam 'management-framework'.

De taken en functies zijn gegroepeerd in 5 gebieden:

- Fault mgt
- Performance mgt
- Configuration mgt
- Accounting mgt
- Security mgt

### **1. Fault mgt**

Gericht op snel optreden en nemen van maatregelen bij storingen:

- Het *ontdekken*, melden en zo mogelijk (automatisch) herstellen van fouten;
- Het *diagnosticeren* van fouten (bestuderen van logbestanden, tests) en eventueel het reproduceren van het probleem;
- *Het herstel* van de gevolgen van de fouten (vb het herstel van routes volgens schema's die voor de fout werden gebruikt), opnieuw laden van software in netwerkkapparatuur en eventuele vervanging van hardware

### **2. Performance mgt**

Netwerken hebben meestal een wisselend verkeersaanbod die de prestaties en daarmee de kwaliteit van het netwerk negatief kunnen beïnvloeden. (Naast piekgebruik zijn er over langere perioden ook tendensen).

Performance mgt richt zich op de prestaties van het netwerk door:

- Vergaren van informatie via tellers en timers in de netwerkcomponenten
- Analyseren van de beschikbaarheids- en belastingscijfers
- Instellen van drempelwaarden voor het signaleren van prestatievermindering zodat kan worden ingegrepen (=> faultmgt)

### **3. Configuration mgt**

Configuration mgt bestaat uit administreren, aansluitingen (de)activeren enz. De taken bestaan uit:

- Topologie van het netwerk en weten waar wat staat
- Configuratieparameters moeten vastgelegd zijn
- Gegevens van de aangesloten systemen op het netwerk: op welke poort, voor welke services, tegen welke kwaliteit tot en met de adresgegevens van de gebruiker/klant
- Operationeel maken van nieuwe softwareversies, voorbereiden van upgrades, enz.

#### **4. Accounting mgt**

De kosten van exploitatie moeten verrekend worden binnen het bedrijf of voor de verrichte commerciële dienstverlening. Volgende taken komen hierbij voor:

- Bijhouden van het gebruik van de verschillende gebruikers, en het periodiek uitlezen van de tellers
- Overzichtelijke gebruiksgegevens genereren (billing)
- Kennen van de kostenbepalende factoren, weten wanneer het netwerk kostendekkend is, bovendien voor commerciële dienstverlening het kennen van de concurrerende tarieven en tariefstructuren.

#### **5. Security mgt**

Afhankelijk van type network en de aard van het gebruik kent beveiliging een aantal niveaus. Taken die onder security mgt vallen zijn:

- Beheer van toegang door middel van passwords, toegangssleutels enz.
- Beveiliging van de ruimten
- Signaleren van onbevoegd gebruik
- Beheer van coderingssleutels (encryption keys) als de te transporteren data versleuteld zijn.

De veelheid aan taken worden onderverdeeld in operationeel en tactisch beheer:

#### **Operationeel beheer:**

Taken uit de 5 gebieden waarbij de nadruk ligt op het laten werken van het netwerk.

#### **Tactisch beheer:**

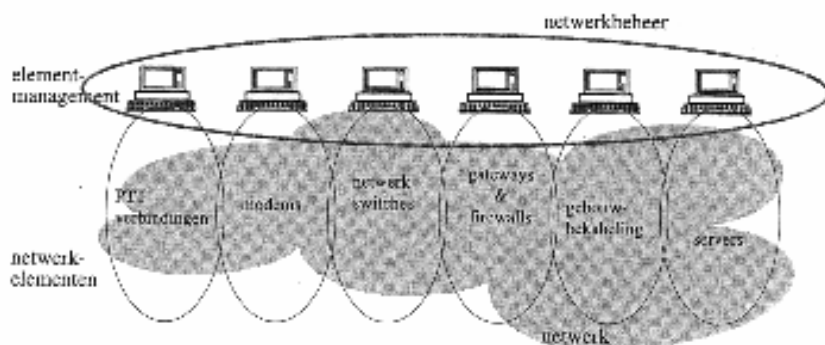
Vorbereidingen voor uitbreidingen, verzamelen van gegevens om het gebruik te analyseren en te factureren, enz.

## Agents en element-managers

Netwerken bestaan uit verschillende componenten, dikwijls van verschillende fabrikanten. Iedere leverancier zal zijn eigen mgt-systeem hebben om ‘zijn’ apparatuur te beheren. Bij grote netwerken is de praktijk van een netwerkmanager dan ook een muur van beeldschermen. Eén enkele netwerkverstoring veroorzaakt hierbij soms een waterval van foutmeldingen...

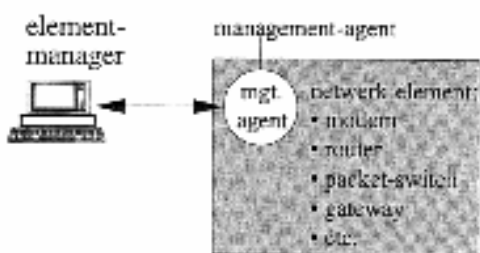
Ieder netwerkelement heeft een eigen mgt-systeem, dat bestaat uit twee delen:

- Mgt-agent, software die in de apparatuur is geïntegreerd
- Element-mgr, een set applicaties die de netwerkbeheerder in staat stelt de apparatuur te beheren door communicatie met de agent software in de apparatuur



Zodoende is het mogelijk op afstand de netwerkapparatuur te configureren.

Meestal is er een lokale mgtpoort aanwezig waarop direct een PC kan worden aangesloten voor de service engineers.

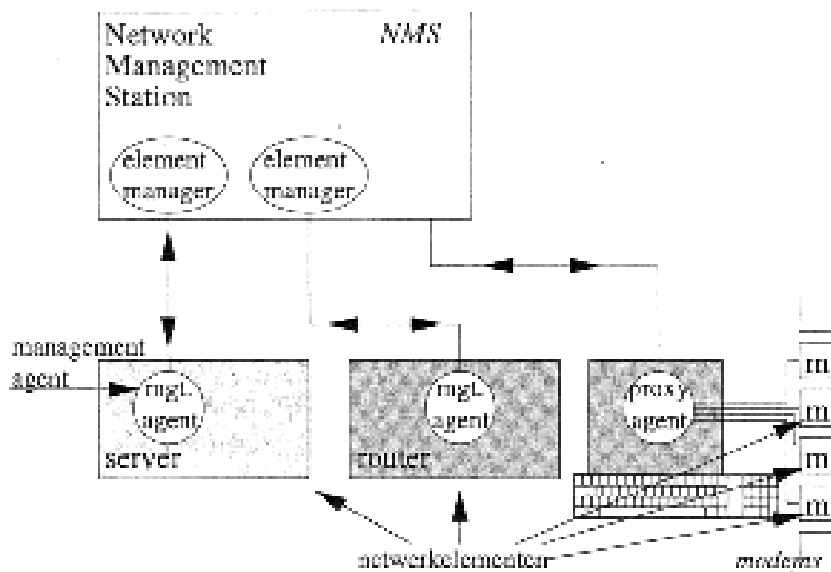


Fabrikanten bouwen in de agents en de applicatie zoveel mogelijk functies die het beheer zo efficiënt en krachtig mogelijk maken. Communicatie tussen agent en element mgr verloopt volgens gestandaardiseerde of breed aanvaarde protocollen (blok IV).

## Manager of manager

Eén **Network Management Station (NMS)** verzamelt alle meldingen van de elementen en presenteert ze eenvoudig.

Het NMS kan deze taken uitvoeren door te communiceren met de element-managers of direct met de agents. Software op de element-mgrs die dit mogelijk maakt noemt, wordt **proxy agent** genoemd.



Netwerkbeheer bekommert zich om de netwerkelementen in het veld maar ook voor de computers erop aangesloten. Dit beheer noemt men **systemmanagement**. Hiervoor gelden soortgelijke taken als voor het netwerkmgt.

## 4.2 Adressering en naamgeving

- Netwerkadres
- Nummerplan
- Adres en naam
- Directory

Aangesloten systemen hebben een uniek netwerkadres nodig. Meestal is dit adres een getal. Bekende netwerkadressen zijn:

Telefoonnummers	00 44 181 2567890 (UK)
Adressen in openbare pakketnetwerken	204 123456852 00 <i>of</i> 205 9876543210 99
Adressen in internet	145.200.5.5

Spaties of punten in het adres komen overeen met de structuur van het adres; ook de waarden van de nummers hebben een bepaalde logica.

Netwerkadressen zijn in OSI-termen een laag-3 adres.

Een netwerkadres is vaak onvoldoende. Binnen het systeem moeten de data bij de juiste applicatie terechtkomen. Adressering moet dus op meer lagen geregeld worden.

## Nummerplannen

Een nummerplan moet consistent zijn (geen dubbele nummering) om bereikbaarheid te garanderen. De routing moet kloppen.

De beschikbare adresseringstechniek hangt tevens af van het type netwerk en het gebruikte protocol; (de meeste protocollen bepalen in de header de hoeveelheid ruimte voor het adres, bv: 32 bits in het internet protocol).

De adresruimte om netwerken te maken wordt opgedeeld in netwerknummers en aansluitnummers \*\*\* zie vb fig blz 287\*\*\*:  
 Netwerknummers: bv. geografische indeling, regio's, gebouwen, subnetwerken  
 Aansluitnummers: poort waar het netwerk de informatie aflevert.

Het adres ziet er als volgt uit: LLL.RR.GG.HHHH.xxx

LLL: Landencode, 3 digits  
 RR: Regiocode, 2 digits  
 GG: Gebouwcode, 2 digits  
 HHHH: Systeemcode, 4 digits  
 xxx: Vrij te gebruiken, 3 digits

De verzameling voor de verschillende codes moet vastgelegd worden:

Voor de Landencode		Voor de Regiocode		Voor de Gebouwcode		Voor de Systeemcode	
000-099	gereserveerd	0-9	gereserveerd	0-19	gereserveerd	0-100	gereserveerd
100-200	Europa	10-99	opeenvolgende nummers gebruiken, te beginnen bij 10	20-99	opeenvolgende nummers gebruiken, te beginnen bij 20	100-149	netwerk-management
100	NL					150-249	LAN-servers
105	BE					250-300	hubs
110	DU					1000-9999	PC's
115	CH						
etc							
200-300	Amerika						
200	USA						
205	CAN						
210	MEX						
etc							

Bij de opbouw van het nummerplan moet er voldoende ruimte zijn voor uitbreiding.

Bovendien moet een nummerplan na ontwerp ook beheerd worden.

Vb.: bij het koppelen van netwerken is er een risico dat er routingproblemen ontstaan doordat netwerk of subnetwerknummers meer dan één keer voorkomen.

Landnummers (cfr. Telefonie) is geen oplossing voor netwerken die zich uitstrekken over meerdere landen. Nummering zoals in het internet is hier meer aangewezen.

Land	Landnummer
Amerika en Canada	1
Nederland	31
België	32
Frankrijk, Andorra en Monaco	33
Spanje	34
Zwitserland	41
Tsjechië en Slowakije	42
Oostenrijk	43
Groot-Brittannië en Noord-Ierland	44
Zweden	46

Vaak kiest men voor adresvertaling als bestaande netwerken gekoppeld worden.



## Adressen en namen

In een directory (adresboek) wordt de relatie gelegd tussen de voor de gebruiker logische naam en het netwerkadres (netwerkadressen zijn meestal niet praktisch in gebruik).

De centrale directory is opgeslagen in de name-server (administratie door de netwerkbeheerder op één centraal punt).

Ook voor naamgeving moet er een plan ten grondslag liggen (cfr. netwerkadressen).

Eén centrale directory is goed uitvoerbaar voor een netwerk dat zich uitstrekt over één organisatie. Als het grote en/of verschillende typen netwerken betreft, die bovendien beheerd worden door verschillende organisaties, wordt het technische en organisatorisch een stuk ingewikkelder.

Directorysystemen worden ontwikkeld als onderdeel van een netwerksysteem. Hierdoor zijn directories ontstaan met een beperkte reikwijdte en voor bepaalde technologieën, protocollen en structuren (cfr. Blok IV: X.500 en DNS- het naamgevingssysteem in TCP/IP-netwerken)

### 4.3 Congestie in netwerken

- Flow control
- Blocking en delay
- Queues
- Wacht- en servicetijden

Netwerken moeten betaalbaar zijn:

- Ze worden daarom niet ontworpen op het grootst mogelijke hoeveelheid verkeer van alle aansluitingen;
- Als flow control in onvoldoende mate succesvol is bij het regelen van verkeersaanbod, zal het netwerk vertoppen (congestie).

#### Flow control

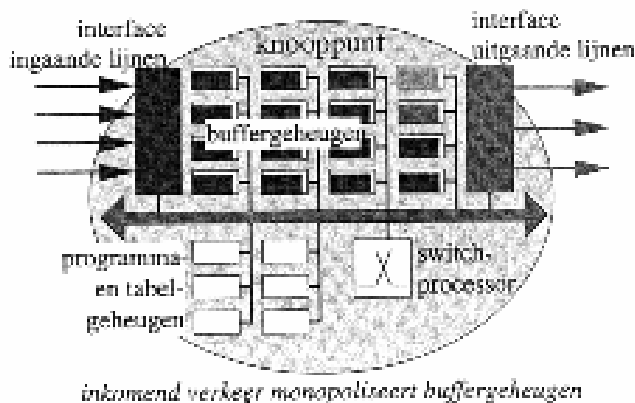
Het overvol geraken van de buffers kent een aantal oorzaken:

- Aan de uitgang van een knooppunt
  - het volgende knooppunt of de eindbestemming kan geen verkeer meer verwerken
  - de bandbreedte van de verbinding naar het knooppunt of de eindbestemming is te gering
- Aan de ingang van een knooppunt:
  - door problemen aan de uitgang kan een knooppunt na enige tijd ook geen verkeer meer in behandeling nemen
  - een gebrek aan schakelcapaciteit kan betekenen dat te veel data zich ophopen

Vertraging of delay is typisch voor pakketgeschakelde netwerken.

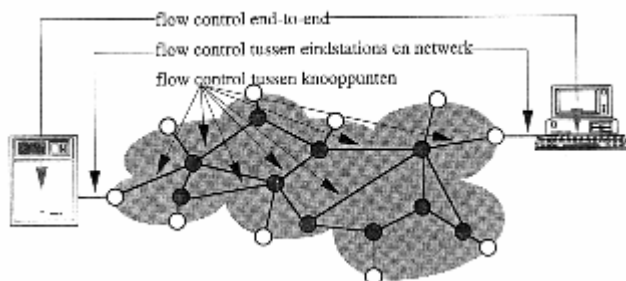
Vollopende buffers zorgen voor vertraging, in het ergste geval is geen verkeer meer mogelijk. Flow control treedt in werking als de buffers dreigen vol te lopen om te voorkomen dat datapakketten verloren gaan.

Het mechanisme is gebaseerd op feedback of terugkoppeling, waardoor kenbaar wordt gemaakt dat de verkeerstrom moet geremd worden.



Flow control kan voorkomen tussen:

- twee eindstations -end-to-end flow control- OSI-laag 4
- tussen eindstations en het netwerk OSI-laag 3
- in het netwerk tussen twee stations (knooppunten) OSI-laag 3



Flow-control mechanismen zijn geïmplementeerd in protocollen

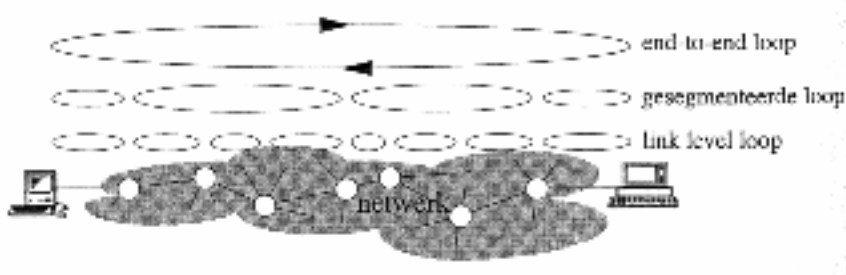
Er bestaan verschillende mechanismen waarop flow control kan gebaseerd worden:

XON/XOFF of Ack/Nack	Zetten de communicatie stil (zie II.4.1)
Windowing	
Congestion notification	Melden dat congestie dreigt en vragen of het wat 'minder' kan

## Loops

De grootte van de loop is een belangrijk aspect bij de werking van flow control (**loop**: afstand knooppunt dat congestiedreiging meldt en het knooppunt of eindstation dat de actie onderneemt om te remmen).

- Bij grote loops kan het even duren tot de zender het zwijgt
- Kleine loops zijn directer



Bij een ‘open loop’ is er geen vorm van flow control in het netwerk geïmplementeerd. Bij verstopping als de buffers overlopen, is er simpel verlies van informatie.

De ‘link level loop’, meestal op basis van windowmechanismen tussen twee knooppunten, is een veel voorkomend mechanisme.

De ‘end-to-end loop’ wordt gesloten door een eindstation. Als er een doorvoerprobleem is geven de knooppunten dit door aan één van de eindstations die actie kunnen ondernemen (lijkt op open loop, maar het netwerk is actief betrokken bij het regelmechanisme). Er zijn twee vormen:

- Forward:  
het knooppunt meldt met de datastroom mee, het probleem aan het ontvangende station. Het ontvangende eindstation zendt het zendende station een fc-bericht (eigenlijk een end-to-end flow control)
- Backward:  
Waarbij het knooppunt het probleem terugmeldt aan het zendende station tegen de stroom in

De gesegmenteerde loop is een variant op de end-to-end loop. In het netwerk worden een aantal punten opgenomen, waardoor de end-to-end loop verkleint en de reactiesnelheid van het mechanisme verbetert.

## 4.4 Beveiliging

- Open netwerken en beveiliging
- Authenticatie
- Vertrouwelijkheid
- Encryptie
- DES en RSA
- Welke beveiliging en waar?

### Tegenstrijdigheid:

Netwerken moeten willekeurige verbindingen mogelijk maken; Beveiliging wil dit verhinderen => weinig interesse van netwerkmensen en gebruikers die er alleen last van hebben. Computervirussen, hackers en afluisterpraktijken tonen de noodzakelijkheid aan.

### **Bedreigingen**

- Wachtwoordbeveiliging is niet voldoende
- PC-virussen hebben catastrofale gevolgen
- Meerderheid van de inbreuken gebeurt door eigen medewerkers

Het tweede addendum van het OSI-model, document ISO7498-2, biedt een overzicht van mogelijke beveiligingsmaatregelen.

De belangrijkste vier vragen zijn:

1. Identiteit: is het degene die hij of zij voorgeeft te zijn ?
2. Vertrouwelijkheid of confidentialiteit: kan niemand meeluisteren?
3. Integriteit: heeft niemand geknoeid met de inhoud van de data ?
4. Repudiation:
  - kan de zender de elektronische bestelling ontkennen
  - of kan de ontvanger ontvangst van de betaling ontkennen ?

Security-services, technische voorzieningen die implementeerbaar en veelal te koop zijn, bieden hierop een antwoord..

## Identificatie

Het vaststellen van de identiteit gebeurt via authenticatiemechanismen (bescherming tegen ‘masquerading’)

De meest bekende vorm zijn

- Passwords
- PIN-codes (Persoonlijk Identificatie Nummer/betaalkaarten)

Deze codes moeten beveiligd opgeslagen worden. Pass-wordfiles zijn gegeerd.

Identificatie kan veiliger door volgende maatregelen:

One time passwords	Iedere keer wordt een ander paswoord gebruikt. Gebruiker en systeem moeten dan wel over een systeem beschikken om het goede paswoord te kiezen. Een lijst is het eenvoudigst.
Tijdelijke passwords	De gebruiker wordt regelmatig om zijn identiteit gevraagd. B.v. om de 10 minuten. (ook hier is weer een systeem van te gebruiken passwords nodig).
Challenge/response	<p>Mechanisme waarbij een paswoord berekend wordt. De gebruiker heeft een soort rekenmachine die geactiveerd wordt met een pincode (een gewoon paswoord dus).</p> <p>Het systeem dat de identiteit wil kennen zendt een code (de challenge). De response wordt berekend met de calculator; waardoor een eenmalig paswoord ontstaat.</p> <p>De uitvoering kan een kleine rekenmachine zijn of geïntegreerd zijn in het computersysteem, waarvan de identiteit vastgesteld moet worden.</p>

## Vertrouwelijkheid

Door encryptie , het versleutelen van de bits kan men een niet-afluisterbare bitstroom realiseren.

De plaintext is de ongecodeerde versie.

Door op de plaintext een versleutelproces los te laten verkrijgt men een gecodeerd bericht, de ciphertext.

Aan ontvangtzijde moet een gecodeerd bericht weer worden omgezet tot een plain text.

Ontvanger en zender moeten dus beschikken over de methode tot versleutelen en ontgrendelen op basis van cryptografische sleutels.



\*\*\* zie verder: cryptografie \*\*\*

## **Integriteit**

De ontvanger moet weten dat er onderweg niet geknoeid is met de inhoud van het bericht.

De zender zal daarom een code toevoegen die niet iedereen kan genereren.

De toegevoegde code wordt ‘Message Authentication Code (MAC) genoemd.

De MAC beschermt tegen wijzigingen in de datastroom, net zoals bij de encryptie.

Met encryptie begrijpt die afluistert niets van het bericht, en kan het dus ook niet zinvol wijzigen. De hacker kan het bericht echter wel nog een keer versturen !

Hiertegen biedt de MAC echter bescherming. Dit wordt vooral gebruikt bij financiële transacties.

## Repudiation

De oplossing tegen het ontkennen van een elektronisch bericht:

- verzonden te hebben
- of ontvangen te hebben

bestaat uit het gebruiken van een digitale handtekening

\*\*\* toelichting: zie RSA blz 300 \*\*\*

Bedreiging	Wat te doen?	Mechanisme
masquerading	identificatie	authenticatie
afluisteren	vertrouwelijkheid	versluten
wijziging/herhaling	integriteit	MAC's
ontkennen	repudiation	digitale handtekening

## Cryptografie

Cryptografie, geheimschrift - of het versluieren of het vercijferen van gewone taal - bestaat reeds zeer lang. Het lijkt wel een menselijke behoefte.

Het bestond vooral uit het verschuiven van letters en het toevoegen van tekens.

De rekenkracht van computers maakte ingewikkelder cryptosystemen mogelijk, maar maakte ook de crypto-analyse - het ontcijferen van geheimschrift - eenvoudiger.

Het toepassen van cryptografie is gebaseerd op drie elementen:

- vercijferen
- ontcijferen
- vercijfer- en ontcijfersleutel

Vercijferen en ontcijferen zijn wiskundige bewerkingen, die meestal niet geheim zijn, zeker niet geheim te houden.

De vercijfering staat of valt met de sleutel die aangeeft hoe de wiskundige algoritme uitgevoerd moet worden.

In de praktijk treffen we drie cryptografische systemen aan:

- keyless-systemen
- private key-systemen
- public key-systemen

## Keyless-systemen

Er is enkel een wiskundig algoritme nodig, geen sleutel.

Het bericht wordt via een algoritme versleuteld en levert zo een onleesbare rij bits op. Het is zeer moeilijk om uit deze bitrij terug het origineel af te leiden.

De methode is zeer geschikt om controle uit te voeren door te vergelijken.

Voorbeeld: password op een computer

Passwords zijn meestal via een keyless algoritme versleuteld en zo opgeslagen op een disk. De hacker die het password vindt, beschikt alleen over de versleutelde passwords die onbruikbaar zijn.

Enkel door het juiste password in te voeren en daar weer dezelfde algoritme op los te laten, ontstaat een code die gelijk is aan het opgeslagen password wat verdere toegang tot het systeem verleend.

## Private key-systemen

Alles draait hier om een geheime sleutel, die nodig is bij het vercijferen en het ontcijferen. Hierdoor spreekt men ook over symmetrische algoritmen.

### DES

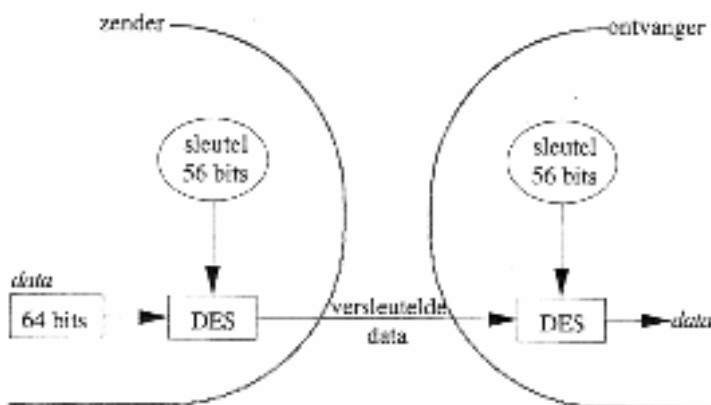
#### Data Encryption Standard

het bekendste symmetrische algoritme, ontwikkeld door IBM in 1977

*Bekende toepassingsvarianten zijn ECB en CBC*

**ECB** (Electronic Code Book - de eenvoudigste vorm):

Versleutelt datablokken van 64 bits, waarbij het een geheime sleutel van 56 bits gebruikt.



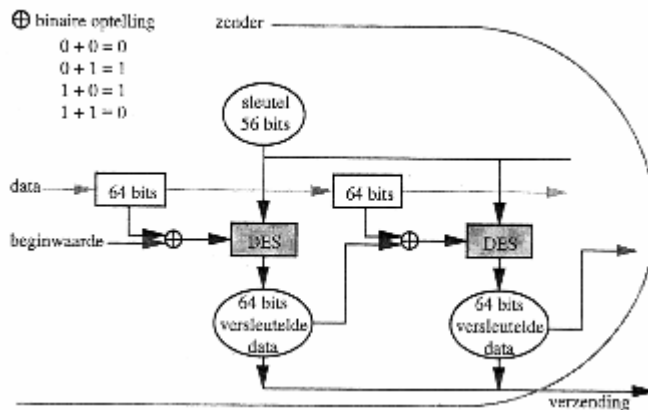
Is enkel te gebruiken voor:

- het vercijferen van passwords en pincodes
- het veilig oversturen van nieuwe -56-bits lange DES-sleutels

**CBC** (Cipher Block Chaining – voor encryptie van grotere blokken):

De data worden verdeeld in blokken van 64 bits

Het gecijferde resultaat wordt gebruikt voor cijfering van het volgende datablok



De methoden ECB en CBC noemt men ook blokvercijfering en gebruikt men om een gegevensblok binnen een toepassing te versleutelen.

Voor het versleutelen van een stroom bits, bv. aan de uitgang van een modem, wordt met kleine blokken van 1 byte (8 bits) gewerkt. Men spreekt dan van stroomvercijfering.

Het regelmatig wisselen van de sleutels is onderdeel van een goed sleutelbeheer en vergroot de veiligheid.

Om sleutels via datacommunicatie te verzenden gebruikt men een hiërarchie van sleutels.

De masterkey wordt handmatig in alle apparaten geladen, meestal door twee of drie mensen die elk een deel van de sleutel inbrengen. Deze sleutel gaat jaren mee.

De KEK (Key Encryption Key) wordt versleuteld met de masterkey en daarna verzonden. De KEK vervangt men frequenter dan de masterkey en dient om de DEK te versleutelen.

De DEK (Data Encryption Key) die dient om de data te vercijferen wordt regelmatig gewijzigd.

Hoe dieper de hiërarchie, hoe groter de veiligheid maar hoe complexer het sleutelbeheer.

## Public key-systemen

Bij public key-systemen gebruikt men twee sleutels; één om te versleutelen, één om te ontcijferen. Men spreekt daarom ook van asymmetrische systemen.

RSA-algoritme (de bekendste methode)

vernoemd naar de drie bedenkers: Rivest – Shamir – Adelman

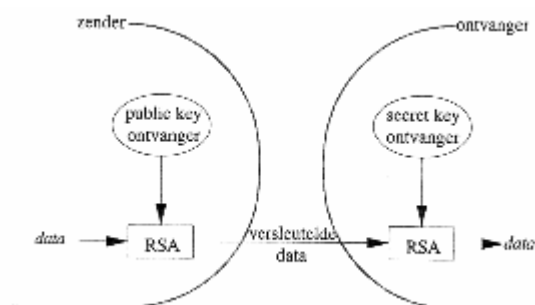
Iedere gebruiker heeft twee sleutels berekend uit grote priemgetallen (meer dan honderd cijfers):

- een public key en
- een secret key

De partij die deze sleutelparen aanmaakt en beheert is de trusted party (voornamelijk telecommunicatiebedrijven zijn geroepen).

Men bereikt nu vertrouwelijke communicatie tussen zender A en ontvanger B doordat de zender de public key bekend maakt aan de partners waarmee gegevens worden uitgewisseld.

encryptie: cipher text =  $E_p(\text{plain text})$ , waarbij  $E_p$  de public key van de ontvanger B is;  
 decryptie: plain text =  $D_s(\text{cipher text})$ , waarbij  $D_s$  de secret key van de ontvanger B is;



Met deze werkwijze weet de ontvanger alleen dat het bericht vertrouwelijk is, maar hij weet niet wie de afzender is.

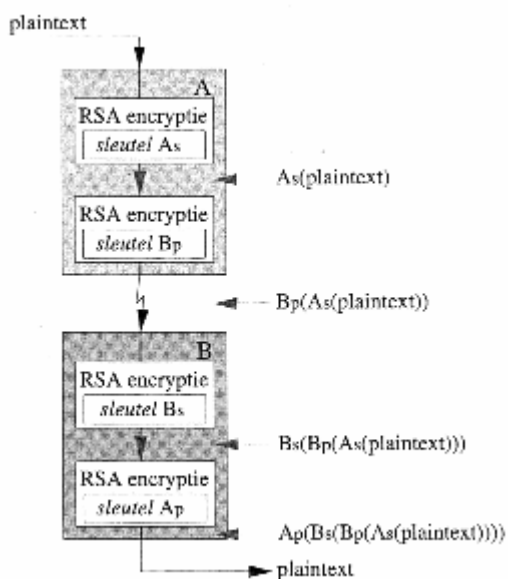
Indien men ook wil weten wie de afzender is kan men dit bereiken door een dubbele RSA-slag. Deelnemer A versleutelt twee keer:

- eenmaal met zijn eigen geheime sleutel
- eenmaal met de publieke sleutel van de ontvanger.

Bij de ontvanger vindt het proces plaats in de omgekeerde richting.

- $\text{cipher text} = B_p(A_s(\text{plain text}))$ , waarbij  $A_s$  de secret key van zender A en  $B_p$  de public key van ontvanger B is;
- $\text{plain text} = A_p(B_s(\text{cipher text}))$ , waar  $B_s$  de secret key van ontvanger B en  $A_p$  de public key van zender A is.

Door deze dubbele operatie weet ontvanger dat het bericht alleen van A kan komen, omdat gebruik van de public key van A uiteindelijk plain text oplevert.

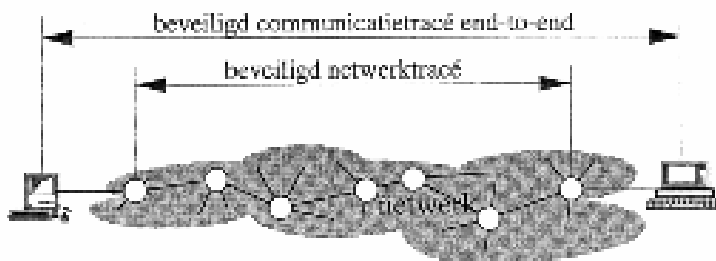


## Beveiliging en datacommunicatie

Bij beveiligen moet het duidelijk zijn welke risico's men beoogt en waar men de maatregelen in de communicatiekanalen wil implementeren. (Vermijd het dichtspijkeren van de voordeur en het oplaten van de achter-deur!).

Er zijn twee categorieën plaatsen van beveiliging:

- end-to-end encryptie
- link by link of netwerkencryptie



### end-to-end encryptie

De beveiligingsmaatregelen worden getroffen in de toepassing. Veel beveiligingssystemen zijn hierop gebaseerd bv. digitale handtekeningen en password-encryptie.

Softwaremodules zijn te koop en kunnen relatief eenvoudig geïmplementeerd worden.

End-to-end encryptie kan men implementeren boven op de link-by-link of netwerk-encryptie om de beveiliging verder op te voeren

### link by link of netwerkencryptie

Hier wordt de beveiliging onder in de protocol-stapel geregeld.

Als beveiligingsfuncties alleen in het netwerk zijn geïmplementeerd, zijn extra maatregelen nodig op het tracé eindstation-netwerk

## Netwerkfraude

In een wereld waar steeds meer gekoppeld en verbonden wordt is beveiliging van het netwerk nodig:

- ter beveiliging van de applicatie, maar ook
- van het netwerk zelf

Controle op toegang tot het netwerk is een eerste stap maar er is meer nodig.

Bekende vormen van netwekfraude komen voor bij mobiele netwerken, bij betaal-TV, telefoonkaarten, enz.

Bekende gevolgen hiervan zijn:

- spookrekeningen
- verlies aan inkomsten van de netwerkexploitant
- gerommel met eind-apparatuur