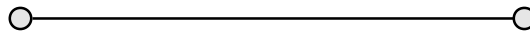
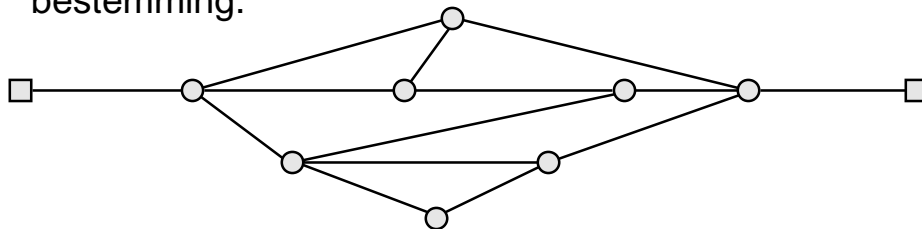

5. De netwerklaag

De functie van de netwerklaag

- De datalink brengt frames van het ene punt van een transmissiekanaal naar een ander.



- De netwerklaag brengt pakketten van bron naar bestemming.



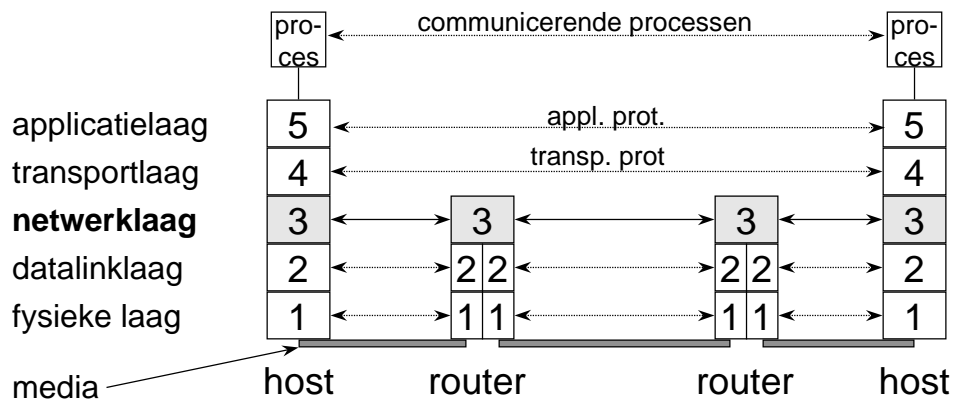
□ Station (*host*)

○ Knooppunt (*router*)

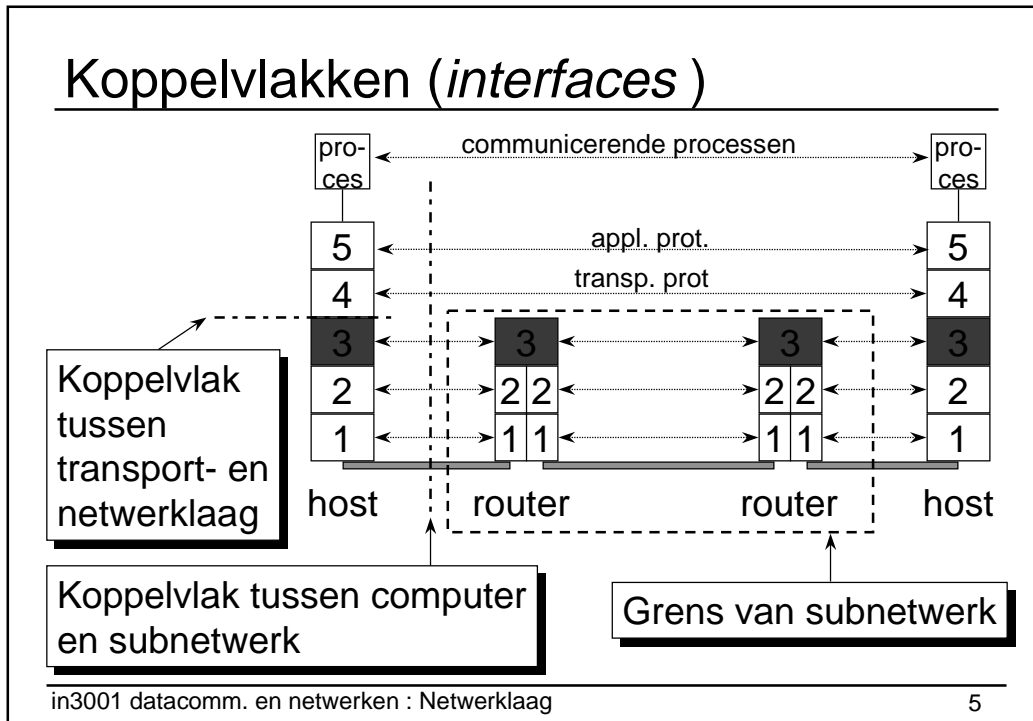
Taken van de netwerklaag

- Een pad van bron naar bestemming door het subnet zoeken (kennis hebben over de topologie).
- Routes zo kiezen dat het netwerk gelijkmatig belast wordt.
- Pad zoeken indien bron en bestemming in verschillende (gekoppelde) netwerken liggen.
- De problemen door verschillen tussen netwerken oplossen.

Plaats van de netwerklaag

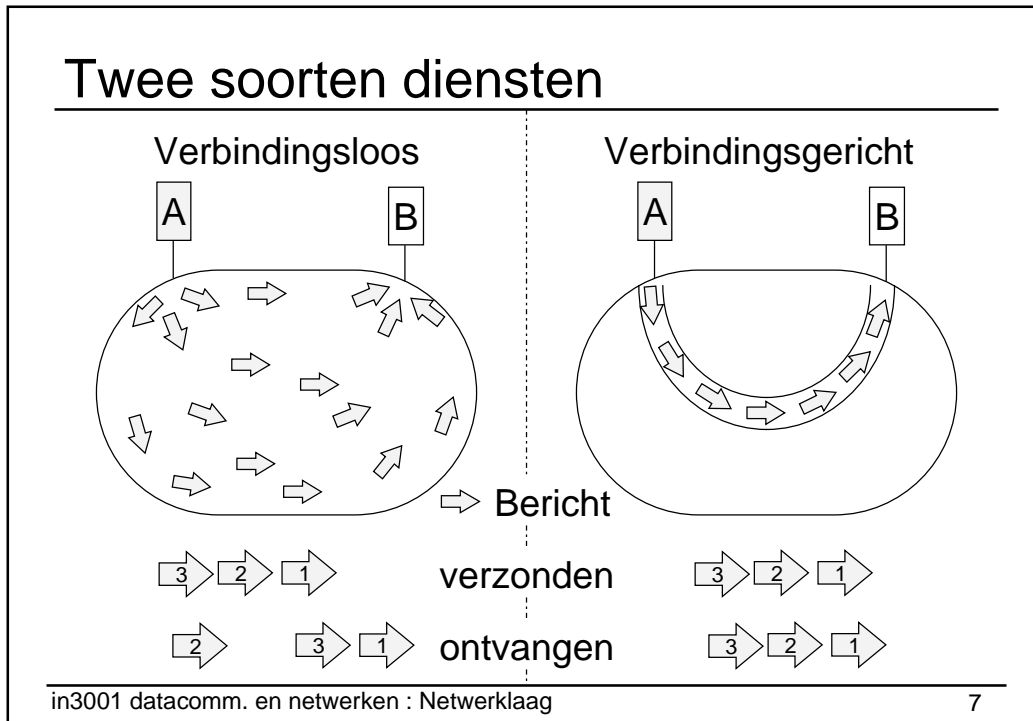


- Netwerklaag de laagste laag die zich bezighoudt met transmissie van eind tot eind, zij doet dat echter stapsgewijs.
- Transportlaag en applicatielaag doen dat direct van eind to eind.



5.1 Ontwerpaspecten v.d. netwerklaag

- De geleverde diensten moeten onafhankelijk zijn van de gebruikte technieken in het subnet
- De transportlaag moet afgeschermd zijn voor
 - het aantal subnetten tussen de eindstations
 - type van de subnetten
 - topologie van de subnetten
- De netwerkadressen moeten volgens een uniform nummerplan zijn dat zowel LAN's en WAN's beslaat



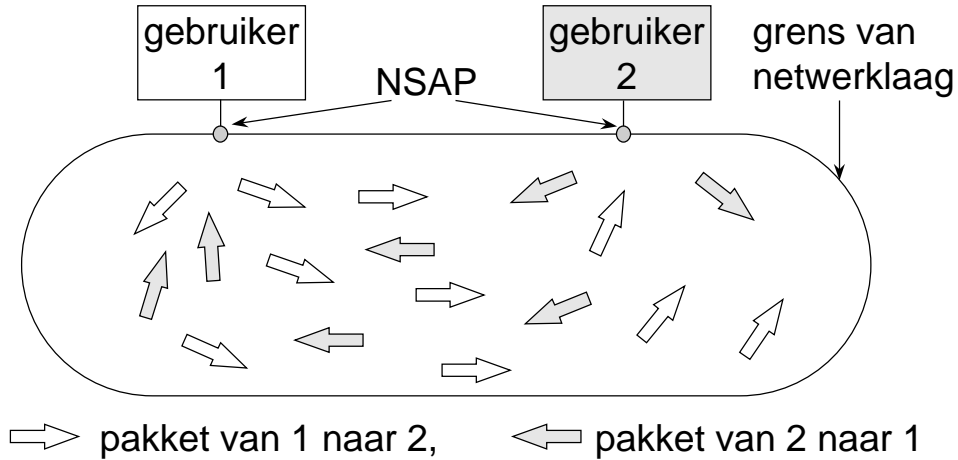
Diensten aan de transportlaag (1)

Verbindingsloos

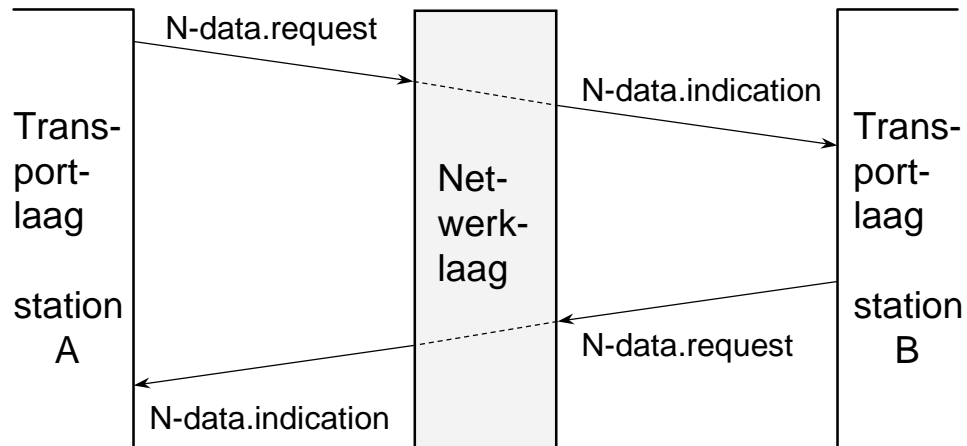
- primitieven: N-data.request (zend pakket)
 N-data.indication (ontvang pakket)
- geen stroombeheersing
- geen volgordebewaking
- complexiteit zit in de stations (transportlaag), niet in de stations.

Verbindingsloze dienst

- Beeld dat de gebruikers (transportentiteiten) hebben van het netwerk:



Verbindingsloze primitieven

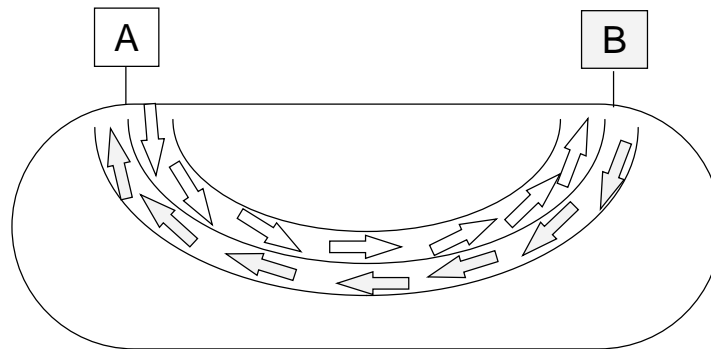


Diensten aan de transportlaag (2)

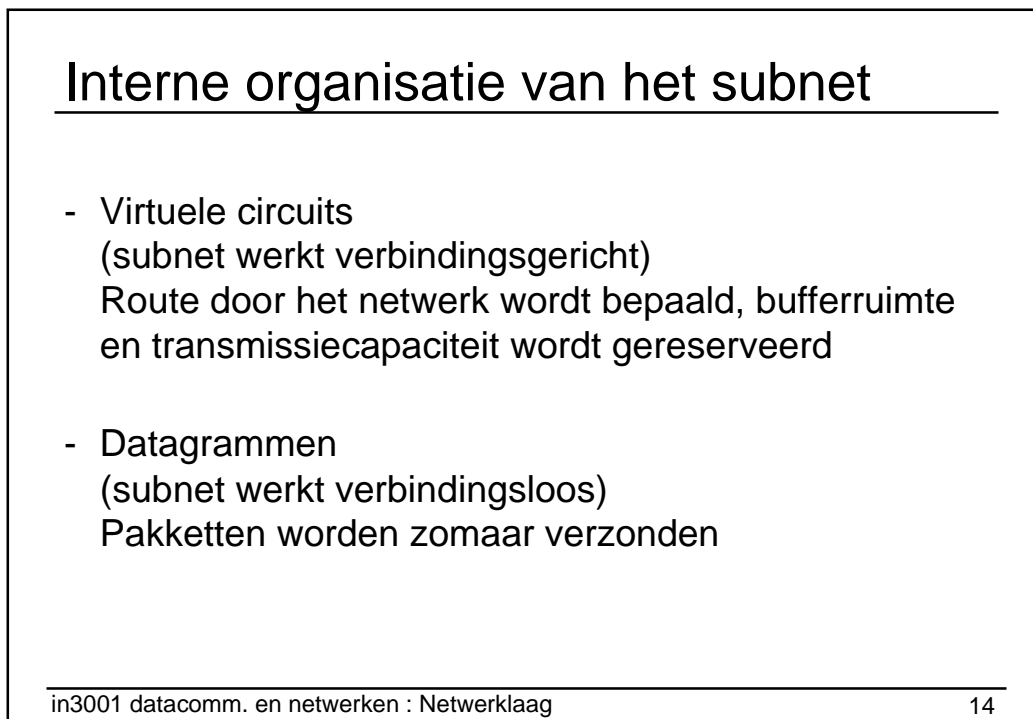
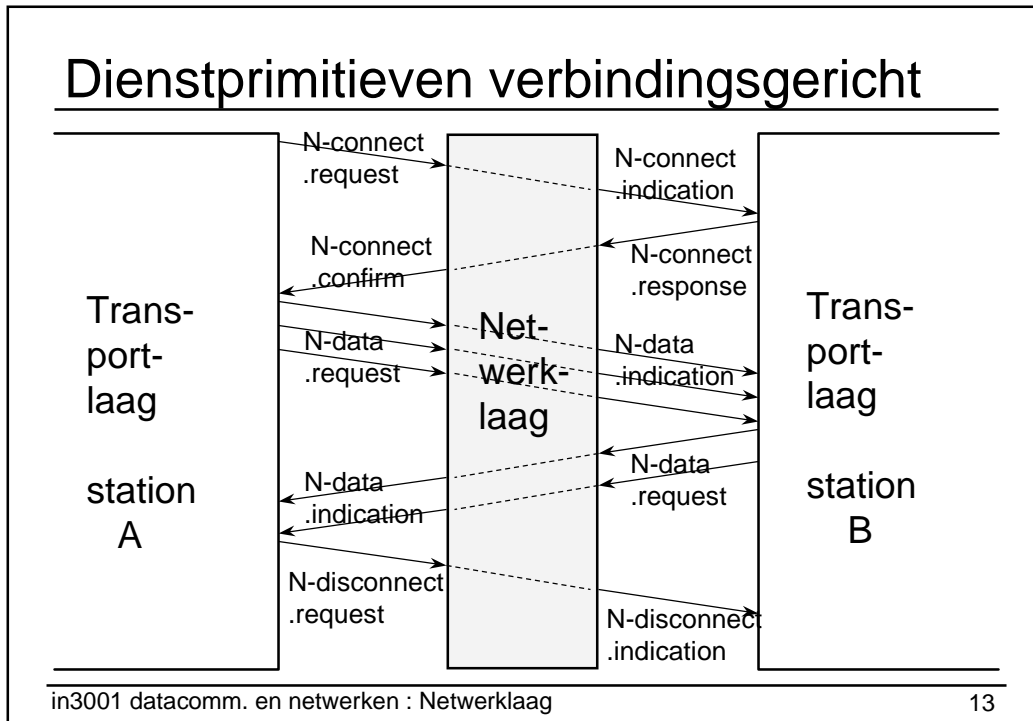
Verbindingsgericht

- Opzetten verbinding
- Onderhandelen over kwaliteit en kosten van de dienst (bv. snelle of nauwkeurige bezorging)
- full-duplex communicatie
- pakketten in volgorde afgeleverd
- stroombeheersing tussen zender en ontvanger
- naar keuze: gegarandeerde bezorging, bevestiging door subnet, prioriteit.
- verbreken van de verbinding na afloop
- complexiteit zit in het subnet, niet in de stations

Verbindingsgerichte dienst



Verbinding = kanaal met het karakter van een wachtrij
(FIFO)



De twee soorten pakketschakelen

Virtuele circuits

Datagrammen

Let op!
Een pakket wordt pas weer uitgezonden als het geheel binnen is.

in3001 datacomm. en netwerken : Netwerklaag 15

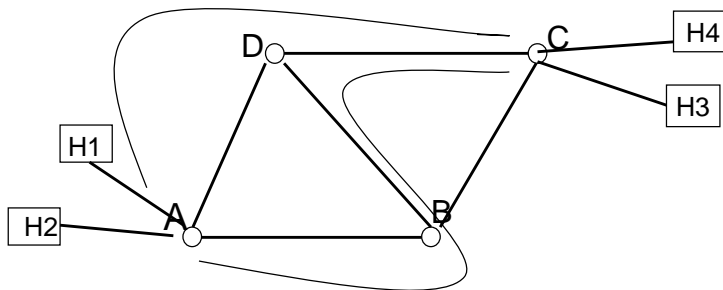
voorbeeld: datagrammen

- Router tabellen (bijvoorbeeld)
- router A

	router B	router D
A	A A	A D
B	B -	B B
C	C D	C C
D	D D	D -

in3001 datacomm. en netwerken : Netwerklaag 16

voorbeeld Virtual Circuits



router A		router B		router D		router C	
IN	UIT	IN	UIT	IN	UIT	IN	UIT
H1	1	D	1	A	1	D	1
H2	1	B	1	B	1	C	2

De twee netwerktechnieken

aspect	datagram-subnet	v.c.-subnet
opzetten circuit	niet mogelijk	vereist
adressering	elk pakket bevat geheel bron- en doeladres	elk pakket bevat kort v.c.-nummer
status-informatie over verbinding	subnet bevat geen status-informatie	Elk v.c. vereist tabelruimte in knooppunten
routing	elk pakket apart	route bepaalt bij opzetten van verb.
effect van fout in knooppunt	slechts verlies van pakketten	alle v.c.'s door uitgevallen knooppunt worden afgebroken
congestie beheersing	moeilijk	gemakkelijk; voor elk gemaakt v.c. wordt bufferruimte gemaakt

5.2. Routing

Eisen:

- Eenvoudig
 - Correct
 - Robuust
 - Stabiel
 - Rechtvaardig
 - Optimaal
- ← Kan tegenstrijdig zijn
- ← Kan tegenstrijdig zijn

Robuust <-> stabiel

Robuust wil zeggen bestand tegen wijzigingen in de topologie, uitvallende lijnen etc.

Stabiel wil zeggen het algoritme is niet steeds zeer snel na elkaar routes aan het wijzigen

Robuustheid vraagt snel ingrijpen, dat kan instabiliteit in het netwerk veroorzaken, bijvoorbeeld doorlopend verleggen van routes.

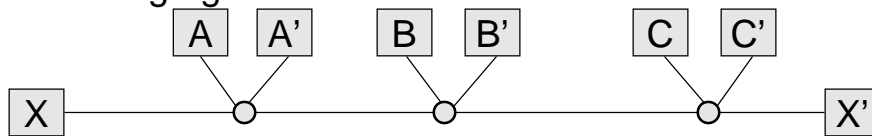
(pakketten kunnen in het ergste geval gaan zwerven door het netwerk of zelfs rondjes afleggen.)

Rechtvaardig <-> optimaal

Optimaliseren naar bijvoorbeeld

- Totale doorvoer
- Gemiddelde vertraging
- Optimale totale doorvoer kan onrechtvaardig zijn voor sommige gebruikers:

Kan op zich ook tegenstrijdig zijn



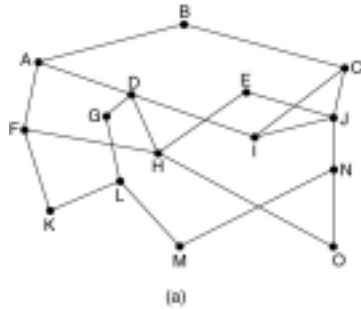
Voorrang geven aan A-A', B-B' en C-C' is goed voor de prestatie van het netwerk als geheel, maar niet voor X-X'.

Optimaliteitsprincipe (1)

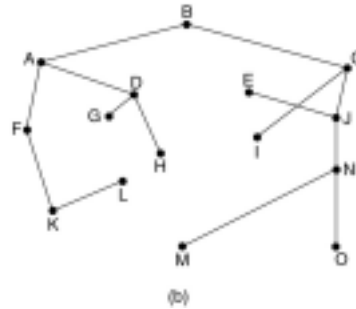
Het *optimaliteitsprincipe*

- Als J ligt op het optimale pad van I naar K, dan is het optimale pad van J naar K, onderdeel van het optimale pad van I naar K
- Een *Sink tree* van een bestemming X is een verzameling van optimale routes naar X. Hierbij is X de root van de boom.

Optimaliteitsprincipe (2)



Een netwerk



Een sinktree voor B
(niet uniek)

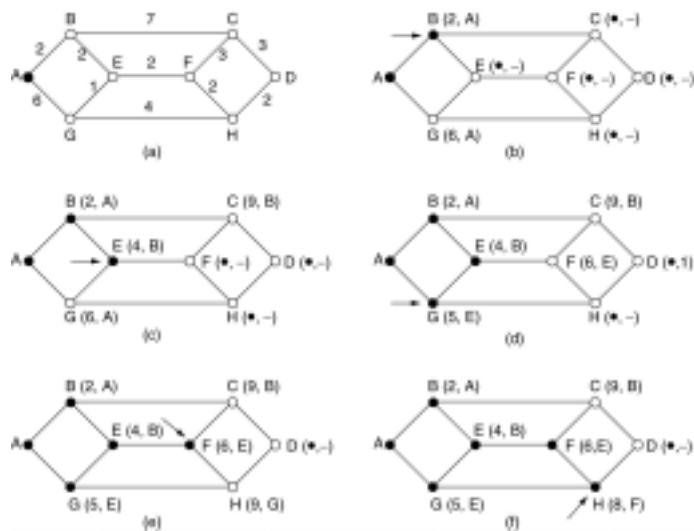
5.2.2 Shortest path routing (1)

- Doel: kortste paden van een router naar alle andere routers bepalen.
- metriek ('lengtemaat') te kiezen, b.v.
 - aantal hops
 - afstand in km's
 - gemiddelde vertraging
 - kosten
- Algoritme van Dijkstra

Shortest path routing (2)

- gaat uit van een graaf, iedere tak heeft een lengte
- kies een beginknoop
- iedere knoop bevat afstand tot beginknoop
 - aanvankelijk een tijdelijke waarde
 - later definitieve waarde
- begin bij beginknoop
- geeft buurknopen tijdelijke waarde (geef hierbij ook de vorige knoop op de bijbehorende route aan)
- knoop met minimale afstand krijgt definitieve waarde
- ga verder bij de knoop met de laagste definitieve waarde, etc

Shortest path routing (3)



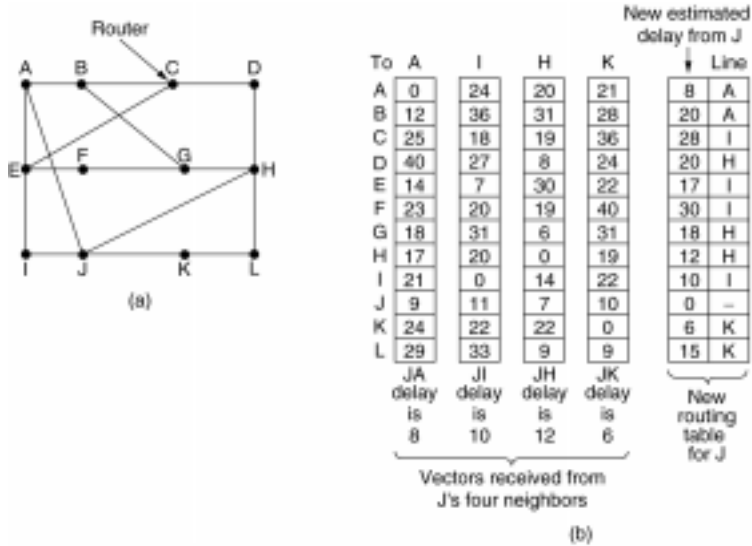
5.2.3 Flooding

- principe: ieder pakket wordt uitgezonden over iedere uitgaande lijn
- duplicaten verminderen door
 - hop count
 - sequence nummers
- variant: *selective* flooding
 - pakketten alleen uitzenden over uitgaande lijnen die ongeveer de goede kant uitgaan
- toepassingen van flooding b.v.
 - militaire systemen
 - gedistribueerde databases
 - radio netwerken
 - vergelijking met andere algoritmen

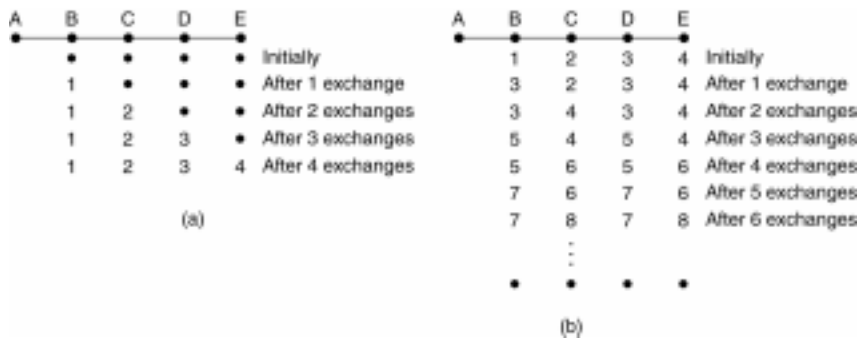
5.2.4 Distance Vector Routing (1)

- ook aangeduid als: Bellman-Ford of Ford-Fulkerson, in (vroeger) Internet: RIP
- Iedere router bevat een tabel met voor iedere mogelijke bestemming (router) een entry, deze entry bevat:
 - te nemen uitgaande lijn voor die bestemming
 - geschatte afstand naar die bestemming
- Onderhoud van de tabel:
 - iedere router kent de afstand tot zijn burens
 - Iedere T seconden zendt iedere router zijn volledige tabel naar zijn burens
 - Een router die zo'n tabel ontvangt, werkt zijn tabel bij en houdt hierbij rekening met de afstand naar de buur van wie hij de tabel ontving

Distance Vector Routing (2)



Distance Vector Routing (3)



Count to infinity

Link State Routing (1)

1. Ontdek buren

Hello pakket

2. Meet "afstand" naar de buren

Echo pakket

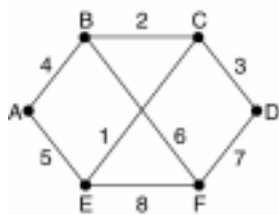
vraag: wel/geen rekening houden met de load

- voor: betere spreiding van verkeer mogelijk
- tegen: oscillaties mogelijk

3. maak link-state pakketten, met

- bron
- sequencenummer
- age
- lijst van buren plus afstand

Link state routing (2)



(a)

	Link	State	Packets
A	B	C	D
Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age
B 4	A 4	B 2	C 3
E 5	C 2	D 3	F 7
	F 6	E 1	
			E
			Seq.
			Age
			A 5
			C 1
			F 8
			F
			Seq.
			Age
			B 6
			D 7
			E 8

(b)

Link-state pakketten

Link State Routing (3)

4. Verstuur de link-state pakketten naar iedere andere router in het netwerk

- basis: flooding
- iedere router bepaalt op grond van bron en sequencennummer of een link-state pakket wordt doorgestuurd.
 - mogelijke probleem:
 - fout in een sequencennummer
 - oplossing d.m.v. age
- alle pakketten bevestigen

Link State Routing (4)

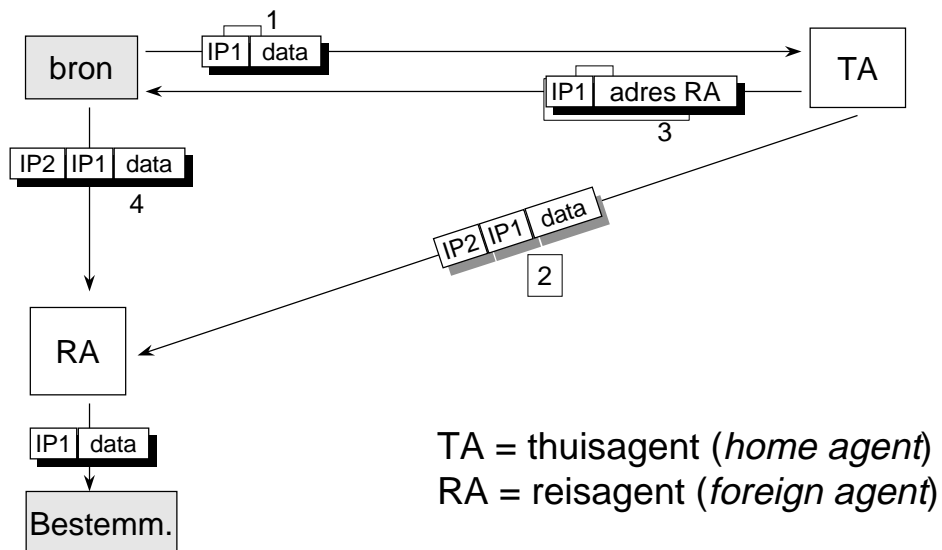
Source	Seq.	Age	Send flags			ACK flags			Data
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Link State Routing (5)

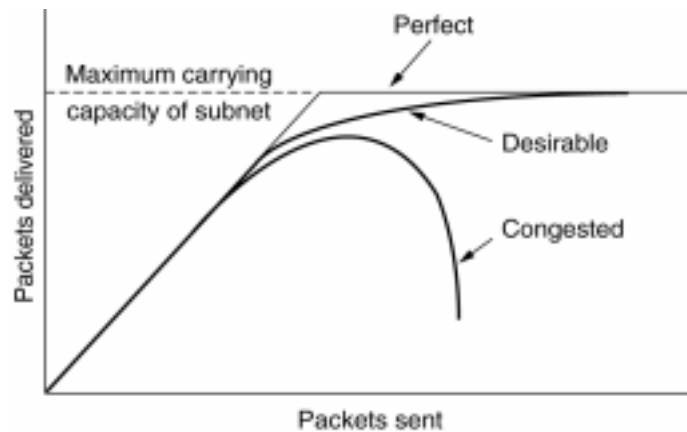
5. Bereken nieuwe route

- Dijkstra's shortest path algoritme
- benodigd geheugen
 - bij n routers met gemiddeld k buren,
van orde nk
- problemen:
 - geheugengrootte
 - rekestijd
 - falende routers

5.2.9 Routeren bij mobiele stations



5.3 Congestie (1)



Bij congestie stort de capaciteit van het netwerk in als de belasting toeneemt

Oorzaken congestie

- Aanbod aan pakketten $>$ verwerkingscapac. router
 - geheugen te klein
 - processor capaciteit te laag
- Aanbod aan pakketten $>$ capac. uitgaande lijnen van een router
- Lokale congestie:
aantal pakketten naar router $>$ uit router
- Subnetcongestie:
aantal pakketten naar subnet $>$ uit subnet

Congestie- en stroombeheersing

Vaak worden stroombeheersing en congestie met elkaar verward.

- Stroombeheersing is afstemmen van de snelheid van de zender op de snelheid van de ontvanger
- Soms wordt stroombeheersing gebruikt om congestie te bestrijden.
 - Knooppunten in het netwerk zenden berichten naar zenders om ze te laten stoppen met zenden.

Congestiebeh. zonder terugkoppeling (open loop)

Beslissen zonder de toestand in de rest van het netwerk in acht te nemen.

- "Ruim" ontwerp;
- Wanneer nieuw verkeer aannemen;
- Wanneer en welke pakketten weggooien;
- Dienstregelingen op diverse plaatsen in het net.

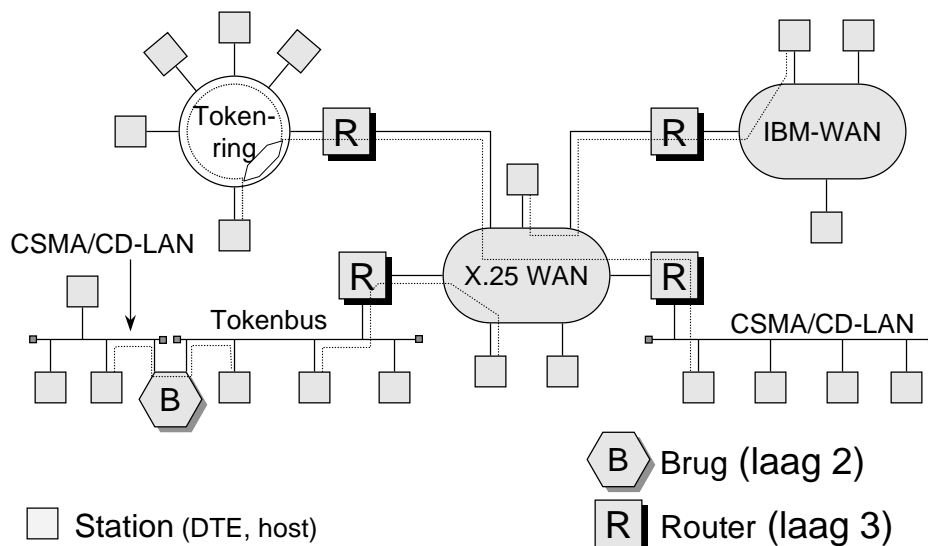
Congestiebeheersing met terugkoppeling (closed loop)

- Bewaken van het net op congestie;
- Info doorgeven naar de aangrijppunten in het net;
- Correctie van de werking van het netwerk om het probleem te verhelpen.
- Stabiliteit vaak niet eenvoudig

Terugkoppeling mogelijk:

- Expliciet: Pakketten met opdrachten naar de bron sturen
- Impliciet: De bron lijdt congestie af uit lokale waarnemingen

5.5 internetworking

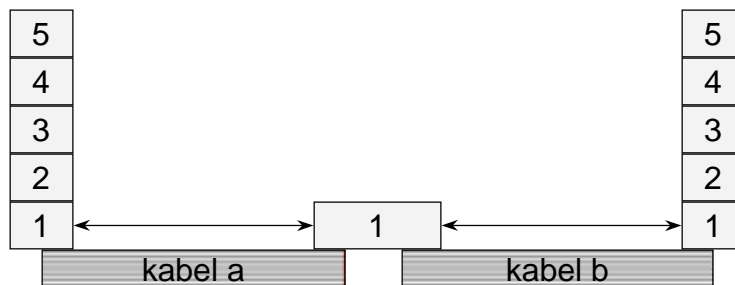


Vijf soorten relais

Indeling naar OSI-laag waarop gekoppeld wordt:

- Laag 1 repeater
- Laag 2 brug
- Laag 3 router of multiprotocol-router
- Laag 4 transport gateway
- Laag 5 applicatie gateway

Repeater (koppelen op laag 1)

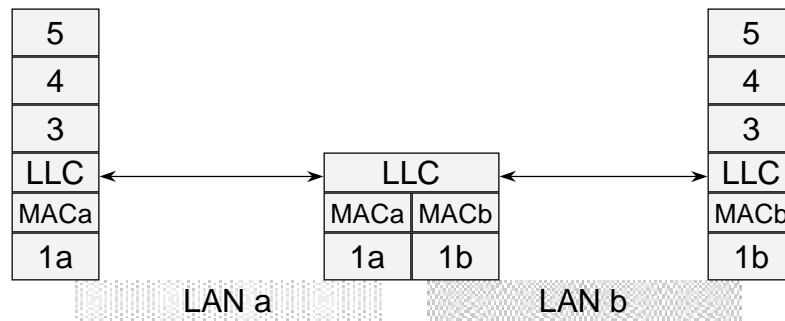


Koppelt kabelsegmenten.

Leest signalen in, reconstrueert de bits en zendt ze door.

Compenseert verzwakking van het signaal bij lange lijn.

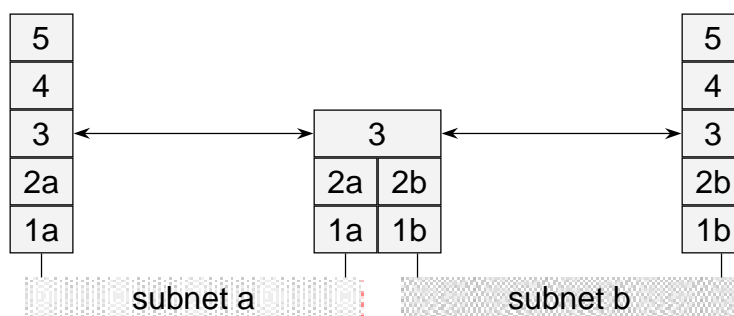
Brug (koppelen op laag 2)



Koppelt LAN's.

Leest frames (DL-PDU's) in, slaat ze op en zendt ze door.

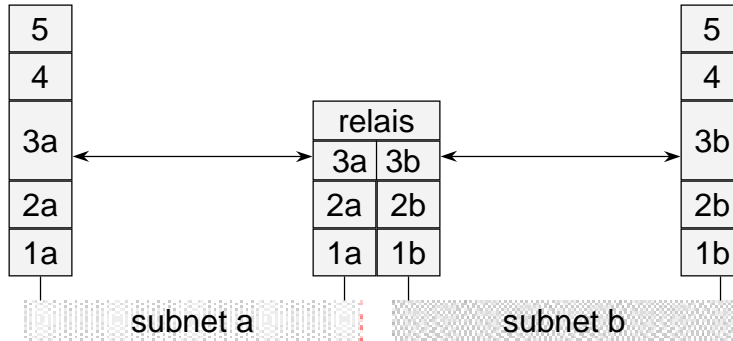
Routers (koppelen op laag 3)



Koppelt netwerken met een zelfde netwerkprotocol en gedeelde adresruimte.

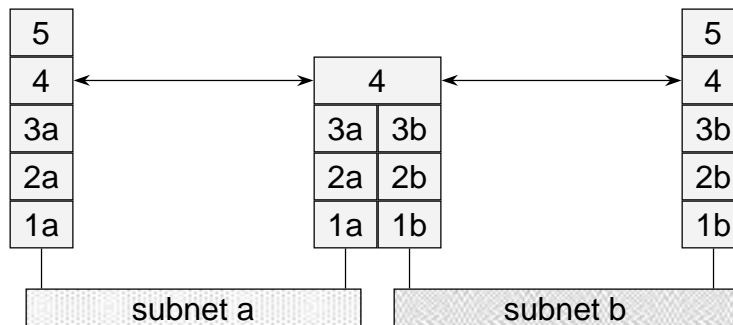
Leest pakketten (N-PDU's) in, slaat ze op en zendt ze door.

Multiprotocol-routers (koppelen op laag 3)



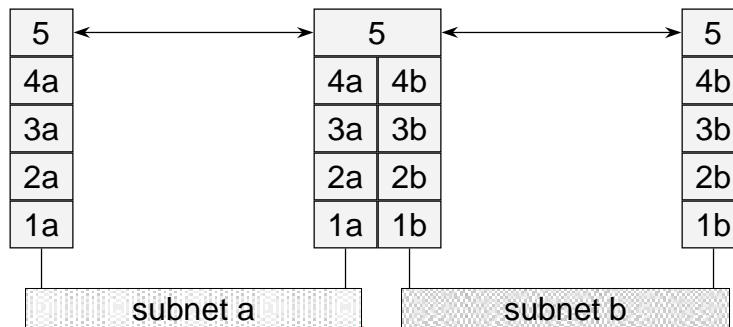
Koppelt netwerken met een verschillend netwerkprot.
 Leest pakketten (N-PDU's) in, slaat ze op, zet ze om
 en zendt ze door.
 (relais: omzetten, adressen vertalen, doorzenden en routeren)

Transport gateway (koppelen op laag 4)



Koppelt netwerken die verschillend transportprotocol
 hebben.
 Leest T-PDU's in, slaat ze op en zendt ze door.

Applicatie gateway (koppelen op laag 5)



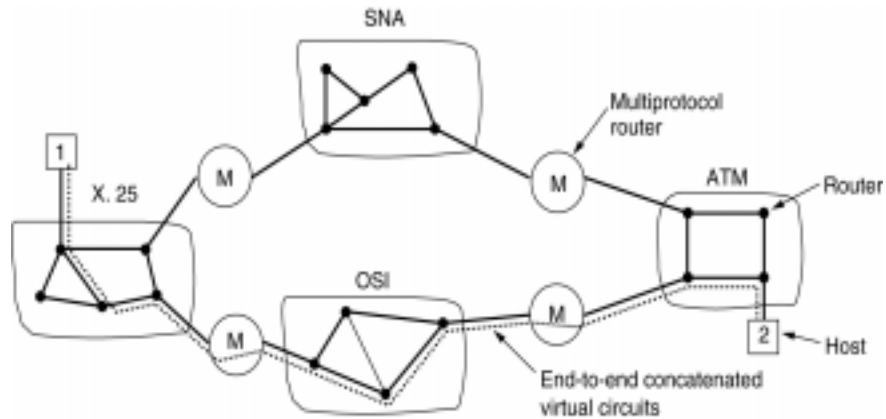
Leest A-PDU's in, slaat ze op en zendt ze door (evt. na conversie).

Bijv. doorgeven van E-post tussen netwerken die niet een gezamenlijk netwerk- of transportprotocol hebben.

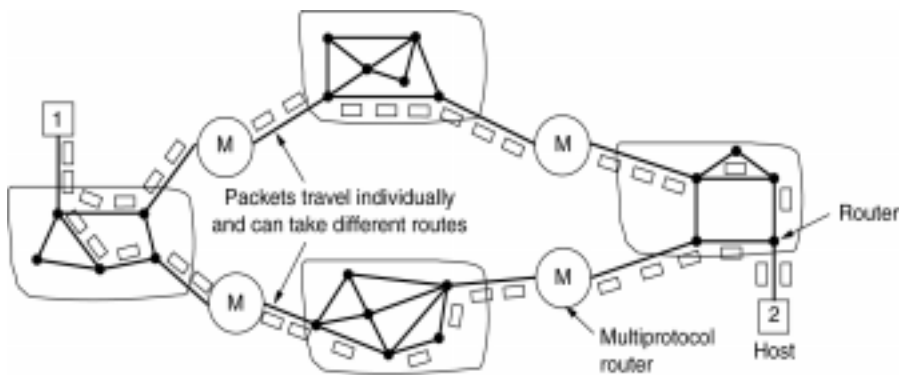
Vormen van internetworking

- Geconcateneerde Virtual Circuits
 - internet VC bestaat uit aaneenschakeling van subnet VC's en VC's via multiprotocol routers (gateways)
 - werkt het best bij subnetten met ongeveer gelijke eigenschappen
 - Voor en nadelen als bij subnet VC's
- Verbindingsloos
 - datagrammen kunnen via verschillende subnetten worden overgebracht
 - voor en nadelen als bij subnet datagrammen

Concatenated VC's

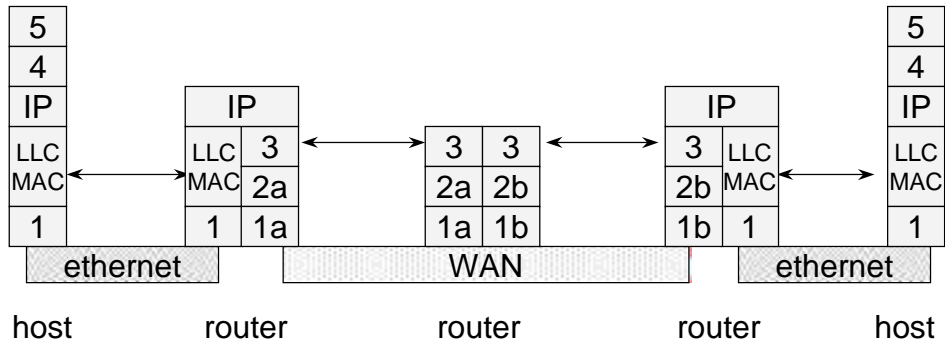


Verbindingsloos internetwerken

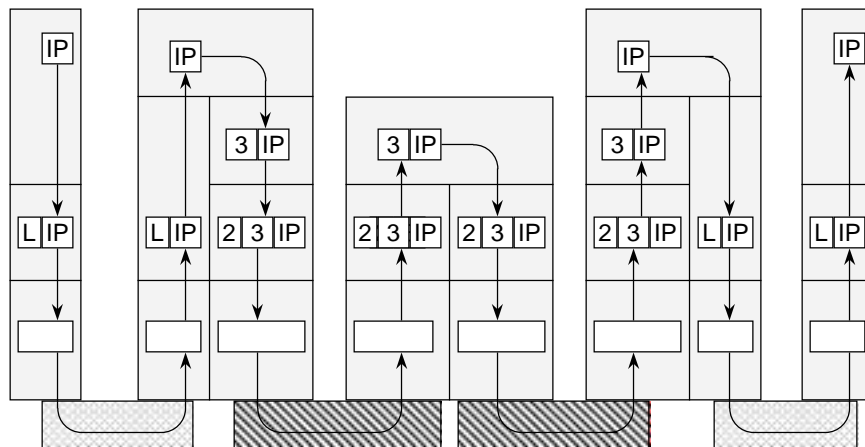


Tunneling van b.v. een IP-pakket

Het IP-pakket wordt getransporteerd over het WAN in een pakket dat hoort bij het protocol van het betreffende WAN.



Tunneling van een IP-pakket (PDU-s)



- IP Internetaanpak
- L Kop en staart van LLC+MAC
- 3 Kop van netwerkprotocol
- 2 Kop en staart van DL-prot.

internet routing

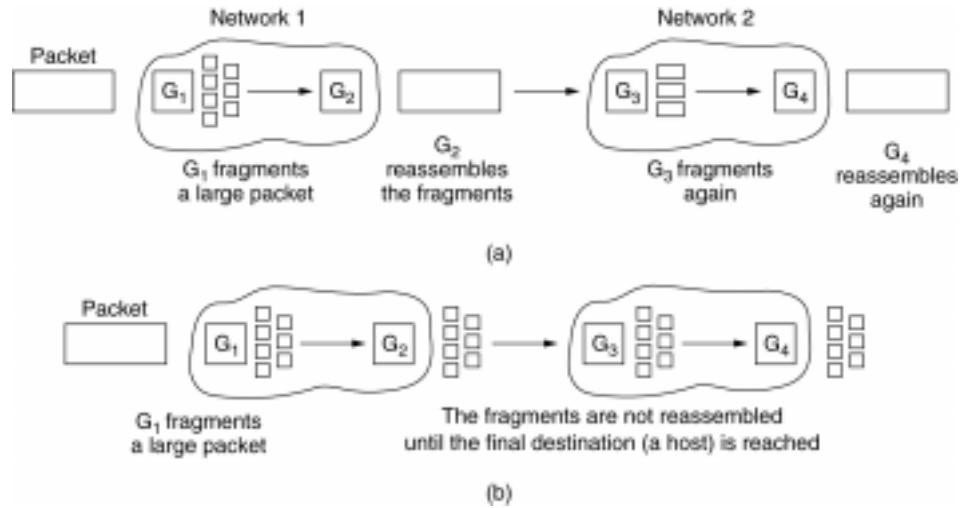
twee niveaus

- Binnen netwerk: Interior gateway protocol
netwerk vaak aangeduid als *Autonoom Systeem*,
kan zelf zijn routeringsalgoritme kiezen
- Tussen netwerken: exterior gateway protocol
 - iedere multiprotocol router R kan “direct”
communiceren met alle routers verbonden met
netwerken verbonden met X
 - internetwork routing heeft ook te maken met
politiek. Verschillende landen, verschillende wetten
en regimes.

Fragmentatie (1)

- Fragmentatie nodig wanneer verschillende
netwerken verschillende maximum pakketgrootte
hebben.
- Gateway splitst te groot pakket in fragmenten
- vraag: wanneer reassembleren?
 - Na passeren van het eerste netwerk (*transparante
fragmentatie*)
nadeel: overhead, misschien weer fragmenteren
bij volgen netwerk
 - In de eindbestemmings host (*niet transparant*)
nadeel: iedere host moet kunnen reassembleren

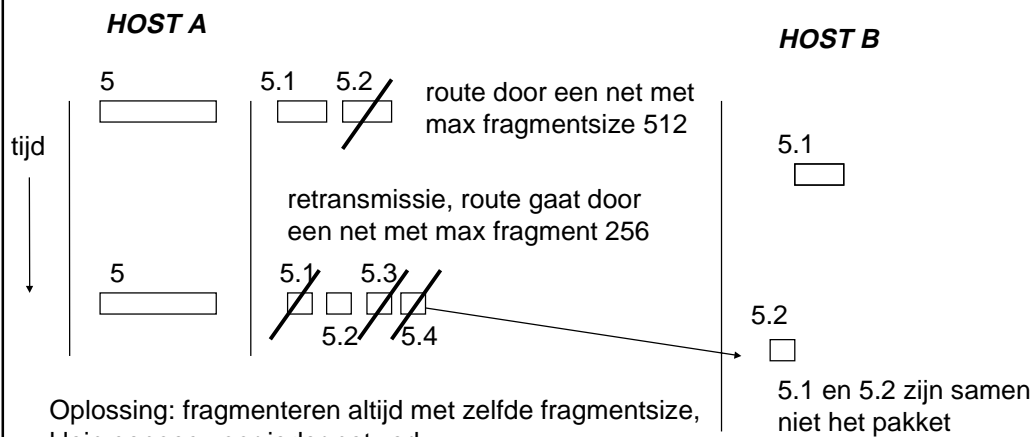
Fragmentatie (2)



Fragmentatie (3)

Probleem bij reassembleren in de eindhost:

- fragmentnummering, en hoe om te gaan met ontbrekende fragmenten

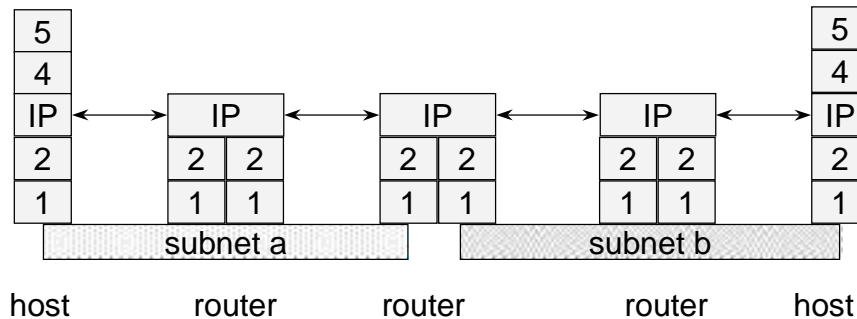


5.6 De netwerk laag in het Internet

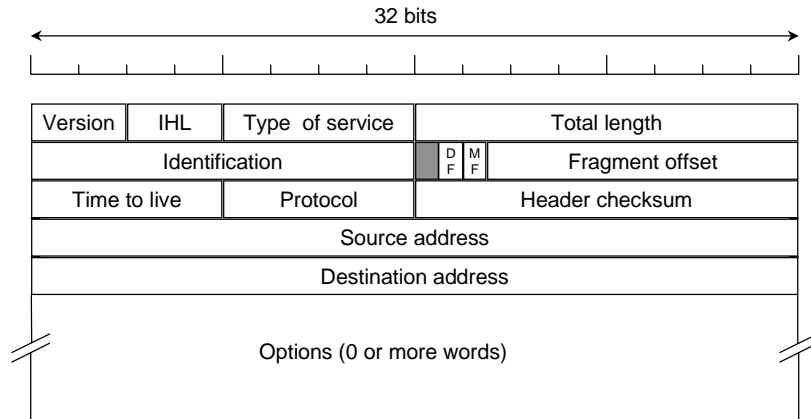
- *Backbones* (ruggesgraten)
 - snelle knooppunten
 - snelle lijnen (momenteel 155 of 622 Mbit/s en hoger)
- Autonome systemen (AS's)
 - Regionale of nationale netwerken
 - LAN's

Internetprotocol (IP)

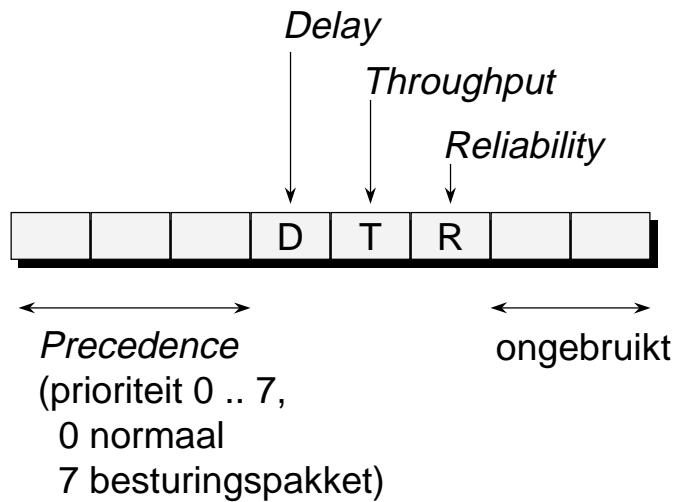
IP is het netwerkprotocol op alle routers van de netwerken.



Internet Protocol versie 4 (IPv4)



Type of service veld



Options veld

- *Security* - Geeft aan hoe geheim het bericht is.
Wordt in de praktijk genegeerd.
- *Strict source routing* - Geeft het complete te volgen pad
- *Loose source routing* - Geeft een aantal routers die in die volgorde aangedaan moeten worden
- *Record route* - Adres van routers die aangedaan zijn wordt aan het *Options* veld toegevoegd
- *Timestamp* - Adres + tijdstip van routers die aangedaan zijn wordt toegevoegd

5.6.2 IP adressen (1)

klasse		# netw.	# hosts
A	0 7 24 <input style="width: 100px; height: 15px; border: 1px solid black;" type="text"/>	128	16 M
B	10 14 16 <input style="width: 100px; height: 15px; border: 1px solid black;" type="text"/>	16384	64 K
C	110 21 8 <input style="width: 100px; height: 15px; border: 1px solid black;" type="text"/>	2097152	256
D	1110 28 <input style="width: 100px; height: 15px; border: 1px solid black;" type="text"/>		multicasting
E	11110 27 <input style="width: 100px; height: 15px; border: 1px solid black;" type="text"/>		reserved for future use

IP adressen (2)

- IP adressen meestal weergegeven in 4 groepen van 1 tot 3 decimalen, b.v. 130.161.158.218
- Speciale adressen
 - alleen nullen, betekent: 'dit netwerk' of 'deze host'
 - alleen enen voor host adres betekent broadcast in het aangegevn netwerk
 - 127.xx.yy.zz betekent *loopback*
- netwerkadressen worden uitgegeven door het ICANN (Internet Corporation for Assigned Names and Numbers), deze delegeert weer aan regionale organisaties

IP adressen (3) Subnetting

Binnen een netwerk subnetten te definiëren

- alleen intern zichtbaar
- subnet gedefinieerd door subnet mask

voorbeeld

tudelft, netwerk adres	130.161	(in hex)	82 A1
mogelijk subnet mask	255.255.240.00		FF FF F0 00
(alternative notatie: /20)			
Stel inkomend adres:	130.161.158.218		82 A1 9E DA
AND met subnetmask geeft	130.161.9.0		82 A1 90 00

subnet

IP adressen (4) CIDR

CIDR = Classless InterDomain Routing

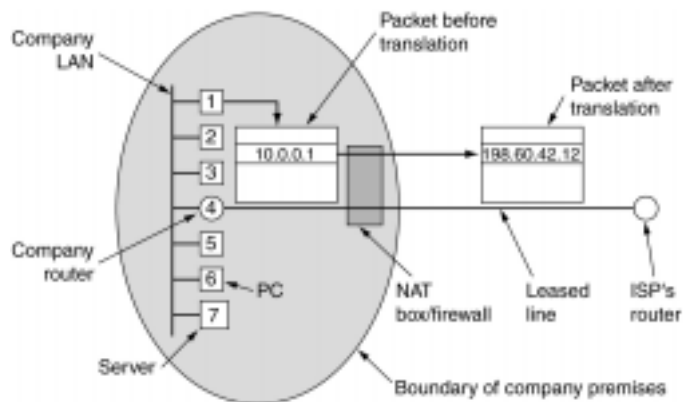
- adressen toegewezen in blokken ipv volledige netwerken
- netwerk aanduiden met beginadres/k
(/k is subnet mask, k is aantal 1-bits links, gevolgd door 0-bits)
- entry in routertable bevat netwerk adres = subnet mask
- op te zoeken adres wordt geAND met subnetmask, er is een hit wanneer resultaat klopt met begin adres
- meerdere hits bij een inkomend pakket zijn mogelijk, de hit met de grootste waarde van k, is de juiste

IP adressen (5) NAT

NAT = Network Adress Translation

- Is oplossing voor gebrek aan IP adressen voor Internet Service Providers.
- Idee:
 - verschillende grote klanten, gebruiken intern ieder dezelfde adresgroepen. (deze groepen zijn voor dit doel aangewezen)
 - naar buiten (naar de ISP) heeft de klant maar een adres.
 - bij binnenkomst en verlaten van het klant-netwerk vindt vertaling plaats in NAT-box

IP adressen (6) NAT (vervolg)



company address = 198.60.42.12

IP adressen(7) NAT (vervolg)

- vraag: hoe weet NAT box voor welk intern adres een antwoord bestemd is?
- oplossing: "misbruik" poortnummerveld in TCP en UDP headers
 - vervang bij uitgaand pakket sourcepoort door een index in een vertaaltabel.
 - entry in vertaaltabel bevat oorspronkelijke adres van source en poortnummer
 - pas ook CRC in TCP of UDP header aan!
- Bij ontvangst van een pakket, vertaal naar intern adres met behulp van "poortnummer" en vertaaltabel

5.6.3 Internet Control Protocollen

- ICMP (Internet Control Message Protocol)
 - t.b.v rapportage en testen
- ARP (Address Resolution Protocol)
 - voor het vinden van Ethernet-adressen bij IP-adres
- RARP (Reverse Address Resolution Protocol)
 - voor het vinden van het Internet-adres bij een Ethernet-adres
- BOOTP
 - voor bepalen van IP-adres
- DHCP (Dynamic Host Configuration Protocol)
 - voor het krijgen van een IP adres

Internet Message Control Protocol (ICMP)

- rapporteert over events in het netwerk
- de belangrijkste berichttypen:

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Address Resolution Protocol (ARP)

Bepaalt Ethernet adres bij IP-adres

Probleem

- Pakket komt in juiste router op grond van IP-adres (32 bits, bepaald door Internet structuur)
- Moet via Ethernet adres naar goede machine (48 bits, bepaald door fabrikant Ethernetkaart)

Werkwijze

- router doet broadcast in LAN:
“Wie heeft dit IP-adres?”
- Het juiste station meldt zich en geeft zijn Ethernet adres

Reverse Address Resolution Protocol

Starten van een werkstation zonder vaste schijf

- Werkstation *broadcasts* een pakket met Ethernetadres en vraagt om zijn IP-adres
- Een server met RARP erop zendt IP-adres naar werkstation

Voordeel:

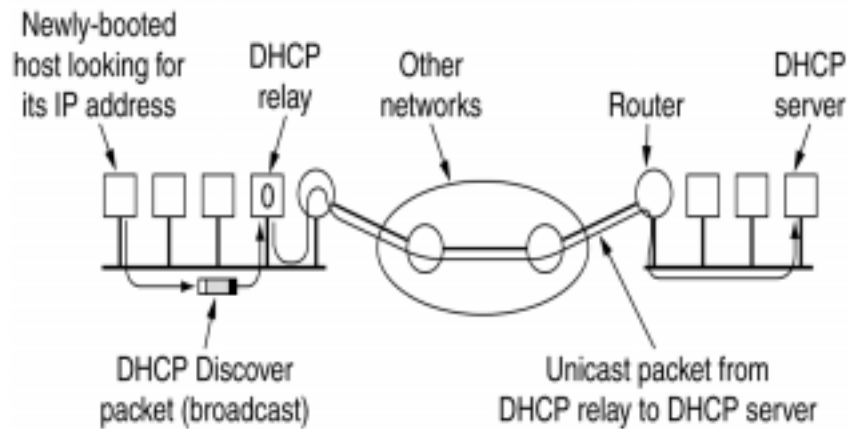
- Zelfde *memory image* in al werkstations op subnet

Nadeel:

- *Broadcast* op eigen subnetwerk (allemaal enen) => Elk subnetwerk heeft een server nodig met RARP

DHCP

Kan dynamisch IP adressen toewijzen, maakt gebruik van DHCP server en DHCP relay agents



5.6.8 Internet Protocol versie 6

In de toekomst:

- Sterke uitbreiding aangesloten stations
- Wellicht elke TV in de toekomst Internet station
=> Huidige IPv4 gebrek aan adressen
- Veel draadloze mobile stations
=> IPv4, de huidige versie, is daarvoor niet goed uitgerust.

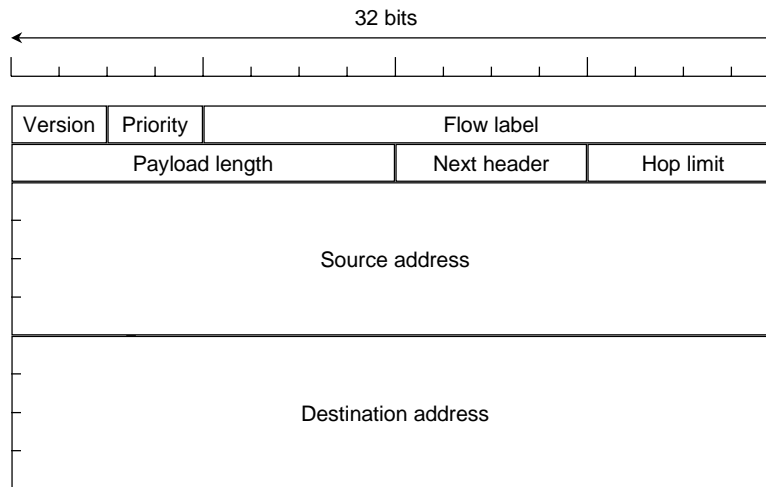
Belangrijkste doelen IPv6

1. Ondersteunen van miljarden stations
2. Omvang van de routingstabellen verkleinen
3. Vereenvoudigen van IP om routers sneller te maken
4. Betere beveiliging
5. Meer aandacht voor type dienst (vooral tijdgebonden data)
6. Betere ondersteuning multicasting
7. Mobiliteit zonder verandering van adres
8. Mogelijkheid van ontwikkeling van het protocol in de toekomst
9. Nog jarenlang samengaan van het oude en het nieuwe protocol

Veranderingen t.o.v. IPv4

1. Langere adressen
2. eenvoudigere header (7 ipv. 13 velden)
3. Betere ondersteuning van options (enkele oude standaardvelden zijn nu opties)
4. Beveiliging
5. Meer mogelijkheid voor specificeren van de soort dienst (*type of service*)

Vaste IPv6-header



Laatste transparant van
hoofdstuk 5
De netwerklaag