

Ontwerpen van netwerken

Beheer

Willem Brouwer

Architectuurontwerp

9.1	Inleiding	150
9.2	Aanwijzingen voor de leerling	151
9.3	Praktijkopdracht	151
9.4	Ontwerpen	152
9.5	Fysiek ontwerp	154
	9.5.1 Kleine LAN's	154
	9.5.2 Core-ontwerp van WAN's	155
	9.5.3 Legacy-systemen	159
9.6	Logisch ontwerp	160
9.7	Vragen en opdrachten	163
	9.7.1 Open vragen	163
	9.7.2 Opdrachten	163



Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Architectuurontwerp

9.1 Inleiding

In de laatste paragrafen van het vorige hoofdstuk hebben we gegevens verzameld en geanalyseerd die gebruikt worden om de architectuur van een omvangrijk netwerk te ontwerpen. Daarna moeten de stappen doorlopen worden om de functionaliteit te realiseren en de (systeem)software te kiezen. In dit hoofdstuk gaan we in op de architectuur.

9.2 Aanwijzingen voor de leerling

Bij het ontwerp van een groot netwerk kunnen kleine beslissingen in het beginstadium van het ontwerp grote gevolgen hebben voor het uiteindelijke netwerk. Dit betekent dat je bij het ontwerpproces niet zorgvuldig genoeg te werk kan gaan.

In dit hoofdstuk gaan we in op het fysieke en logische ontwerp van grote en kleine LAN's en WAN's. Verder behandelen we kort de redenen van het bestaan van legacy systemen en de wijze waarop ze in een (later) LAN gehandhaafd kunnen worden.

9.3 Praktijkopdracht

Het ontwerp van de architectuur is de structuur waarop het latere netwerk zal gaan draaien. Het gebouw waar jij je opleiding volgt, maakt deel uit van een groter geheel.

Binnen de organisatie bestaat al een tijdje het idee dat de dienstverlening wel goed is, maar dat deze wat minder zou moeten kosten. Het College van Bestuur heeft daarom een adviesbureau in de arm genomen. Jij werkt daar toevallig.

Onderzoek hoe op dit moment de (netwerk)structuur er uit ziet. Daartoe interview je bij voorkeur iemand van de afdeling infrastructuur van je ROC. Gebruik dit hoofdstuk om een lijst met te stellen vragen te ontwikkelen, die je bij dit interview als leidraad gebruikt. Formuleer vervolgens een advies om dezelfde dienstverlening op een even goede manier, maar goedkoper, te realiseren.



Index

9.4 Ontwerpen

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Als de requirements-analyse is afgerond, zal de ontwerper een globaal plan voor het netwerk maken. We noemen dit ook wel de (onderliggende) **architectuur** van het netwerk. Dit ontwerp heeft dan betrekking op de verbindingen tussen de knooppunten van het nieuwe netwerk. Details als servers en inrichting van locaties zullen hier nog buiten beschouwing worden gelaten. In het gekozen voorbeeld wordt nu het WAN tussen de locaties ontworpen.

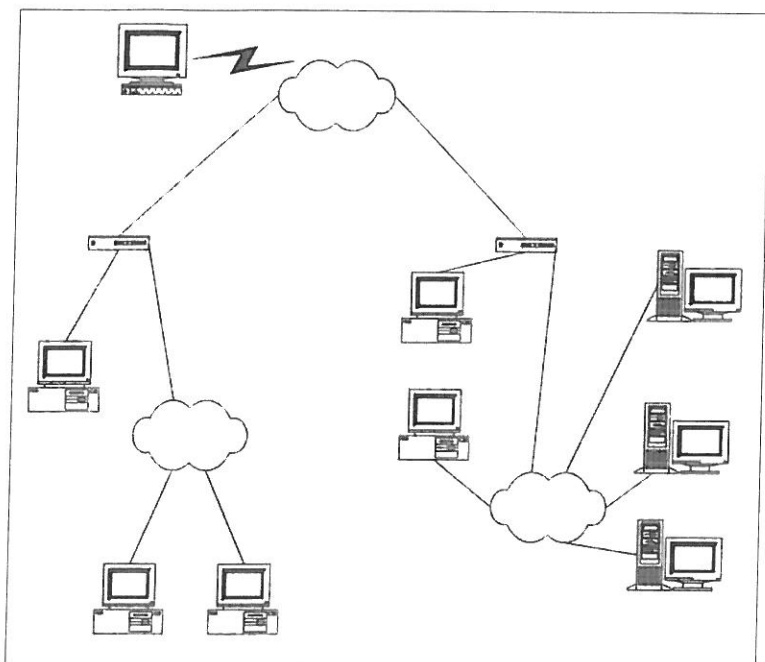
De vragen waar de ontwerper zich voor gesteld ziet zijn:

- Hoe realiseer ik een ontwerp voor de architectuur op dit niveau van het netwerk?
- Hoe laat ik zien dat dit ontwerp recht doet aan de vereisten?
- Hoe bepaal ik met een redelijke mate van nauwkeurigheid de kosten van het ontwerp?
- Hoe geef ik aan waar nog eventuele bottlenecks zitten? Wat moet nog opgelost worden?

Vier belangrijke aspecten in dit stadium zijn:

1. de kosten van de diverse mogelijke technologieën;
2. performance (network delay en doorvoer);
3. betrouwbaarheid;
4. potentiële risico's (bijvoorbeeld door gebruik van nog onvoldoende in de praktijk geteste technologie).

De fysieke layout van het netwerk komt nu aan de orde. In het geval van ons WAN zijn dat de **verbindingen** tussen de locaties.



Figuur 9.1 Netwerkontwerp op WAN-niveau.

Ook in het geval dat het niet om een WAN maar om een LAN gaat, zal de ontwerper zich eerst buigen over de vraag welke topologieën en technologieën hem ter beschikking staan. Het voornaamste verschil zijn de beschikbare technologieën: voor connecties binnen een WAN zijn andere technologieën voorhanden dan voor een LAN.

De kosten van WAN-verbindingen moeten niet onderschat worden. Een dienst als KPN Eurorings hanteerde in augustus 2003 de volgende tarieven:

- Een 64 kbps internationale verbinding tussen Amsterdam en Frankfurt kost per maand circa € 900 en een 2 Mbps verbinding rond de € 3000.
- Vergelijkbare verbindingen vanaf Amsterdam naar New York zijn respectievelijk circa € 1800 en € 5000 per maand.

De verbindingen in ons WAN zijn van zo'n type dat waarschijnlijk voor externe leveranciers van dataverbindingen zal worden gekozen. Als we als voorbeeld een campusnetwerk zouden hebben genomen, was het goed mogelijk dat de verbindingen tussen de diverse locaties op de campus in eigen beheer gerealiseerd konden worden.

Index

LAN
 Ethernet
 backbone
 10BaseT-netwerk
 100BaseT-netwerk
 busnetwerk
 Token Ring
 MAU
 sternetwerk

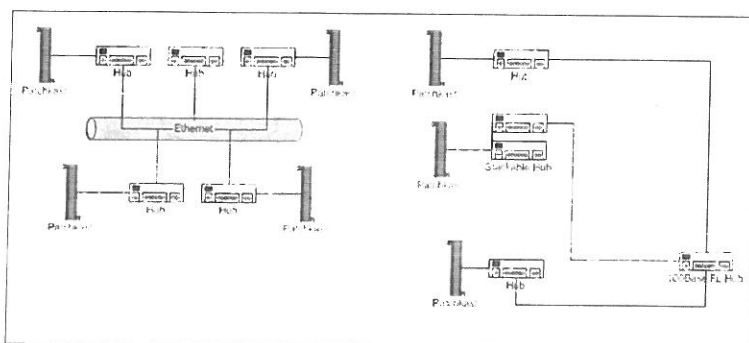
9.5 Fysiek ontwerp

9.5.1 Kleine LAN's

In kleine LAN's zijn er in theorie vele manieren om de structuur te implementeren. In de praktijk worden er eigenlijk maar twee gebruikt: Ethernet en Token Ring.

Ethernet

In het geval van een Ethernet kan voor twee typen **backbone** gekozen worden; zie figuur 9.2.



Figuur 9.2 Ethernet-backbones.

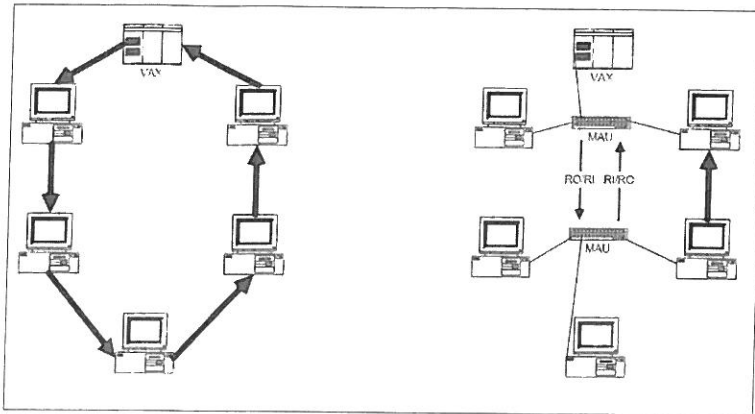
Het 10BaseT- en 100BaseT-netwerk hebben beide fysiek een stervorm. Logisch gezien zijn het echter **busnetwerken**. Er kan voor een busstructuur op backbone-niveau gekozen worden, of voor een ster. Er zijn hier verder hubs en twee stackable hubs gebruikt, maar switches zijn natuurlijk ook mogelijk (afhankelijk van de situatie). We gaan er wel van uit dat deze netwerken de performance bieden die in de user requirements zijn vastgelegd. Eventueel kan voor de backbone natuurlijk ook voor glasvezel worden gekozen.

Token Ring

Een Token Ring netwerk wordt fysiek gerealiseerd met behulp van MAU's. Deze worden via de Ring In- en Ring Out-connectors met elkaar doorverbonden en vormen dan verder elk op zich een fysiek **sternetwerk**. Logisch gezien gaat het om een sternetwerk.

Knipsel

Een MAU is een Multi Access Unit.



Figuur 9.3 Token Ring, logisch en fysiek ontwerp.



Index

WAN, ontwerp
LAN, ontwerp

9.5.2 Core-ontwerp van WAN's

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER- PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

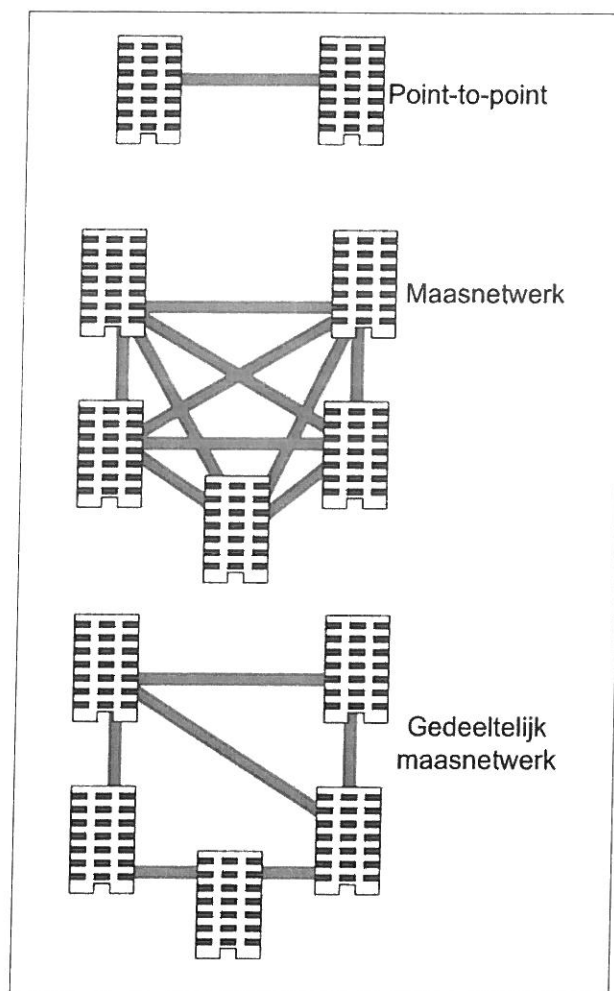
Voor WAN's is de keuze wat gevarieerder dan voor LAN's. Een WAN is vaak aangewezen op relatief trage verbindingen tussen de LAN's. Het zodanig ontwerpen dat er een minimale hoeveelheid data tussen de locaties vervoerd hoeft te worden, is kostentechnisch een must. Dat criterium is bij een LAN-ontwerp nauwelijks van belang. Daar kan vaak tegen relatief geringe kosten een vertienvoudiging van de bandbreedte worden geregeld. Bij een WAN is dit ondenkbaar (lees: onbetaalbaar).

Om de koppelingen te realiseren zijn meerdere technologieën beschikbaar:



- bridges
- switches
- routers

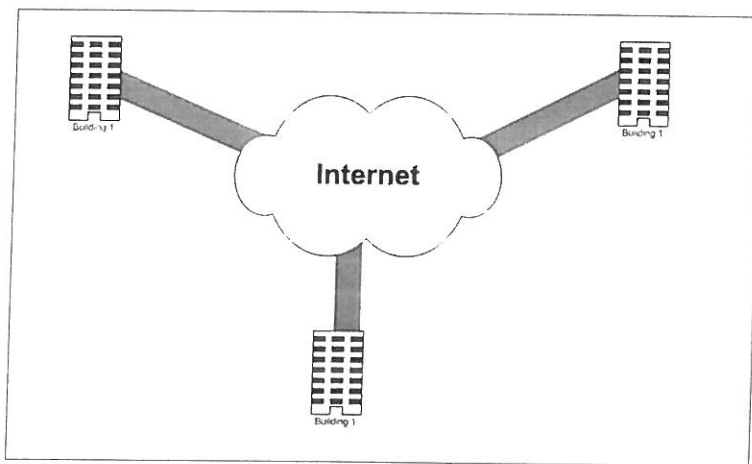
Deze apparatuur is in andere delen van je opleiding aan de orde geweest. VLAN's, worden de laatste jaren vaak gebruikt om binnen het LAN (maar ook op hogere niveaus) structuur aan te brengen. Je hebt er in paragraaf 6.7 over kunnen lezen. Alle genoemde technologieën zijn zowel voor Token Ring als Ethernet te gebruiken.



Figuur 9.4 WAN.

Binnen een WAN zijn diverse vormen van interconnectie tussen de locaties mogelijk; in figuur 9.4 zijn er een aantal getekend. In het geval van twee locaties volstaat een eenvoudige **point-to-point verbinding**. Bij een groter netwerk (meer locaties) kan elke locatie met elke andere worden verbonden. We krijgen dan een **maasnetwerk**. Dit is bij grote netwerken een dure, maar wel heel betrouwbare, oplossing. In de praktijk zie je dat netwerken vaak gedeeltelijk maasvormig worden uitgevoerd. Alle belangrijke locaties worden met elkaar verbonden. Dat betekent dat er tussen belangrijke locaties altijd (tenminste: bij maximaal één storing) een verbinding opgebouwd kan worden.

Een optie die ook wel wordt gekozen is weergegeven in figuur 9.5.



Figuur 9.5 Internet als connectie.

Als elke vestiging een internetverbinding heeft, kan daarover een **VPN** (Virtual Private Network) worden gelegd. Het verdient dan natuurlijk aanbeveling om met de ISP een goede SLA af te sluiten. In al deze gevallen moet vervolgens natuurlijk nog een fysieke connectie worden gekozen. Ontwikkelingen gaan nog steeds erg snel en de hier gegeven informatie zal waarschijnlijk snel verouderd zijn, maar de volgende services en snelheden zijn op dit moment (begin 2004) beschikbaar:

Index

point-to-point verbinding
maasnetwerk
VPN
Virtual Private Network



Index

verbinding, keuze

MTU

CBR

Constant Bit Rate

Quality of Service

QoS

Committed Information Rate

CIR



Knipsel

MTU staat voor: Maximum Transfer Unit, oftewel maximale pakketgrootte.

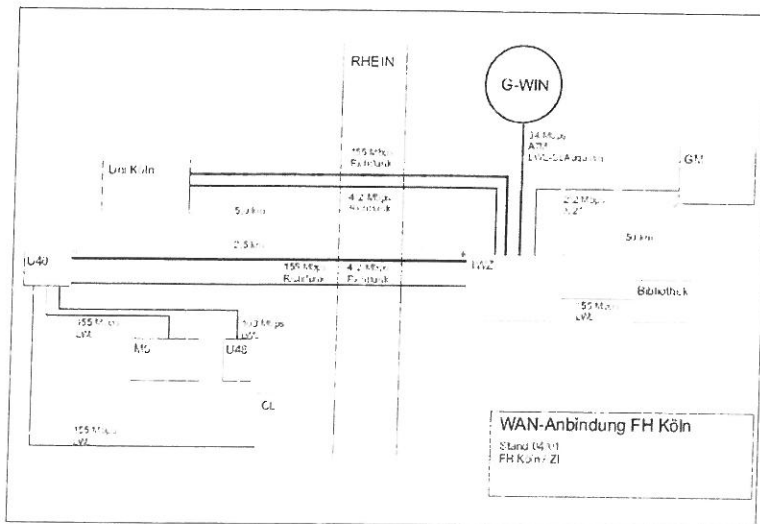
Technologie	Snelheid	Opmerkingen
PSTN Dial up	300 bps - 56 kbps	Normale telefoonmodem. Snelheid afhankelijk van verbinding. Bij hogere snelheden downstream kanaal groter dan upstream (asynchroon).
ISDN Dial up	64 kbps - 2 Mbps	2*64 kbps of 30*64 (24 in de USA).
X.21	64 kbps of 56 kbps	
Digital point-to-point	9.6kbps - Gbps	In de praktijk vanaf 64 kbps tot 2 Mbps (E1) (1,5 Mbps in de USA T1). Bij hogere snelheden vaak glasvezel met SDH- of SONET-technologie.
X.25	2.4 kbps - 2Mbps	Niet veel in gebruik als LAN-interconnectie.
Frame Relay	64 kbps - 2 Mbps	Vaak als gateway naar ATM. Ontwerper moet zelf per PVC (Permanent Virtual Circuit) parameters vastleggen.
ATM	2 Mbps - 2,4 Gbps	
IP VPN	64 kbps - Gbps	Relatief nieuwe (veelbelovende) service.

Belangrijke vragen bij de keuze van het type verbinding zijn:

- Welke bandbreedte is nodig?
- Hoe groot zijn de datapakketten die verzonden moeten worden?
Als de MTU kleiner is dan de te verzenden pakketgrootte, heeft dit (in verband met overhead door fragmentatie etc.) consequenties voor de bandbreedte. Vaak kan dit door 'tuning' optimaal ingesteld worden.
- Is deze bandbreedte constant nodig of alleen op piekmomenten?
Dat kan in kosten nogal uitmaken. Als van ATM een constante bandbreedte wordt vereist, kan een CBR-verbinding (**Constant Bit Rate**) worden afgesproken; overigens wel tegen een forse (meer)prijs. Als de verbinding niet constant dezelfde snelheid hoeft te hebben – of delen van de dag zelfs helemaal niet nodig is – kan een ander verbindingsstype worden gekozen. Het centrale begrip is hier 'Quality of Service' (QoS). De meeste verbindingen garanderen een **Committed Information Rate** (CIR), die altijd beschikbaar is, met daarbij de belofte (niet de garantie) dat de verbinding een (groot) deel van de tijd sneller is. Door een protocol te gebruiken dat in staat is pakketten weg te gooien als de bandbreedte even tot de CIR zakt, kan dit opgevangen worden. Om informatieverlies tegen te gaan moet daarboven dan wel een protocol gebruikt worden dat een betrouwbare end-to-end communicatie garandeert (bijvoorbeeld TCP).

- Hoe vaak en hoe lang is de verbinding in gebruik?

Vaak worden verbindingen voor 24 uur per dag gedurende zeven dagen per week gehuurd. Het is goed mogelijk dat een verbinding alleen overdag nodig is. Als de gewenste bandbreedte laag is, kan een gewone inbelverbinding soms volstaan (tegen een fractie van de kosten). Een verbinding die alleen 's nachts nodig is, kan misschien worden gedeeld met een bedrijf of organisatie met een tegenovergestelde wens.



Figuur 9.6 De verbindingen in het netwerk van de stad Keulen.

9.5.3 Legacy-systemen

Met legacy-systemen worden bedoeld: systemen die al een functie binnen de organisatie hebben en die moeten blijven draaien, maar waar het netwerk eigenlijk niet voor ontworpen is. Vaak gaat het om systemen die zo'n cruciale rol in de bedrijfsvoering spelen dat ze niet afgeschaft kunnen worden. Je ziet bijvoorbeeld wel eens dat er ooit een applicatie op een minicomputer is ontwikkeld die de complete personeelsadministratie omvat. Je kunt dan niet eenvoudig zeggen dat daar even een nieuwe applicatie voor moet komen. Je wilt een dergelijke applicatie toch ook op het nieuwe netwerk aan de gebruikers aanbieden.

Het kan ook gaan om een veel groter systeem, waarmee het bedrijf een verbinding heeft. Als je een nieuw netwerk voor KLM/Air France zou mogen ontwerpen, kun je niet eisen dat het wereldwijde reserveringssys-



legacy-systeem



Index

Scrap
 Trap
 Wrap
 logisch ontwerp
 uid
 MAC-adres
 SRB



Assist

Een uid is een Unit Identifier.



Knipsel

Dit is volgens sommigen de reden dat Ethernet-kaarten tegenwoordig vaak een 'instelbaar' MAC-adres hebben. Dit betekent dat in een SNA-omgeving, als er een netwerkkaart vervangen moet worden, alleen het MAC-adres hoeft te worden ingesteld zonder dat de configuratie gewijzigd hoeft te worden.

teem dat alle luchtvaartmaatschappijen onderling gebruiken tegelijkertijd mee wordt vernieuwd volgens jouw normen.

Er zijn diverse manieren om legacy-systemen over een LAN te ondersteunen:

- **Scrap.** Als een legacy-systeem aan het eind van zijn levenscyclus komt, kan er gekeken worden of in de ontwikkeling van het LAN/WAN tegelijkertijd een mogelijkheid is voor het vervangen van deze applicatie. Vervangen kan inhouden: het aanschaffen van een nieuwe applicatie, of het implementeren van de functionaliteit van de legacy-applicatie in één of meer van de nieuw te ontwikkelen applicaties.
- **Trap.** Laat de applicatie gewoon draaien, reserveer tijd en geld voor het onderhoud en laat voldoende van het oude netwerk (software en hardware) in stand om de applicatie te ondersteunen.
- **Wrap.** Een optie kan zijn om de legacy-systemen te handhaven, maar te kijken of het mogelijk is een connectie met het nieuwe netwerk te maken en ze via dat netwerk te benaderen. Misschien kan hun protocol 'ingepakt' ('gewrapped') over het netwerk en is het implementeren/ontwikkelen van enige protocolconverters voldoende.

9.6 Logisch ontwerp

In de vorige paragraaf is het netwerk fysiek ontworpen. In deze paragraaf gaan we verder met het **logische ontwerp**. Alle items (computers, routers, enzovoort) moeten op de een of andere wijze een unieke identificatie krijgen. Deze uid's worden later onder meer bij het beheer gebruikt

Er zijn diverse wijzen om dit te aan te pakken:

1. Op basis van het MAC-adres. In het oude IBM mainframe-tijdperk kon netwerkkaparaatuur op basis van het **MAC-adres** worden ingedeeld. Aan de hand van dit adres kan in een modern netwerk de DHCP-server ingesteld worden en deze kan dan IP-adressen uitdelen op basis waarvan stations geïdentificeerd zijn.
2. Token Ring netwerken maken vaak gebruik van 'source routing bridge technology' (**SRB**) om pakketten rechtstreeks door meerdere LAN-segmenten heen te vervoeren. Bij deze technologie kennen netwerkbeheerders aan elke ring een (uniek) ringnummer toe. Bridges

zijn ook genummerd, maar een bridge heeft alleen een ander nummer dan 1 als meer dan één bridge twee ringen verbindt. Dit laatste kan bijvoorbeeld voorkomen als er redundante verbindingen zijn.

Op deze wijze wordt het verkeer van bridge tot bridge gezonden tot de bestemmingsring bereikt is. Het algoritme is dus eigenlijk:

- Als deze ring mijn nummer heeft, dan ga ik op zoek naar mijn bestemmingstation;
- zo nee, dan ga ik naar 1;
- als dat niet werkt dan zijn er redundante verbindingen en wordt teruggevallen op standaard routeringsprotocollen die bij de technologie horen.

3. IP is natuurlijk een voor de hand liggende optie. Welke IP-adresreeks kan gebruikt worden? Is er een A-, B- of C-adres? Of toch CIDR? Is er sprake van NAT? Zal er een proxy worden ingezet? Is er een eigen namespace? Is er een eigen nameserver nodig? Hoe wordt deze geconfigureerd? Waar is dan de secundaire nameserver? In dit geval moet er, zoals al eerder is betoogd, natuurlijk ook een nummerplan gemaakt worden. Aangegeven moet worden welke **IP-adressen** en **-adresreeksen** waarvoor zijn gereserveerd. Bovendien is van belang hoe deze zo verdeeld worden dat een logisch netwerk ontstaat, dat ook nog onderhoudbaar en uitbreidbaar is. (Let op een logische, haalbare en vooral efficiënte routing!)
4. Is er sprake van een VLAN? Op basis waarvan worden stations in een VLAN geplaatst en hoe wordt dit verder verwerkt?
5. Tegenwoordig worden in een netwerk steeds vaker **draadloze stations** ondersteund. Volgens de standaard **IEEE 802.11b** (11 Mbps) of **IEEE 802.11a** of g (54 Mbps) worden **wifi**-stations aangesloten. Ook deze moeten ergens in het LAN opgenomen worden. Vaak wordt uit beveiligingsoogpunt een extra authenticatie vereist (bijvoorbeeld **IEEE 802.1X**) en plaatsing in een VLAN (**IEEE 802.1Q**). Dit dient om te voorkomen dat elke willekeurige gebruiker met een laptop en een wifi-kaartje zomaar internettoegang heeft. Meestal eist de ISP dat elke actie op het internet aan een individuele gebruiker te koppelen is. Dan kun je niet 'zomaar' een open DHCP-server neerzetten die aan 'iedereen' een IP-adres geeft.
6. **TCP/IP** is tegenwoordig ook bij Novell de default en te prefereren instelling. Daarom kan er tegenwoordig ook als het NOS van **Novell NetWare** gebruikt gaat worden, voor het protocol **TCP/IP** worden gekozen. Dan kunnen de adressering en naming daarvan gebruikt



Index

IP
CIDR
IP-adres
draadloos netwerk
IEEE 802.11b
IEEE 802.11a
wifi
IEEE 802.1X
IEEE 802.1Q
TCP/IP
Novell NetWare



Attentie

SRB is alweer opgevolgd door SRT (source-routing transparent). We gaan daar hier niet verder op in.



Assist

Bij Classless Inter-Domain Routing (CIDR) worden grotere segmenten IP-adressen uitgereikt. In het boek 'Verbindingen en protocollen' wordt dit nader uiteengezet.



Index

IPX/SPX
routing
nummerplan



Attentie

Op de verschillen tussen de beide belangrijkste routingsprotocollen (distance vector en link state) gaan we hier niet nader in, noch op OSPF-achtige structuren. Deze zijn al in een andere context aan de orde geweest.

worden. Wordt toch voor IPX/SPX gekozen, dan wordt het MAC-adres gebruikt door IPX en moet elk netwerksegment een eigen (uniek) netwerknummer krijgen. Dit vereist zorgvuldig configureren, zeker omdat de default-instellingen van NetWare eigenlijk niet correct zijn voor een groot, complex netwerk.

7. **Routing.** In dit stadium moet de basisrouting worden vastgelegd. Wordt alles dynamisch gedaan? Welke statische routes worden vastgelegd? Wordt er in (een deel van) het netwerk source routing toegepast?

Op basis van deze en andere argumenten kan vervolgens een logisch ontwerp van het netwerk gemaakt worden. Daarmee komt alle apparatuur op zijn logische plaats in het netwerk terecht. Hoewel je kunt verdedigen dat het logisch ontwerp losstaat van het latere fysieke ontwerp, is dat natuurlijk niet zo. Als je bijvoorbeeld een **nummerplan** maakt omdat het netwerk op TCP/IP gaat draaien, dan doe je dat natuurlijk met de huidige fysieke structuur in gedachten, zodat je keuzes ook later te implementeren zijn. Ook een VLAN-indeling moet niet alleen logisch zijn maar ook en vooral implementeerbaar.

9.7 Vragen en opdrachten

9.7.1 Open vragen

1. Op welke twee manieren kunnen Ethernet-backbones gerealiseerd worden?
2.
 - a. Wat is een VPN?
 - b. Wat kan het belang van een VPN zijn voor een groot corporate netwerk?
3. Is het altijd verstandig om een service provider in te zetten om een connectie tussen vestigingen te realiseren?
4.
 - a. Leg uit wat CIR is en wat CBR is.
 - b. Wat is het belang van beide voor een netwerkontwerp?
 - c. Beschrijf twee situaties waarin je voor een verbinding met een grote CIR zou kiezen, en wanneer je een verbinding met een grote CBR zou prefereren.
5.
 - a. Wat zijn legacy-systemen?
 - b. Waarom kunnen deze systemen bij het ontwerpen van een netwerk voor problemen zorgen?
6. Beschrijf de drie manieren om legacy-systemen in een (nieuw) netwerk op te nemen.
7. Volgens welke methode is het logisch ontwerp gemaakt van het netwerk waar jij op school het meest zit?

9.7.2 Opdrachten

1. Ontwerp een fysieke en logische structuur van een netwerk voor een (internationaal) reisbureau.
 - a. Het bureau heeft vestigingen in de meeste Europese hoofdsteden alsmede in Sydney, Buenos Aires, New York, Los Angeles en Houston.
 - b. Het systeem is verbonden met de belangrijke boekingssystemen van luchtvaart- en hotelmaatschappijen.

2. Een aluminiumspuiterij heeft drie vestigingen in Nederland en één in Duitsland. Elke locatie heeft een LAN. Het management van het bedrijf wil inzage in de kosten van een eventuele koppeling. Aangezien ze veel kleine series maken, zou het kostenbesparend moeten zijn als de productiecapaciteit beter benut zou kunnen worden. De applicatie hiervoor wordt al ontwikkeld. Zoek uit welke mogelijkheden tot koppeling er zijn en wat ze kosten. Wat zijn de eigenschappen en voor- en nadelen van de diverse mogelijkheden?