Evolutie en Revolutie in de Campusinfrastructuur

Rapport uitgebracht aan:
SURFnet
www.surfnet.nl
GigaPort User Board
www.gigaport.nl

Uitgebracht door:
Stratix Consulting B.V.
www.stratix.nl

Utrecht, 14 juni 2005

Evolutie en revolutie in de campusinfrastructuur

1 SAMENVATTING 3

2 ICT ONTWIKKELINGEN IN HOGER ONDERWIJS & ONDERZOEK 5

2.1 Ontwikkelingen in de toepassingsgebieden 5

2.2 Eisen van de verschillende gebruikscategorieën aan het netwerk 8

2.3 Hybride netwerken als oplossing 9

3 SURFNET DIENSTENPORTFOLIO 10

3.1 Inleiding: SURFnet6 op hoofdlijnen 10

3.2 Netwerkdiensten 10

3.3 Nieuwe toepassingsdiensten 13

4 BETEKENIS VOOR DE CAMPUSINFRASTRUCTUUR 16

4.1 Inleiding: impact op de lokale infrastructuur 16

4.2 Aandachtspunten voor de campusinfrastructuur 16

4.2.1 Ondersteuning multimediale eindgebruikers en operationele toepassingen 17

4.2.2 Ondersteuning high-end onderzoekstoepassingen 21

4.3 Aanbevelingen 24

4.3.1 Ondersteuning multimediale eindgebruikers en operationele toepassingen 24

4.3.2 Ondersteuning high-end onderzoekstoepassingen 25

4.4 Open issues 25

BIJLAGE A AFKORTINGEN 26

1 Samenvatting

De ontwikkelingen in het gebruik van ICT in het hoger onderwijs en onderzoek vragen om nieuwe diensten en nieuwe functionaliteit waarvoor aanpassingen in de ICT-infrastructuur noodzakelijk zijn. SURFnet6, het resultaat van het GigaPort Next Generation project, is ontwikkeld volgens een concept dat nauw aansluit op deze ontwikkelingen en dat revolutionaire mogelijkheden biedt. Teneinde optimaal van deze nieuwe mogelijkheden gebruik te kunnen maken zijn tevens aanpassingen vereist in de campusinfrastructuur van de aangesloten instellingen. Dit rapport beschrijft een visie op de ontwikkelingen, de wijze waarop het SURFnet dienstenportfolio hierop inspeelt en wat dit vervolgens betekent voor de campusinfrastructuur. Het rapport is opgesteld door Stratix in opdracht van SURFnet en de GigaPort User Board. De redactie van het document is uitgevoerd door het bestuur van de GigaPort User Board, bestaande uit drs. P.J. Schelleman MBA, ir. G.J.T.A. Bakx en drs. R.F. Janz.

Conclusies

De ontwikkelingen in het gebruik van ICT zijn voor een belangrijk deel evolutionair van aard en vereisen snelle en betrouwbare op IP-gebaseerde diensten voor onder andere multimediale toepassingen in onderwijs en onderzoek als ook voor operationele doeleinden. Anderzijds vragen nieuwe *revolutionaire* wetenschappelijke toepassingen om zeer breedbandige point-to-point transportdiensten tegen acceptabele kosten. Om in deze gecombineerde vraag te kunnen voorzien zijn aanpassingen in zowel het SURFnet-netwerk als in de campusinfrastructuur noodzakelijk.

De inzet van steeds grotere routers en steeds snellere IP-verbindingen voldoet functioneel niet langer en is ook vanuit kostenoogpunt niet schaalbaar. De oplossing ligt in het gebruik van hybride netwerken: netwerken waar IP-routing voor gangbare toepassingen en lichtpaden voor zware point-to-point verbindingen naast elkaar kunnen worden aangeboden, gebruikmakend van een gezamenlijke optische transmissielaag. Gebruikers met zeer grote bandbreedtebehoeftes (*power users*) krijgen daarmee de mogelijkheid op de optische laag transparante end-to-end verbindingen in de vorm van lichtpaden op te zetten.

De ontwikkelingen rond multimediale toepassingen kunnen grotendeels worden opgevangen door overprovisioning in het IP-domein. Hetzelfde geldt voor de meer operationele toepassingen. De bestaande vraagstukken van IT-managers op het gebied van netwerkbeheer, performance en beveiligingsproblematiek veranderen hierdoor niet noemenswaardig. Het lokaal faciliteren van lichtpaden ten behoeve van high-end onderzoekstoepassingen heeft echter aanzienlijke gevolgen voor zowel de campusinfrastructuur als het netwerkbeheer en -beveiliging.

In de operationele omgeving kunnen statische lichtpaden worden gebruikt om vestigingen in verschillende steden te koppelen via een Optical Private Network (OPN). Dit is een relatief eenvoudige oplossing om lokale netwerken op verschillende lokaties volledig transparant samen

te voegen tot één LAN-omgeving. Deze oplossing heeft een aantal beheersmatige voordelen ten opzichte van gangbare VPN-oplossingen en biedt interessante mogelijkheden voor bijvoorbeeld server-consolidatie, beheercentralisatie en outsourcing.

Aanbevelingen

Afhankelijk van de eisen en wensen van de eigen gebruikers en de functionaliteit die een instelling wil faciliteren zal een campusinfrastructuur aan een aantal voorwaarden moeten voldoen. Dit rapport doet een aantal concrete aanbevelingen die kunnen dienen als ontwerprichtlijnen. De aanbevelingen worden hieronder kort weergegeven, voor een uitwerking hiervan wordt verwezen naar hoofdstuk 4.

Ondersteuning multimediale eindgebruikers en operationele toepassingen

- Overdimensioneer de WAN-aansluiting (overprovisioning);
- Overdimensioneer de campusbackbone (overprovisioning);
- Kies voor een toekomstvaste glasvezelinfrastructuur;
- Gebruik multicast voor betere performance van multimediale toepassingen;
- Richt een adequate authenticatie- en autorisatie-infrastructuur in;
- Overweeg lichtpaden en OPN's voor het koppelen van vestigingen en ter ondersteuning van centralisatie van beheer en systemen.

Ondersteuning high-end onderzoekstoepassingen

- Realiseer een campusinfrastructuur die aanvullend op het operationele IP-netwerk tevens lichtpaden kan faciliteren;
- Zorg voor voldoende glasvezelcapaciteit in zowel de campus-backbone als ten behoeve van *power users*;
- Voorzie in de noodzakelijke apparatuur ter ondersteuning van langere afstanden of meer lichtpaden;
- Zorg voor een veilige koppeling van het operationele netwerk met het onderzoeks-LAN.

Open issues

In het huidige ontwikkelingsstadium van hybride netwerken, waarin er nog slechts beperkt *hands-on* ervaring is opgedaan met het faciliteren van lichtpaden binnen het domein van campusinfrastructuren, zijn er noodzakelijkerwijs een aantal zaken die in dit document slechts als *open issues* kunnen worden bestempeld.
Deze aandachtspunten zullen in de komende periode verder moeten worden uitgewerkt. Dit betreft tenminste de volgende zaken:

- Het ontwikkelen en documenteren van *best practices* voor het doorzetten van lichtpadfunctionaliteit naar *power users*, waarbij onder meer de impact van lichtpaden op het gebied van beveiliging en netwerkbeheer moeten worden verkend;
- Het ontwikkelen van *best practices* voor het automatisch opzetten van dynamische lichtpaden door eindgebruikers;
- Het verder integreren van authenticatie- en autorisatie-infrastructuren met als doelstelling Universal Single Sign-On.

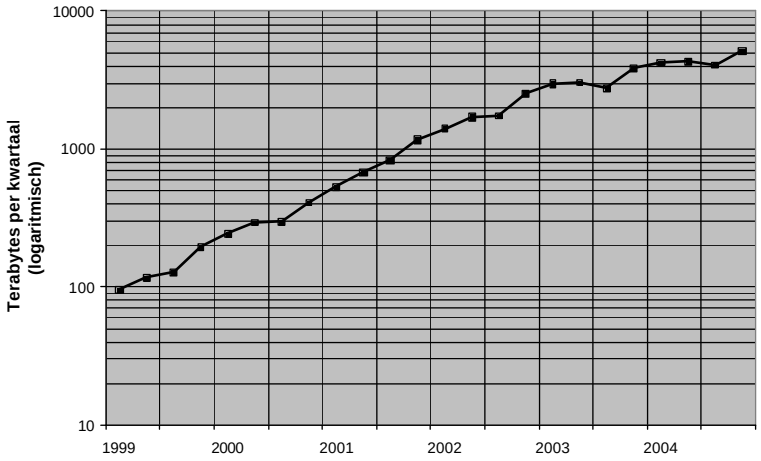
2 ICT ontwikkelingen in Hoger Onderwijs & Onderzoek

2.1 Ontwikkelingen in de toepassingsgebieden

Een groeiend aantal veeleisende gebruikers in hoger onderwijs en onderzoek vraagt om nieuwe hoogwaardige netwerkdiensten. Enerzijds is er hierbij sprake van een "evolutie" van snelle en betrouwbare IP-diensten voor o.a. multimediale toepassingen in onderwijs en onderzoek en voor operationele doeleinden. Anderzijds vragen specifieke high-end onderzoekstoepassingen om "revolutionaire" zeer breedbandige point-to-point transportdiensten tegen acceptabele kosten. Om in deze gecombineerde vraag te voorzien zijn aanpassingen in de (campus) netwerkinfrastructuur noodzakelijk.

In de onderwijs- en onderzoeksomgeving, maar ook in de organisatie van de instellingen, speelt communicatie een steeds belangrijkere rol. De betrokken gebruikers eisen daardoor vanzelfsprekend ook meer ten aanzien van de kwaliteit en beschikbaarheid van communicatiemiddelen. Binnen de instellingen wordt over het algemeen onderscheid gemaakt tussen onderwijstoepassingen ("e-learning"), wetenschappelijke toepassingen ("e-science") en meer operationele toepassingen ("e-organisation"). Binnen deze drie toepassingsgebieden zijn een aantal ontwikkelingen gaande, die verschillende eisen stellen aan de onderliggende infrastructuur.

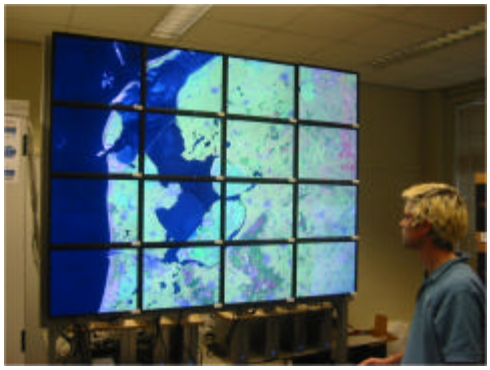
Onderwijs: een evolutie van multimediale toepassingen
In het onderwijs zien we dat de digitale leeromgeving een steeds prominentere rol krijgt in het onderwijsproces. Multimediale toepassingen zoals streaming video maken nieuwe vormen van onderwijs mogelijk, zoals virtuele trainingen, samenwerken op afstand en het volgen van real-time college. De doelmatigheid van de inzet van innovatieve communicatiemiddelen in het onderwijs wordt sterk bepaald door de kwaliteit van het communicatie-kanaal. Met name de multimediale toepassingen stellen hoge eisen aan de onderliggende infrastructuur waarbij zowel prestatie en kwaliteit als veiligheid en beschikbaarheid gewaarborgd dienen te zijn.



Figuur 1 *Totale verkeersontwikkeling over SURFnet uitgezet op een logaritmische schaal*

Het grootschalige gebruik van dit type toepassingen is onder meer zichtbaar in het toenemende verkeersvolume op het SURFnet-netwerk. Lange tijd groeide het totale verkeer over SURFnet exponentieel met een factor 2,5 per jaar. Deze groeifactor is het afgelopen jaar enigszins afgenomen maar de absolute groei is nog steeds fors zoals te zien in figuur 1.
Door onder meer het nieuwe BaMa[1] model neemt de mobiliteit van studenten toe en daarmee de behoefte om vanaf verschillende lokaties op de campus, maar ook thuis, onderweg of bij een andere instelling dezelfde diensten c.q. werkomgeving te kunnen gebruiken. Toegankelijkheid en gebruiksgemak spelen daarbij een steeds grotere rol. Naast het aanbieden van nieuwe communicatietoepassingen ligt de uitdaging hier dan ook met name in het 'beter' aanbieden van bestaande toepassingen. Door bepaalde diensten bijvoorbeeld mobiel beschikbaar te maken of toegankelijk vanaf verschillende netwerken ontstaan niet zozeer nieuwe toepassingen maar wel nieuwe communicatiemogelijkheden. Om dit te realiseren zijn onder meer uniforme authenticatie- en autorisatie-infrastructuren in het hoger onderwijs een noodzaak.

Onderzoek: een revolutie van high-end onderzoekstoepassingen
De "evolutie" van op IP-gebaseerde toepassingen zoals vooral zichtbaar is in het onderwijs is uiteraard ook terug te vinden in de onderzoeksomgeving. Daarnaast vindt in dit domein echter een andere "revolutionaire" ontwikkeling plaats.
Het netwerk als zodanig wordt steeds vaker onderdeel van de onderzoeksomgeving of zelfs van het onderzoeksinstrument. Belangrijke resources zoals dataopslag en rekenkracht worden via het netwerk voor onderzoekers toegankelijk gemaakt. Er vindt bovendien in toenemende mate samenwerking plaatst tussen onderzoeksgroepen, vaak op internationaal niveau, waarbij zeer grote hoeveelheden gegevens door wetenschappers op afstand kunnen worden geanalyseerd. Denk hierbij aan virtual laboratories en de visualisatie van grote data sets. Een aantal specifieke onderzoekstoepassingen zoals de Tile-display van SARA, te zien in figuur 2, is in staat om dusdanige datastromen te genereren dat het overige IP-verkeer daar serieus hinder van kan ondervinden. De Tile-display genereert – afhankelijk van de gekozen resolutie – meer verkeer dan gemiddeld op een willekeurig moment over het SURFnet-netwerk getransporteerd wordt. Daarnaast zien we dat netwerkinfrastructuren integraal onderdeel worden van wetenschappelijke instrumenten. Voorbeelden hiervan zijn VLBI (Very Long Baseline Interferometry / JIVE), LOFAR (LOw Frequency ARray / ASTRON) en de LHC (Large Hadron Collider / CERN). Dergelijke toepassingen genereren zeer grote verkeersvolumes op specifieke point-to-point verbindingen. Essentieel voor dit soort wetenschappelijke toepassingen is dat de benodigde bandbreedte tegen acceptabele kosten beschikbaar is.



Figuur 2 *Tile display van SARA: veeleisend**!***

[1] BaMa: Bachelor – Master model

Organisatie: een evolutie in operationele toepassingen
Binnen de onderwijs- en onderzoeksinstellingen spelen tenslotte een aantal voornamelijk operationele ICT ontwikkelingen. Er is bijvoorbeeld een duidelijke trend te zien van centralisatie, consolidatie en integratie van applicaties en IT-systemen. Het doel hiervan is de dienstverlening te verbeteren en daarnaast ook vooral het realiseren van de hieruit voortvloeiende besparing op beheerskosten. Een toenemend aantal instellingen kijkt dan ook naar mogelijkheden voor centralisatie van server-functionaliteit en outsourcing van specifieke netwerkvoorzieningen zoals storage bij Application Service Providers (ASP's). Over het algemeen betreft het hierbij een afweging tussen een investering in WAN verbindingen en (gecentraliseerde) apparatuur versus de mogelijke besparingen op de beheerskosten.

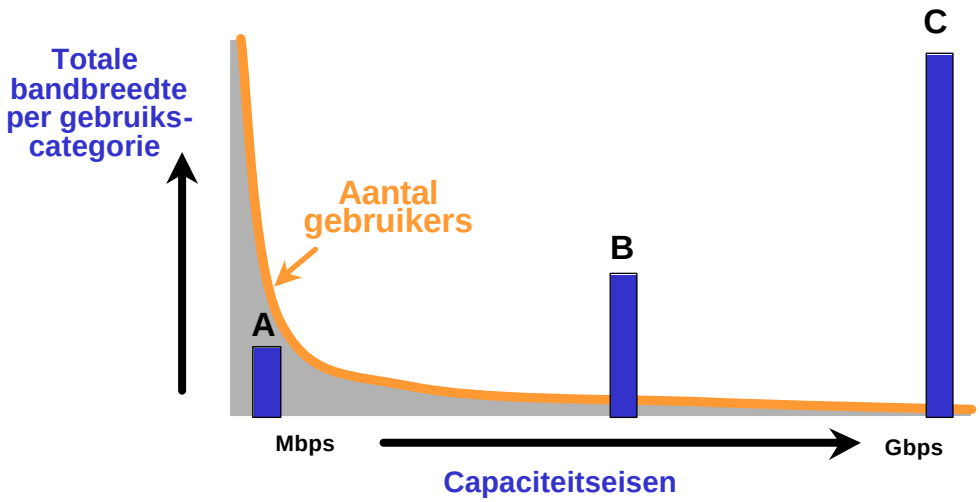
De kwaliteit en toegankelijkheid van multimediadiensten zoals videoconferencing en IP-telefonie (VoIP) is de afgelopen jaren verder ontwikkeld, waardoor deze toepassingen in toenemende mate worden ingezet voor operationele doeleinden. Deze diensten krijgen bovendien meer en meer een *peer-to-peer* karakter waarbij applicaties niet vanaf een centrale server maar vanaf een desktop PC worden aangeboden. Ook vindt hier integratie plaats met *Instant Messaging* -, *file transfer* - en *presence* functionaliteit. Dit is onderdeel van een meer algemene trend, waarbij applicaties die tot nu toe individueel werden gebruikt en/of aangeboden, worden geïntegreerd, zowel qua functionaliteit als qua toegankelijkheid. Een goed voorbeeld van dit laatste is het eenmalig inloggen op een portal om vervolgens diverse applicaties te kunnen gebruiken, het zogenaamde *single-sign-on*. Deze integratie van diensten vraagt een hoge mate van standaardisatie van de onderliggende (authenticatie)processen en een goede organisatie van de gegevensstromen.

Instellingen zullen de komende jaren door onder meer de centralisatie en consolidatie van systemen en het beschikbaar stellen van breedbandige multimediale diensten steeds zwaarder gaan leunen op de netwerkinfrastructuur. Voor instellingen met geografisch verspreide lokaties geldt dit in nog sterkere mate.

2.2 Eisen van de verschillende gebruikscategorieën aan het netwerk

Revolutionaire high-end onderzoekstoepassingen stellen eisen aan de infrastructuur die niet door de huidige gerouteerde netwerken worden ondersteund. De gecombineerde vraag van de verschillende gebruikscategorieën vraagt om aanpassingen in de architectuur en de functionaliteit van de onderliggende netwerkinfrastructuur.

Medewerkers van instellingen en studenten gebruiken naast al langer bestaande e-mail en web-applicaties in toenemende mate nieuwe multimediale toepassingen voor onderlinge communicatie. Deze toepassingen stellen hoge eisen aan de onderliggende IP-netwerken, zowel voor wat betreft de kwaliteit in termen van *delay* en *jitter* als qua bandbreedte-prestaties. Daarnaast vraagt een groeiend aantal wetenschappelijke toepassingen om zeer hoge bandbreedtes tussen specifieke lokaties. Onderstaande figuur geeft een typologie van de drie categorieën van netwerkgebruik.



Figuur 3 *Bandbreedte behoefte van verschillende gebruikscategorieën.*[2]

Categorie A betreft het reguliere gebruik voor e-mail, web, en in toenemende mate multimediale applicaties. Deze categorie kenmerkt zich door een behoefte aan IP-connectiviteit met een *many-to-many* karakter. De gebruikersgroep is relatief groot, maar legt gemiddeld per gebruiker het minste beslag op de bandbreedte. **Categorie B** betreft zwaardere applicaties en operationele multimediale toepassingen die met name binnen LAN omgevingen worden gebruikt en waarbij VPN's worden gebruikt om vestigingen (LAN's) te koppelen. Deze categorie vraagt om *several-to-several* IP-connectiviteit. **Categorie C** tenslotte betreft het gebruik voor revolutionaire high-end onderzoekstoepassingen en wetenschappelijke instrumenten. Hierbij gaat het typisch om zeer breedbandige verbindingen met hoge kwaliteitseisen tussen een beperkt aantal lokaties (*few-to-few*). Hoewel het aantal power users relatief klein is, legt deze vorm van netwerkgebruik een grote claim op de bandbreedte.

[2] Bron: Cees de Laat (Universiteit van Amsterdam)

Het toestaan van de combinatie van de verschillende gebruikscategorieën op één gerouteerd netwerk zou leiden tot een aantal complicaties. Ten eerste zorgen de zeer breedbandige high-end onderzoekstoepassingen voor een zware belasting van het IP-netwerk, waardoor de kwaliteit van het overige verkeer, in het bijzonder van de real-time toepassingen, in gevaar komt. Ten tweede zijn de kosten voor een gerouteerd netwerk met de bandbreedtes die categorie C gebruikers vereisen, dermate hoog dat gebruik voor deze doeleinden al snel onbetaalbaar wordt.

2.3 Hybride netwerken als oplossing

De oplossing voor het faciliteren van het groeiende aantal "power users" ligt in hybride netwerken. Hybride in de zin dat via een gezamenlijke optische transmissielaag zowel IP routing voor gangbare toepassingen als lichtpaden voor zware point-to-point verbindingen worden geleverd.

Hoewel IP routing apparatuur per Mbit/s steeds goedkoper wordt, groeien de kosten doordat het verkeer harder groeit dan de prijzen dalen. Optische- en Ethernet-apparatuur zijn relatief goedkoper dan IP routing apparatuur. Om de gecombineerde vraag van de verschillende gebruikscategorieën kosteneffectief te kunnen ondersteunen dienen deze technologieën meer te worden ingezet. Voor de kosten van 10 Gbit/s interfaces geldt op dit moment grofweg dat een gerouteerde Laag 3 (L3) IP-poort tien maal duurder is dan een geswitchte Laag 2 (L2) poort die weer grofweg het tienvoudige kost van een optische Laag 1 (L1) switchpoort. Bij het opschalen van het netwerk moet dus goed worden gekeken naar de noodzaak om verkeer af te handelen op IP-niveau. Dit mede gezien het feit dat juist het zware categorie C verkeer dat point-to-point over het netwerk wordt getransporteerd vaak geen volledige IP functionaliteit (routering) nodig heeft.

Figuur 4 *De verschillende netwerklagen (L1, L2 en L3)*

In de afgelopen periode hebben organisaties als SURFnet, CANARIE en DANTE laten zien dat de oplossing voor deze problematiek in het gebruik van hybride netwerken ligt. Netwerken die zowel IP routing voor gangbare toepassingen als lichtpaden voor zware point-to-point verbindingen door het netwerk ondersteunen. Het bieden van hoge kwaliteit end-to-end lichtpad-diensten op L1, beschermt de op IP-gebaseerde diensten en ondersteunt veeleisende high-end onderzoekstoepassingen op een economisch voordelige wijze.

3 SURFnet dienstenportfolio

3.1 Inleiding: SURFnet6 op hoofdlijnen

De ontwikkelingen in het gebruik van ICT in hoger onderwijs en onderzoek hebben SURFnet er toe aangezet nieuwe diensten te ontwikkelen die inspelen op de eisen van verschillende gebruikscategorieën. Paragraaf 3.2 en 3.3 geven een korte beschrijving van de in dit verband meest relevante netwerk- en toepassingsdiensten uit het SURFnet dienstenportfolio.

SURFnet6, het resultaat van het GigaPort Next Generation Network-project, wordt ontwikkeld als een hybride optisch en pakket-geschakeld netwerk waarbij zowel IP-connectiviteit als lichtpad-diensten worden aangeboden over een gemeenschappelijke optische netwerklaag. Waar lichtpaden in SURFnet5 enkel fungeerden als bouwsteen in het netwerk om IP-connectiviteit te leveren worden deze in SURFnet6 ook als dienst aangeboden aan de aangesloten instellingen en eindgebruikers. De optische laag van het SURFnet6-netwerk bestaat uit een aantal DWDM ringen die gebruik maken van de *Managed Dark Fiber* infrastructuur die SURFnet de afgelopen jaren heeft verworven. De DWDM transmissielaag is opgebouwd met apparatuur uit het Nortel Common Photonic Layer (CPL) portfolio. Het netwerk is zowel fysiek als logisch *resilient* uitgevoerd om maximale beschikbaarheid te waarborgen. Teneinde het aantal kostbare router interfaces te minimaliseren is er in het ontwerp voor gekozen het aantal gerouteerde lokaties te beperken tot de twee core lokaties die zich bevinden bij SARA en TeleCity2, beide in Amsterdam. Ten opzichte van het bestaande SURFnet5-netwerk - dat 18 lokaties kent waar routers staan opgesteld - is het aantal L3 lokaties dus aanzienlijk gereduceerd, met significante kostenvoordelen tot gevolg. *Overprovisioning* van bandbreedte volgens het KIS[3] adagium, dat vanaf de eerste generaties SURFnet-netwerken als leidend uitgangspunt voor het ontwerp is gehanteerd, zorgt ervoor dat SURFnet6 een congestievrij en beheersbaar netwerk zal zijn met een hoge beschikbaarheid. Daarnaast maakt de hoge mate van *resiliency* een zeer betrouwbare dienstverlening mogelijk.

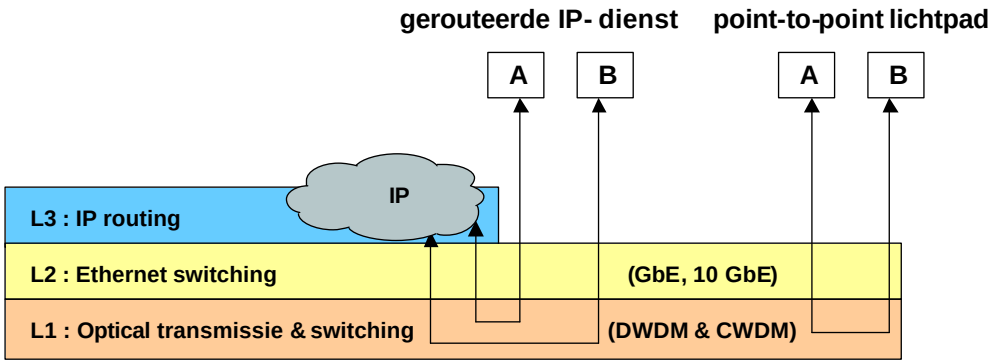
3.2 Netwerkdiensten

SURFnet6 biedt een aantal nieuwe geavanceerde netwerkdiensten met additionele functionaliteit. De belangrijkste netwerkdiensten zijn:

- hoge capaciteit IP-diensten (met GbE of 10 GbE interfaces)
- lichtpaden (met GbE of 10 GbE interfaces)

Het concept van deze diensten is weergegeven in Figuur 5.

[3] KIS: “Keep It Simple”



Figuur 5 *Hybride netwerkdiensten over gezamenlijke optische transmissielaag*

IP-connectiviteit
De aansluitingen van alle instellingen op het SURFnet6 IP-netwerk worden uitgevoerd met een minimale bandbreedte van 1 Gbit/s met Gigabit Ethernet (GbE) interfaces. Daarnaast is er de mogelijkheid om via een 10 GbE interface aan te sluiten. De IP-diensten van SURFnet6 omvatten zowel IPv4 als IPv6 als unicast en multicast functionaliteit.

Lichtpaden
Lichtpaden bieden de mogelijkheid om tegen relatief lage kosten snelle (1 Gbit/s of 10 Gbit/s), hoogwaardige en veilige point-to-point verbindingen te realiseren. Deze verbindingen op L1 zijn transparant voor willekeurige transportprotocollen en zeer betrouwbaar. Het ontbreken van packet re-ordering en packet-drop, een voorspelbare vertraging (dus geen jitter) en de hoge transmissiecapaciteit biedt nieuwe mogelijkheden. Deze eigenschappen maken lichtpaden interessant voor zowel wetenschappelijke toepassingen en instrumenten als voor het koppelen van vestigingen voor operationele toepassingen.

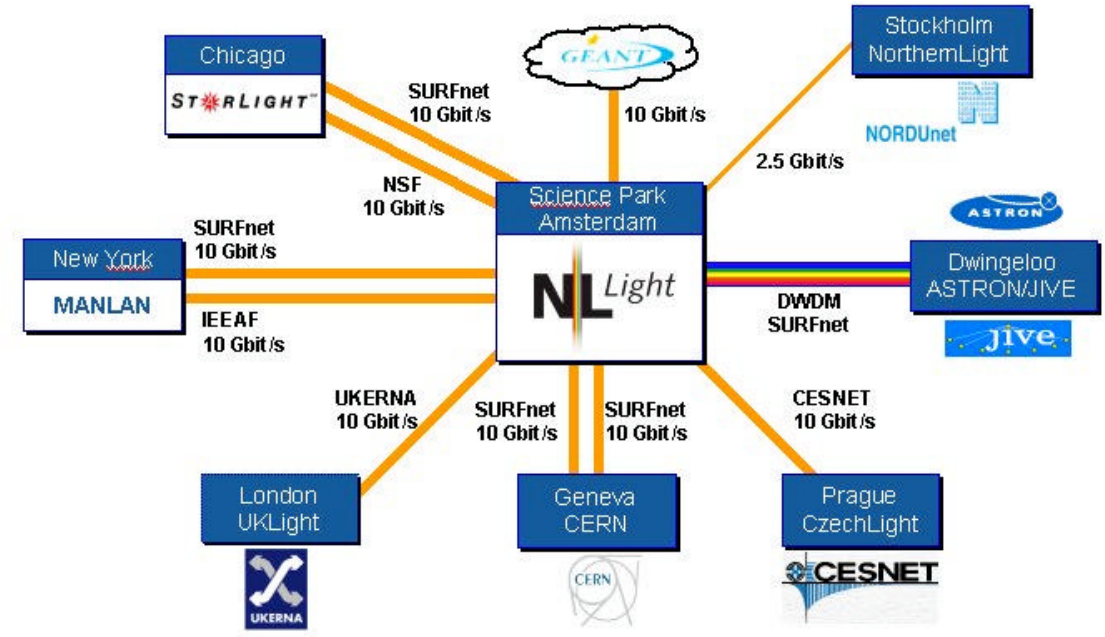
Vanaf 1 januari 2006 zijn de semi-automatische lichtpad-diensten operationeel. Op dat moment zullen gebruikers zelf lichtpaden kunnen configureren door middel van geauthenticeerde webservices of via het Network Operation Center (NOC). Tegen eind 2008 is het vervolgens de bedoeling te voorzien in automatische lichtpad *provisioning* via:
- een broker applicatie die multi-domain lichtpad provisioning mogelijk maakt
- L3 verkeersstroom-analyse op basis waarvan de routers verkeer kunnen ‘off-loaden’ naar een lichtpad (deze zogenaamde Cloud-Bypass feature is nog onderwerp van onderzoek)

Is deze fase eenmaal bereikt, dan zullen lichtpaden volledig automatisch opgezet kunnen worden zonder tussenkomst van beheerders.

Een interessante operationele toepassing van lichtpaden is het creëren van een Optisch Privaat Netwerk (OPN). Hierbij worden de LAN’s van twee of meer vestigingen via statische lichtpaden gekoppeld. Deze constructie biedt een aantal voordelen ten opzichte van L2 en L3 VPN’s. Naast de hoge kwaliteit en capaciteit van de lichtpadverbindingen en de gunstige verhouding tussen prijs en prestatie zijn dat met name voordelen op het gebied van security en beheer. Omdat het verkeer tussen vestigingen op een privaat netwerk zit en niet gerouteerd of ‘getunneld’ hoeft te worden, spelen conventionele problemen die hier doorgaans mee

samenhangen geen rol. Daarnaast biedt het op deze wijze koppelen van vestigingen interessante mogelijkheden voor consolidatie van systemen en centralisatie van beheer.

SURFnet6 biedt tevens de mogelijkheid internationaal lichtpaden op te zetten via NetherLight. NetherLight is de open Optical Exchange in Amsterdam die deel uitmaakt van het Global Lambda Integrated Facility (GLIF) initiatief. Zoals te zien in figuur 6 biedt NetherLight op dit moment verbindingen met onder meer StarLight (Chicago), MAN LAN (New York), UKLight (Londen), CERN (Geneve), CzechLight (Praag) en NorthernLight (Stockholm). Vandaar uit zijn internationale instellingen en andere netwerken te bereiken.



Figuur 6 *Internationale koppelingen via NetherLight.*

De lichtpaddienst wordt aangeboden via de DWDM technologie van het Nortel Common Photonic Layer (CPL) platform. Het SURFnet6-netwerk is opgebouwd uit vijf van deze DWDM ringen. Initieel heeft CPL per ring negen banden met vier lambda's per band. Elke band biedt de mogelijkheid tot 40 Gbit/s bi-directionele verbindingen op te zetten. Een lambda kan worden gebruikt om IP-verbindingen op te zetten alsmede om point-to-point lichtpaden te creëren.

Voor alle universiteiten geldt dat de lichtpadfunctionaliteit zonder extra kosten beschikbaar is. Voor de overige instellingen zal deze functionaliteit worden verrekend via het basistarief. Daarbij moet worden opgemerkt dat de lichtpadfunctionaliteit niet voor alle instellingen vanaf hetzelfde moment beschikbaar zal zijn. Uitgangspunt bij de toepassing van lichtpaden is dat het gebruik tegen marginale kosten voor de instelling wordt gefaciliteerd. Om gebruik te kunnen maken van deze faciliteiten zullen instellingen echter wel de hiervoor noodzakelijke investeringen moeten doen in de eigen campusinfrastructuur. Een uitwerking hiervan is opgenomen in hoofdstuk 4 van dit document.

3.3 Nieuwe toepassingsdiensten

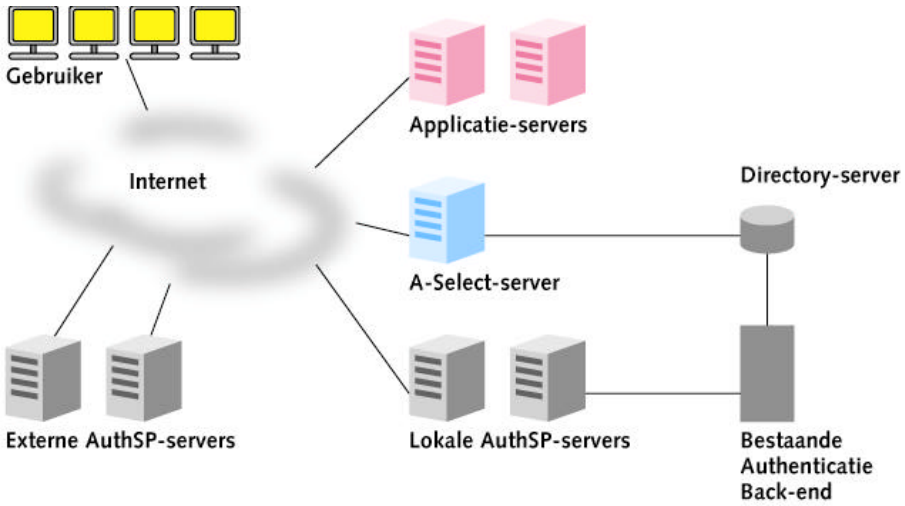
Naast netwerkdiensten ontwikkelt SURFnet binnen de innovatieprojecten SURFworks NG en SURFnet/Kennisnet toepassingen gericht op respectievelijk instellingen en eindgebruikers. Het SURFworks NG programma richt zich voornamelijk op de ontwikkeling van geavanceerde *middleware* en security gerelateerde services voor onderzoek en onderwijs. Daarbij ligt de focus op de ontwikkeling van Authenticatie- en Autorisatie-Infrastructuur (AAI) en CSIRT[4]-gerelateerde dienstverlening. Het samenwerkingsprogramma tussen Kennisnet en SURFnet richt zich in hoofdlijnen op het ontwikkelen van innovatieve toepassingen voor onderwijsdoeleinden zoals multimediale toepassingen. Een volledige beschouwing van de diensten die uit deze programma's voortkomen valt buiten het kader van dit document. In het licht van dit rapport is er voor gekozen met name de onderwerpen authenticatie- en autorisatie-infrastructuur en video streaming te behandelen.

Authenticatie- en autorisatie-infrastructuur
Voor eindgebruikers is het van belang om de functionaliteit die binnen het domein van de eigen instelling beschikbaar is ook op andere lokaties (bijvoorbeeld bij andere instellingen) te kunnen gebruiken. Een operationeel voorbeeld hiervan is EduRoam[5], dat zich richt op netwerktoegang op basis van authenticatie middels IEEE 802.1x. Deze dienst maakt gastgebruik mogelijk van de (wireless) netwerken van de participerende instellingen. SURFnet is in de onderliggende RADIUS infrastructuur de nationale *trusted third party*.

Op het gebied van applicatietoegang biedt SURFnet de authenticatievoorziening A-select. A-select is een innovatief '*open source*' middleware product dat *single-sign-on* (SSO) en de keuze van verschillende authenticatiemechanismen mogelijk maakt voor een breed scala aan toepassingen. De authenticatie-infrastructuur die hiermee kan worden ingericht dient zowel het gemak als de veiligheid. Gemak voor de gebruikers die maar één keer hoeven in te loggen, en gemak vanuit het oogpunt van beheer van de authenticatiemethoden dat nu centraal en dus eenvoudiger kan worden georganiseerd. Daarnaast kan de veiligheid beter gewaarborgd worden door het gebruik van de juiste authenticatiemethoden (met een sterkteniveau naar keuze) in combinatie met versleuteling van het dataverkeer. Bij sterke authenticatie, zoals de SURFkey, wordt gebruik gemaakt van de combinatie van iets dat de gebruiker heeft en iets dat de gebruiker weet (ook wel twee-factor authenticatie genaamd) zoals een bankpas of mobiele telefoon in combinatie met een pincode. A-select maakt het mogelijk ook externe Authenticatie Service Providers te gebruiken waardoor de lokale authenticatie infrastructuur beperkt kan blijven terwijl de authenticatiemogelijkheden toenemen. Figuur 7 laat zien hoe een dergelijke architectuur er uit ziet waarbij de A-select server via Internet kan communiceren met gebruikers, applicaties en lokale en externe authenticatie-servers.

[4] Computer Security Incident Response Team

[5] Zie http://www.eduroam.nl/



Figuur 7 *De A-select server zorgt er voor dat de applicatie-servers van een instelling kunnen communiceren met de lokale of externe authenticatie-servers*

In de administratieve *identity management* omgeving speelt naast authenticatie (Wie ben je?) ook autorisatie (Wat mag je?) een belangrijke rol. Op basis van gegeven gebruikerskenmerken kunnen bepaalde bevoegdheden worden verleend. Internet2 heeft hiervoor de middleware applicatie Shibboleth ontwikkeld. Shibboleth bepaalt op basis van 'attributen' (persoonlijke kenmerken) tot welke informatie of applicatie een gebruiker wel of geen toegang krijgt. A-select en Shibboleth zijn complementair. SURFnet werkt daarom samen met Internet2 om een complete identity management oplossing te kunnen bieden.

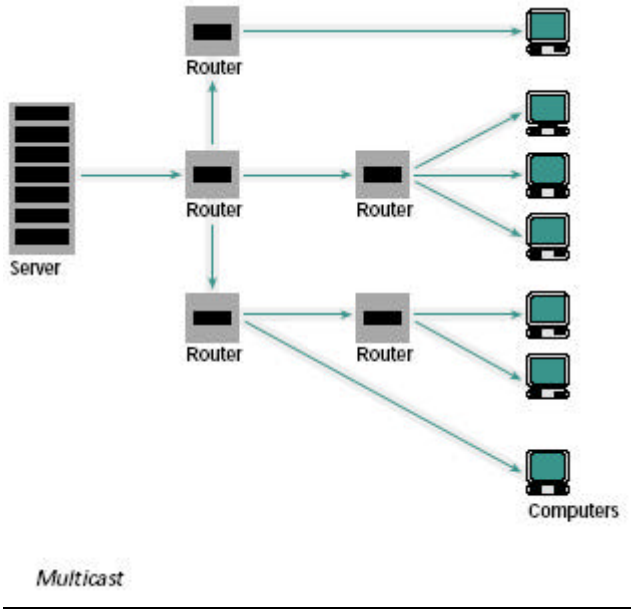
Streaming media

SURFnet biedt *streaming* diensten aan via de SURFnet Videotheek (eerder het SURFnet Video Portal). Deze biedt instellingen en eindgebruikers de mogelijkheid zelf *on-demand* streaming audio en video aan te bieden. Daarnaast is het mogelijk live uit te zenden. Het portal ondersteunt de formaten MPEG-1, -2 en – 4, MP3 en Windows Media. De on-demand audio en videobestanden kunnen naar wens worden afgeschermd. Er is reeds voor vele duizenden uren streaming audio en video beschikbaar en al 75 instellingen hebben audio- en videobestanden van en voor hun gebruikers opgeslagen op de SURFnet Videotheek. Naast de mogelijkheid dat instellingen zelf hoge kwaliteit audio en video kunnen uitzenden, bijvoorbeeld van een congres, een collegereeks of bijeenkomsten in de aula, zendt SURFnet ook een aantal kanalen uit. Alle SURFnet-TV uitzendingen zijn in verschillende formaten te bekijken, waarbij de hoge (TV) kwaliteit kanalen alleen op voor multicast-ingerichte netwerken te ontvangen zijn.

Hoewel streaming met compressietechnieken de benodigde bandbreedte met een factor 10 tot 100 kan reduceren, kunnen videostromen een aanzienlijke hoeveelheid verkeer genereren (orde grootte 1,5 Mbit/s[6] per stream). Indien gebruik gemaakt wordt van *unicast* worden deze multimedia verkeerstromen parallel over het netwerk vervoerd. Afhankelijk van de beschikbare bandbreedte kan het cumulatieve effect bij grootschalige (live-) uitzendingen al snel voor

[6] Afhankelijk van het gebruikte format; MPEG 2 met TV kwaliteit behoeft bijvoorbeeld 5 Mbit/s.

congestie in het netwerk zorgen. *Multicast* functionaliteit biedt hiervoor een oplossing door verkeersstromen naar verspreide gebruikers maar één keer te versturen zolang deze verkeersstroom dezelfde route volgt. Hiermee wordt de netwerkbelasting aanzienlijk gereduceerd doordat er efficiënter wordt omgesprongen met bandbreedte en is de beschikbaarheid en de kwaliteit veel hoger dan bij het gebruik van alleen unicast. Voorwaarde is wel dat alle routingapparatuur op de betreffende route deze multicast functionaliteit ondersteunt, zie Figuur 8. Overigens moeten in een campusomgeving ook de Ethernet switches de juist features ondersteunen om te zorgen dat multicast correct functioneert.



Figuur 8 : *Enkelvoudige verkeersstromen via routers met multicast functionaliteit*

Multicast is niet alleen interessant voor gebruikers maar ook van groot belang voor aanbieders van content. Onder meer het NOB heeft aangegeven grote hoeveelheden voor het onderwijs relevante content beschikbaar te willen stellen via het SURFnet-netwerk mits multicast op grotere schaal wordt ingevoerd. Het SURFnet-netwerk ondersteunt deze functionaliteit sinds jaar en dag, echter een belangrijk deel van de aangesloten instellingen heeft deze technologie tot nu toe niet geïmplementeerd. In 2005 voert SURFnet een multicast-diffusieproject uit (incl. hands-on support on-site) teneinde het aantal aangesloten instellingen dat deze technologie tot in de haarvaten van het netwerk ondersteunt significant te verhogen.

4 Betekenis voor de campusinfrastructuur

4.1 Inleiding: impact op de lokale infrastructuur

De ontwikkelingen in het gebruik van ICT in het hoger onderwijs en onderzoek, die SURFnet er toe hebben aangezet het dienstenportfolio en de netwerkfunctionaliteit aan te passen, hebben ook infrastructurele gevolgen voor de aangesloten instellingen. De benodigde aanpassingen in de campusinfrastructuur zijn afhankelijk van het soort gebruik en de functionaliteit die de instellingen wensen te faciliteren. Met name het doorzetten van de lichtpadfunctionaliteit ten behoeve van high-end onderzoekstoepassingen vereist investeringen in apparatuur en glasvezelbekabeling en vraagt om nieuwe beheerprocedures.

De evolutionaire ontwikkelingen rond multimediale eindgebruikers kunnen grotendeels worden opgevangen door overprovisioning in het IP-domein. Hetzelfde geldt voor de, in hoofdstuk 2 geschetste, operationele toepassingen. De bestaande vraagstukken van IT-managers ten aanzien van netwerkbeheer, performance, beveiligingsproblematiek e.d. veranderen hierdoor dan ook niet noemenswaardig. Voor wat betreft het faciliteren van revolutionaire high-end onderzoekstoepassingen geldt dit echter niet. De introductie van point-to-point lichtpaden in een campusomgeving heeft aanzienlijke gevolgen voor zowel de infrastructuur als het netwerkbeheer.

Paragraaf 4.2 gaat verder in op de aandachtspunten voor de campusinfrastructuur. Op basis daarvan worden in paragraaf 4.3 een aantal concrete aanbevelingen gedaan. Onderwerpen die meer aandacht behoeven en die in de komende periode in samenwerking met de instellingen moeten worden aangepakt worden benoemd in 4.4.

4.2 Aandachtspunten voor de campusinfrastructuur

De betekenis van de geschetste ICT ontwikkelingen voor de campusinfrastructuur is in de volgende paragrafen aan de hand van de nieuwe SURFnet-diensten beschreven. Hierbij is een onderverdeling gemaakt tussen enerzijds de evolutionaire ontwikkelingen in het onderwijs- en organisatiedomein en anderzijds revolutionaire high-end onderzoekstoepassingen. Er is gekozen voor een vrij generieke beschrijving van de betreffende aandachtsgebieden. In veel gevallen zijn de consequenties van de besproken thema’s afhankelijk van de lokale situatie en zal een daaruit volgende infrastructurele aanpassing maatwerk zijn. De volgende paragrafen zijn dan ook vooral richtinggevend bedoeld.

4.2.1 Ondersteuning multimediale eindgebruikers en operationele toepassingen

De geschetste ontwikkelingen rondom multimediale eindgebruikers en operationele toepassingen kunnen grotendeels worden opgevangen door het campusnetwerk inclusief de WAN aansluiting over te dimensioneren op IP niveau. Wat betreft de WAN aansluiting kunnen instellingen gebruik maken van de 1 Gbit/s en 10 Gbit/s IP-diensten van SURFnet6. De lokale campusinfrastructuur dient uiteraard ook zodanig gedimensioneerd te worden dat de groeiende gebruikersvraag kan worden gefaciliteerd. Hieronder volgt een korte beschrijving van de belangrijkste aandachtspunten ten aanzien van de SURFnet-aansluiting, de backbone apparatuur, de glasvezelbekabeling, beveiliging en het koppelen van vestigingen.

4.2.1.1 De SURFnet aansluiting: IP-connectiviteit met GbE en 10 GbE interfaces
De SURFnet IP-aansluiting vraagt aan de kant van de instellingen om de volgende functionaliteit op de L3 apparatuur:

- 1 GbE interfaces of 10 GbE interfaces (LAN PHY[7])
- 1 of 2 poorten, afhankelijk van de fysieke en/of logische plek in het netwerk[8]
- Afhankelijk van hoe de resiliency geregeld wordt: ofwel door statische routering over één poort met resiliency in het SURFnet6 netwerk (Virtual Router Redundancy Protocol) ofwel met behulp van het Border Gateway Protocol tussen de SURFnet6 routers en de router(s) van de instelling. In dit laatste geval is ondersteuning van BGP4 noodzakelijk.[9]
- IPv4 en IPv6 unicast (SURFnet adviseert hiervoor een dual-stack oplossing te gebruiken)
- IPv4 en IPv6 multicast (SURFnet adviseert hiervoor een dual-stack oplossing te gebruiken)

In het geval een instelling ook lokaties aan de lokale zijde op redundante (en op fysiek gescheiden) wijze wil aansluiten, met één poort als back-up, zal in de meeste gevallen ook ondersteuning van BGP noodzakelijk zijn.

4.2.1.2 Backbone apparatuur: functionaliteit vs. performance (en prijs)
Bij het opschalen van de campus-backbone spelen een aantal architectuurvraagstukken. Een belangrijk aspect is het vaststellen van de gewenste L2 en L3 functionaliteit voor het netwerk. Naast de prijsprestatie verhouding zal er een afweging moeten worden gemaakt tussen flexibiliteit (routing) en performance (switching). Het consolideren van dure routing apparatuur, zoals in het SURFnet6-netwerk, kan ook binnen campusinfrastructuren kostenbesparingen opleveren. Het SURFnet ontwerpprincipe van overprovisioning geldt ook voor de campusbackbone. Het implementeren van de eerder besproken multicast functionaliteit in de backbone is bij uitstek geschikt om de performance van multimediale toepassingen zoals video streaming te verbeteren.

---

[7] LAN PHY: 10 GbE interface met LAN *Physical Layer* en lijnsnelheid 10,3 Gbit/s. Dit i.t.t. de 10 GbE WAN PHY waarbij is voorzien in SDH *framing* en *overhead* resulterend in een *payload* van 9,3 Gbit/s.
[8] Voor verdere details wordt verwezen naar het SURFnet document: " De overgang naar SURFnet 6: Wat staat u te wachten?" Dit document is beschikbaar via http://netwerk.surfnet.nl/
[9] Zie voetnoot 8.

Op het moment dat het verkeersvolume daarom vraagt zal de campus-backbone opgeschaald moeten worden naar GbE, multiple GbE of zelfs 10 GbE. Indien de bestaande apparatuur 10 GbE interfaces ondersteunt, is een upgrade van apparatuur relatief eenvoudig. Bij het opwaarderen van de interfaces dient echter altijd rekening gehouden te worden met de te overbruggen afstanden. Voor 1 GbE en 10 GbE over multimode (MM) en singlemode (SM) glasvezel gelden typisch de specificaties zoals te zien in tabel 1.

Interfaces	**Short Range 850 nm (MM)**	**Long Range 1310 nm (SM)**	**Extended Range 1550 nm (SM)**
1 GbE	550 m	5 km *	70 km
10 GbE	300 m **	10 km	40 km

* Dit betreft de specifieke standaardwaarde. Deze is sterk afhankelijk van het vermogen van de lichtbron en fabrikanten leveren daarom vaak andere specificaties (Cisco's LX/LH haalt bijvoorbeeld ruim 10 km).
** Dit geldt enkel voor multimode glasvezel met geoptimaliseerde index en 50 micron kern (zogenaamde OM3 vezel).

Tabel 1 *Afstanden volgens IEEE standaarden bij verschillende gangbare Ethernet interfaces.*

Algemeen geldt dat vanwege de dispersie-eigenschappen[10] een 1GbE signaal verder getransporteerd kan worden dan een 10GbE signaal. Dat dit niet consequent zichtbaar is in de tabel is een gevolg van door standaardisatie-fora gekozen waarden. Naast de lichtbron spelen met name de optische eigenschappen van de glasvezel een belangrijke rol bij de maximale afstand. De verschillende eigenschappen van multimode en singlemode glasvezel worden kort besproken in de volgende paragraaf.

4.2.1.3 Glasvezelbekabeling: een toekomstvaste infrastructuur?

Een hogere bitsnelheid in de backbone stelt ook eisen aan de bekabeling. Bij gebouwbekabeling wordt vaak multimode glasvezel gelegd om goedkopere lichtbronnen (apparatuur) te kunnen gebruiken. Bij hogere bitrates is de afstand waarover deze multimode bekabeling kan worden gebruikt echter zeer beperkt. Vandaar dat outdoor over het algemeen singlemode glasvezelbekabeling wordt toegepast. Ter indicatie zijn de maximale afstanden voor de verschillenden typen glasvezel zoals opgesteld in de huidige bekabelingstandaarden[11] weergegeven in Tabel 2.

	Transmissie afstand		
Transmissie snelheid	**300 m**	**500 m**	**2000 m**
100 Mbit/s	OM1	OM1	OM1
1000 Mbit/s	OM1	OM2	OS1
10000 Mbit/s	OM3	OS1	OS1

Tabel 2 *Maximale transmissiesnelheden voor diverse gebouw-glasvezelbekabeling.*

[10] Dispersie is het fenomeen van pulsverbreding waardoor "nullen en enen" onherkenbaar worden. Dit effect is sterker bij hoge bitrates en/of langere afstanden.

[11] ISO 11801 2nd edition, standaard voor gebouwbekabeling, zie ook TIA/EIA 568B.

OM1 t/m OM3 zijn verschillende typen multimode glasvezelbekabeling. OS1 is singlemode glasvezel. De geoptimaliseerde OM3 vezel is de enige multimode vezel die geschikt is om 10 Gbit/s te transporteren, echter tot maximaal 300 meter. Een 10 Gbit/s link over langere afstanden vraagt dus altijd om singlemode glasvezel. Bij de keuze voor singlemode glasvezel is het vooral van belang er op te letten dat het type vezel geschikt is voor het transporteren van meerdere lichtsignalen (Wave Division Multiplexing). De veelvoorkomende ITU G.652 vezel en de nieuwere G.655 standaard voldoen beide aan deze eis en bieden daardoor een toekomstvaste oplossing. Binnen gebouwen wordt bij twijfel tegenwoordig vaak voor een flexibele invulling gekozen: *blowable ducts*. Dit is een buizeninfrastructuur waar glasvezel naar wens kan worden ingeblazen. Hiermee wordt een schaalbare infrastructuur gecreëerd waarin multimode glasvezel in een later stadium eenvoudig kan worden aangevuld of vervangen door singlemode glasvezel. Tabel 3 geeft een samenvattend overzicht van de voor- en nadelen van de verschillende bekabelingmogelijkheden.

	Bekabelingmogelijkheden		
Eigenschappen	**Multimode**	**Singlemode**	**Blowable duct**
Overbrugbare afstand	-	+	o
Kosten (incl.apparatuur)	+	-	+/-
Schaalbaarheid	-	+	++

Tabel 3 *Eigenschappen van de verschillende oplossingen voor gebouw-glasvezelbekabeling*

Bekabeling is ook een belangrijk aspect indien wordt besloten de aansluitingen op de werkplek op te waarderen van 10 Mbit/s of 100 Mbit/s naar 1 Gbit/s. Hiervoor dient de gebruikte UTP bekabeling te voldoen aan de Cat 5e of Cat 6 standaarden[12]. Beide standaarden ondersteunen 1 Gbit/s zij het op basis van verschillende technische oplossingen. Gezien de vooralsnog beperkte beschikbaarheid van op Cat 6 aangepaste apparatuur is het moeilijk een duidelijke voorkeur uit te spreken. Er wordt momenteel overigens ook gewerkt aan een 10 GbE standaard[13] over UTP tot 100 meter waarvan reeds de eerste pre-standaard producten op de markt verkrijgbaar zijn.

4.2.1.4 Beveiliging: DDoS risico's

Op het gebied van beveiling zijn er geen noemenswaardige veranderingen die samenhangen met het opschalen van de IP infrastructuur. Een uitzondering betreft de kwetsbaarheid voor Distributed Denial of Service (DDoS) aanvallen, die hier wel aan is gerelateerd. Op het moment dat de WAN aansluiting van een instelling een hogere capaciteit krijgt vergroot dit tevens de risico's ten aanzien van DDoS aanvallen vanuit de instelling / campus naar buiten. Voor het collectief neemt het risico voor een DDoS aanval van buiten gericht op een systeem van een instelling dan ook toe. Filtering biedt hier een matige oplossing omdat het filterende systeem of het systeem dat zich net daarvóór bevindt, zoals bijvoorbeeld een firewall, op dat moment al overbezet raakt en niet meer door legitieme gebruikers te benaderen is. Op dit moment wordt er

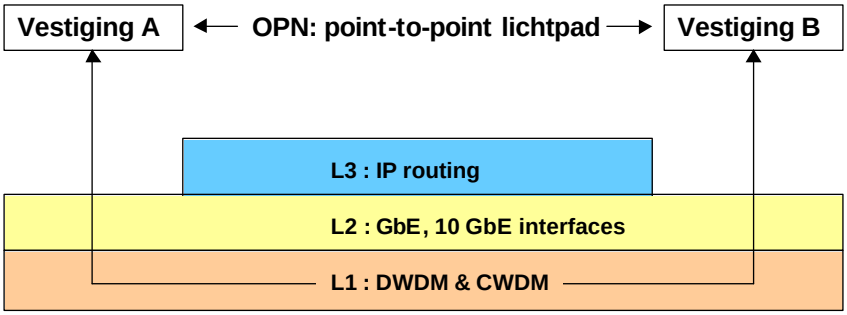
[12] ISO 11801 2nd edition, standaard voor gebouwbekabeling, zie ook TIA/EIA 568B.

[13] IEEE 802.3an, planning 2006

gewerkt aan tools om dergelijke aanvallen reeds in de backbone van SURFnet te detecteren en daar maatregelen te treffen.

4.2.1.5 Het koppelen van vestigingen: Een Optisch Privaat Netwerk (OPN)
Het koppelen van vestigingen brengt een aantal problemen met zich mee, vooral wanneer grote bandbreedtes of korte responstijden worden gevraagd. De lichtpadfunctionaliteit van SURFnet6 maakt het mogelijk op eenvoudige wijze vestigingen te koppelen via een OPN. De OPN configuratie biedt een eenvoudig beheersbare oplossing omdat switches van de verschillende lokaties met GbE of 10 GbE 'rechtstreeks' en volledig transparant (via L1 point-to-point verbindingen) aan elkaar worden gekoppeld. Aan de kant van de instellingen is alleen een standaard GbE of 10 GbE interface nodig. Het verkeer blijft binnen het eigen netwerk en hoeft niet door een firewall heen. Het LAN wordt als het ware transparant doorgezet naar de overige OPN lokaties. Daarbij heeft de instelling uiteraard de keuze of het LAN daadwerkelijk wordt verbonden op laag 2 of dat er gerouteerd wordt tussen subnets op verschillende lokaties.

De karakteristieken van lichtpaden: capaciteit, kwaliteit en veiligheid maken een OPN zeer geschikt als onderliggende infrastructuur voor het consolideren van systemen en het centraliseren van beheer.



Figuur 9 *Optical Private Network: statische point-to-point lichtpaden tussen vestigingen*

Eén van de instellingen die kijkt naar de mogelijkheden van een OPN is Wageningen UR. De geografisch verspreide lokaties worden in de huidige situatie middels verschillende IP-VPN verbindingen en huurlijnen verbonden met Wageningen. Het resultaat is een redelijk complexe configuratie met encryptie en tunnelling ten behoeve van multicast en routeringsprotocollen. Daarnaast moet al het VPN verkeer door de lokale firewalls geleid worden, wat zowel de prestatie van de firewall als die van de verbindingen vermindert. Op het moment dat de grotere lokaties met een OPN verbinding worden gekoppeld levert dit een aantal voordelen op:

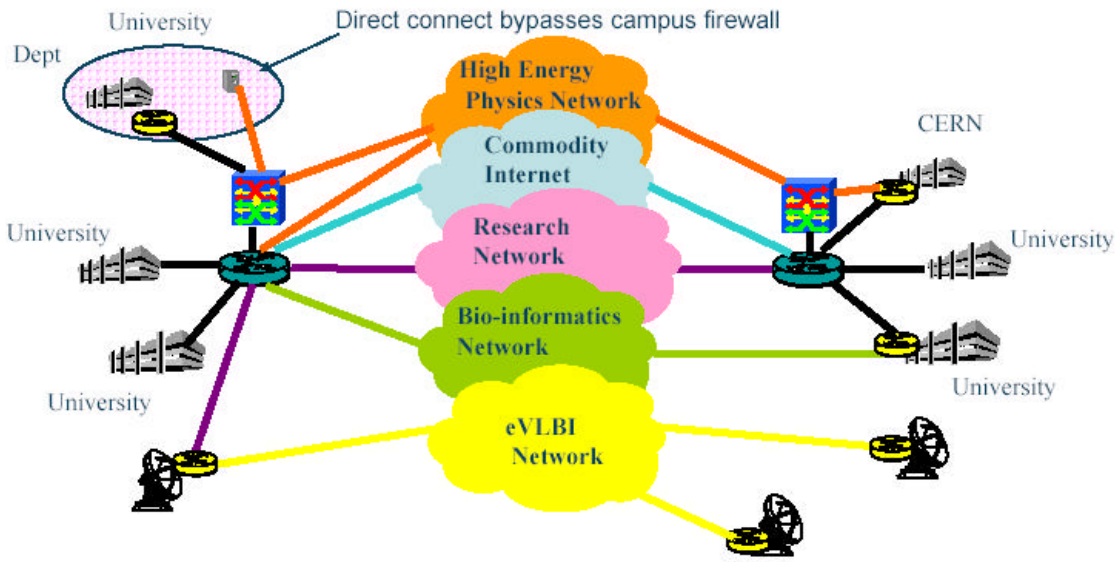
- Het verkeer hoeft niet langer door een firewall tussen twee lokaties;
- Het verkeer is gescheiden op laag 1 waardoor geen encryptie nodig is;
- De laag 1 verbinding is transparant voor het Ethernet protocol. Er is dus geen tunneling meer nodig van routeringsprotocollen e.d.

Een OPN constructie is aantrekkelijk voor instellingen met verschillende vestigingen die met betrouwbare zware verbindingen gekoppeld moeten worden. Inmiddels zijn OPNs tevens

aangevraagd door de Hogeschool INHOLLAND, de Avans Hogeschool, de Hogeschool Leiden, de Hogeschool Arnhem en Nijmegen en de Hogeschool Drenthe.

4.2.2 Ondersteuning high-end onderzoekstoepassingen

De in hoofdstuk 3 besproken power users in gebruikscategorie C, vragen om zeer breedbandige verbindingen en om onderzoeksnetwerken gericht op specifieke toepassingen. Figuur 10 laat een schema zien dat dit illustreert. Een aantal toepassingen vraagt om transparante point-to-point verbindingen die ook door de lokale campusinfrastructuur gefaciliteerd zullen moeten worden. Dergelijke verbindingen worden noodzakelijkerwijs om de campus-firewalls heen geleid en in het beheer van deze verbindingen spelen de betrokken onderzoeksgroepen een belangrijke rol. Het doorzetten van lichtpaden vanaf de SURFnet PoP naar wetenschappelijke gebruikers heeft daarom ingrijpende gevolgen voor zowel de apparatuur- en glasvezelinfrastructuur als op het gebied van netwerkbeheer en -beveiliging.



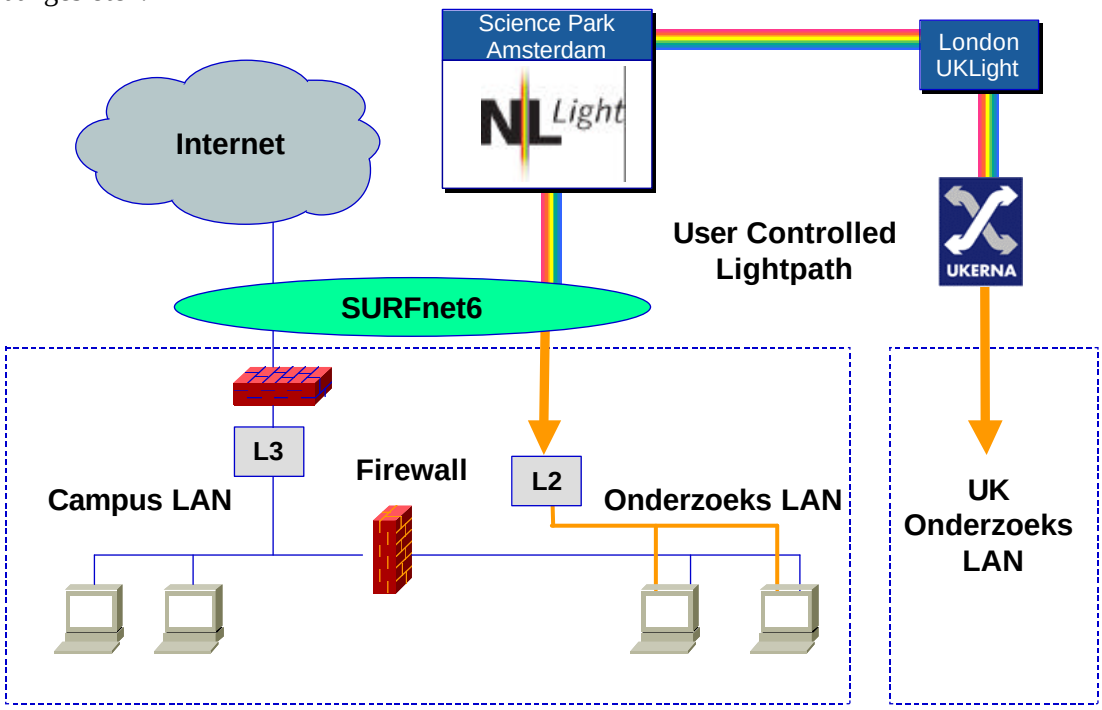
Figuur 10: *Er ontstaan onderzoeksnetwerken voor specifieke toepassingen die in sommige gevallen de campus firewall omzeilen.* [14]

4.2.2.1 Glasvezelinfrastructuur en/of additionele apparatuur?

Het doorzetten van lichtpaden naar wetenschappelijke eindgebruikers of onderzoeksopstellingen vraagt afhankelijk van de gewenste implementatie de nodige aandacht. Het lichtpad wordt door SURFnet op de lokaal ingerichte PoP uitgekoppeld met GbE of 10 GbE framing. Het verdient aanbeveling deze verbinding vervolgens gescheiden te houden van het operationele campus IP-

[14] Bron: Bill St. Arnaud, CANARIE

netwerk. Het handhaven van een hybride structuur garandeert de prestaties van de betreffende verbinding en ontziet bovendien de rest van het campusverkeer. Figuur 11 laat zien hoe een dergelijke lokale lichtpad-infrastructuur kan worden ingericht naast het operationele IP-netwerk. Door gebruik te maken van de SURFnet lichtpad-functionaliteit kunnen power users via NetherLight internationale point-to-point verbindingen opzetten. Een lokale campusinfrastructuur die de betreffende onderzoekssystemen verbindt met de SURFnet PoP is hierbij uiteraard een voorwaarde. Afhankelijk van de specifieke toepassing kan er voor worden gekozen een onderzoeks-LAN in te richten waaraan verschillende eindsystemen worden opgehangen, zoals in figuur 11, of kan een eindsysteem direct op een lichtpad worden aangesloten.



Figuur 11 : *Vereenvoudigd schema van een hybride campus netwerkarchitectuur*

Er zijn vervolgens verschillende implementatiemogelijkheden die onder meer afhankelijk zijn van de afstand van de betrokken power users tot de SURFnet PoP, het aantal vereiste lichtpaden en de reeds beschikbare (glasvezel)infrastructuur:

- De eenvoudigste constructie biedt de eindgebruiker een rechtstreeks glasvezelpaar naar de SURFnet PoP. Daarbij dient rekening gehouden te worden met de problematiek rond afstanden en interfaces voor wat betreft glasvezelverbindingen zoals besproken in paragraaf 4.2.1. Voordeel van deze configuratie is dat de verbinding relatief eenvoudig losgekoppeld kan worden van het reguliere campusnetwerk.

- Indien er voor wordt gekozen om meer lichtpaden door te zetten naar eindgebruikers dan wel deze op meer (werk)plekken beschikbaar te maken, zijn er verschillende mogelijkheden. Om dit efficiënt te doen dient men afwegingen te maken voor wat betreft het gebruik van

glasvezel en apparatuur. Naast het gebruiken van meer point-to-point glasvezels kan ook worden gekeken naar Coarse Wave Division Multiplexing (CWDM) oplossingen waarbij binnen bepaalde afstanden tegen relatief lage kosten meer lichtpaden op één vezelpaar kunnen worden doorgezet. Hiermee kan door middel van een ringconfiguratie op verschillende plekken een lichtpad worden af- en aangekoppeld. De afwegingen ten aanzien van de inzet van CWDM apparatuur zijn vanzelfsprekend sterk afhankelijk van de beschikbare glasvezelcapaciteit en de ligging van eindgebruikerlokaties ten opzichte van de SURFnet PoP.

- Aangezien de lichtpaden worden aangeboden via een Ethernet interface is het ook mogelijk deze in het campusnetwerk af te handelen met L2 apparatuur. Het heeft de voorkeur hierbij te kiezen voor *dedicated* switches die samen een afgescheiden onderzoeks-LAN vormen. Eventueel kan hier ook operationele netwerkapparatuur voor worden ingezet. In dit laatste geval zal er echter een afweging gemaakt moeten worden tussen het beschermen van het operationele verkeer en het aanbieden van “gegarandeerde lichtpad-functionaliteit”.

4.2.2.2 Netwerkbeheer en beveiliging

Vanuit de netwerkbeheerder gezien is het aanbieden van lichtpaden aan eindgebruikers een revolutionaire ontwikkeling. Lichtpaden zullen in de meeste gevallen het operationele gerouteerde campusnetwerk inclusief de campus firewall omzeilen. Het zijn in principe transparante end-to-end verbindingen tussen onderzoeksgroepen. Uiteraard gaat het hier om partijen die elkaar onderling vertrouwen maar de lokale netwerkbeheerder heeft dus geen inzicht in het gebruik. De power users krijgen bovendien op termijn faciliteiten om zelf extern aan dynamische lichtpad provisioning te doen. Hiervoor worden in het kader van het GigaPort Next Generation Network project verschillende platformen onderzocht zoals User Controlled Lightpath Provisioning (UCLP). De vraag is dan ook waar de grens komt te liggen tussen de beheerverantwoordelijkheden van de netwerkbeheerder en die van de eindgebruiker.

Het ligt voor de hand dat op een lichtpad aangesloten onderzoekssystemen tevens operationele IP connectiviteit nodig hebben. Het koppelen van werkstations in het onderzoeks-LAN met het IP campusnetwerk moet echter wel zorgvuldig gebeuren. Het is mogelijk om te werken met dubbele netwerkkaarten in dezelfde host/server maar dit kan leiden tot “een achterdeur in de beveiliging” en brengt daarmee beveiligingsrisico’s met zich mee.
Om het onderzoeks-LAN verantwoord te koppelen met het operationele netwerk (en het Internet) moet er daarom een firewall tussen worden geplaatst analoog aan het schema in figuur 11. De beveiliging van de lichtpad-diensten zelf is iets wat geregeld zal moeten worden op middleware- en applicatieniveau. Middleware toepassingen zoals A-select en Shibboleth kunnen bij de afscherming een rol spelen; dit aspect vraagt eveneens aandacht in de komende periode.

4.3 Aanbevelingen

Een aantal elementen in de besproken aandachtsgebieden zijn generiek. De lokale situatie is echter vaak bepalend en infrastructurele aanpassingen zullen over het algemeen dan ook maatwerk zijn. In de paragrafen hieronder volgen op basis van de voorgaande discussie van aandachtspunten een aantal generieke aanbevelingen die dienen als ontwerpregels voor toekomstige campusinfrastructuren.

4.3.1 Ondersteuning multimediale eindgebruikers en operationele toepassingen

- *Overprovisioning van de WAN aansluiting*. Kies afhankelijk van de voorziene behoefte aan IP-bandbreedte de juiste IP-dienst van SURFnet. Hierbij dient de L3 apparatuur van de instellingen te voldoen aan de voorgeschreven functionaliteit. Dat wil zeggen GbE of 10 GbE interfaces, noodzakelijke routeringprotocollen etc. Daarnaast beveelt SURFnet ondersteuning aan van IPv6 en multicast.
- *Overprovisioning van de backbone*. Maak bij een eventuele opwaardering van de backbone apparatuur een goede afweging tussen flexibiliteit (routering) vs. performance (switching). Bij het opwaarderen van GbE backbones kan in eerste instantie worden gedacht aan meerdere parallelle GbE kanalen. Op het moment dat de stap naar 10 Gbit/s wordt gemaakt zal goed naar de combinatie van beschikbare interfaces en de onderliggende glasvezelinfrastructuur moeten worden gekeken.
- *Kies voor een toekomstvaste glasvezelinfrastructuur*. In verband met de afstandenproblematiek rondom multimode glasvezel is het verstandig bij nieuwe investeringen voor een flexibele, toekomstvaste infrastructuur te kiezen. Zeker in de backbone moet de keuze voor singlemode glasvezel of een blowable duct systeem worden overwogen. Echter ook in de uitlopers moeten de beperkingen van multimode glasvezel in ogenschouw worden genomen.
- *Gebruik multicast ten behoeve van multimediale toepassingen*. Overprovisioning in het IP-domein blijkt nog steeds een eenvoudig en goed ontwerpprincipe, ook voor de campusinfrastructuur. Het implementeren van multicast functionaliteit in het netwerk kan de belasting door multimediale toepassingen zoals video streaming echter behoorlijk reduceren. Daarnaast is ondersteuning van multicast vaak een voorwaarde vanuit content aanbieders.
- *Richt een adequate authenticatie en autorisatie-infrastructuur in.* Om gebruikers beter te bedienen is een goede AAI-infrastructuur met aandacht voor netwerktoegang en applicatietoegang essentieel. Instellingen wordt geadviseerd om aan te sluiten bij de lopende initiatieven rond EduRoam en A-select.
- *Overweeg OPNs voor het koppelen van vestigingen.* De lichtpadfunctionaliteit kan worden gebruikt om op een eenvoudige en transparante wijze vestigingen te koppelen via een OPN. Vanuit beheersoogpunt is dit een zeer interessante oplossing voor de beperkingen van de gangbare (IP-) VPN’s.

4.3.2 Ondersteuning high-end onderzoekstoepassingen

- *Realiseer een lokale infrastructuur voor lichtpaden.* Vanuit het oogpunt van performance is het verstandig lichtpaden die worden aangeboden aan power users zoveel mogelijk gescheiden te houden van het overige verkeer. Het ontwerp van een hybride structuur beschermt het operationele campusverkeer en garandeert tevens de kwaliteit van het end-to-end lichtpad.
- *Voorzie in voldoende glasvezelcapaciteit*. Teneinde de vraag naar lichtpaden te faciliteren is er voldoende glasvezelcapaciteit nodig zowel in de backbone als in de richting van eindgebruikers.
- *Voorzie in adequate apparatuur.* Indien er meer lichtpaden naar eindgebruikers worden doorgetrokken zal een afweging moeten worden gemaakt tussen een investering in glasvezel of (CWDM/LAN) apparatuur.
- *Zorg voor een veilige koppeling van het operationele netwerk met het onderzoeks-LAN*. De lokale lichtpaden omzeilen de campus firewall. Het onderzoeks-LAN zal via een firewall moeten worden gekoppeld aan het operationele IP netwerk.

4.4 Open issues

Niet alle noodzakelijke aanpassingen zijn op dit moment uitgewerkt, een aantal specifieke aandachtspunten moet in de komende periode verder worden uitgewerkt, waarbij ook de ervaringen in het buitenland zullen worden meegenomen. Het betreft dan onder meer de volgende zaken:

- Onderzoek naar de optimale wijze waarop lichtpadfunctionaliteit naar power users kan worden doorgezet, waarbij onder meer de gevolgen van een lokale infrastructuur voor lichtpaden op het gebied van beveiliging en netwerkbeheer zullen worden verkend. Daarvoor wordt onder meer gekeken naar University College London
- Het ontwikkelen van *best practices* voor het automatisch opzetten van dynamische lichtpaden door eindgebruikers;
- Het verder integreren en uitwerken van authenticatie- en autorisatie-infrastructuren met als doelstelling Universal Single Sign-On.

Bijlage A Afkortingen

AAI	Authenticatie- en Autorisatie-Infrastructuur
ASP	Applicatie Service Provider
BaMa	Bachelor-Master-model
BGP	Border Gateway Protocol
CPL	Common Photonic Layer
CWDM	Coarse Wave Division Multiplexing
DDoS	Distributed Denial of Service (aanval)
DWDM	Dense Wave Division Multiplexing
GbE	Gigabit Ethernet
Gbit/s	Gigabit per seconde
GLIF	Global Lambda Integrated Facility
IEEE	Institute of Electrical and Electronics Engineers
KIS	Keep It Simple
L1,2,3	OSI laag 1,2,3
LAN	Local Area Network
LHC	Large Hadron Collider
LOFAR	LOw Frequency ARray
Mbit/s	Megabit per seconde
MDF	Managed Dark Fiber
MM	Multimode
MPEG	Moving Picture Experts Group
NOC	Network Operation Center
OPN	Optical Private Network
OM1,2,3	Optical Multimode 1,2,3
OS1	Optical Singlemode 1
OSI	Open Systems Interconnection
RADIUS	Remote Authentication Dial-In User Service
SM	Singlemode
SSO	Single Sign-On
SVP	SURFnet Video Portal
UCLP	User Controlled Lightpath Provisioning
UTP	Universal Twisted Pair
VLBI	Very Long Baseline Interferometry
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network