Techniek - Architectuurblauwdruk architectuurgebied Netwerk V1.1

Kaders en richtlijnen

Inhoudsopgave

Documentbeheer

Revisiegeschiedenis

Versie	Opmerkingen
0.1	Opzet document en opname beschrijvingen module Backbone
0.2	Generieke update module Backbone en opname beschrijvingen module Locatie, Datacenter, Cloud en use cases
0.9	Generieke update o.b.v. feedback versie 0.2 + opname WLAN en Azure
1.0	Laatste update o.b.v. feedback versie 0.9 (WLAN + Azure)
1.1	Update use cases

Contactpersonenlijst

Classificatie

	Categorie	Toelichting
	Laag	Informatie geschikt voor algemene publicatie en externe distributie.
✓	Midden	Informatie die gevoelig is en enkel bestemd voor een beperkte groep.
	Hoog	Informatie die zeer gevoelig is en enkel bestemd voor specifiek benoemde personen.

1 Introductie en achtergrond

1.1 Werken onder architectuur

Met het 'werken onder architectuur' wordt ervoor gezorgd, dat losse onderdelen in hun samenhang worden ontworpen, zowel op het niveau van de business, de informatievoorziening als de technische middelen. Een architectuurblauwdruk bevat een samenhangende beschrijving van de door het ROC gebruikte en geleverde ICT-services, informatie-uitwisseling en infrastructurele onderdelen. Het stelt daarmee de kaders voor ontwerp en beheer. Samenwerking en het bereiken van een gezamenlijk doel op het niveau van de business is de voornaamste reden, waarbij de beginselen, grondslagen en richtlijnen op het gebied van architectuur worden gedragen door het senior management.

In deze architectuurblauwdruk wordt het architectuurdomein *Netwerk* beschreven.

1.1.1 Doelstelling architectuurblauwdruk *Techniek - domein Netwerk*?

In de blauwdruk worden de volgende onderwerpen beschreven:

- De onderlinge uitwerking van de business-, informatie-, en technische architectuurdomeinen van het ROC.
- De standaarden (ontwerpregels) die bij het ontwerpen van de technische architectuur gehanteerd dienen te worden. De beschreven/geïllustreerde onderdelen worden door ontwerpregels gevolgd.
- De ontwerpregels die richtlijnen geven bij het opstellen van HLDs, LLDs en andere afgeleide technische ontwerpen.
- De architectuurbouwblokken ofwel functionele modules waaruit het te beschrijven architectuur sub-domein is opgebouwd.
- Eventuele architectuurpatronen die binnen het beschreven architectuurdomein onderkend worden.

1.1.2 Wat zijn ontwerpregels?

Ontwerpregels zijn richtinggevend op het gebied van de (technische) architectuur. Deze zijn gebaseerd op:

- Beleid en business-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de business en vertaald naar de technische eigenschap van de infrastructuur,
- Informatie-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de informatievoorziening en vertaald naar de technische eigenschap van de infrastructuur,

- Technische-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de techniek en vertaald naar de technische eigenschap van de infrastructuur.
- Security-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden op het vlak van informatieveiligheid en vertaald naar de technische eigenschap van de infrastructuur.

Gebruikte ontwerpregels in dit document zijn als volgt vormgegeven:

Ontwerpregel #	**Onderwerp**
[Uitleg van de ontwerpregel]	

Alle ontwerpregels zijn in Bijlage A: Ontwerpregels Technische Architectuur - domein netwerk gegroepeerd opgenomen.

1.1.3 Wat zijn architectuurbouwblokken/ functionele modules[1]?

Architectuurbouwblokken ofwel functionele modules zijn entiteiten binnen een architectuurdomein die services bieden aan hun omgeving. Een bouwblok kan:

- zelfstandig services leveren aan de omgeving,
- interactie hebben met één of meerdere andere bouwblokken om services te realiseren,
- samengesteld zijn uit meerdere (andere) bouwblokken binnen een architectuurdomein,
- onderdeel uitmaken van een groter samengesteld bouwblok,
- (bij voorkeur) herbruikt worden,
- op diverse manieren samengesteld worden zonder de specifieke kenmerken en interfaces van het bouwblok te veranderen.

Een bouwblok wordt onderkend door domeinexperts als een aparte entiteit vanwege:

- de samenhang in, of tussen, de functies die het heeft, en/of,
- de set diensten die het levert.

Een bouwblok heeft:

- expliciet en eenduidig te definiëren grenzen,
- specifieke functies, kenmerken en eigenschappen,
- interfaces via welke interactie met aanpalende bouwblokken plaatsvindt.

Een bouwblok is *loosely coupled* met de architectuur omgeving.

[1] *Met referte aan https://pubs.opengroup.org/architecture/togaf9-doc/arch/ ; Part IV - Architecture Content Framework, 33.Building Blocks*

De opdeling van een architectuurdomein in bouwblokken is specifiek voor een bepaalde organisatie of bedrijf. Echter, een goede opdeling van een architectuur in bouwblokken levert voordelen op bij de integratie van, en interoperabiliteit tussen systemen. Tevens vergroot een goede opdeling flexibiliteit bij de realisatie van systemen en applicaties.

De in dit document onderkende bouwblokken worden in de volgende tabelvorm beschreven of samengevat, waarbij antwoord wordt gegeven op de gestelde vragen en taakstellingen:

TA-bouwblok: <naam>	
(Beknopte) Conceptuele beschrijving van het bouwblok	[Geef een beknopte conceptuele beschrijving van het bouwblok. E.g. waaruit bestaat het bouwblok? Welk doel dient het? Welke interfaces heeft het bouwblok? Op welke wijze vindt interactie met de omgeving plaats?]
Functies van het bouwblok	[Beschrijf de functies die het bouwblok heeft en waardoor het services kan realiseren.]
Services dat het bouwblok biedt (aan de omgeving)	[Beschrijf de services die het bouwblok realiseert en die kunnen worden geconsumeerd door andere architectuur componenten (objecten, bouwblokken, et cetera)]
Kwaliteitskenmerken	[Beschrijf de (kwaliteits)eisen en beperkingen in termen van, schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, et cetera.]

1.1.4 Wat zijn architectuurpatronen[2]?

Architectuurpatronen zijn combinaties van architectuurbouwblokken en/of componenten waarvan de toegevoegde waarde wordt onderkend en is bewezen in de context van de enterprise architectuur. Architectuurpatronen zijn herbruikbaar en bieden een oplossing/ invulling voor een specifiek probleem.

Een architectuurpatroon beschrijft:

- wanneer bepaalde bouwblokken worden toegepast,
- waarom bepaalde bouwblokken worden toegepast en
- in welke gevallen bepaalde bouwblokken worden toegepast.

De in dit document beschreven architectuurpatronen zijn volgens de onderstaande tabelvorm vormgegeven, waarbij antwoord wordt gegeven op de beschreven taakstellingen.

[2] *Met referte aan https://pubs.opengroup.org/architecture/togaf9-doc/arch/ ; Part IV - Architecture Content Framework, 22. Architecture Patterns*

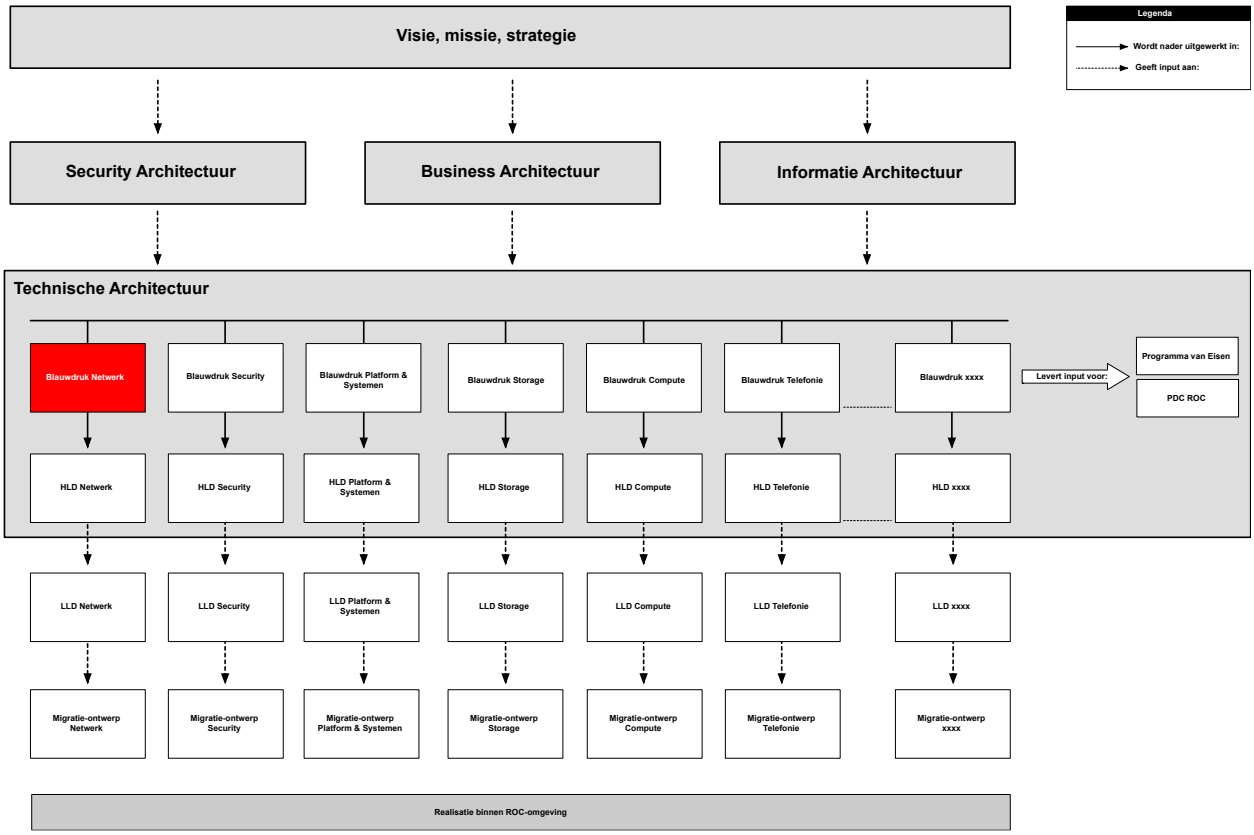
TA-patroon: <naam>	
Toepassing	[Beschrijf het probleem dat het patroon oplost/doel dat bereikt wordt.]
Context	[Beschrijf de condities waaronder het patroon wordt toegepast. Wanneer is het nodig?]
Eisen en beperkingen	[Beschrijf de (kwaliteits)eisen en beperkingen aan het patroon. E.g. op het vlak van schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, et cetera.]
Functionele beschrijving patroon	[<Beschrijf tekstueel op conceptueel niveau wat het doel is van het patroon en hoe dit wordt gerealiseerd. Visualisatie middels platen helpt hierbij.]

1.2 Positie architectuurblauwdruk en scope

In figuur 1-1 op de volgende pagina is de positie van deze architectuurblauwdruk *Techniek – architectuurblauwdruk domein Netwerk* (rood) afgebeeld in relatie tot andere documentatie op het gebied van de Enterprise Architectuur. Een architectuurblauwdruk wordt gebruikt als management- en stuurinstrument en vormt de basis voor afgeleide documentatie. Tevens levert het input in het kader van vervolgtrajecten (e.g. RFP-trajecten).

Door in afgeleide technische documentatie als het HLD de ontwerpregels vanuit de architectuur-blauwdruk als leidraad te nemen, zijn alle functioneel en technisch uitgewerkte onderdelen herleidbaar tot aan de betreffende ontwerpregels in deze architectuurblauwdruk. Op deze manier ontstaat een consistent architectuurlandschap, waarbij onderdelen in samenhang worden ontworpen. Dit geldt zowel binnen een architectuurdomein als in relatie tot aanpalende architectuurdomeinen.

Deze architectuurblauwdruk beschrijft de diverse services die geleverd worden door de te onderscheiden (architectuur) bouwblokken (ofwel functionele modules) in het architectuur domein *Netwerk.*



Figuur 1-1: *Positie architectuurblauwdruk Techniek - domein Netwerk*

1.3 Belanghebbenden architectuurblauwdruk

Tabel 1-1: *Overzicht belanghebbenden*

Belanghebbenden	Concerns	Invloed (R,A,C,I)[3]	Toelichting
Lead architect Design Office	Conformiteit met technische doelarchitectuur	A	Quality Assurance rol. De technische architectuur zorgt voor het technisch fundament voor de business (en informatie) architectuur. De doelarchitecturen op het vlak van de business en techniek zijn en moeten op elkaar afgestemd blijven, ook bij de doorontwikkeling hiervan.

[3] *RACI = Responsible (verantwoordelijk), Accountable (eindverantwoordelijk), Consulted (geraadpleegd), Informed (geïnformeerd).*

Lead architect Netwerk	Conformiteit met technische doelarchitectuur	R	De blauwdruk geeft de technische kaders voor onderliggende architectuur-ontwerpen. Een kwalitatief goede en volledige blauwdruk is essentieel bij het realiseren van de vereiste diverse onderdelen/ diensten/ services binnen de technische doelarchitectuur
Manager Operationeel Beheer	Kwaliteit technische dienstverlening	C	Het daadwerkelijk conform SLA aanbieden van technische automatiseringsdiensten aan klanten van het ROC gebeurt door de operationele afdeling(en) van het ROC. Manager Operationeel Beheer is op dit vlak derhalve operationeel eindverantwoor-delijke.
Service Level Management	Volledigheid PDC/ dienstenportfolio	I	ROC heeft als missie om het primaire en secondaire proces maximaal te ondersteunen bij het halen van haar doelstellingen. Deze ondersteuning bestaat uit automatiseringsdiensten die geleverd worden via (standaard) producten en services uit de PDC.
Security Architect	Conformiteit met security doelarchitectuur	C,I	De Security Architect verifieert of onderdelen van de technische architectuurblauwdruk in overeen-stemming zijn met het vigerende informatiebeveiligingsbeleid van het ROC en in lijn zijn met relevante wet- en regelgeving vanuit de gangbare informatie-beveiligingspraktijk.

1.4 Doelgroep architectuurblauwdruk

- Organisatieonderdelen op het gebied van Beleid en Strategie,
- Organisatieonderdelen op het gebied van Project en Architectuur,
- Organisatieonderdelen op het gebied van Uitvoering en Beheer,
- Business Architecten,
- Informatie Architecten,
- ICT Architecten,
- Security Architecten,
- Technisch Architecten,
- Externe partijen na voorlopige gunning bij aanbestedingen.

1.5 Uitgangspunten

Tijdens het schrijven van dit document zijn de volgende uitgangspunten gehanteerd:

- Het ROC bevindt zich in een transitieperiode. Men is bezig de IT-organisatie te veranderen van een beheerorganisatie in een regie-organisatie. Dit houdt in, dat men:
    - outtasking van standaard ICT-middelen nastreeft,
    - afname van door externe partijen gehoste en beheerde diensten prefereert boven (de eigen ontwikkelde) inhouse-diensten.
- In het kader van dienstverlening in de onderwijssector heeft de SURF-organisatie een speciale rol. Normaliter wordt in een architectuurblauwdruk geen of nauwelijks namen van producten en vendoren opgenomen, gezien de doelstellingen van een architectuurblauwdruk. In concreto -> het (generiek) beschrijven en duiden van architectuureisen waaraan de technische architectuur dient te voldoen. De technische architectuur kan namelijk worden ingevuld door verschillende producten en diensten van verschillende vendoren. Gezien de speciale rol die de SURF-organisatie echter heeft in de onderwijssector in het algemeen en in relatie tot het ROC in het bijzonder, is in deze blauwdruk op verschillende plaatsen bewust de naam SURF opgenomen.
- Architectuurbouwblokken en architectuurpatronen zijn generiek beschreven en voorzien van ontwerpregels. Nadere uitwerking van ontwerpregels dient in afgeleide technische documentatie als HLDs te worden vormgegeven en vastgelegd, waarbij de ontwerpregels vanuit deze blauwdruk als fundament dienen. Dit leidt tot de vraagstelling:

  Wanneer is een nadere uitwerking compleet of volledig en wie bepaalt dat?

  Het antwoord op deze vragen wordt door het gremium Design Office gegeven. Leden[4] van dit gremium stellen onderling vast of functionele uitwerkingen in afgeleide technische documentatie voldoen aan:

[4] *Het gremium Design Office bestaat in hoofdzaak uit de architecten van het ROC. Er zijn in dit kader echter geen beperkingen. Indien noodzakelijk kunnen ook materiedeskundigen (intern/extern) of andere rollen (e.g. engineers (intern/extern), Informatie Management)) worden uitgenodigd zitting te nemen in het gremium (waar nodig)).*

- de generieke ontwerpregels vanuit de architectuurblauwdruk en
- de vigerende wet- en regelgeving waaraan de oplossing(en) dienen te voldoen.

Zodoende kan worden gesteld, dat de architectuurblauwdruk het kader schept voor ontwerp en beheer, maar waarbij ontwerpregels niet per definitie in 'beton zijn gegoten'. Immers, de praktijk is in het algemeen complexer en weerbarstiger waardoor niet 'alles voor 100%' kan worden afgevangen in een architectuurblauwdruk.

- In navolging van de voorgaande bullet dient derhalve te worden uitgegaan van het principe *pas-toe-of-leg-uit*. Ontwerpregels in deze blauwdruk dienen te worden opgevolgd, tenzij met goede redenen kan worden gemotiveerd waarom van de 'baseline' is afgeweken.

1.6 Indeling architectuurblauwdruk

De architectuurblauwdruk bestaat uit de volgende onderdelen:

- **Hoofdstuk 1: Introductie en achtergrond**
  Dit hoofdstuk bevat een inleiding bij de architectuurblauwdruk. De onderbouwing van de blauwdruk en de doelgroepen voor wie het geschreven is, worden kort toegelicht. Tevens worden onderdelen als scope van de architectuurblauwdruk en de belanghebbenden behandeld.

- **Hoofdstuk 2: Diensten en normenkader technische architectuur ROC**
  Dit hoofdstuk bevat een beknopt overzicht van de ROC-diensten (informatie-eigenschappen, producteigenschappen e.d.) die door de Technische Architectuur- *domein Netwerk* dienen te worden geaccommodeerd. Business- en informatie-architecturen zijn opgenomen in aparte brondocumentatie, waarnaar voor meer informatie wordt verwezen. Op de hoofdlijn zijn in dit hoofdstuk de relevante kenmerken van de ROC-diensten opgenomen die noodzakelijk zijn voor de invulling van de technische architectuur - *domein Netwerk*.

  In dit hoofdstuk is ook het normenkader beschreven zoals dat binnen de technische kaders voor het domein Netwerk wordt gebruikt.

- **Hoofdstuk 3: Modules Technische Architectuur - architectuurgebied Netwerk**
  In dit hoofdstuk is de technische architectuur voor het architectuurgebied Netwerk nader beschreven.

- **Bijlage A: Ontwerpregels Technische Architectuur - architectuurgebied Netwerk**
  Deze bijlage bevat een gegroepeerd overzicht van alle ontwerpregels die in het document zijn beschreven. Dit voor het overzicht, zodat per topic in één oogopslag de betreffende

ontwerpregels kunnen worden achterhaald.

- **Bijlage B: Gebruikte afkortingen**
  Deze bijlage bevat een lijst met afkortingen die gebruikt worden in dit document.

2 Diensten en normenkader ROC

2.1 Diensten ROC

Voor een overzicht van de diensten die binnen en buiten het ROC worden geboden en afgenomen wordt verwezen naar de productencatalogus 'PDC ROC Friese Poort '.

2.2 Normenkader technische architectuur - netwerk

In de onderstaande tabel is het normenkader opgenomen zoals dit gebruikt dient te worden binnen de technische architectuur van het ROC en derhalve betrekking heeft op het architectuurgebied dat wordt beschreven in deze blauwdruk. Het generieke normenkader is bewust op deze plaats opgenomen, vanwege het verdere gebruik in vervolgillustraties en onderdelen van de blauwdruk.

Tabel 2-1: *Normenkader*

Norm	Toelichting
Architectuurbouwblok	Zie par. 1.1.3
Architectuurgebied	Een architectuurgebied beschrijft een afgebakend deel van de technische architectuur. Architectuurgebieden in het kader van de technische architectuur zijn: • Netwerk, • Security, • Unified communications, • Platformen & Systemen (inclusief Cloud) • Enterprise Mobility • Werkplek
Architectuurpatroon	Zie par. 1.1.4
Domein	Een deel van een bepaald architectuurgebied. In het kader van het netwerk -> e.g. domein LAN, domein Datacenter-LAN, domein WAN.
Koppelvlak	Interface tussen twee of meerdere architectuurbouwblokken.
Module	De technische infrastructuur van het ROC is opgedeeld in vaste modules waarbinnen zich architectuurbouwblokken bevinden. Door gebruik te maken van vaststaande modules wordt ervoor gezorgd, dat iedere architectuurgebied hetzelfde stramien volgt c.q. 'geplot wordt' binnen de vaststaande modules. Dit zorgt voor samenhang in ontwerp van en een gestructureerd overzicht tussen verschillende architectuurgebieden. De vaststaande modules zijn: • Locatie, • Backbone,

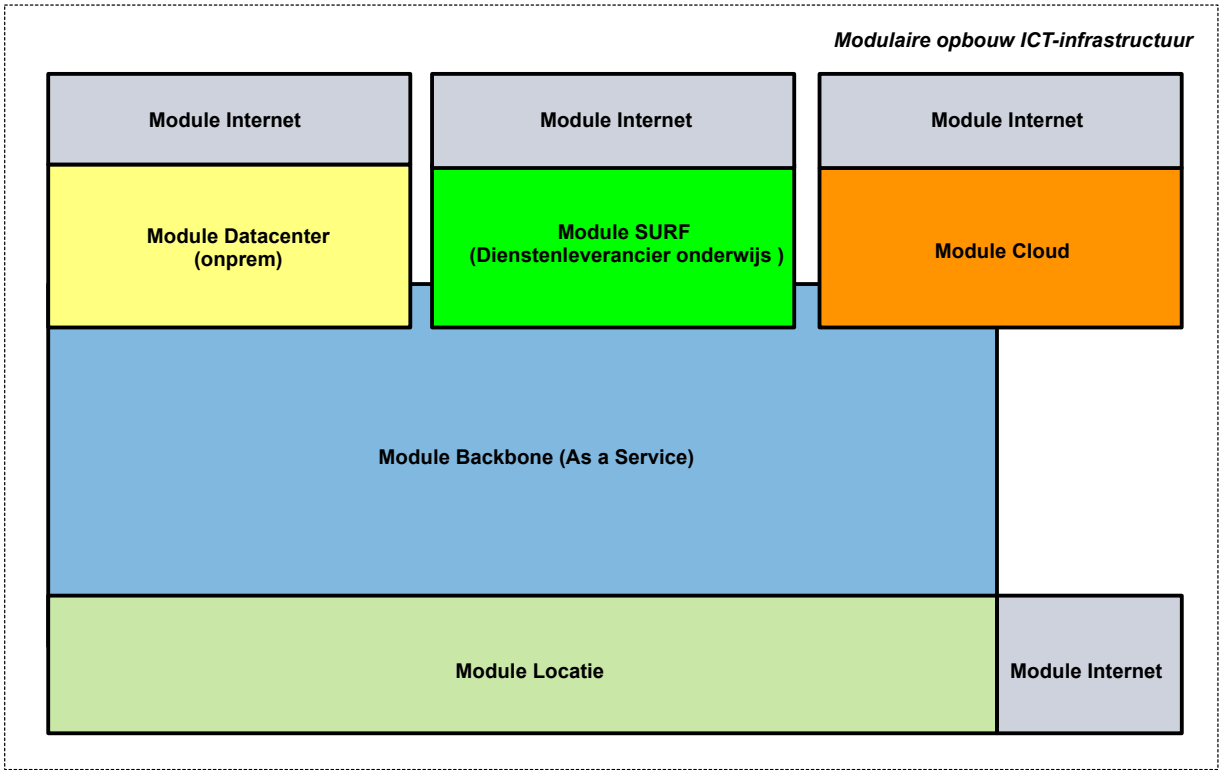
	• Datacenter (onprem), • Cloud (clouddatacenters, IaaS, PaaS, SaaS), • SURF (gezien de bijzondere positie als dienstenleverancier), • Internet.
Node	Een switch, router, firewall, loadbalancer et cetera.

3 Modules Technische Architectuur - architectuurgebied netwerk

3.1 Generiek overzicht modules

De ROC-infrastructuur is modulair opgebouwd zoals afgebeeld in de onderstaande illustratie. Dit betreft een generiek model dat gebaseerd is op:

- de regio Nederland,
- waarbij de organisatieonderdelen van het ROC gevestigd zijn te:
    - Leeuwarden,
    - Drachten,
    - Emmeloord,
    - Sneek,
    - Dokkum,
    - Urk.



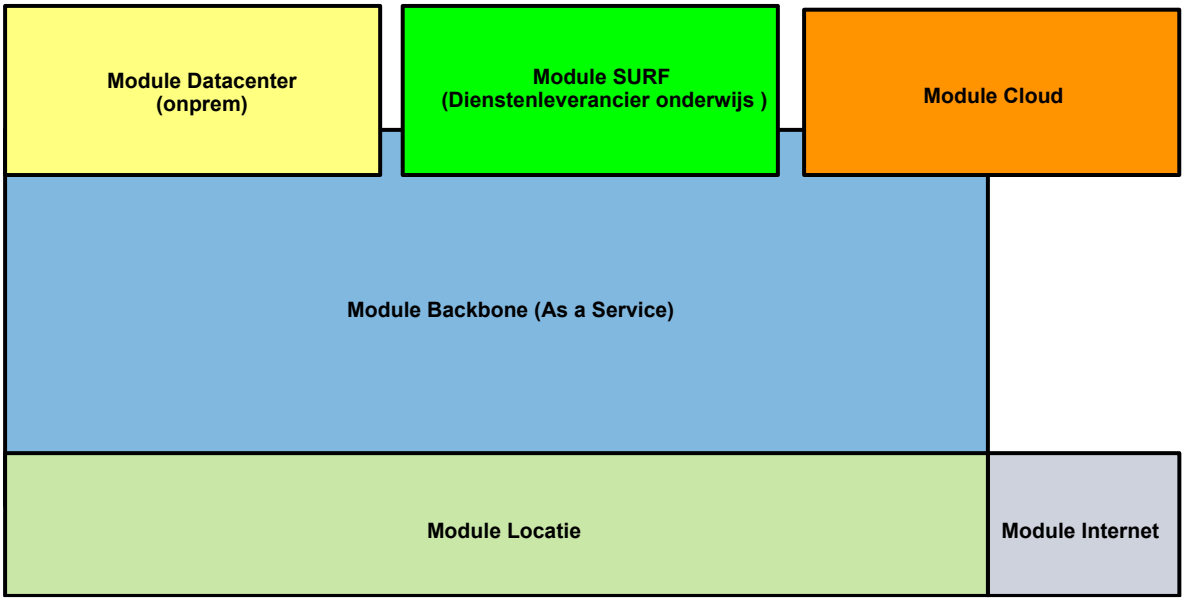
Figuur 3-1: *Overzicht modules ROC*

Door de ROC-infrastructuur op te delen in verschillende modules wordt ervoor gezorgd, dat deze infrastructuur:

- Gestandaardiseerd,
- Betrouwbaar,
- Voorspelbaar,
- Beveiligingsfuncties ondersteunt (e.g. segmentatie),
- Sourceable en,
- Schaalbaar is.

3.2 Module Backbone (As a Service)

In de onderstaande figuur is de module Backbone afgebeeld, waarbij de overige modules t.o.v. de Backbone zijn gepositioneerd. De module Backbone ontsluit de aanpalende modules en reguleert de verkeersstromen hiertussen. Dit houdt niet in dat alle verkeersstromen per definitie via de backbone verlopen. Immers, indien een student, docent of medewerker van het ROC mobiel werkt (e.g. vanuit huis) kunnen de door het ROC geboden diensten direct middels het internet worden benaderd. Zie hiervoor de beschrijvingen van de overige modules en de betreffende use cases in par. 3.8.



Figuur 3-2: *Module Backbone (As a Service)*

3.2.1 TA-bouwblokken

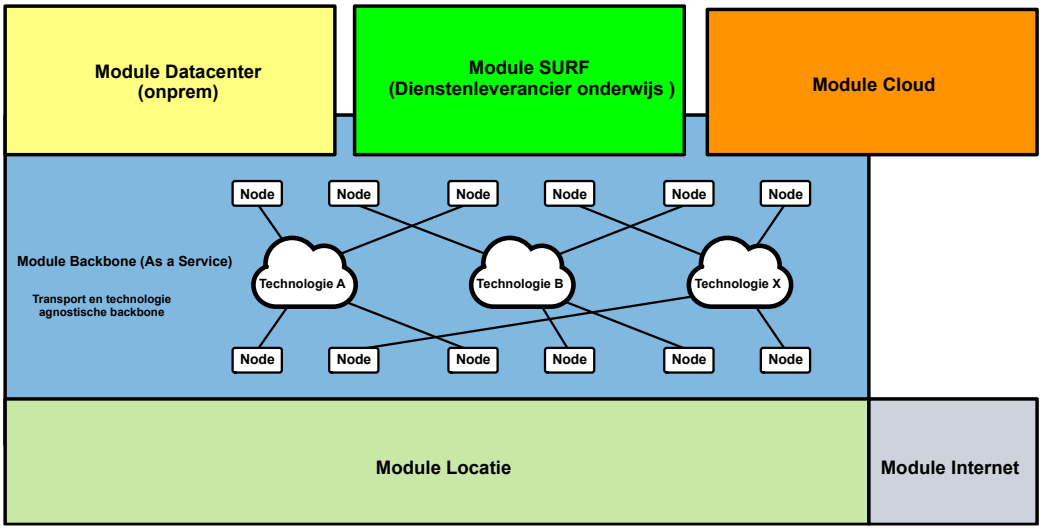
TA-bouwblok: Backbone (As a Service)	
(Beknopte) Conceptuele beschrijving van het bouwblok	De module Backbone vormt de basis voor transportservices tussen de modules die op de Backbone zijn aangesloten. Communicatie tussen deze modules is mogelijk op basis van functionele/ applicatieve behoeftes conform de policies van het ROC.
Functies van het bouwblok	• Ontsluiting aanpalende modules, • Datatransport tussen modules.

Services die het bouwblok biedt (aan de omgeving)	• Connectiviteit Services voor communicatie tussen:
	  ○ De modules Locatie en Datacenter onprem,
	  ○ De modules Locatie en Cloud,
	  ○ De modules Locatie en SURF als dienstenleverancier onderwijs,
	  ○ Instanties van de module Locatie (i.e. communicatie tussen locaties onderling waar nodig),
	  ○ Instanties van de module Datacenter (i.e. communicatie tussen onprem datacenters.

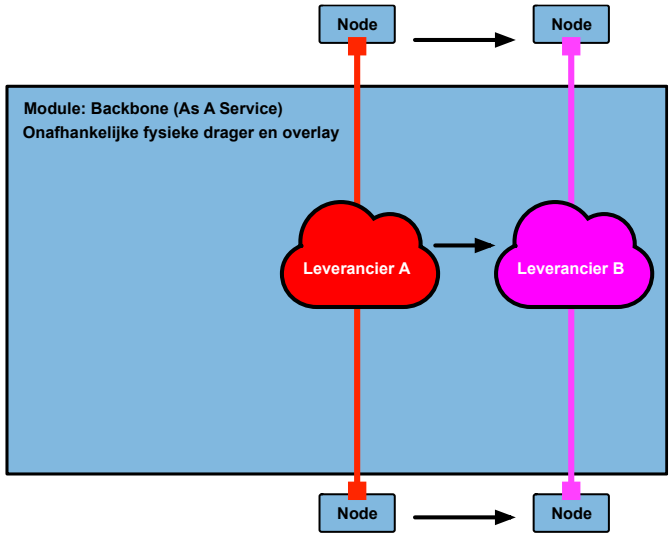
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service), • Ondersteuning van een beschikbaarheid van 99,99% in de keten met aanpalende modules (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Flexibel kunnen ontsluiten van nieuwe (tijdelijke) locaties middels ieder denkbaar transport, waarbij de Backbone één entiteit vormt. • Onafhankelijkheid tussen fysieke drager/technologie en het logische overlay netwerk. • Flexibele en dynamische ondersteuning van alle typen applicaties en per applicatie noodzakelijke metrics (e.g. performance, topologie). • Foutherstel (error correction mechanisms).

3.2.2 TA-patronen

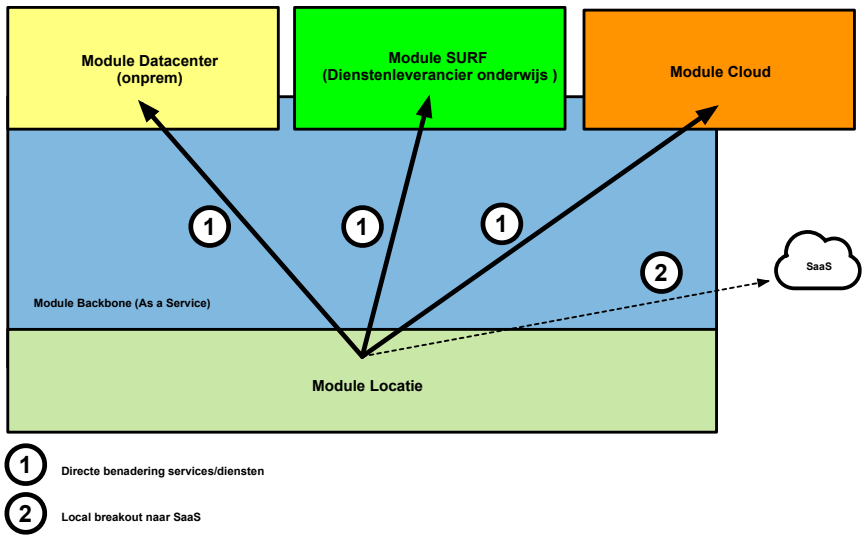
TA-patroon: Technologie-agnostisch	
Toepassing	Ieder type transport (e.g. internet, MPLS, 4G LTE, 5G LTE, xDLS et cetera) dient deel te kunnen uitmaken van de Backbone. De Backbone is hierdoor *technologie agnostisch*. Het doel hiervan is gebruik te kunnen maken van verschillende typen technologieën in de Backbone vanwege: • Leverings- en aanlegmogelijkheden (niet ieder type transport kan eenvoudig en/of snel worden aangelegd voor ieder type locatie. Denk aan het ad hoc inrichten van een nieuwe (tijdelijke) locatie of het gebruik moeten maken van reeds aanwezige WAN-/internet-technologieën die worden geleverd door andere partijen (e.g. gebruik maken van reeds bestaande internetontsluitingen in een pand dat niet door het ROC wordt geëxploiteerd, maar waar het ROC wel een *presence* heeft). • Kostenefficiëntie. De ene technologie is goedkoper dan de andere technologie.
Context	Bij ieder type module of instantie daarvan die direct op de Backbone kan worden ontsloten, dient te worden vastgesteld welk type transport het beste invulling kan geven aan de eisen die het ROC stelt aan beschikbaarheid, schaalbaarheid e.d.
Eisen en beperkingen	De combinatie van: • eisen aan de beschikbaarheid van diensten die de Backbone transporteert en

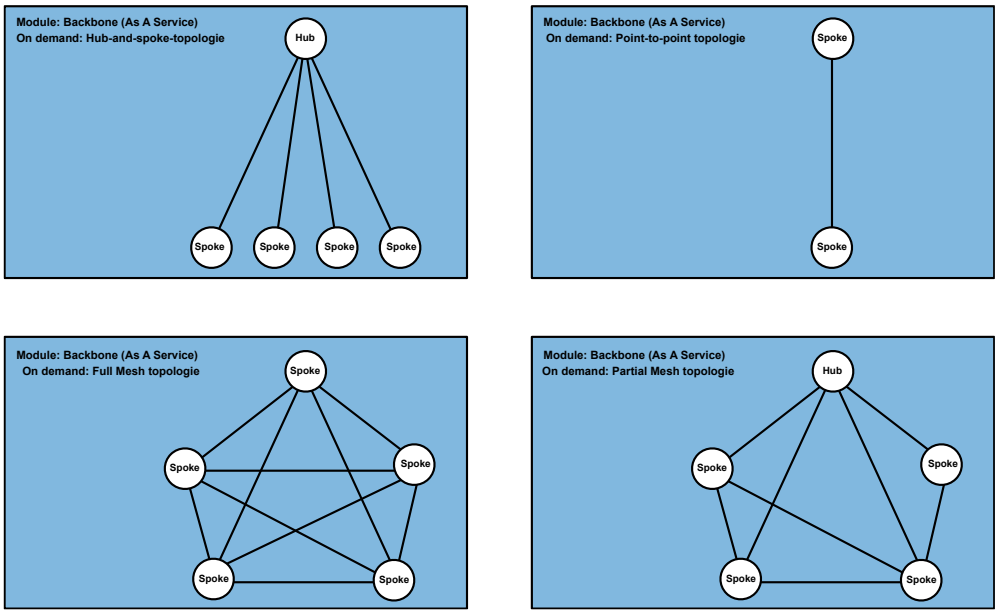
	• de technische mogelijkheden voor ondersteuning van deze diensten per type transport, leidt tot een juiste invulling van de technische ontsluiting per type module of instantie daarvan die direct op de Backbone kan worden ontsloten. In deze technische architectuurblauwdruk zijn hiervoor richtlijnen opgenomen (zie hiervoor de beschrijvingen bij de overige modules), maar de exacte invulling hiervan zal per type module of instantie daarvan nader moeten worden vastgesteld tijdens bijvoorbeeld RFP-uitvragen, LCM-trajecten en constante monitoring van koppelvlakken met de Backbone.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patroon: Gescheiden overlay en fysieke drager	
Toepassing	De fysieke drager en daarmee technologie dient onafhankelijk te zijn van het overlay-netwerk c.q. de logische paden waarmee de Backbone wordt vormgegeven. Een wijziging van transportleverancier dient zonder noemenswaardige configuratie- en topologiewijzigingen aan de kant van het ROC te kunnen worden doorgevoerd. Tevens dient in het kader van bijvoorbeeld RFP-uitvragen een scheiding van domeinen te kunnen worden aangebracht. Een leverancier kan zich inschrijven voor het fysieke transport (i.e. de fysiek drager/ontsluiting/transport), terwijl een andere leverancier zich inschrijft voor de overlay-dienstverlening.
Context	Zoals hierboven gesteld zijn er twee situaties denkbaar, waarin dit TA-patroon noodzakelijk is: 1. Verandering van transportleverancier, 2. Duale inschrijvingen bij RFP-uitvragen.
Eisen en beperkingen	De onderliggende fysieke drager en de logische nodes die de Backbone samenstellen, dienen in samenhang te worden ontworpen. Flexibiliteit is hierbij het kernbegrip. Verandering van transportleverancier A naar transportleverancier B mag geen (noemenswaardige) invloed

	hebben de samenstelling van het overlay-netwerk. Veranderingen in het overlay-netwerk mogen geen invloed hebben op de onderliggende fysieke dragers/het transportnetwerk. Opschaling of afschaling van fysieke dragers moet passend zijn met de Backbone-nodes die als actieve onderdelen de overlay verzorgen.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patroon: Traffic steering capabilities	
Toepassing	De Backbone dient trends in het onderwijs te kunnen accommoderen. Trends zijn bijvoorbeeld: • Cloud-oplossingen (e.g. SaaS, PaaS, O365, IaaS middels publieke clouddatacenters), • ELO-systemen (centralisatie middels bijvoorbeeld SaaS). Door deze trends in het onderwijs zal het bandbreedtegebruik aanzienlijk toenemen, hetgeen door de Backbone flexibel moet kunnen worden opgevangen. Duidelijke trends in het kader van transport zijn bijvoorbeeld: • een substantiële toename van het internetgebruik en, • een toename in samenwerkingsverbanden en integraties tussen leveranciers van Backbone-oplossingen en leveranciers van clouddiensten. Het is hierbij van belang het dataverkeer zo efficiënt mogelijk middels de Backbone te transporteren naar de betreffende dienst, waarbij zo min mogelijk *hairpinning/backhauling van verkeer* plaatsheeft via het onprem datacenter van het ROC. Anders kan het onprem datacenter een bottleneck zijn/worden voor al het verkeer dat ook direct via de Backbone naar

	de betreffende module kan verlopen (dus zonder tussenkomst van het onprem datacenter). De verhouding tussen diensten die geleverd worden vanuit het onprem datacenter en diensten die geleverd worden vanuit de module Cloud (in de breedste zin des woords) zal substantieel wijzigen ten opzichte van de IST-situatie per Q2 2020. Het ROC hanteert immers een *cloud, tenzij…* strategie.
Context	Het is van belang het onprem datacenter naar de toekomst toe zo min mogelijk als *regionale hub* te gebruiken voor het benaderen van diensten die direct middels de Backbone benaderd kunnen worden. Hierdoor wordt het onprem datacenter ontlast, zodat de substantiële toename van bandbreedtegebruik niet hoeft te worden geaccommodeerd door oprem datacenterverbindingen en fysieke nodes (e.g. firewalls, routers, switches e.d.) binnen dit type datacenter.
Eisen en beperkingen	Waar mogelijk en opportuun dienen diensten direct op de Backbone te worden ontsloten, zonder gebruik te hoeven maken van het onprem datacenter als *regionale hub*. Indien dit niet mogelijk is omdat bijvoorbeeld bepaalde SaaS-diensten alleen via het internet ontsloten kunnen worden, dient het onprem datacenter alsnog zoveel mogelijk te worden ontlast door op een slimme manier het internet via de Backbone te kunnen benaderen. Dit kan bijvoorbeeld door gebruik te maken van een directe internet breakout alsmede door het gebruik van een andere regionale (internet)hub die als dienst door het ROC kan worden afgenomen.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patroon: On demand topologie per type applicatie	
Toepassing	De Backbone dient ieder type dienst te kunnen ondersteunen, waarbij de Backbone de per dienst gevraagde netwerktopologie on demand ondersteunt. De applicatie is hierbij dus leidend en niet het netwerk. Op deze manier kunnen bijvoorbeeld nieuwe diensten snel worden uitgerold, zonder aanpassingen te hoeven doorvoeren op het niveau van de Backbone.
Context	Een *snelle time-to-market* van nieuwe diensten is vandaag de dag noodzakelijk, zonder de leverancier van de Backbone (i.e. het overlay netwerk) te hoeven betrekken bij de inrichting hiervan. Indien een bepaalde dienst een any-to-any topologie behoeft, dient dit zonder interventie van de Backbone-leverancier te kunnen worden geïmplementeerd.
Eisen en beperkingen	De Backbone dient verschillende door diensten/applicaties gevraagde typologieën on demand te ondersteunen, zonder tussenkomst van de Backbone-leverancier.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

3.2.3 Ontwerpregels

Ontwerpregel 1	Communicatie modules
1.1	Communicatie tussen: • locaties onderling, • datacenters (onprem) onderling, • locaties en het onprem datacenter, • locaties en het publieke clouddatacenter (onderdeel module Cloud), • locaties en de onderwijsdienstenleverancier SURF, • locaties en PaaS/SaaS-diensten (onderdeel module Cloud) die direct op de Backbone gekoppeld kunnen worden, dient te verlopen via de module Backbone.
1.2	Het is toegestaan de modules Datacenter (onprem) direct aan elkaar te verbinden zonder tussenkomst van de module Backbone. In dit laatste scenario is sprake van een DCI (Datacenter Interconnect).
1.3	De module Backbone dient als fallbackscenario te kunnen worden gebruikt, zodra de DCI-interconnect niet meer functioneert.
1.4	Communicatie tussen publieke clouddatacenters die deel uitmaken van de module Cloud verloopt via de Backbone van de provider van het publieke clouddatacenter).
1.5	Voor zover mogelijk en opportuun dient dataoverdracht tussen modules direct middels de module Backbone te verlopen, waarmee *hairpinning* in het onprem datacenter wordt voorkomen. Dit op grond van trends in het onderwijs, waarbij steeds vaker gebruikgemaakt zal worden van diensten die niet meer geleverd worden vanuit het onprem datacenter.

Ontwerpregel 2	Backbone As A Service
2.1	De Backbone dient als een Service te kunnen worden afgenomen bij een Backbone-provider die connectiviteitsafspraken heeft met leveranciers van clouddatacenters en andere clouddiensten-leveranciers.
2.2	De aansturing, monitoring, provisioning van de Backbone As A Service dient bij voorkeur te worden gereguleerd middels een SaaS-dienst, waarbij het ROC via een portal inzicht heeft in minimaal: • De status van diensten, • De status van de overall Backbone, • Trends in de Backbone, waarmee voorspelbaarheid en daardoor beheerbaarheid van de omgeving optimaal kan worden nagestreefd (e.g. O.b.v. ML/AI voorspellende karakteristieken voor bijvoorbeeld capaciteitsmanagement).

	Hierbij dient het mogelijk te zijn: • Business rules (intelligence) op te nemen via de portal voor alle diensten, waarmee de Backbone op een intelligente en automatische manier invulling kan geven aan de technische vereisten voor de diensten (e.g. thresholds voor metrics als delay, jitter waarbij andere netwerkpaden gebruikt kunnen worden indien thresholds worden overschreden. E.g. gebruik maken van de meest kostenefficiënte onderliggende fysieke dragers, waarbij in geval van overschrijding van bepaalde thresholds (simultaan) een duurdere backup-verbinding kan worden benut). • De Portal locatie-onafhankelijk te kunnen benaderen. • De Backbone te laten doorwerken, indien de onderliggende NMS-systemen (tijdelijk) geen verbinding meer hebben met de module Backbone.
2.3	De backbone dient in een beschikbaarheid te voorzien van 99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
2.4	De geboden service dient de access-nodes of aggregatie-nodes op locaties te ontsluiten conform de ontwerpregels zoals opgesteld in paragraaf 3.3. Hierbij dient het mogelijk te zijn de service te laten 'meegroeien' of 'inkrimpen' met het type en/of subtype locatie.
2.5	De geboden service dient de aggregatie-nodes in onprem datacenters te ontsluiten conform de ontwerpregels zoals opgesteld in paragraaf 4.3.
2.6	De service dient te voorzien in koppelingen met clouddatacenters en andere clouddiensten die direct op de backbone kunnen worden aangesloten.
2.7	Het ROC dient controle te kunnen uitoefenen op het backbone-netwerk. Toegang is nodig voor: • Het toepassen van security-policies op basis van het vigerende informatiebeveiligingsbeleid van het ROC, • Inzage in de verkeersstromen (Application Visibility & Control) opdat tijdig kan worden bijgestuurd conform de policies van het ROC (e.g. QoS-toepassing/wijziging, bandbreedtewijzigingen et cetera).

Ontwerpregel 3	**Technologie**
De Backbone dient te kunnen worden vormgegeven middels verschillende technologische dragers, waarbij verandering van leverancier en technologie geen of nauwelijks impact mag hebben op het overlay-netwerk van het ROC. Dit overlay-netwerk wordt gevorm door actieve Backbone-nodes die integraal deel uitmaken van de Backbone As A Service.	

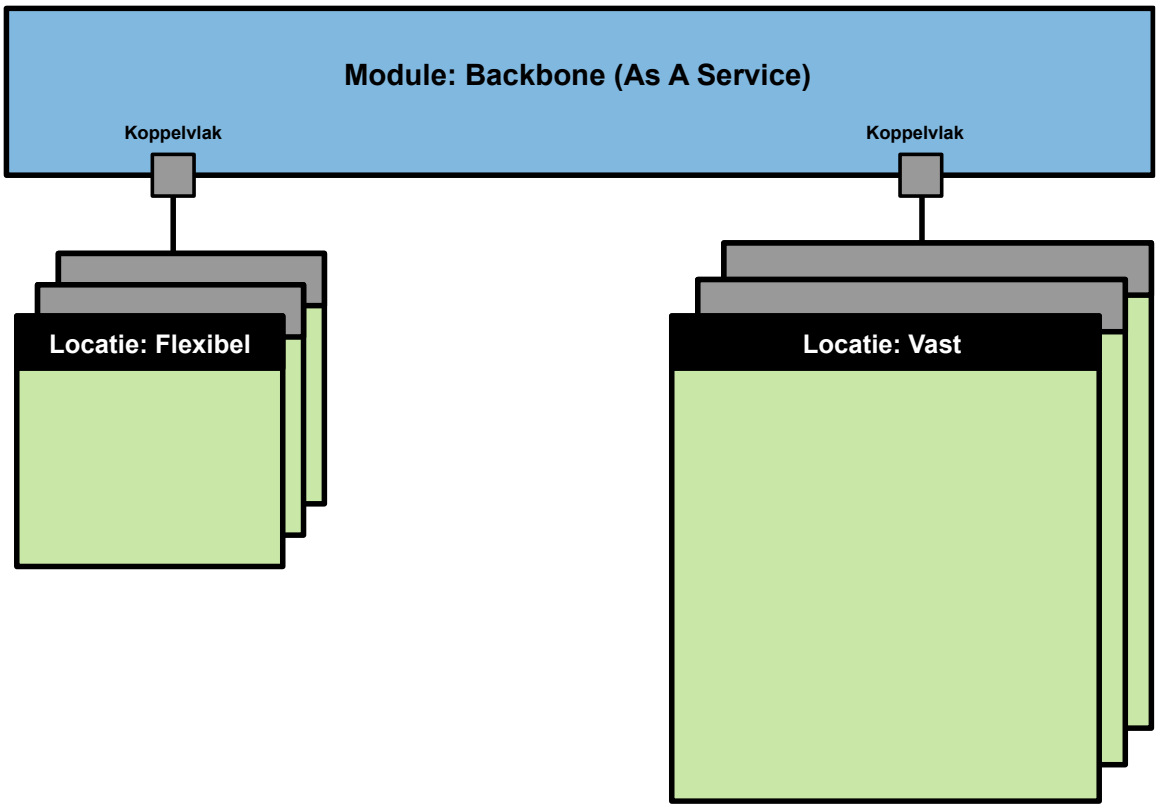
Ontwerpregel 4	**Functies**
4.1	De Backbone dient te voorzien in data-overdracht waarbij het mogelijk is op grond van specifieke business rules/intelligence de Backbone automatisch aan te passen aan de

	eisen van de applicatie. Indien bijvoorbeeld een normaliter geprefereerd overlay-pad niet optimaal functioneert, dient een ander overlay-pad automatisch te kunnen worden geactiveerd c.q. opgeschaald.
4.2	De Backbone dient te voorzien in foutendetectie en automatisch herstel.
4.3	De Backbone dient te voorzien in Quality of Service.
4.4	De Backbone dient te voorzien in IPv4- en IPv6-functies.
4.5	Redundante uplink/downlinkverbindingen dienen middels linkbundelings-technologie te kunnen worden vormgegeven.
4.6	De Backbone dient automatisch de door de applicatie/dienst gevraagde netwerktopologie te ondersteunen, zijnde: • Any-to-any topologie, • Hub-and-spoke topologie, • Full-mesh topologie, • Point-to-point topologie.
4.7	De Backbone dient te voorzien in traffic-steering-mogelijkheden, waarbij het onprem datacenter als *hub* zoveel als mogelijk wordt ontlast van verkeer dat niet bestemd is voor services die vanuit dit type datacenter worden aangeboden.
4.8	Backbone-nodes dienen te kunnen worden geclusterd, waarbij de beide nodes simultaan verkeer kunnen verwerken afhankelijk van de business rules/intelligentie die worden toegekend aan de betreffende diensten/ applicaties.
4.9	De Backbone dient flexibel te zijn. Met flexibiliteit wordt bedoeld: • Eenvoudig en snel opschaalbaar, • Eenvoudig en snel afschaalbaar, • Eenvoudig en snel leverbaar op locaties waar bijvoorbeeld vaste/bedrade verbindingen niet/nauwelijks en/of niet snel genoeg kunnen worden geleverd. • De implementatie van nieuwe diensten dient snel en zonder tussenkomst van de leverancier te kunnen worden uitgevoerd (snelle *time-to-market*).

3.3 Module Locatie

De module Locatie biedt eindgebruikers toegang tot het netwerk van het ROC daarmee toegang tot ICT-services die intern binnen het ROC (e.g. intranet) of extern buiten het ROC (e.g. internet, SaaS, diensten SURF) worden aangeboden. Eindgebruikers kunnen zowel studenten, docenten, medewerkers als ICT-systemen zijn.

De module Locatie bestaat uit twee locatietypen zoals in de onderstaande illustratie is afgebeeld.



Figuur 4-3: *Module Locatie*

Locatie: Flexibel
Dit type locatie moet worden beschouwd als een flexibel in te richten locatie. Met flexibiliteit wordt in dezen bedoeld:

- Een locatie die tijdelijk van aard is en derhalve een relatief korte levensduur heeft,
- Een locatie waarvan het ROC geen pandeigenaar is en waarbij het ROC afhankelijk is van de door de pandeigenaar geboden dienstverlening (e.g. internetverbinding die door de pandeigenaar wordt geboden).

Locatie: Vast
Dit betreft de locaties die geen korte levensduur hebben en waarover het ROC de gehele regievoering kan uitoefenen.

De volgende subparagrafen beschrijven de modulariteit, schaalbaarheid en andere eigenschappen van de verschillende typen locaties, incluis ontsluitingen van deze locaties naar de module Backbone. Hierbij is een onderscheid aangebracht tussen twee verschillende modellen:

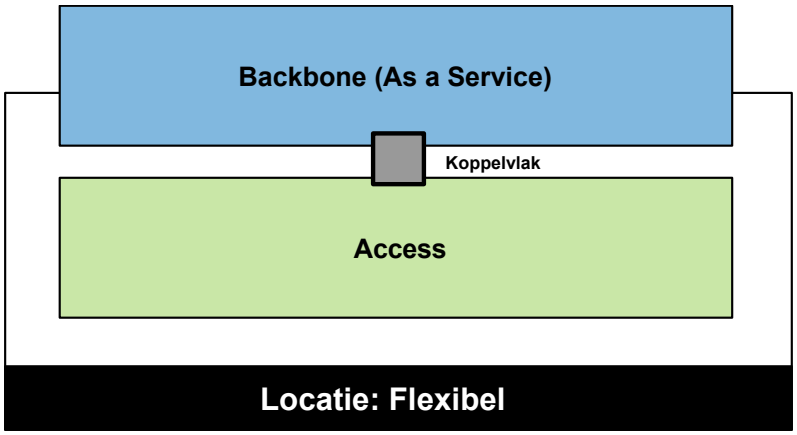
- Traditioneel model (par. 3.3.1),
- SDN-model (par. 3.3.2).

De reden voor dit onderscheid is het kunnen voorzien in technologische ontwikkelingen op het gebied van SDN. De technische ontwikkelingen op SDN-vlak vinden momenteel razendsnel plaats. Op het moment van opstellen van deze technische architectuurblauwdruk kan er vanwege het maturity niveau van SDN-technologie echter (nog) geen duidelijke voorkeur uitgesproken worden voor een bepaald model. Bovendien kunnen gebruikssituaties voorkomen, waarin het ene model beter past dan het andere. Dit zal dan per gebruikssituatie moeten worden vastgesteld in afgeleide documentatie zoals een HLD of middels een RFP-uitvraag.

3.3.1 Locatie: traditioneel model

3.3.1.1 Locatietype: Flexibel

In de onderstaande illustratie is dit type locatie conceptueel afgebeeld:



Figuur 4-4: *Locatietype: Flexibel*

TA-bouwblokken:

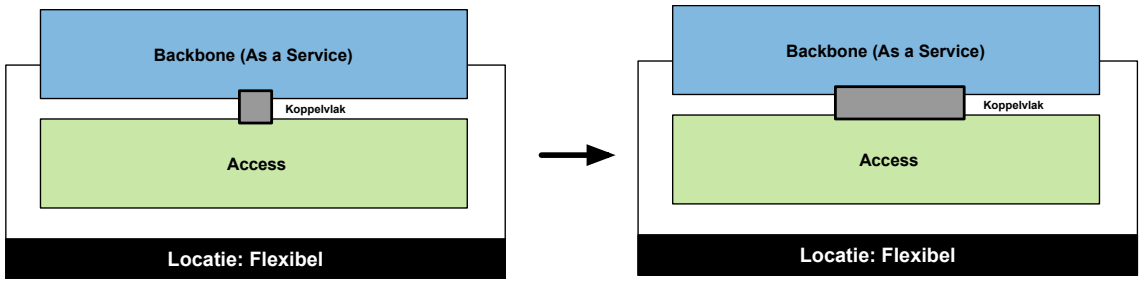
TA-bouwblok: Access	
(Beknopte) Conceptuele beschrijving van het bouwblok	• De accesslaag geeft gebruikers en systemen toegang tot het netwerk van het ROC. • De accesslaag faciliteert zowel bedrade als draadloze netwerktoegang.
Functies van het bouwblok	Ontsluiting van gebruikers en systemen.

Services die het bouwblok biedt (aan de omgeving)	• Toegangsservices voor gebruikers en systemen. • Connectiviteitsservices naar/vanaf de module Backbone.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Flexibel kunnen ontsluiten van gebruikers en systemen (zowel draadloos als bedraad).

TA-bouwblok: Koppelvlak access & module Backbone	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de accesslaag en de module Backbone voorziet in datatransport tussen de beide omgevingen. Datatransport vindt plaats zowel vanaf als naar de accesslaag. *Vanaf de accesslaag:* • Benaderen van diensten die worden aangeboden in de module Datacenter Onprem. • Benaderen van diensten die worden aangeboden in de module Cloud. • Benaderen van diensten die worden aangeboden in de module SURF. • Benaderen van het internet • Benaderen van diensten die worden aangeboden in de module Locatie (anders dan de eigen locatie). *Naar de accesslaag:* • Retourverkeer vanaf de hierboven genoemde modules en internet. • Verkeer geïnitieerd vanaf de module Datacenter Onprem (e.g. voor beheerdoeleinden). • Verkeer geïnitieerd vanaf de module Cloud (e.g. voor beheerdoeleinden BYOD middels Mobile Management platformen).
Functies van het bouwblok	Koppeling tussen de accesslaag en de module Backbone t.b.v. datatransport
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de accesslaag en de module Backbone.

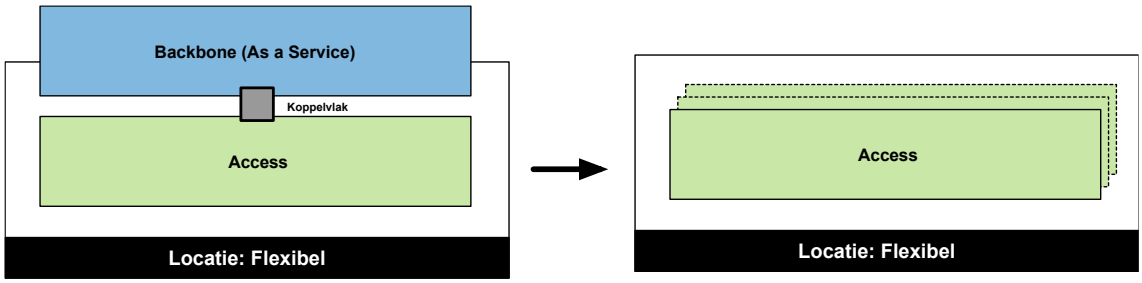
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de accesslaag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-patronen:

TA-patroon: Verticale uitbreidbaarheid	
Toepassing	De locatie dient verticaal schaalbaar te zijn door het kunnen verhogen of verlagen van de interfacesnelheden op het niveau van het TA-bouwblok koppelvlak access & module Backbone.
Context	Indien een locatie groeit in termen van bandbreedtetoename dient de accesslaag mee te kunnen groeien om deze groei in bandbreedte te accommoderen. Het omgekeerde is ook waar: indien een locatie minder bandbreedte behoeft, dient de accesslaag navenant verticaal te kunnen inkrimpen.
Eisen en beperkingen	Nodes die deel uitmaken van de accesslaag en de module Backbone dienen te voorzien in verticale schaalmogelijkheden, waarbij een opwaardering (en afwaardering) van interface-snelheden flexibel kan worden doorgevoerd. Verticale schaalbaarheid dient flexibel te kunnen worden ingevuld middels het medium tussen de accesslaag en de module Backbone, zonder nieuwe componenten of nodes te hoeven aanschaffen.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patronen:

TA-patroon: Horizontale uitbreidbaarheid	
Toepassing	De locatie dient horizontaal schaalbaar te zijn door het kunnen toevoegen van nodes die deel uitmaken van de accesslaag.
Context	Indien een locatie groeit in aantallen personen en/of systemen dient de accesslaag mee te kunnen groeien om toename in capaciteit te accommoderen. Het omgekeerde is ook waar: indien een locatie minder capaciteit behoeft, dient de accesslaag navenant horizontaal te kunnen inkrimpen.
Eisen en beperkingen	Afhankelijk van de pandeigenaar, de gemaakte afspraken en voor het ROC beschikbaar gestelde ruimte is horizontale uitbreiding wel/niet mogelijk. Dit zal per geval / situatie moeten

	worden beoordeeld. Horizontale uitbreidbaarheid dient te geschieden middels clustering/stacking van nodes in de accesslaag, waarbij de accesslaag zich als één logische entiteit gedraagt.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

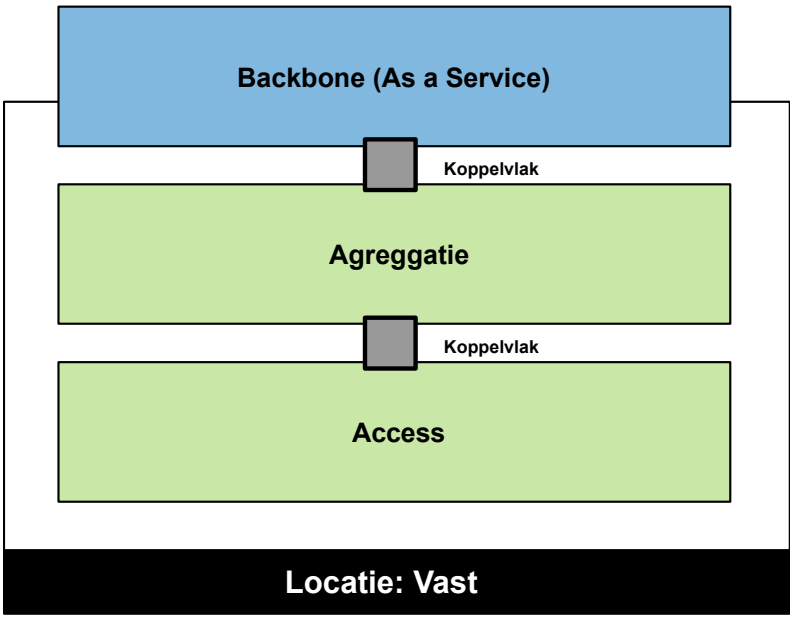
3.3.1.2 Ontwerpregels locatietype Flexibel

Ontwerpregel 5	**Traditioneel model: Eigenschappen locatie-type: Flexibel**	
Ontwerpregel 5.1	Aantal personen & systemen	Max. 100
Ontwerpregel 5.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 5.3	Medium tussen nodes accesslaag en nodes module Backbone	minimaal 1 Gbit/s met opschaalmogelijkheden tot 10 Gbit/s (en vice versa)
Ontwerpregel 5.4	Clustering/stacking	Nodes die deel uitmaken van de accesslaag dienen te kunnen worden geclusterd/gestacked, waarbij iedere node simultaan verkeer kan afhandelen.
Ontwerpregel 5.5	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 1 Gbit/s met opschaal-mogelijkheden tot 10 Gbit/s (haalbaarheid moet worden vastgesteld i.o.m. marktpartij).
Ontwerpregel 5.6	Beschikbaarheid	99,99% -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 5.7	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).

Ontwerpregel 5.8	SLA access-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 5.9	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal.
Ontwerpregel 5.10	Toekomstige groei	Bij toekomstige groei dient het type locatie te kunnen doorgroeien naar het locatietype vast. Per geval / situatie dienen hiertoe de mogelijkheden te worden bekeken.

3.3.1.3 Locatietype: Vast

In de onderstaande illustratie is dit type locatie conceptueel afgebeeld:



Figuur 4-5: *Locatietype: Vast*

TA-bouwblokken:

TA-bouwblok: Access	
(Beknopte) Conceptuele beschrijving van het bouwblok	De access-laag geeft gebruikers en systemen toegang tot het netwerk van het ROC. De access-laag faciliteert zowel bedrade als draadloze netwerktoegang.
Functies van het bouwblok	Ontsluiting van gebruikers en systemen.

Services die het bouwblok biedt (aan de omgeving)	• Toegangsservices voor gebruikers en systemen. • Connectiviteitsservices naar/vanaf de module Backbone.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende aggregatielaag (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Flexibel kunnen ontsluiten van gebruikers en systemen (zowel draadloos als bedraad).

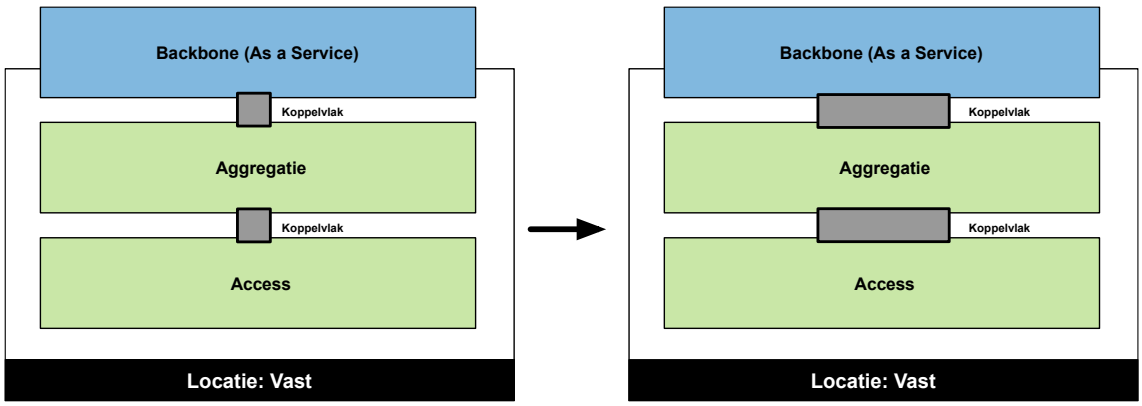
TA-bouwblok: Aggregatie	
(Beknopte) Conceptuele beschrijving van het bouwblok	De aggregatielaag fungeert als verlengstuk van de accesslaag in de richting van de module Backbone. Het zorgt ervoor, dat op een gestandaardiseerde manier verschillende access-nodes vanuit de accesslaag toegang krijgen tot de module Backbone voor datatransport naar/vanaf de verschillende modules.
Functies van het bouwblok	• Aggregatie van nodes die deel uitmaken van de accesslaag. • Koppeling tussen de nodes die deel uitmaken van de accesslaag en nodes die deel uitmaken van de module Backbone.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices naar/vanaf de module Backbone. • Routeringservice voor ROC-diensten die zonder tussenkomst van een PEP-functie (e.g. firewall) direct decentraal op locatieniveau met elkaar mogen communiceren.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende accesslaag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-bouwblok: Koppelvlak access & aggregatie	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de accesslaag en de aggregatielaag voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats naar/vanaf de accesslaag en naar/vanaf de module Backbone. *Vanaf de accesslaag naar de module Backbone:* • Ontsluiting van verkeersstromen voor: ○ Het benaderen van diensten die worden aangeboden in de module Datacenter Onprem.

	○ Het benaderen van diensten die worden aangeboden in de module Cloud. ○ Het benaderen van diensten die worden aangeboden in de module SURF. ○ Het benaderen van het internet. *Naar de accesslaag vanaf de module Backbone:* • Ontsluiting van verkeerstromen voor: ○ Retourverkeer vanaf de hierboven genoemde modules en internet. ○ Verkeer geïnitieerd vanaf de module Datacenter Onprem (e.g. voor beheerdoeleinden). ○ Verkeer geïnitieerd vanaf de module Cloud (e.g. voor beheerdoeleinden BYOD middels Mobile Management platformen).
Functies van het bouwblok	• Koppeling tussen de accesslaag en de module Backbone t.b.v. datatransport. • Aggregatie van access nodes die deel uitmaken van de accesslaag.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices tussen de accesslaag en de module Backbone. • Connectiviteitsservices tussen systemen/gebruikers op het niveau van de module Locatie zelf.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de accesslaag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

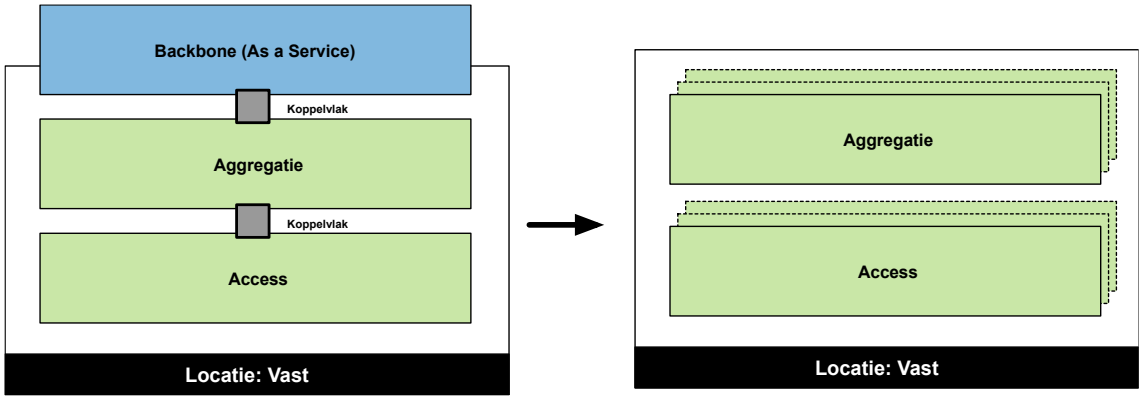
TA-bouwblok: Koppelvlak aggregatie & module Backbone	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de aggregatielaag en de module Backbone(laag) voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats zowel vanaf als naar de aggregatielaag voor doeleinden die bij het voorgaande bouwblok zijn opgenomen (met uitzondering van decentrale verkeersstromen die direct zijn toegestaan op het niveau van de module Locatie).
Functies van het bouwblok	Koppeling tussen de aggregatielaag en de module Backbone t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices tussen de aggregatielaag en de module Backbone.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de aggregatielaag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-patronen:

TA-patroon: Verticale uitbreidbaarheid	
Toepassing	De locatie dient verticaal schaalbaar te zijn door het verhogen van de interfacesnelheden op het niveau van het TA-bouwblok koppelvlak access & de module Backbone
Context	Indien een locatie groeit in termen van bandbreedtetoename dient de accesslaag mee te kunnen groeien om de groei in bandbreedte te accommoderen. Het omgekeerde is ook waar: indien een locatie minder bandbreedte behoeft, dient de accesslaag navenant verticaal te kunnen afnemen.
Eisen en beperkingen	Nodes die deel uitmaken van de accesslaag en de module Backbone dienen te voorzien in verticale schaalmogelijkheden, waarbij een opwaardering (en afwaardering) van interface-snelheden flexibel kan worden doorgevoerd.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patronen:

TA-patroon: Horizontale uitbreidbaarheid	
Toepassing	De locatie dient horizontaal schaalbaar te zijn door het kunnen toevoegen van nodes die deel uitmaken van de accesslaag. Dit geldt ook voor nodes die deel uitmaken van de aggregatielaag.
Context	Indien een locatie groeit in aantallen personen en/of systemen dient de accesslaag mee te kunnen groeien om toename in capaciteit te accommoderen. Het omgekeerde is ook waar: indien een locatie minder capaciteit behoeft, dienen de accesslaag en aggregatielaag navenant horizontaal te kunnen inkrimpen. De aggregatielaag dient te kunnen worden uitgebreid indien het aantal nodes dat deel uitmaakt van de accesslaag groeit.
Eisen en beperkingen	Zowel accessnodes als aggregatienodes dienen geclusterd / gestacked te kunnen worden, opdat alle nodes simultaan verkeer kunnen verwerken. Hierbij dient optimaal gebruik te kunnen worden gemaakt van alle beschikbare netwerkpaden tussen de beide lagen.

Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

3.3.1.4 Ontwerpregels locatietype Vast

Ontwerpregel 6	**Traditioneel model: Eigenschappen locatie-type: Vast**	
Ontwerpregel 6.1	Aantal personen & systemen	> 5
Ontwerpregel 6.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 6.3	Medium tussen nodes accesslaag en nodes aggregatielaag	minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 6.4	Medium tussen nodes aggregatielaag en nodes module Backbone	minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 6.5	Clustering/stacking	Nodes die deel uitmaken van de accesslaag en aggregatielaag dienen te kunnen worden geclusterd/gestacked, waarbij iedere node simultaan verkeer kan afhandelen.
Ontwerpregel 6.6	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 10 Gbit/s met opschaal-mogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s.
Ontwerpregel 6.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).

Ontwerpregel 6.8	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.9	SLA aggregatie-node	MTTR 8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.10	SLA access-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal.
Ontwerpregel 6.12	Toekomstige groei/krimp	Bij toekomstige groei dient het type locatie deze groei flexibel te kunnen accommoderen zonder wijzigingen te hoeven aanbrengen in de LAN-topologie. Bij toekomstige krimp dient het type locatie te kunnen afschalen naar het locatietype flexibel.

3.3.1.5 Generieke kenmerken access-nodes en aggregatie-nodes

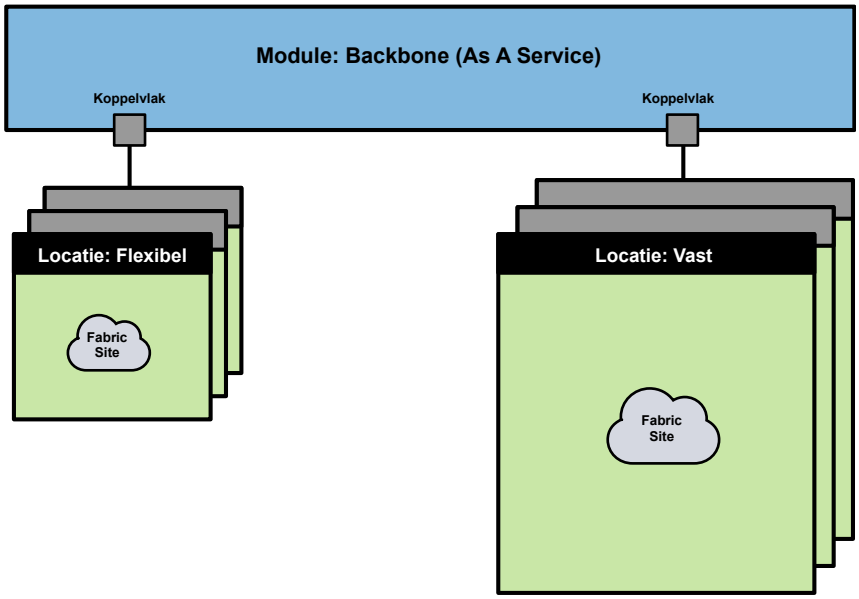
Ontwerpregel 7	**Tradtioneel model: Generieke kenmerken access-nodes en aggregatie-nodes**
Ontwerpregel 7.1	Access-nodes zijn redundant aangesloten op meerdere aggregatienodes, waarbij simultaan gebruikgemaakt kan worden van alle beschikbare paden tussen de beide lagen.
Ontwerpregel 7.2	De access-poorten van een access-node zijn van het type koper 10/100/1000 Mbit/s.
Ontwerpregel 7.3	Access-nodes dienen te voorzien in Power-over-Ethernet-mogelijkheden om Access Points en IP-telefoons van stroom te kunnen voorzien. Hierbij dient per locatie/gebruikssituatie bekeken te worden welk type POE (type 15W, 30W, 60W)
Ontwerpregel 7.4	Access-nodes dienen het gebruik van Wake-on-LAN te ondersteunen.
Ontwerpregel 7.5	Aggregatie-nodes dienen het LAN richting de module Backbone te kunnen ontsluiten op basis van het IP-protocol, waarbij gebruikgemaakt kan worden van open standaarden routeringsprotocollen.
Ontwerpregel 7.6	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 7.7	Nodels dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.

Ontwerpregel 7.8	De access-nodes zijn niet voorzien van redundante voedingen, de aggregatienodes wel.
Ontwerpregel 7.9	De nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 7.10	De software-architectuur is bij voorkeur modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien 'pay as you grow' kunnen worden ingevuld.
Ontwerpregel 7.11	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de backbone-node, maar in ieder geval binnen de module Locatie.
Ontwerpregel 7.12	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 7.13	Nodes communiceren met hun omgeving op basis van open standaarden.
Ontwerpregel 7.14	De node(s) van de module Backbone mogen geen deel uitmaken van de aggregatie-laag in verband met: • Het kunnen scheiden van de modules Locatie en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.

3.3.2 Locatie: SDN-model

Het SDN-model voor de module Locatie dient in een breder perspectief te worden gezien. Dit bredere perspectief is in de onderstaande illustratie conceptueel afgebeeld. Ieder type locatie (flexibel, vast) bevat een SDN-fabric en is daarmee een separate SDN-fabric-site in het SDN-ecosysteem. Het SDN-ecosysteem fungeert als één SDN-domein over alle typen locaties heen, waarbij de module Backbone connectiviteitsservices verzorgt voor communicatie tussen:

- De verschillende SDN-fabric-sites onderling en,
- Tussen een SDN-node op een SDN-fabric-site en centraal gepositioneerde SDN-controllers in de module Datacenter of aangebracht in de hoedanigheid van een SaaS-dienst (beide niet afgebeeld).



Figuur 4-6: *Overzicht SDN-model in relatie tot module Locatie*

Het SDN-model voor het ROC is gebaseerd op de principes van de 'multi-site', waarbij iedere locatie (SDN-fabric-site) is voorzien van een eigen set aan gelijkwaardige SDN-functionaliteiten (i.e. control plane en data plane functies). Dit in tegenstelling tot het SDN-model 'single site', waarbij in de regel op centrale sites (e.g. datacenters) de SDN-nodes zijn ondergebracht die control plane functies uitoefenen en op decentrale sites (i.e. de locaties van het ROC) de SDN-nodes die de data plane functies uitoefenen. In dit model ('single-site') is derhalve geen sprake van separate SDN-fabric-sites; alle locaties maken deel uit van één SDN-fabric-site. Het model 'single site' leidt ertoe, dat:

- Alle decentrale locaties niet (optimaal) standalone kunnen functioneren indien de control plane op de centrale site niet bereikbaar/beschikbaar is,

- De technologie van de module Backbone de betreffende protocollen (dit kunnen proprietary protocollen zijn) dient te ondersteunen die benodigd zijn voor communicatiedoeleinden tussen de decentrale nodes en centrale nodes die deel uitmaken van het SDN-ecosysteem,
- De module Backbone minder flexibel is indien deze wordt afgenomen als backbone as a service. De kans is immers aanwezig, dat leveranciers van Backbones de benodigde communicatieprotocollen (dit kunnen zoals gezegd proprietary protocollen zijn), niet ondersteunen.

In het geval van het type 'multi-site' is de Backbone een separate en maximaal flexibele laag die geen deel hoeft uit te maken van het SDN-ecosysteem. De functies van control plane en data plane bevinden zich namelijk op iedere SDN-fabric-site, zodat communicatie tussen SDN-nodes die de control plane functie uitoefenen en SDN-nodes die alleen de dataplane functie uitoefenen op decentraal (locatie)niveau worden afgehandeld. De communicatie tussen:

- De verschillende SDN-fabric-sites,
- De centraal (in het datacenter of als SaaS-dienst) opgestelde SDN-controllers en decentrale SDN-nodes in SDN-fabric-sites,

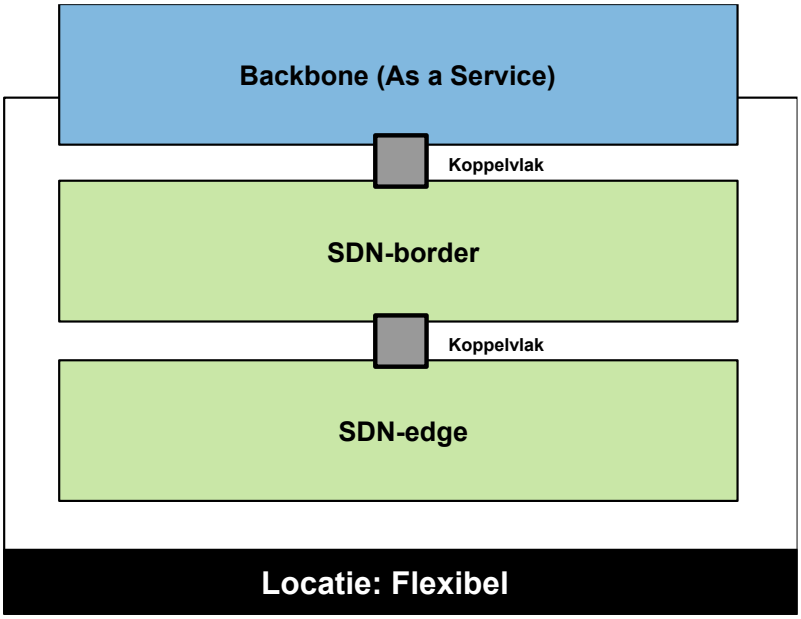
wordt hierbij gefaciliteerd door het flexibele IP-protocol op het niveau van de module Backbone.

Van belang te vermelden is het volgende: Control plane functies moeten niet worden verward met de functies van SDN-controllers die separate entiteiten zijn en het gehele SDN-ecosysteem 'aansturen'.

Ontwerpregel 8	**Positie module Backbone binnen het SDN-model**
Ontwerpregel 8.1	De module Backbone dient separaat en (technologisch) flexibel te zijn in relatie tot het SDN-model op LAN/WLAN-niveau. Dit in verband met de mogelijkheid de module Backbone sourceable te houden door een duidelijk demarcatiepunt tussen de module Backbone en de module Locatie te creëren (dus ook qua technologie indien dit de flexibiliteit en sourceability van de module Backbone ten goede komt).
Ontwerpregel 8.2	Locaties waar SDN-functies worden aangebracht dienen te worden ondergebracht conform het SDN-model type 'multi-site'.
Ontwerpregel 8.3	Communicatie tussen SDN-fabric-sites onderling en communicatie tussen SDN-nodes en de centraal in het datacenter opgestelde SDN-controllers (of SDN-controllers die als SaaS-dienst worden afgenomen) wordt gefaciliteerd door de module Backbone, waarbij het flexibele IP-protocol gebruikt moet kunnen worden.

3.3.2.1 Locatietype: Flexibel

In de onderstaande illustratie is dit type locatie conceptueel afgebeeld:



Figuur 4-7: *Locatietype Flexibel*

TA-bouwblokken:

TA-bouwblok: SDN-edge	
(Beknopte) Conceptuele beschrijving van het bouwblok	• De SDN-edge-laag geeft gebruikers en systemen toegang tot het netwerk van het ROC. • De SDN-edge-laag faciliteert zowel bedrade als draadloze netwerktoegang.
Functies van het bouwblok	• Ontsluiting gebruikers en systemen. • Routeringservice voor verkeersstromen die decentraal op locatieniveau direct zijn toegestaan.
Services die het bouwblok biedt (aan de omgeving)	• Toegangsservices voor gebruikers en systemen. • Connectiviteitsservices naar/vanaf de SDN-border-laag.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende SDN-border-laag (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Flexibel kunnen ontsluiten van gebruikers en systemen (zowel draadloos als bedraad).

	• Aanstuurbaar via een SDN-controller met uitgebreide portalfuncties voor inzage verkeersstromen, monitoring en controle.

TA-bouwblok: SDN-border	
(Beknopte) Conceptuele beschrijving van het bouwblok	De SDN-border-laag fungeert als verlengstuk van de SDN-edge-laag in de richting van de module Backbone. Het zorgt ervoor, dat op een gestandaardiseerde manier verschillende SDN-edge-nodes vanuit de SDN-edge-laag toegang krijgen tot de module Backbone voor datatransport naar/vanaf de verschillende modules en het internet.
Functies van het bouwblok	• Aggregatie van nodes die deel uitmaken van de SDN-edge-laag. • Koppeling tussen de nodes die deel uitmaken van de SDN-border-laag en nodes die deel uitmaken van de module Backbone.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices naar/vanaf de module Backbone.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende SDN-edge-laag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Aanstuurbaar via een SDN-controller met uitgebreide portalfuncties voor inzage verkeersstromen, monitoring en controle.

TA-bouwblok: Koppelvlak SDN-edge en SDN-border	

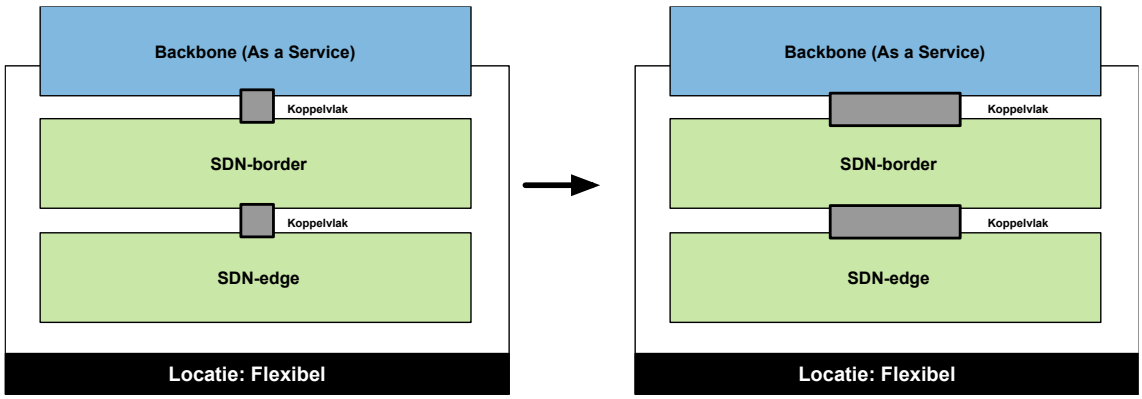
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de SDN-edge-laag en de SDN-border-laag voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats naar/vanaf de SDN-edge-laag en naar/vanaf de SDN-border-laag
	
	Vanaf de SDN-edge-laag naar de SDN-border-laag:
	
	• Ontsluiting van verkeersstromen voor:
	  ○ Het benaderen van diensten die worden aangeboden in de module Datacenter Onprem.
	  ○ Het benaderen van diensten die worden aangeboden in de module Cloud.
	  ○ Het benaderen van diensten die worden aangeboden in de module SURF.
	  ○ Het benaderen van het internet.
	  ○ Het benaderen van diensten die op een andere locatie worden aangeboden.

	Naar de SDN-edge-laag vanaf de SDN-border-laag:
	
	• Ontsluiting van verkeerstromen voor:
	  ○ Retourverkeer vanaf de hierboven genoemde modules en het internet.
	  ○ Verkeer geïnitieerd vanaf de module Datacenter Onprem (e.g. voor beheerdoeleinden).
	  ○ Verkeer geïnitieerd vanaf de module Cloud (e.g. voor beheerdoeleinden BYOD middels Mobile Management platformen).

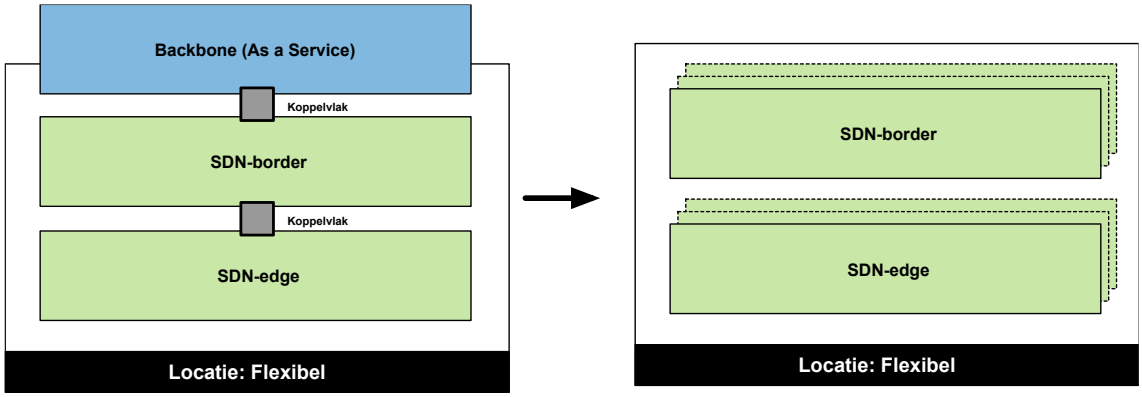
Functies van het bouwblok	Koppeling tussen de SDN-edge-laag en de SDN-border-laag t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de SDN-edge-laag en de SDN-border-laag.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de SDN-edge-laag en SDN-border-laag (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-bouwblok: Koppelvlak SDN-border en module Backbone	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de SDN-border-laag en de module Backbone voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats zowel vanaf als naar de SDN-border-laag voor doeleinden die bij het voorgaande bouwblok zijn opgenomen.
Functies van het bouwblok	Koppeling tussen de SDN-border-laag en de module Backbone t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de SDN-border-laag en de module Backbone.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de SDN-border-laag en de SDN-edge-laag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-patronen:

TA-patroon: Verticale uitbreidbaarheid	
Toepassing	De locatie dient verticaal schaalbaar te zijn door het verhogen van de interfacesnelheden op het niveau van de TA-bouwblokken koppelvlak SDN-edge & SDN-border en koppelvlak SDN-border & module Backbone.
Context	Indien een locatie groeit in termen van bandbreedtetoename dienen de lagen SDN-edge en SDN-border mee te kunnen groeien om de groei in bandbreedte te accommoderen. Het omgekeerde is ook waar: indien een locatie minder bandbreedte behoeft, dienen de voornoemde lagen navenant verticaal te kunnen afnemen.
Eisen en beperkingen	Nodes die deel uitmaken van de lagen SDN-edge & SDN-border en van de module Backbone dienen te voorzien in verticale schaalmogelijkheden, waarbij een opwaardering (en afwaardering) van interface-snelheden flexibel kan worden doorgevoerd.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patroon: Horizontale uitbreidbaarheid	
Toepassing	De locatie dient horizontaal schaalbaar te zijn door het kunnen toevoegen van nodes die deel uitmaken van lagen SDN-edge en SDN-border.
Context	Indien een locatie groeit in aantallen personen en/of systemen dienen de lagen SDN-edge en SDN-border mee te kunnen groeien om toename in capaciteit te accommoderen. Het omgekeerde is ook waar: indien een locatie minder capaciteit behoeft, dient de voornoemde lagen navenant horizontaal te kunnen inkrimpen.
Eisen en beperkingen	Afhankelijk van de pandeigenaar, de gemaakte afspraken en voor het ROC beschikbaar gestelde ruimte is horizontale uitbreiding wel/niet mogelijk. Dit zal per geval / situatie moeten worden beoordeeld.

Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

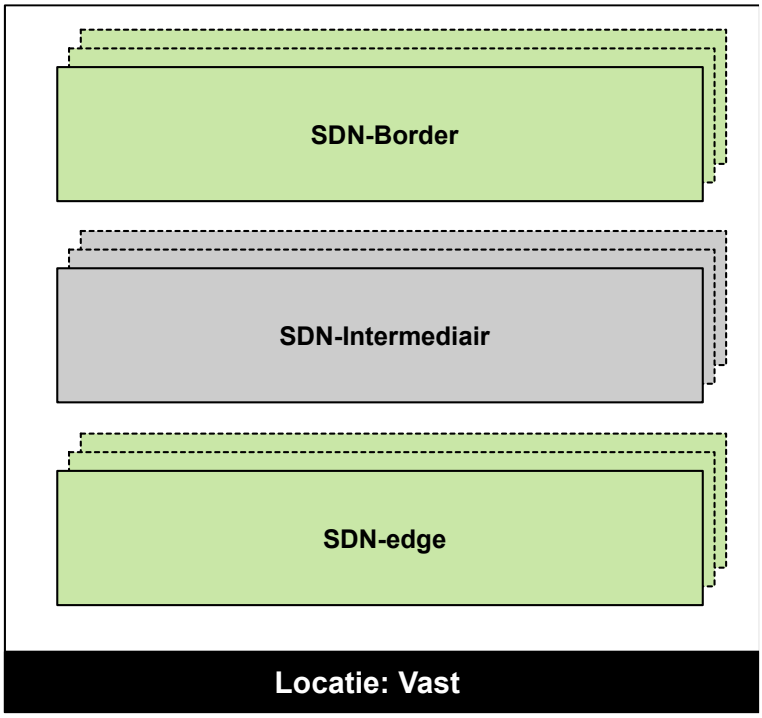
3.3.2.2 Ontwerpregels locatietype Flexibel

Ontwerpregel 9	**SDN-model: Eigenschappen locatie-type: Flexibel**	
Ontwerpregel 9.1	Aantal personen & systemen	Max. 100
Ontwerpregel 9.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 9.3	Medium tussen nodes SDN-edge-laag en nodes SDN-border-laag	Glas, minimaal 1 Gbit/s met opschaalmogelijkheden tot 10 Gbit/s (en vice versa)
Ontwerpregel 9.4	Medium tussen nodes SDN-border-laag en nodes module Backbone	Glas, minimaal 1 Gbit/s met opschaalmogelijkheden tot 10 Gbit/s (en vice versa)
Ontwerpregel 9.5	Clustering/stacking	De nodes die deel uitmaken van de fabric-site dienen als één logische SDN-wolk te kunnen worden aangestuurd.
Ontwerpregel 9.6	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 1 Gbit/s met opschaal-mogelijkheden tot 10 Gbit/s (en vice versa) (haalbaarheid moet worden vastgesteld i.o.m. marktpartij).
Ontwerpregel 9.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).

Ontwerpregel 9.8	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.9	SLA SDN-border-node	8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.10	SLA SDN-edge-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal. Zodra meer dan één SDN-border-node wordt ondergebracht, dient het principe van de leaf-spine-architectuur te worden toegepast waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes.
Ontwerpregel 9.12	Toekomstige groei	Bij toekomstige groei dient het type locatie te kunnen doorgroeien naar het locatietype vast. Per geval / situatie dienen hiertoe de mogelijkheden te worden bekeken.

3.3.2.3 Locatietype: Vast

In de onderstaande illustratie is dit type locatie conceptueel afgebeeld:



Figuur 4-8: *Locatietype Vast*

TA-bouwblokken:

TA-bouwblok: SDN-edge	
(Beknopte) Conceptuele beschrijving van het bouwblok	• De SDN-edge-laag geeft gebruikers en systemen toegang tot het netwerk van het ROC. • De SDN-edge-laag faciliteert zowel bedrade als draadloze netwerktoegang.
Functies van het bouwblok	• Ontsluiting gebruikers en systemen. • Routeringservice voor communicatiestromen die direct op het niveau van de module Locatie worden afgehandeld.
Services die het bouwblok biedt (aan de omgeving)	• Toegangsservices voor gebruikers en systemen. • Connectiviteitsservices naar/vanaf de SDN-border-laag.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende SDN-border-laag (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

	• Flexibel kunnen ontsluiten van gebruikers en systemen (zowel draadloos als bedraad). • Aanstuurbaar via een SDN-controller met uitgebreide portalfuncties voor inzage verkeersstromen, monitoring en controle.

TA-bouwblok: SDN-intermediair	
(Beknopte) Conceptuele beschrijving van het bouwblok	Deze laag is grijs afgebeeld temeer de meeste SDN-topologieën in een Enterprise-omgeving bestaan uit een SDN-edge-laag en een SDN-border-laag. De SDN-intermediaire-laag wordt gebruikt als verlengstuk tussen de SDN-edge-laag en SDN-border-laag.
Functies van het bouwblok	Aggregatie van de SDN-access-laag.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de SDN-access-laag en de SDN-border-laag.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende SDN-border-laag en SDN-access-laag (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Aanstuurbaar via een SDN-controller met uitgebreide portalfuncties voor inzage verkeersstromen, monitoring en controle

TA-bouwblok: SDN-border	
(Beknopte) Conceptuele beschrijving van het bouwblok	De SDN-border-laag fungeert als verlengstuk van de SDN-edge-laag in de richting van de module Backbone. Het zorgt ervoor, dat op een gestandaardiseerde manier verschillende SDN-edge-nodes vanuit de SDN-edge-laag toegang krijgen tot de module Backbone voor datatransport naar/vanaf de verschillende modules en het internet.
Functies van het bouwblok	• Aggregatie van nodes die deel uitmaken van de SDN-edge-laag (indien geen gebruik wordt gemaakt van de SDN-intermediaire-laag). • Koppeling tussen de nodes die deel uitmaken van de SDN-border-laag en nodes die deel uitmaken van de module Backbone.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices naar/vanaf de module Backbone. • Connectiviteitsservices naar/vanaf de SDN-access-laag (indien geen gebruik wordt gemaakt van de SDN-intermediaire-laag). • Connectiviteitsservices naar/vanaf de SDN-intermediaire-laag (indien gebruikt).
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service).

	• Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende SDN-edge-laag of SDN-intermediaire-laag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Aanstuurbaar via een SDN-controller met uitgebreide portalfuncties voor inzage verkeersstromen, monitoring en controle.

TA-bouwblok: Koppelvlak SDN-edge en SDN-border	

(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de SDN-edge-laag en de SDN-border-laag voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats naar/vanaf de SDN-edge-laag en naar/vanaf de SDN-border-laag
	
	Vanaf de SDN-edge-laag naar de SDN-border-laag:
	
	• Ontsluiting van verkeersstromen voor:
	  ○ Het benaderen van diensten die worden aangeboden in de module Datacenter Onprem.
	  ○ Het benaderen van diensten die worden aangeboden in de module Cloud.
	  ○ Het benaderen van diensten die worden aangeboden in de module SURF.
	  ○ Het benaderen van het internet.
	
	Naar de SDN-edge-laag vanaf de SDN-border-laag:
	
	• Ontsluiting van verkeerstromen voor:
	  ○ Retourverkeer vanaf de hierboven genoemde modules en het internet.
	  ○ Verkeer geïnitieerd vanaf de module Datacenter Onprem (e.g. voor beheerdoeleinden).
	  ○ Verkeer geïnitieerd vanaf de module Cloud (e.g. voor beheerdoeleinden BYOD middels Mobile Management platformen).

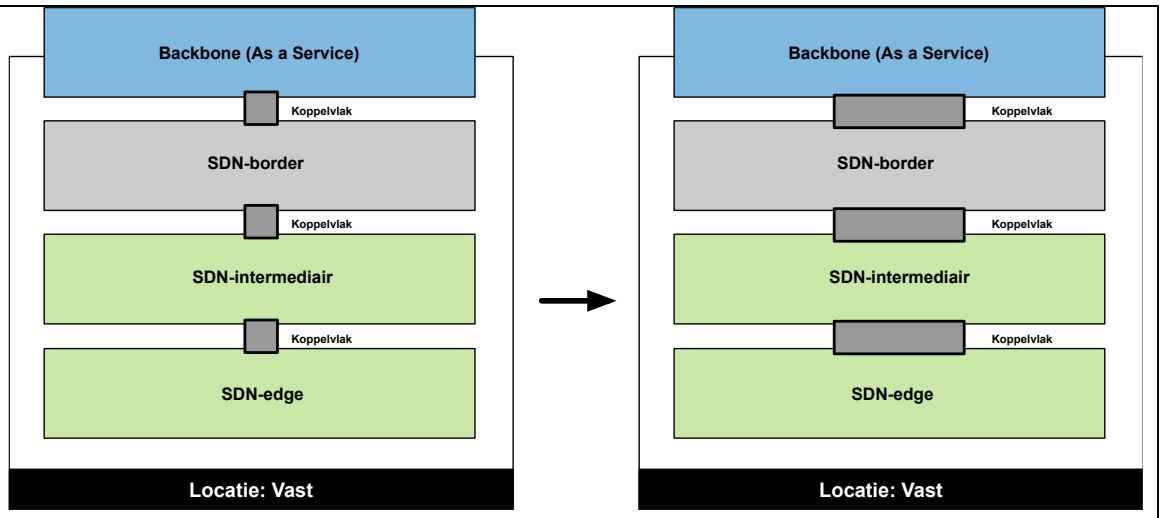
Functies van het bouwblok	Koppeling tussen de SDN-edge-laag en de SDN-border-laag t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de SDN-edge-laag en de SDN-border-laag.

Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de SDN-edge-laag en SDN-border-laag (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

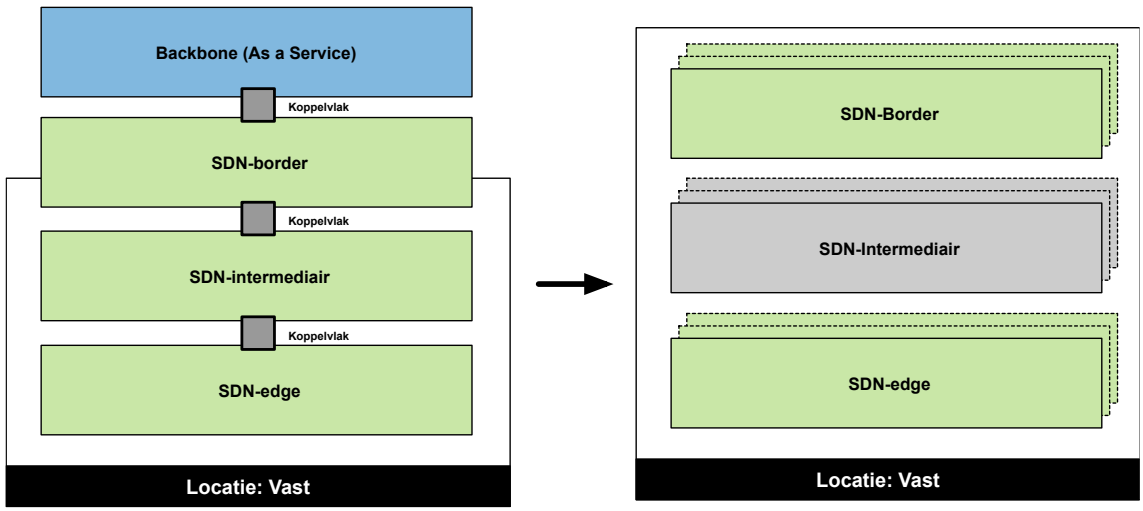
TA-bouwblok: Koppelvlak SDN-border en module Backbone	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de SDN-border-laag en de module Backbone voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats zowel vanaf als naar de SDN-border-laag voor doeleinden die bij het voorgaande bouwblok zijn opgenomen.
Functies van het bouwblok	Koppeling tussen de SDN-border-laag en de module Backbone t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de SDN-border-laag en de module Backbone.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de SDN-border-laag en de SDN-edge-laag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-patronen:

TA-patroon: Verticale uitbreidbaarheid	
Toepassing	De locatie dient verticaal schaalbaar te zijn door het verhogen van de interfacesnelheden op het niveau van de TA-bouwblokken *koppelvlak SDN-edge* & *koppelvlak SDN-intermediair* & *koppelvlak SDN-border* en *koppelvlak SDN-border* & *module Backbone.*
Context	Indien een locatie groeit in termen van bandbreedtetoename dienen de lagen SDN-edge en SDN-border (en indien aanwezig/noodzakelijk de laag SDN-intermediair) mee te kunnen groeien om de groei in bandbreedte te accommoderen. Het omgekeerde is ook waar: indien een locatie minder bandbreedte behoeft, dienen de voornoemde lagen navenant verticaal te kunnen afnemen.
Eisen en beperkingen	Nodes die deel uitmaken van de lagen SDN-edge & SDN-border & SDN-intermediair en van de module Backbone dienen te voorzien in verticale schaalmogelijkheden, waarbij een opwaardering (en afwaardering) van interface-snelheden flexibel kan worden doorgevoerd.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld.



TA-patronen:

TA-patroon: Horizontale uitbreidbaarheid	
Toepassing	De locatie dient horizontaal schaalbaar te zijn door het kunnen toevoegen van nodes die deel uitmaken van lagen SDN-edge, SDN-intermediair en SDN-border.
Context	Indien een locatie groeit in aantallen personen en/of systemen dienen de lagen SDN-edge SDN-intermediair en SDN-border mee te kunnen groeien om toename in capaciteit te accommoderen. Het omgekeerde is ook waar: indien een locatie minder capaciteit behoeft, dient de voornoemde lagen navenant horizontaal te kunnen inkrimpen.
Eisen en beperkingen	Alle SDN-nodes dienen simultaan verkeer kunnen verwerken. Hierbij dient optimaal gebruik te kunnen worden gemaakt van alle beschikbare netwerkpaden tussen de SDN-lagen.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

3.3.2.4 Ontwerpregels locatietype Vast

Ontwerpregel 10	SDN-model: Eigenschappen locatie-type: Vast	
Ontwerpregel 10.1	Aantal personen & systemen	> 100
Ontwerpregel 10.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 10.3	Medium tussen nodes SDN-edge-laag en nodes SDN-border-laag	Glas, minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 10.4	Medium tussen nodes SDN-border-laag en nodes module Backbone	Glas, minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 10.5	Clustering/stacking	De nodes die deel uitmaken van de fabric-site dienen als één logische SDN-wolk te kunnen worden aangestuurd. Border nodes dienen geclusterd te kunnen worden.
Ontwerpregel 10.6	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 10 Gbit/s met opschaal-mogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s.
Ontwerpregel 10.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.8	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.9	SLA SDN-edge-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.10	SLA SDN-border-node	8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal. Zodra meer dan één SDN-border-node wordt ondergebracht, dient het principe

		van de leaf-spine-architectuur te worden toegepast waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes.
Ontwerpregel 10.12	Toekomstige groei/krimp	Bij toekomstige groei dient het type locatie deze groei flexibel te kunnen accommoderen zonder wijzigingen te hoeven aanbrengen in de SDN-topologie. Bij toekomstige krimp dient het type locatie te kunnen afschalen naar het locatietype flexibel.

3.3.2.5 Generieke kenmerken SDN-edge-nodes en SDN-border-nodes

Ontwerpregel 11	SDN-model: Generieke kenmerken SDN-edge-nodes en SDN-border-nodes
Ontwerpregel 11.1	De functies van de SDN-edge-lagen en SDN-border-lagen mogen in één SDN-node zijn ondergebracht indien dit technologisch kan worden doorgevoerd. Deze SDN-node dient dan direct verbonden te worden aan de module Backbone. Indien de functies van SDN-edge- en SDN-border-lagen niet in één SDN-node kunnen worden ondergebracht, geldt het volgende: SDN-edge-nodes zijn redundant aangesloten op één SDN-border-node, tenzij de onderhavige SDN-technologie/systematiek een dergelijke ontsluiting niet toestaat. Indien deze redundante ontsluiting technologisch niet kan worden verwezenlijkt, dient te worden teruggevallen op de leaf-spine-architectuur, waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes. Deze SDN-border-nodes dienen als cluster te kunnen worden aangebracht.
Ontwerpregel 11.2	De access-poorten van een SDN-edge-node zijn van het type koper 10/100/1000 Mbit/s.
Ontwerpregel 11.3	Access-nodes dienen te voorzien in Power-over-Ethernet-mogelijkheden om Access Points en IP-telefoons van stroom te kunnen voorzien. Hierbij dient per locatie/gebruikssituatie bekeken te worden welk type POE (type 15W, 30W, 60W)
Ontwerpregel 11.4	SDN-edge-nodes dienen het gebruik van Wake-on-LAN te ondersteunen.
Ontwerpregel 11.5	SDN-border-nodes dienen te zijn voorzien van de control plane functies die noodzakelijk zijn binnen het SDN-ecosysteem.
Ontwerpregel 11.6	SDN-border-nodes dienen de SDN-fabric-site richting de module Backbone te kunnen ontsluiten op basis van het IP-protocol, waarbij gebruikgemaakt kan worden van open standaarden routeringsprotocollen.
Ontwerpregel 11.7	SDN-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.

Ontwerpregel 11.8	SDN-nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 11.9	De SDN-edge-nodes zijn niet voorzien van redundante voedingen. De SDN-border-nodes zijn wel voorzien van redundante voedingen.
Ontwerpregel 11.10	SDN-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 11.11	De software-architectuur is modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien 'pay as you grow' kunnen worden ingevuld.
Ontwerpregel 11.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de backbone-node, maar in ieder geval binnen de module Locatie. Hiervan kan worden afgeweken, indien bijvoorbeeld: • voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een locatie-overschrijdend OSI Laag 2 pad aan te brengen, • de gekozen technologie in de praktijk dermate anders is c.q. andere inzichten met zich meebrengt dat niet aan dit principe voldaan kan worden.
Ontwerpregel 11.13	SDN-nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 11.14	SDN-nodes communiceren bij voorkeur met hun omgeving op basis van open standaarden, tenzij de voor het ROC gekozen SDN-oplossing alleen middels proprietary protocollen kan worden opgebouwd. Hierbij is het van belang, dat communicatie naar de module Backbone middels open standaarden kan worden gefaciliteerd.
Ontwerpregel 11.15	De node(s) van de module Backbone mogen geen deel uitmaken van de laag SDN-border in verband met: • Het kunnen scheiden van de modules Locatie en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.

3.4 Module Datacenter (onprem)

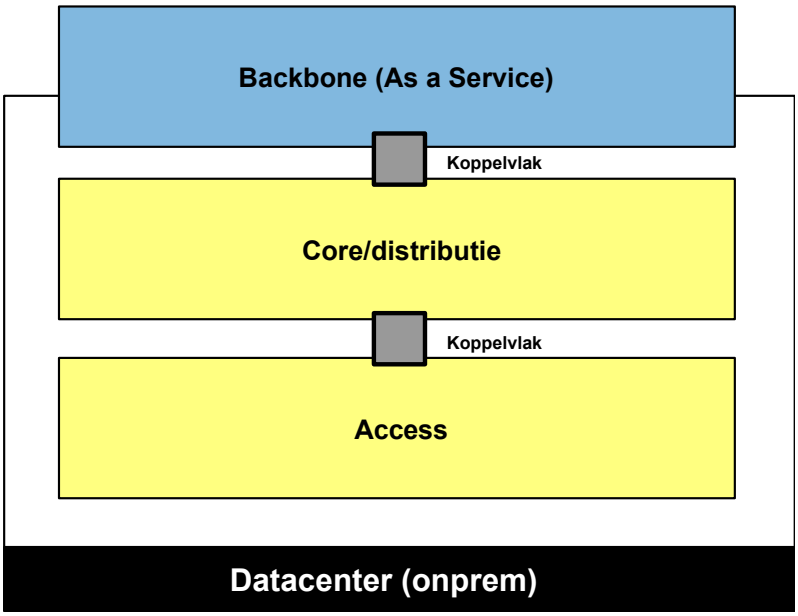
Ook in het kader van het onprem datacenter worden twee verschillende topologieën beschreven:

1. Traditioneel model,
2. SDN-model.

Afhankelijk van de ontwikkelingen in SDN-technologie en specifieke behoeften die zich in de praktijk kunnen voordoen bij het ROC, kan gekozen worden voor SDN of voor een traditioneel model. Beide modellen zijn hieronder toegelicht en voorzien van ontwerpregels. Tijdens het schrijven van afgeleide documentatie of een RFP-aanvraag kan worden besloten welk model op dat moment het beste past bij het ROC.

3.4.1 Datacenter: traditioneel model

In de onderstaande illustratie is dit type datacenter conceptueel afgebeeld:



Figuur 4-9: *Datacenter traditioneel model*

Het LAN-netwerk in de module Datacenter Onprem wordt middels de principes van de fysieke collapsed core vormgegeven, waarbij de Core-laag en Aggregatie-laag worden samengevoegd. Deze architectuurkeuze voorziet in een (toekomstige) afname van het aantal fysieke poorten dat benodigd is om technische systemen te accommoderen, zodat het traditionele model dat uit drie lagen bestaat (i.e. access, aggregatie, core) niet noodzakelijk is.

TA-bouwblokken:

TA-bouwblok: Access	
(Beknopte) Conceptuele beschrijving van het bouwblok	De access-laag geeft systemen in het datacenter toegang tot het netwerk van het ROC. De access-laag faciliteert alleen bedrade netwerktoegang. De access-laag voorziet in: • fysieke interfaces met de eindsystemen/hosts die het faciliteert. • fysieke interfaces met de collapsed core waaraan het direct is verbonden.
Functies van het bouwblok	• Ontsluiting van systemen (e.g. servers, storage). • Koppeling met de collapsed core.
Services die het bouwblok biedt (aan de omgeving)	• Toegangsservices voor systemen in het datacenter. • Connectiviteitsservices naar/vanaf de collapsed core.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende collapsed core (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Flexibel kunnen ontsluiten van systemen (bedraad). • Ondersteuning van jumbo frames. • Chassisvirtualisatie of stacking.

TA-bouwblok: collapsed core	
(Beknopte) Conceptuele beschrijving van het bouwblok	De collapsed core fungeert als verlengstuk van de accesslaag in de richting van de module Backbone. Het zorgt ervoor, dat op een gestandaardiseerde manier verschillende access-nodes vanuit de accesslaag toegang krijgen tot de module Backbone voor datatransport naar/vanaf de verschillende modules. Tevens faciliteert de collapsed core communicatiemogelijkheden tussen systemen binnen het datacenter zelf.
Functies van het bouwblok	• Aggregatie van nodes die deel uitmaken van de accesslaag. • Koppeling tussen de nodes die deel uitmaken van de accesslaag en nodes die deel uitmaken van de module Backbone. • Koppeling van service-nodes die PEP-functies uitoefenen (e.g. DC-firewall) • Koppeling van service-nodes die load-balancing-functies uitoefenen. • Koppeling tussen onprem datacenters.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices naar/vanaf de module Backbone. • Connectiviteitsservices tussen systemen binnen het onprem datacenter. • Routeringservice voor ROC-diensten die direct op DC-LAN-niveau met elkaar mogen communiceren.

	• Ondersteuning van service-nodes die clusterfuncties behoeven (e.g. redundantie firewall, redundantie load-balancers).
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende accesslaag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Ondersteuning van jumbo frames. • Line rate routing & switching. • Chassisvirtualisatie. • ISSU op nodeniveau.

TA-bouwblok: Koppelvlak accesslaag & collapsed core	

(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de accesslaag en de collapsed core voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats naar/vanaf de accesslaag en naar/vanaf de module Backbone.
	
	Vanaf de accesslaag naar de collapsed core:
	
	• Faciliteren van verkeersstromen voor:
	  ○ Retourverkeer voor het benaderen van DC-diensten vanaf andere modules.
	  ○ Beheerverkeer geïnitieerd door systemen in de accesslaag (e.g. updates, patches).
	  ○ Systeemverkeer tussen twee onprem datacenters.
	
	Naar de accesslaag vanaf de collapsed core:
	
	• Faciliteren van verkeerstromen voor:
	  ○ Het benaderen van DC-diensten vanaf andere modules.
	  ○ Retourverkeer in het kader van updates, patches e.d.
	  ○ Retourverkeer van verkeersstromen tussen twee onprem datacenters.

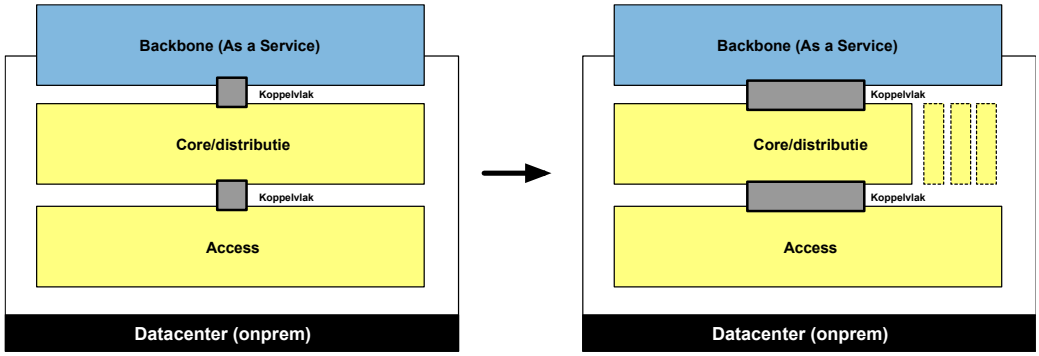
Functies van het bouwblok	Koppeling tussen de accesslaag en de collapsed core t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices vanaf de accesslaag naar de module Backbone. • Connectiviteitsservices tussen systemen binnen het datacenter. • Connectiviteitsservices vanaf de module Backbone naar de accesslaag.

Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de accesslaag en de collapsed core (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

TA-bouwblok: Koppelvlak collapsed core & module Backbone	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de collapsed core en de module Backbone voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats zowel vanaf als naar de collapsed core voor doeleinden die bij het voorgaande bouwblok zijn opgenomen (m.u.v. de afhandeling van verkeersstromen die binnen het datacenter zelf blijven of die direct tussen onprem datacenters verlopen. Dit laatste op grond van de DC-interconnect tussen onprem datacenters die niet op het niveau van de module Backbone wordt gerealiseerd maar direct tussen onprem datacenters).
Functies van het bouwblok	Koppeling tussen de collapsed core en de module Backbone t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices tussen de collapsed core en de module Backbone.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de collapsed core en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid.

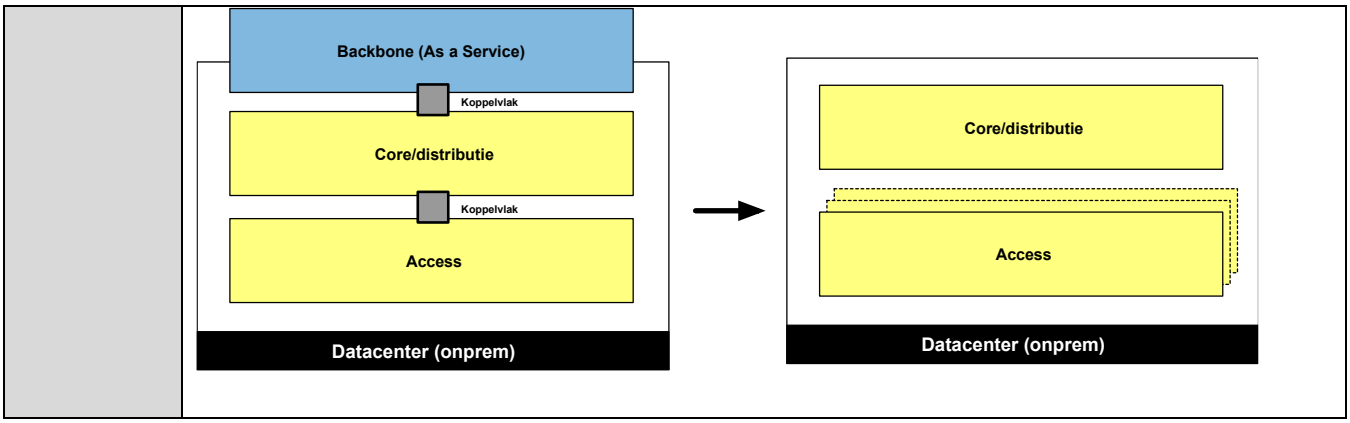
TA-patronen:

TA-patroon: Verticale uitbreidbaarheid	
Toepassing	Het datacenter dient verticaal schaalbaar te zijn door het verhogen van de interfacesnelheden op het niveau van het TA-bouwblok koppelvlak access & collapsed core. Tevens dient op het niveau van de collapsed core verticale uitbreidbaarheid te kunnen worden gerealiseerd door meerdere sloten/lijnkaarten/poorten per node te kunnen gaan benutten. Dit om eventueel tijdelijke groei te accommoderen met dien verstande, dat op termijn de footprint van het onprem datacenter zal afnemen i.v.m. de *cloud, tenzij…* strategie. Het omgekeerde is ook waar: indien de footprint van het datacenter afneemt, dient de collapsed core navenant te kunnen krimpen.
Context	Groei en krimp dienen te kunnen worden geaccommodeerd door nodes die deel uitmaken van de accesslaag en de collapsed core.
Eisen en beperkingen	Nodes die deel uitmaken van de accesslaag en de collapsed core dienen te voorzien in verticale schaalmogelijkheden, waarbij een opwaardering (en afwaardering) van interface-snelheden flexibel kan worden doorgevoerd. Tevens dient de collapsed core te voorzien in voldoende

	uitbreidingsmogelijkheden door een modulaire opbouw van een node/chassis. De modulariteit dient ook te kunnen worden gebruikt voor afschaaldoeleinden.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patronen:

TA-patroon: Horizontale uitbreidbaarheid	
Toepassing	Het datacenter dient horizontaal schaalbaar te zijn door het kunnen toevoegen van nodes die deel uitmaken van de accesslaag (indien noodzakelijk). De nodes dienen te worden geaggregeerd op het niveau van de collapsed core. Het omgekeerde is ook waar. Zodra de noodzaak bestaat af te schalen, dient ook de access-laag navenant te kunnen inkrimpen.
Context	Indien een datacenter tijdelijk groeit in aantallen diensten/systemen dient de accesslaag mee te kunnen groeien om toename in capaciteit te accommoderen. Het omgekeerde is ook waar: indien een datacenter minder capaciteit behoeft, dient de accesslaag navenant horizontaal te kunnen inkrimpen. De collapsed core is niet horizontaal schaalbaar, temeer deze verticaal schaalbaar is door gebruik te maken van uitbreidings- en krimpmogelijkheden middels modules/lijnkaarten/poorten binnen dezelfde node (i.e. verticale schaalbaarheid).
Eisen en beperkingen	Zowel accessnodes dienen gestacked te kunnen worden. Aggregatienodes dienen geclusterd te kunnen worden. Dit zodat alle nodes simultaan verkeer kunnen verwerken. Hierbij dient optimaal gebruik te kunnen worden gemaakt van alle beschikbare netwerkpaden tussen de access-laag en de collapsed core.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld.



3.4.1.1 Ontwerpregels datacenter onprem

De onderstaande kenmerken gelden voor dit model:

Ontwerpregel 12	**Traditioneel model: Eigenschappen datatacenter onprem**	
Ontwerpregel 12.1	Aanwezigheid onderwijskritieke ICT-services	Ja
Ontwerpregel 12.2	Medium tussen nodes lagen Access en collapsed-core	glas, minimaal 10 Gbit/s
Ontwerpregel 12.3	Medium tussen nodes collapsed core en de module Backbone	glas, minimaal 10 Gbit/s
Ontwerpregel 12.4	Ontsluiting nodes module Backbone	glas, minimaal 10 Gbit/s per connectie
Ontwerpregel 12.5	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.6	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.7	SLA access-node	MTTR 8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.8	SLA node collapsed core	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.9	Schaalbaarheid	Accesslaag: horizontale en verticale schaalbaarheid

		Collapsed core: verticale schaalbaarheid
Ontwerpregel 12.10	Toekomstige groei	In principe geen i.v.m. *cloud, tenzij…*principe.

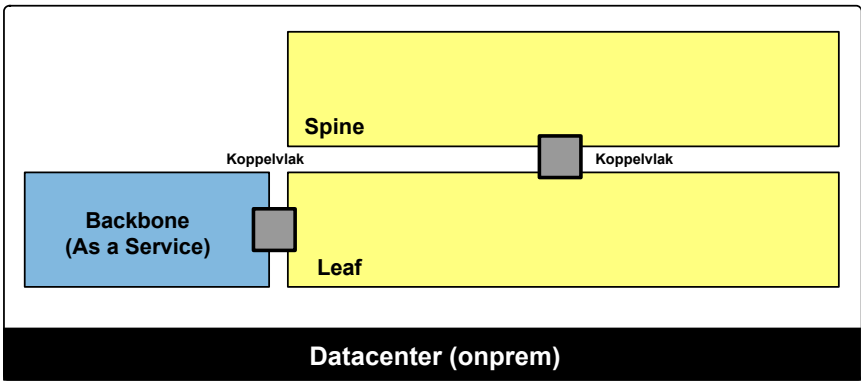
3.4.1.2 Generieke kenmerken nodes collapsed core en access

Ontwerpregel 13	**Traditioneel model: Generieke kenmerken nodes collapsed-core**
Ontwerpregel 13.1	Redundantie van uplink/downlinkverbindingen dienen middels linkbundelingstechnologie te kunnen worden vormgegeven.
Ontwerpregel 13.2	De chassis' van collapsed-core-nodes dienen te kunnen worden gevirtualiseerd, zodat één logische entiteit/cluster ontstaat. Clustering van collapsed-core-nodes hoeft niet beperkt te worden tot één datacenter en mag derhalve worden toegepast 'over' meerdere datacenters, indien dit in een gebruikssituatie de meest doelmatige oplossing is. Ontsluiting tussen de collapsed-core-nodes dient te zijn gebaseerd op Ethernet 40Gbit/s met de mogelijkheid tot afschaalbaarheid naar 10Gbit/s. Eventuele verbindingen voor heartbeats/ keepalives tussen de nodes mogen met een lagere doorvoersnelheid worden vormgegeven.
Ontwerpregel 13.3	Een collapsed-core-node dient te voorzien in een combinatie van 1 Gbit/s en 10 Gbit/s poorten, waarbij een groei naar 25 Gbit/s of hoger voor het ontsluiten van aanpalende nodes mogelijk dient te zijn indien tijdelijke groei geaccomodeerd dient te worden.
Ontwerpregel 13.4	Uplinks/downlinks zijn dusdanig gepositioneerd dat uitval van één collapsed-core-node in een cluster niet leidt tot een algeheel verlies van connectiviteit met de aanpalende node(s).
Ontwerpregel 13.5	Ontsluiting tussen collapsed-core-nodes en backbone-nodes is gebaseerd op minimaal 20Gbit/s, gebruikmakend van linkbundelingstechnologie.
Ontwerpregel 13.6	Een collapsed-core node voorziet in non-oversubscribed poorten (op elke poort).
Ontwerpregel 13.7	In Service Software Upgrade dient te worden ondersteund.
Ontwerpregel 13.8	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 13.9	Nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 13.10	Nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
Ontwerpregel 13.11	Nodes zijn voorzien van redundante power supplies.
Ontwerpregel 13.12	Nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.

Ontwerpregel 13.13	OSI Laag 3 terminatiepunten liggen op bij voorkeur op het niveau van de module Backbone, maar in ieder geval binnen de module Datacenter (onprem). Hiervan kan worden afgeweken, indien bijvoorbeeld voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een DC-overschrijdend OSI Laag 2 pad aan te brengen,
Ontwerpregel 13.14	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 13.15	Nodes communiceren met hun omgeving op basis van open standaarden.
Ontwerpregel 13.16	De node(s) van de module Backbone mogen geen deel uitmaken van de collapsed-core in verband met: • Het kunnen scheiden van de modules Datacenter onprem en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.
Ontwerpregel 13.17	Access nodes zijn voorzien van redundantie powersupplies
Ontwerpregel 13.18	Access nodes moeten voorzien in modulariteit van 10 Gbit/s UTP, 10 Gbit/s Twinax en combinaties MMF, SMF).
Ontwerpregel 13.19	Access nodes moeten voorzien linkbundelingstechnieken voor uplinks naar de collpased core en naar ontsluitende (server)systemen. Uplinks en downlinks dienen simultaan verkeer te kunnen verwerken.

3.4.2 Datacenter: SDN-model

De topologie van het SDN-model is in de onderstaande illustratie conceptueel afgebeeld. De topologie bestaat uit leafs (access) en spines (aggregatie), waarbij de module Backbone is verbonden aan een leaf, de zogenaamde border leaf. Dit is een significant verschil met alle traditionele gelaagde netwerkmodellen, waarin de backbone-nodes zijn verbonden aan de collapsed core. Naast de backbone nodes kunnen ook andere typen nodes verbonden zijn aan leaf switches (e.g. storage nodes middels 'storage leafs', security nodes middels 'service leafs').



Figuur 4-10 *Datacenter SDN-model*

Ontwerpregel 14	**Communicatie tussen SDN en traditioneel model**
Communicatie tussen onderdelen die deel uitmaken van het SDN-model en onderdelen die deel uitmaken van de module Backbone of deel uitmaken van services als storage, security verlopen middels border leafs. Communicatie dient te kunnen worden gestandaardiseerd op protocollen die opereren op de niveaus van OSI laag 2 en OSI laag 3.	

TA-bouwblokken:

TA-bouwblok: Leaf	
(Beknopte) Conceptuele beschrijving van het bouwblok	De leaf-laag geeft systemen in het datacenter toegang tot het netwerk van het ROC. Deze laag faciliteert alleen bedrade netwerktoegang. De leaf-laag voorziet in de volgende onderdelen: • fysieke interfaces met de eindsystemen/hosts die het faciliteert. • fysieke interfaces met de module Backbone waaraan het direct is verbonden. • fysieke interfaces met services als storage en firewalling.
Functies van het bouwblok	• Connectiviteitsservices met service-nodes zoals load balancers en firewalls.

Services die het bouwblok biedt (aan de omgeving)	• Toegangsservices voor systemen in het datacenter. • Connectiviteitsservices naar/vanaf de module Backbone • Ondersteuning van service-nodes die clusterfuncties behoeven (e.g. redundantie firewall, redundantie load-balancers).
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende collapsed core en border-nodes (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Flexibel kunnen ontsluiten van systemen (bedraad). • Ondersteuning van jumbo frames. • Aanstuurbaar via een SDN-controller met uitgebreide portalfuncties voor inzage verkeersstromen, monitoring en controle.

TA-bouwblok: spine	
(Beknopte) Conceptuele beschrijving van het bouwblok	De spine-laag zorgt ervoor, dat op een gestandaardiseerde manier verschillende nodes van de leaf-laag worden geaggregeerd. Tevens faciliteert de spine-laag communicatiemogelijkheden tussen systemen binnen het datacenter zelf.
Functies van het bouwblok	• Aggregatie van nodes die deel uitmaken van de leaf-laag. • Connectiviteitsservices tussen systemen die verbonden zijn aan de leaf-laag.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices tussen systemen binnen het onprem datacenter. • Routeringservice voor ROC-diensten die zonder tussenkomst van een PEP-functie (e.g. firewall) direct op DC-LAN-niveau met elkaar mogen communiceren.
Kwaliteitskenmerken	• Prioritering tussen getransporteerde diensten (i.e. quality of service). • Ondersteuning van een beschikbaarheid van 99,99% in de keten met de aanpalende ‘leaf-laag’ (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Ondersteuning van jumbo frames. • Line rate routing & switching.

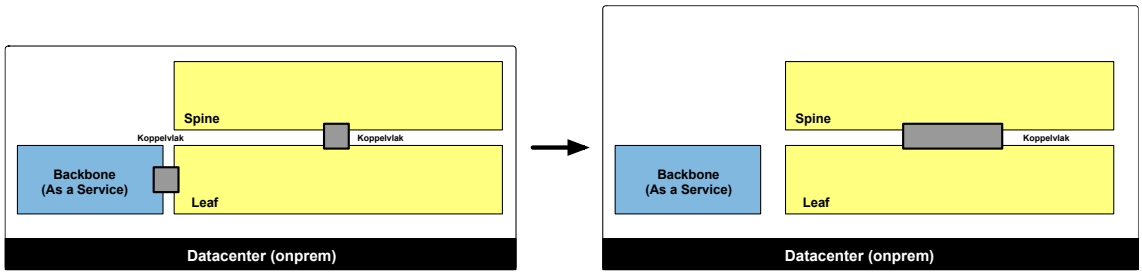
TA-bouwblok: Koppelvlak leaf-laag & module Backbone	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de leaf-laag en de module Backbone voorziet in datatransport tussen de beide omgevingen. Datatransport vindt plaats naar/vanaf de leaf-laag en naar/vanaf de module Backbone *Vanaf de leaf-laag naar de module Backbone:*

	• Faciliteren van verkeersstromen voor:
	  ○ Retourverkeer voor het benaderen van DC-diensten vanaf andere modules.
	  ○ Beheerverkeer geïnitieerd door systemen in de leaf-laag (e.g. updates, patches).
	
	Vanaf de module Backbone naar de leaf-laag:
	
	• Faciliteren van verkeerstromen voor:
	  ○ Het benaderen van DC-diensten vanaf andere modules.
	  ○ Retourverkeer in het kader van updates, patches e.d.

Functies van het bouwblok	Koppeling tussen de leaf-laag en de module Backbone t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	• Connectiviteitsservices tussen de leaf-laag en de module Backbone. • Connectiviteitsservices tussen systemen binnen het datacenter.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de leaf-laag en de module Backbone (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Simultaan gebruik kunnen maken van meerdere paden tussen de leaf-laag en de module Backbone.

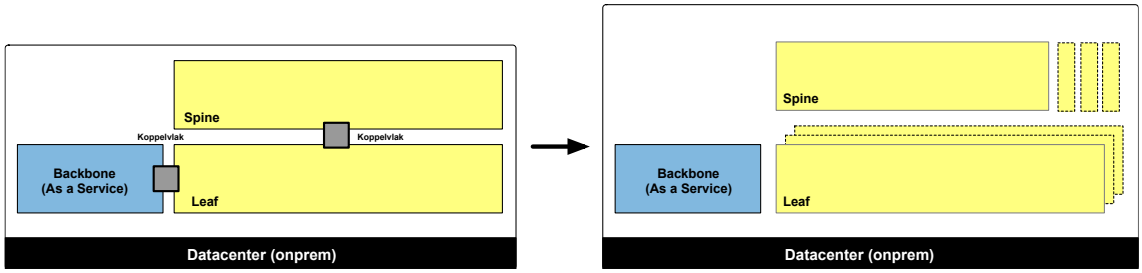
TA-bouwblok: Koppelvlak leaf-laag & spine-laag	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het koppelvlak tussen de leaf-laag en spine-laag voorziet in datatransport tussen de beide lagen. Datatransport vindt plaats voor verkeersafhandeling binnen het onprem datacenter.
Functies van het bouwblok	Koppeling tussen de lagen leaf en spine t.b.v. datatransport.
Services die het bouwblok biedt (aan de omgeving)	Connectiviteitsservices de lagen leaf en spine.
Kwaliteitskenmerken	• Ondersteuning van een beschikbaarheid van 99,99% tussen de lagen leaf en spine (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). • Flexibel kunnen opschalen en afschalen van capaciteit en doorvoersnelheid. • Simultaan gebruik kunnen maken van meerdere paden tussen de lagen leaf en spine.

TA-patronen:

TA-patroon: Verticale uitbreidbaarheid	
Toepassing	Het datacenter dient verticaal schaalbaar te zijn door het verhogen van de interfacesnelheden op het niveau van het TA-bouwblok koppelvlak leaf-laag & spine-laag.
Context	Groei en krimp dienen te kunnen worden geaccommodeerd door nodes die deel uitmaken van de leaf- en spinelagen, zodra hiertoe de noodzaak bestaat. Het omgekeerde is ook waar: indien de groei in bandbreedte afneemt dienen de nodes te voorzien in krimpmogelijkheden (waar nodig). Hetzelfde geldt voor het koppelvlak tussen de leaf-nodes en de backbone-nodes.
Eisen en beperkingen	Nodes die deel uitmaken van de leaf-laag en spine-laag dienen te voorzien in verticale schaalmogelijkheden, waarbij een opwaardering (en afwaardering) van interface-snelheden flexibel kan worden doorgevoerd.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

TA-patronen:

TA-patroon: Horizontale uitbreidbaarheid	
Toepassing	Het datacenter dient horizontaal schaalbaar te zijn door het kunnen toevoegen van nodes die deel uitmaken van de leaf-laag. De nodes dienen te worden geaggregeerd op het niveau van de spine-laag. Het omgekeerde is ook waar. Zodra de noodzaak bestaat af te schalen, dient ook de leaf-laag navenant te kunnen inkrimpen.
Context	Indien een datacenter tijdelijk groeit in aantallen diensten/systemen dient de leaf-laag mee te kunnen groeien om toename in capaciteit te accommoderen. Het omgekeerde is ook waar: indien een datacenter minder capaciteit behoeft, dient de leaf-laag navenant horizontaal te kunnen inkrimpen. De spine-laag is niet horizontaal schaalbaar, temeer deze verticaal schaalbaar is door gebruik te maken van uitbreidings- en krimpmogelijkheden middels modules/lijnkaarten/poorten binnen dezelfde node (i.e. verticale schaalbaarheid).
Eisen en beperkingen	Zowel leaf- en spine-nodes volgen de principes van de ‘leaf-spine-leaf-topologie’ opdat alle nodes simultaan verkeer kunnen verwerken. Hierbij dient optimaal gebruik te kunnen worden gemaakt van alle beschikbare netwerkpaden tussen de voornoemde lagen.

Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

3.4.2.1 Ontwerpregels datacenter onprem SDN-model

De onderstaande kenmerken gelden voor dit model:

Ontwerpregel 15	**SDN-model-Eigenschappen datatacenter onprem**	
Ontwerpregel 15.1	Aanwezigheid onderwijskritieke ICT-services	Ja
Ontwerpregel 15.2	Medium tussen nodes lagen ‘leaf’ en collapsed-core	Glas, minimaal 10 Gbit/s
Ontwerpregel 15.3	Medium tussen nodes lagen ‘leaf’ en ‘spine’	Glas, minimaal 10 Gbit/s
Ontwerpregel 15.4	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 15.5	SLA leaf-node	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 15.6	SLA aggregatie-node	MTTR 8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 15.7	Schaalbaarheid	‘Leaf-laag’: horizontale en verticale schaalbaarheid ‘Spine-laag’: verticale schaalbaarheid
Ontwerpregel 15.8	Toekomstige groei	In principe geen i.v.m. *cloud, tenzij…*principe. Eventuele groei dient wel te kunnen worden

		geaccommodeerd in de ‘leaf’ en ‘spine’ laag.

3.4.2.2 Generieke kenmerken leaf en spine nodes

Het model bevat nodes van het type leaf en spine die generieke kenmerken hebben of kenmerken die dermate overeenkomen dat deze hieronder geroepeerd zijn opgenomen.

Ontwerpregel 16	SDN-model: Generieke kenmerken leaf en spine nodes
Ontwerpregel 16.1	Leaf-nodes zijn verbonden met iedere spine-node in de topologie, zodat uitval van een uplinkverbinding of een spine-node niet leidt tot een algeheel verlies van connectiviteit vanaf een leaf-node. Leaf nodes dienen geclusterd te kunnen worden.
Ontwerpregel 16.2	De access-poorten van een leaf-nodes zijn van het type koper of glas met ondersteuning van de interfacesnelheden 1Gbit/s en 10Gbit/s, waarbij een groei naar 25Gbit/s of hoger mogelijk is.
Ontwerpregel 16.3	Leaf-nodes ontsluiten het SDN-model naar de module Backbone, waarbij: • Gebruikgemaakt kan worden van linkbundelingstechnieken, • De ontsluiting gebaseerd is op minimaal 20Gbit/s (modulariteit moet kunnen voorzien in 10 Gbit/s UTP, 10 Gbit/s Twinax en combinaties MMF, SMF). • Meerdere leaf-nodes gebruikt kunnen worden voor de ontsluiting naar de module Backbone ter voorkoming van SPOFs, • Connectiviteit kan worden gerealiseerd op basis van zowel OSI laag 2 als OSI laag 3.
Ontwerpregel 16.4	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 16.5	Nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 16.6	Spinde-nodes zijn voorzien van redundante power supplies, leaf-nodes niet.
Ontwerpregel 16.7	Nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 16.8	Ontsluiting tussen leaf-nodes en spine-nodes zijn gebaseerd op minimaal 10Gbit/s, waarbij een groei naar 40 Gbit/s of hoger mogelijk dient te zijn.
Ontwerpregel 16.9	De software-architectuur is modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien ‘pay as you grow’ kunnen worden ingevuld.
Ontwerpregel 16.10	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de module Backbone, maar in ieder geval binnen de module Datacenter. Hiervan kan worden

	afgeweken, indien bijvoorbeeld voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een datacenter-overschrijdend OSI Laag 2 pad aan te brengen.
Ontwerpregel 16.11	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 16.12	Nodes die deel uitmaken van de SDN-topologie communiceren met nodes buiten deze topologie op basis van open standaarden.

3.5 Module Cloud en module SURF

3.5.1 Clouddiensten

De opkomst van de publieke cloud is niet meer te negeren. Het gebruik van de publieke cloud biedt nieuwe kansen en mogelijkheden, dan wel kansen en mogelijkheden die ‘on-premise’ niet mogelijk zijn. Om op de toekomst voorbereid te zijn en tijdig kennis- en ervaring op te bouwen, heeft het ROC besloten niet te wachten met cloudadoptie maar het principe van ‘cloud, tenzij’ als beleidsuitgangspunt genomen. Vanuit onderwijsvraagstukken bezien biedt de publieke cloud kansen en mogelijkheden die noodzakelijk zijn om vraagstukken te realiseren die ‘on-premise’ vanuit de vereiste snelheid en het beschikbare budget lastig zijn te realiseren.

De module cloud bestaat uit drie verschillende typen diensten:

1. IaaS,
2. PaaS,
3. SaaS.

IaaS
IaaS staat voor ‘Infrastructure as a Service’. Van de verschillende clouddiensten lijkt IaaS het meest op de traditionele on-premise dienstverlening van het ROC. Bij IaaS wordt de infrastructuur samen met alle netwerkelementen ondergebracht in een clouddatacenter als Azure, AWS, GCP. Het beheer van de fysieke hardware-onderdelen wordt door de clouddatacenterprovider verzorgt. Het ROC behoudt hierbij wel het beheer op het operating systeem, de database, applicaties en data. Daar waar het het netwerk (‘Het LAN’) betreft, is het beheer beperkt tot het vaststellen en beheren van infrastructurele onderdelen (e.g. subnetten, het uitgeven van IP-adressen en serversystemen, Network Appliances, Security Appliances, Gateways et cetera).

PaaS
PaaS staat voor ‘Platform as a Service’. Bij PaaS wordt nog meer beheer uit handen genomen van het ROC. Naast de hardware worden namelijk ook het beheer van operating systeem en databases verzorgd door de clouddatacenterprovider.PaaS kan worden gezien als een platform waarop software op een snelle, eenvoudige en efficiënte manier kan worden ontwikkeld, getest en in productie kan worden ondergebracht. Het beheer van data en applicaties wordt door het ROC uitgevoerd.

SaaS
SaaS staat voor ‘Software as a Service’. Bij SaaS wordt nog meer (dan bij PaaS) beheer uit handen genomen van het ROC. Ook het beheer van de data en applicaties wordt door de leverancier van SaaS-oplossingen uitgevoerd. SaaS-diensten zijn de snelst groeiende clouddiensten waar ook het ROC steeds vaker gebruik van maakt. Soms levert het ROC een dienst (e.g. SQL-dienst) als SaaS-oplossing, waarbij de cloud IDP (Identity Provider) van het ROC wordt gebruikt. In dit geval wordt het beheer van de IDP door het ROC gedaan.

Voor meer informatie over dit topic wordt verwezen naar openbare bronnen als:
https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

3.5.2 Module SURF

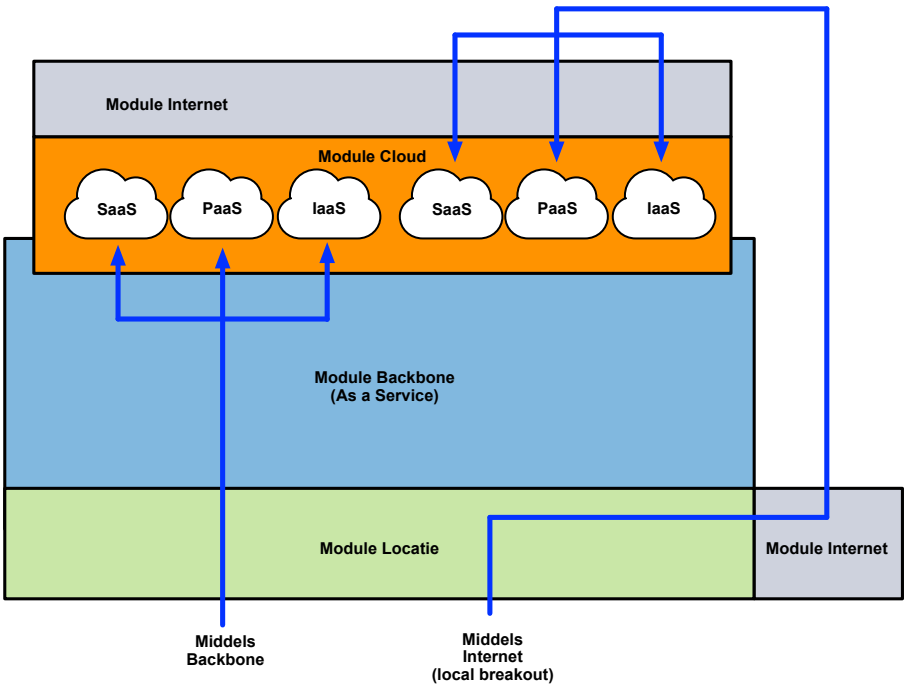
De module SURF is separaat afgebeeld in de technische overzichten in deze technische architectuurblauwdruk. SURF biedt ook clouddiensten aan is daarmee de facto functioneel gelijk als andere leveranciers van clouddiensten. De reden voor het separaat afbeelden van SURF is de speciale positie die SURF in de onderwijssector inneemt. Tevens wordt de module SURF direct verbonden aan de module Backbone in verband met het direct kunnen benaderen van diensten die SURF aanbiedt (vanuit de module Locatie gezien). Indien diensten die SURF aanbiedt niet direct benaderbaar zijn via de module Backbone wordt het reguliere internet gebruikt.

3.5.3 Benadering van clouddiensten

Clouddiensten kunnen op twee manieren benaderd worden:

1. Via de module Backbone waaraan een clouddienst direct is verbonden,
2. Via de module Internet die als local breakout deel uitmaakt van de module Backbone. Tevens kunnen gebruikers buiten de module Locatie om via de module Internet (‘de eigen internetverbinding’) betreffende clouddiensten benaderen.

In de onderstaande illustratie is dit conceptueel afgebeeld:



Figuur 4-11: *Benadering van clouddiensten*

Ontwerpregel 17	Benadering van clouddiensten
Ontwerpregel 17.1	Het dient mogelijk te zijn clouddiensten alleen te ontsluiten via de module Backbone waaraan de module Cloud direct is verbonden. Dit indien bepaalde ROC-diensten alleen vanaf de module Locatie via de module Backbone benaderd mogen worden.
Ontwerpregel 17.2	Het dient mogelijk te zijn clouddiensten alleen te ontsluiten via de module Backbone, waarbij gebruikgemaakt wordt van een local-internetbreakout. Tevens kunnen gebruikers die op afstand werken (e.g. mobiel/vanaf huis) de betreffende clouddiensten benaderen.

3.5.4 Generieke ontwerpregels clouddatacenter

De onderstaande ontwerpregels gelden voor het gebruik van clouddatacenters (e.g. Azure, AWS, GCP).

Ontwerpregel 18	Generieke ontwerpregels clouddatacenter
Ontwerpregel 18.1	ROC-diensten dienen in verschillende availability zones te kunnen worden ondergebracht.
Ontwerpregel 18.2	ROC-diensten dienen in verschillende availability sets te kunnen worden ondergebracht.
Ontwerpregel 18.3	Binnen een clouddatacenter wordt gebruikgemaakt van de door de provider aangeboden default route naar het internet.
Ontwerpregel 18.4	ROC-diensten worden ondergebracht in de regio EER met uitsluiting van de UK.
Ontwerpregel 18.5	Koppeling tussen een clouddatacenter en de module Backbone wordt verzorgd door de leverancier van de module Backbone, waarbij de koppeling met een beschikbaarheid 99,99% wordt aangebracht (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 18.6	Koppeling tussen een clouddatacenter en de module Backbone ondersteunt Quality of Service.
Ontwerpregel 18.7	Koppeling tussen een clouddatacenter en de module Backbone is gebaseerd op minimaal 10Gbit/s, waarbij de afgenomen bandbreedte kan worden afgestemd op het gebruik.
Ontwerpregel 18.8	Zowel IPv4 als IPv6 dienen te worden ondersteund.

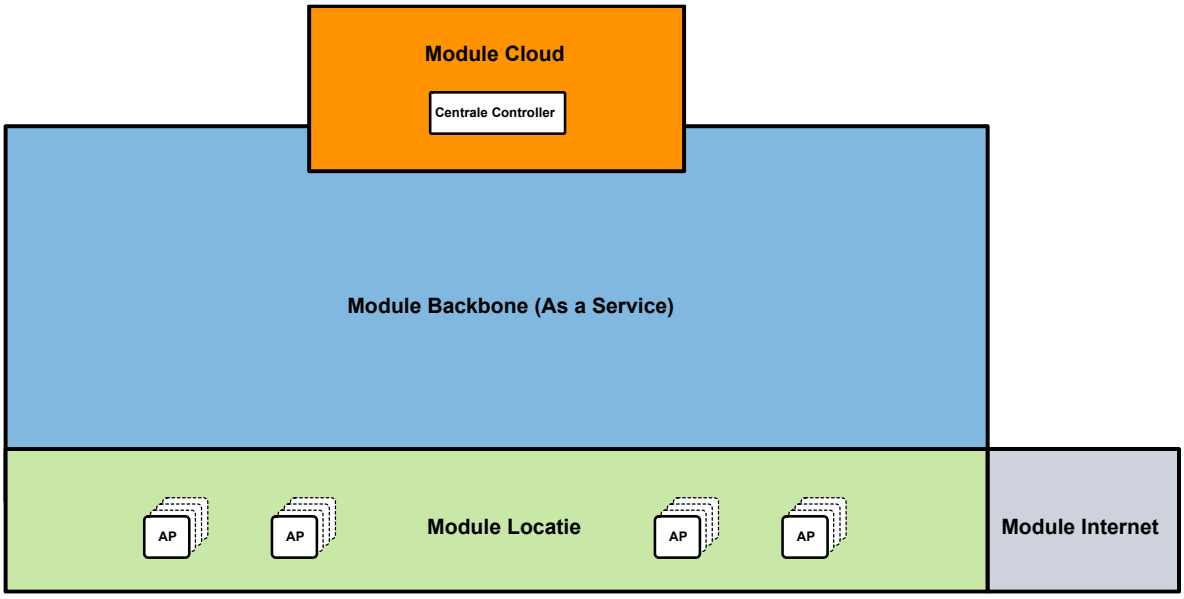
3.6 WLAN

3.6.1 Generiek

Een goed functionerend draadloos netwerk is vandaag de dag steeds belangrijker voor organisaties. Naast persoonsgebonden draadloze clients wordt in het algemeen ook steeds meer randapparatuur als printers, camera's en IOT-devices draadloos ontsloten. Dit is niet anders bij het ROC. Een substantiële groei aan draadloze clients en toename aan bandbreedte wordt dan ook verwacht.

In de onderstaande figuur is de generieke opbouw van het draadloze netwerk afgebeeld. De access points (AP) zijn verbonden aan centrale componenten die als dienst in de module Cloud worden afgenomen. Dit laatste op grond van de *cloud, tenzij* strategie van het ROC. Echter, hierbij dient rekening gehouden te worden met het volgende:

Centrale componenten kunnen ook in het 'eigen/onprem' datacenter worden ondergebracht, indien hiertoe goede redenen bestaan. Met andere woorden: een invulling van het deelprincipe 'tenzij' wordt niet van tevoren uitgesloten!



Figuur 4-12: *Opbouw WiFi-netwerk*

Ontwerpregel 19	WiFi generiek
Ontwerpregel 19.1	Bij voorkeur wordt WiFi aangeboden vanuit de module Cloud op grond van het beleidsuitgangspunt van het ROC: c*loud, tenzij*…Dit houdt in dat: • Centrale functies als controller/management vanuit 'de cloud' worden afgenomen,

	• Management-, provisioning- en beheerportals vanuit ‘de cloud’ worden afgenomen. Indien de leverancier van de module Backbone geen directe connectiviteits-mogelijkheden heeft met de leverancier van WiFi is het toegestaan connectiviteit aan te brengen vanaf de module Locatie naar de betreffende SaaS-oplossing middels een decentrale internet breakout. Hierbij dient de communicatiestroom echter wel te worden beschermd door protocollen met ingebouwde beveiligingsfuncties (e.g.: IPsec, HTTPS e.d.).
Ontwerpregel 19.2	Access points dienen de standaard IEEE 802.11ax te ondersteunen met extra functionaliteiten voor Bluetooth en Zigbee.
Ontwerpregel 19.3	Access points dienen te voorzien in 4x4 MU-MIMO (Multi-User MIMO) met minimaal 4 spatial streams.
Ontwerpregel 19.4	Access points dienen te voorzien in flexibele radio-instellingen op grond van de RF-omgeving, waarbij deze dual band frequenties (2.4 en 5Ghz) ondersteunt.
Ontwerpregel 19.5	Access points dienen middels PoE van stroom te worden voorzien.
Ontwerpregel 19.6	Access points dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 19.7	Quality of Service dient te worden ondersteund in de draadloze netwerk-faciliteiten.
Ontwerpregel 19.8	Het draadloze netwerk dient multicast te ondersteunen. Het draadloze netwerk dient ook mDNS te ondersteunen in verband met te gebruiken digiborden.
Ontwerpregel 19.9	Het draadloze netwerk dient goede ondersteuning/support te leveren voor ‘home oplossingen’ als ‘hue lampen’. Hierbij dient rekening te worden gehouden met de samenhang tussen het bedrade en draadloze netwerk. Deze lampen vereisen namelijk, dat ‘gewerkt’ wordt binnen in hetzelfde broadcastnetwerk.
Ontwerpregel 19.10	De managementomgeving/portal van het draadloze netwerk dient goede inzage te geven in ‘client-gebruik, ‘client-dichtheid’, ‘client failures’, ‘AP-failures’. Tevens dient de managementomgeving/portal te beschikken over goede monitoring & troubleshootfuncties.
Ontwerpregel 19.11	‘Local breakout’ en ‘central breakout’ moet mogelijk zijn (al dan niet als elkaars fallbackoplossing bij storingen), waarbij authenticatie in alle omstandigheden mogelijk moet blijven.
Ontwerpregel 19.12	Het draadloze netwerk dient dezelfde functionaliteit te bieden als het bedrade netwerk voor dezelfde categorieën devices.

3.6.2 Site surveys

Aangezien (naar de toekomst toe) het gebruik van draadloze netwerkfaciliteiten alleen maar zal toenemen en derhalve ook de relevantie van draadloze netwerkcommunicatie voor het ROC, is het van belang over een optimaal functionerend en dekkend WiFi-netwerk te beschikken. In deze paragraaf zijn generieke richtlijnen opgenomen waarmee de bovenstaande doelstellingen kunnen worden behaald. De richtlijnen zijn onderverdeeld in drie categorieën:

1. Pre site survey,
2. Site survey,
3. Post site survey.

Ad 1. Pre site survey

Ontwerpregel 20	**Pre site survey**

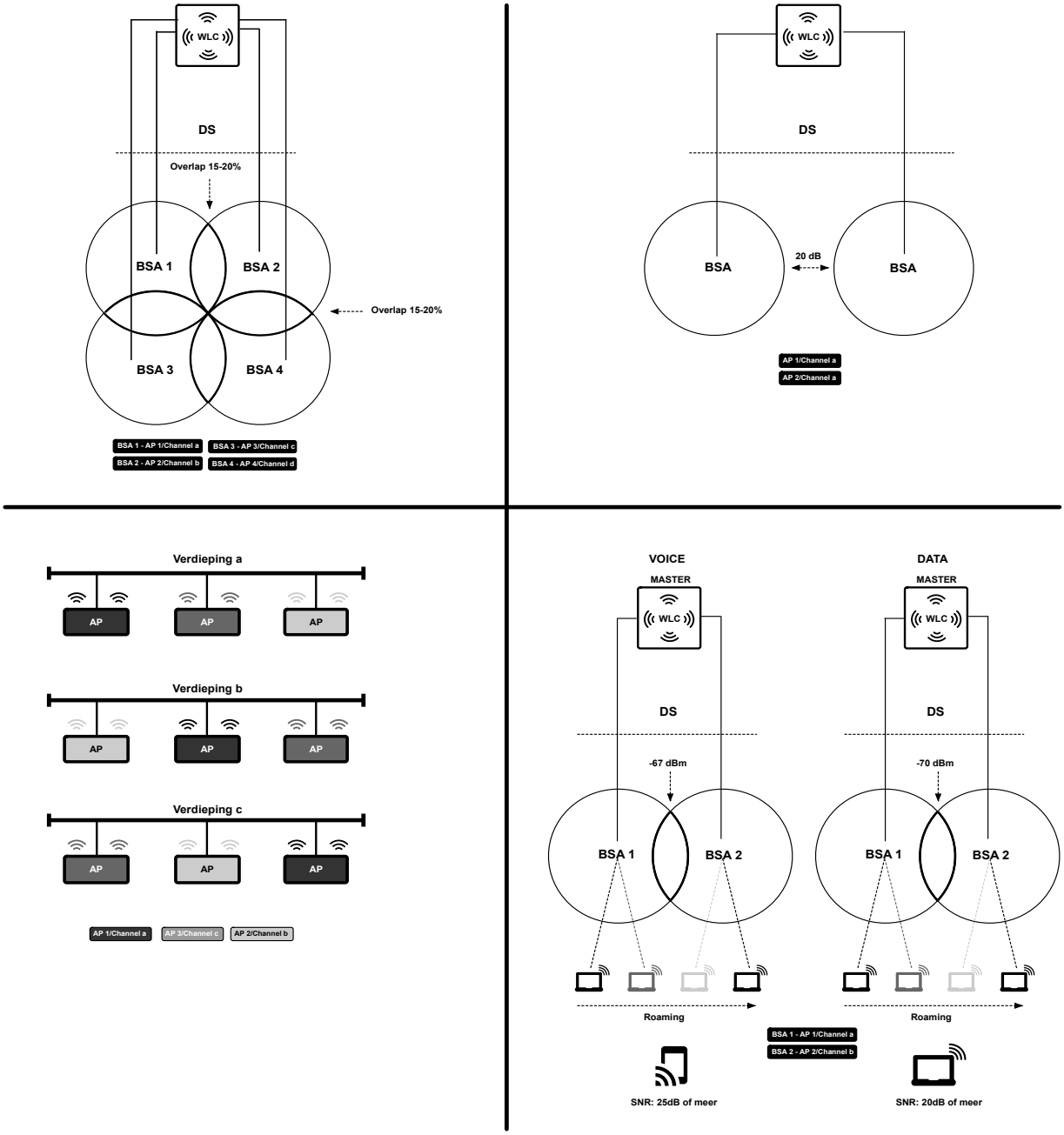
Alvorens een site survey door te voeren, dienen de onderstaande organisatorische onderdelen te worden aanschouwd/vastgelegd/besproken/beantwoord:

- Vaststellen van de business requirements:
  - Afnemers die gebruik maken van het draadloze netwerk?
  - Typen clients die gebruik maken van het draadloze netwerk?
- Vaststellen van dekking en capaciteit waaraan het draadloze netwerk dient te voldoen:
  - Aantal clients dat een access point accommodeert?
  - Simultaan gebruik van het draadloze netwerk?
  - Groei van het aantal wireless clients dat gebruik zal gaan maken van het draadloze netwerk?
  - De locatie/fysieke plaats waar wireless clients zich bevinden?
  - Piekuren van het gebruik van het draadloze netwerk?
  - Welke wireless devices kunnen interfereren met het draadloze netwerk?
  - Mobility?
  - PoE requirements?
- Analyse van het huidige draadloze netwerk:
  - Vaststellen van problemen met betrekking tot het huidige draadloze netwerk,
  - Welke devices interfereren met het huidige draadloze netwerk?
  - Zijn fysieke locaties/plaatsen aanwezig waar geen of slecht signaalbereik is (‘coverage dead zones’)?
  - Is een Radioplan voorhanden vanuit eerdere site surveys?
  - Welke draadloze apparatuur wordt gehanteerd in de huidige setting?
  - Hoe worden de access points voorzien van stroom?
- Vaststellen huidige bedrade netwerkinfrastructuur:
  - Vaststellen huidige topologie bedrade netwerkinfrastructuur,
  - Waar bevindt/begint de bedrade netwerkinfrastructuur i.v.m. plaatsing van access points?

- Welk type koper wordt gebruikt?
- Documentatie/rapporten voorhanden?
- Zijn blueprints/oppervlakteschema's voorhanden?

Ad 2. Site survey

In de onderstaande figuur zijn generieke richtlijnen afgebeeld waaraan een draadloos netwerk in het algemeen dient te voldoen.



Figuur 4-13: *Technische details Site Survey*

Ontwerpregel 21	Site survey

De onderstaande technische gegevens zijn van belang in het kader van het uitvoeren van een site survey:

- De site survey dient gebaseerd te zijn op een draadloze netwerkinfrastructuur die wordt gerealiseerd op basis van de meest recente standaard (op het moment van schrijven is dat de IEEE802.11-ax standaard).
- Het vaststellen van de dekking dient te zijn gebaseerd op de principes van zowel een passieve als actieve site survey, waarbij de informatie uit beide surveys met elkaar kunnen worden vergeleken c.q. als aanvulling op elkaar kunnen werken.
- De site survey dient te worden uitgevoerd met apparatuur die representatief is voor de latere implementatie.
- Uitgangspunt qua aantal gelijktijdige wireless clients per gebruiker:
    - Medewerker -> maximaal 3 devices
    - Studenten -> maximaal 3 devices
    - Docenten -> maximaal 3 devices
- Op grond van:
    - best practices en ervaringen in gelijksoortige omgevingen,
    - huidige gebruikersaantallen en oppervlakten,

  dient een inschatting te worden gemaakt van dekkingsgraden, capaciteitsbehoeften, aantallen access points, aantallen wireless LAN controllers (voorkeur als SaaS-afname) en benodigde licentie(structuren).
- Er dient geen rekening te worden gehouden met ‘backward compatibility’ van wireless devices in het kader van de standaarden IEEE 802.11 a,b,g.
- De draadloze oplossing dient te voldoen aan de wettelijk geldende normen/eisen op het gebied van de maximale elektromagnetische straling.
- Er dient rekening te worden gehouden met een overlap tussen de wireless cellen van 15-20%. Dit in verband met wireless clients waarop voice applicaties kunnen zijn aangebracht.
- ‘Adjacent channel interference’ dient te worden voorkomen door het juist instellen van wireless radio’s op grond van een goed doordacht en berekend RF-plan.
- Indien ‘co-channel interference’ onvermijdelijk blijkt, dient een waarde van 20dB te worden gehandhaafd aan de uiterwaarden van de cellen.
- OSI Layer 2 retransmissions dienen te worden voorkomen. Aandacht dient te worden geschonken aan:
    - Wireless devices die het RF-spectrum interfereren (narrow band interference, wide band interference, all-band interference),
    - ‘Adjacent channel interference’,
    - Lage Signal to Noise Ratio (SNR),
    - Een mismatch in power settings tussen een access point en een wireless client,
    - Disproportionele ‘transmit power settings’ tussen verschillende wireless clients (near/far problematiek),
    - Hidden node problematiek.

- Roaming dient ‘seamless’ te gebeuren zonder voor gebruikers merkbare onderbreking van verkeersstromen en kwaliteit van de gebruikte diensten. Er dient te worden voldaan aan:
    - Fast roaming, waarbij roaming zowel volgens het principe ‘over-the-air’ als ‘over-the-DS’ mag plaatshebben naar gelang de beste kwaliteit van roaming wordt bereikt,
    - Voor voice applicaties geldt een waarde van -67 dBm (of beter) in de uiterwaarde van een cell met een SNR van 25dB (of beter),
    - Op locaties waar geen voice applicaties gebruikt worden geldt een waarde van -70 dBm (of beter) voor de cell-uiterwaarde met een SNR van 20dB (of beter).

Ad 3. Post site survey

Ontwerpregel 22	**Post site survey**

Nadat de site survey is doorgevoerd, dienen de onderstaande organisatorische onderdelen te worden aanschouwd/vastgelegd:

- De exacte dekkingsgraad en capaciteitsbehoefte per locatie zal in goed overleg worden afgestemd.
- De volgende deliverables dienen te worden opgeleverd (afzonderlijk of integraal):
    - Statement/doel met requirements als uitgangspunten,
    - Spectrum Analyse met informatie over potentiële bronnen van interferentie,
    - Dekkings Analyse met informatie over alle RF- cellen/uiterwaarden (heating maps),
    - Aanbevelingen voor het positioneren/implementeren van access points, inclusief de oriëntatie van antennes, kanalen, energie settings, installatietechnieken, bekabeling (implementatie-diagrammen).
    - Capaciteit en Performance Analyse met resultaten van ‘application throughput testing’.

3.7 Microsoft Azure

3.7.1 Achtergrond

Hoewel in een technische architectuurblauwdruk normaliter geen producten/vendoren worden benoemd/behandeld, wordt in dit hoofdstuk echter expliciet Microsoft Azure behandeld. Dit heeft te maken met de reeds gemaakte keuze voor Azure en derhalve het belang om de technische kaders voor Azure als clouddatacenter vast te leggen. Dit laat echter onverlet, dat hetgeen geldt voor Microsoft Azure ook geldt voor andere leveranciers van publieke clouddiensten zoals Amazon AWS, Google Cloud Platform (mocht het ROC in de toekomst opteren voor een andere (aanvullende) leverancier). De beschreven principes dienen zodoende ook door andere leveranciers te kunnen worden 'ingevuld'.

3.7.2 Tenant, management group en subscription

De publieke clouddienst Azure van Microsoft gaat een steeds belangrijkere rol spelen bij het leveren van diensten aan gebruikers en systemen van het ROC. Het is van belang de infrastructuur van Azure van meet af aan correct aan te brengen, zodat in een later stadium geen noemenswaardige veranderingen te hoeven worden aangebracht.

Er is een aantal concepten dat in deze paragraaf wordt behandeld:

<u>Tenant</u>
Een tenant is een representatie van een organisatie. Het is een 'dedicated instance' van Azure Active Directory dat een organisatie krijgt toebedeeld wanneer deze een relatie met Microsoft aangaat, zoals bij het aanmaken van een account voor Azure, Microsoft Intune of Microsoft365. Een belangrijk en specifiek onderdeel van Azure is derhalve het tenantconcept. Het tenantconcept van Azure is gelieerd aan Azure Active Directory (AAD). AAD speelt een belangrijke rol wanneer bijvoorbeeld O365 wordt gebruikt, maar ook bij toegangsverlening tot resources binnen Azure zelf. De AAD wordt (in de regel) verbonden met de on-premise AD(s). Eenvoudiger gesteld bestaat een Azure tenant uit een AAD waaraan O365/Intune is gelinkt en waarin één of meerdere Azure subscriptions zijn opgenomen die vallen onder een contract met een bepaalde organisatie. De juiste initiële configuratiekeuzen ten aanzien van het tenantconcept zijn essentieel voor organisaties, omdat het effect daarvan jaren kan doorwerken.

<u>Management group</u>
Met management groups kunnen subscriptions worden georganiseerd in een hiërarchie met meerdere niveaus, hetgeen een aantal concrete voordelen oplevert:

- **Minder overhead**
  Geen noodzaak om governance toe te passen op afzonderlijke subscriptions.
- **Enforcement**
  Company administrators kunnen governance toepassen op het niveau van management group;

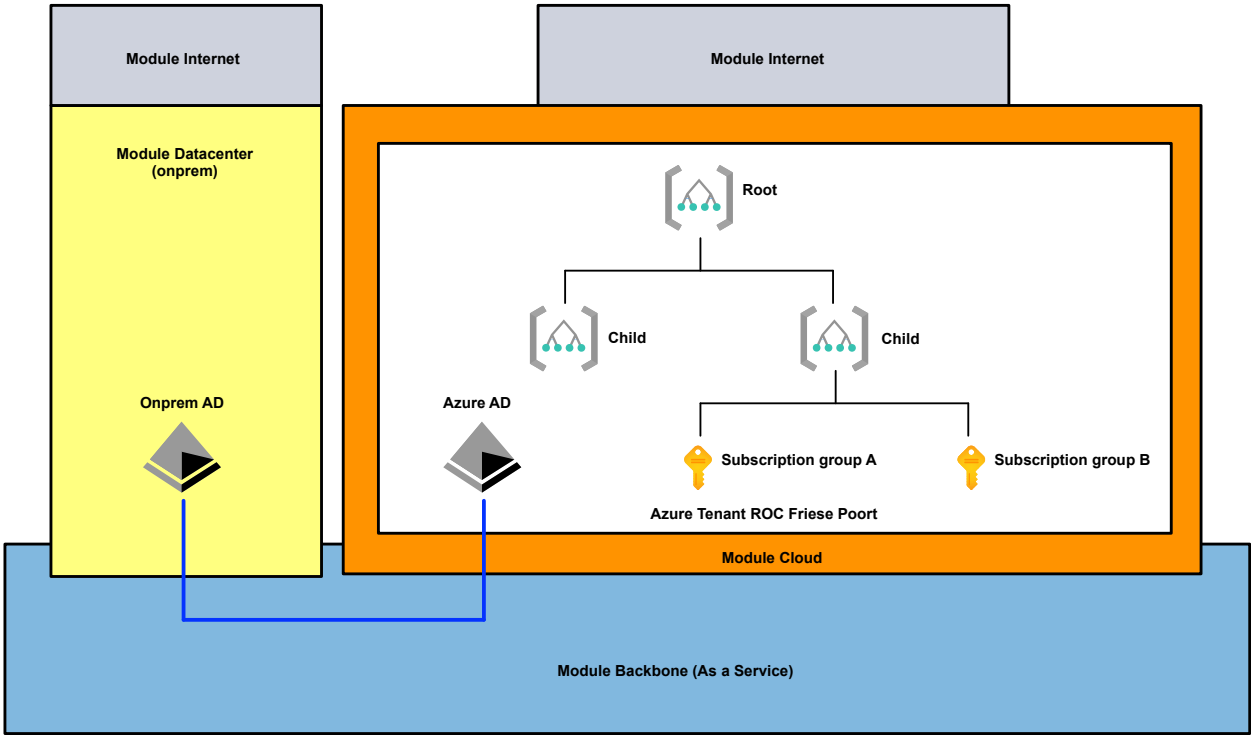
buiten de controle om van de administrators van de subscription. Governance kan eenvoudig worden toegepast op zowel bestaande als nieuwe subscriptions. Dit elimineert inconsistenties in de toepassing van governance, aangezien hetzelfde beleid op dezelfde manier wordt toegepast op de geselecteerde subscriptions.

- **Rapportage**
  Een Management Group kan rapportage van meerdere / alle subscriptions in een organisatie omvatten.

Subscription

Een Azure subscription is een basisonderdeel van elke Azure-implementatie. Elke resource die in Azure wordt aangemaakt, bevindt zich in een Azure subscription. Een Azure subscription is tevens een 'billing boundary' voor Azure-resources.

Met de combinatie van management groups en subscriptions kan een organisatie derhalve invulling geven aan een passende structuur, bijvoorbeeld naar business units, producten, ontwikkel- versus productie omgevingen of afdelingen. In de onderstaande illustratie zijn de concepten 'tenant', 'management group' en 'subscription' afgebeeld op grond waarvan de technische infrastructuur van het ROC binnen Azure wordt vormgegeven.



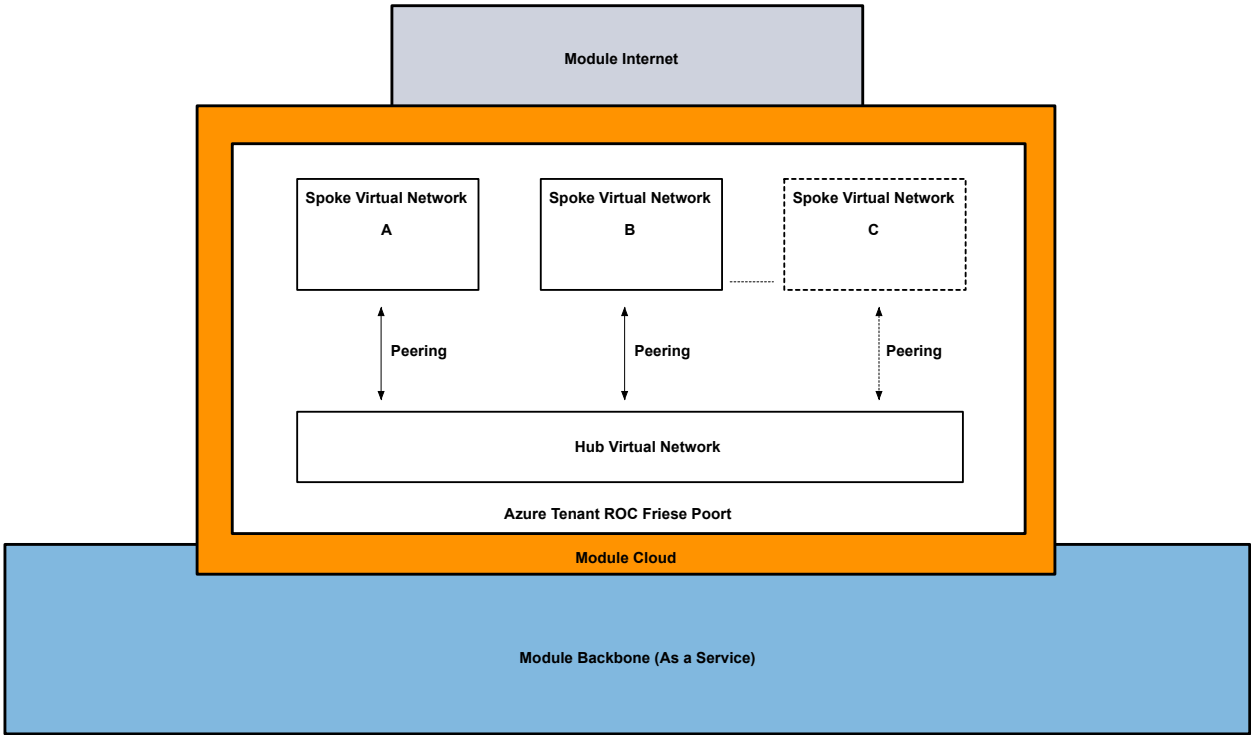
Figuur 4-14: *Tenant, management groups, subscription*

Er staat één root management group aan de basis van de hiërarchie. Deze management group is gekoppeld aan de AAD-tenant die vervolgens wordt gekoppeld aan een Azure subscription. Deze root management group kan niet worden verplaatst of verwijderd. Individuele subscriptions, inclusief nieuwe subscriptions, worden toegevoegd aan een 'child management group'.

Ontwerpregel 23	Ontwerpregels Azure: Tenant, management group, subscription
Ontwerpregel 23.1	Het ROC hanteert het één tenantconcept, waarbij één AAD gebruikt wordt.
Ontwerpregel 23.2	Het ROC hanteert het gebruik van management groups voor het centraal kunnen afdwingen van policies/beleid (governance) over alle subscriptions heen.
Ontwerpregel 23.3	Een subscription heeft limieten. Als deze overschreden (kunnen) worden, dienen deze te worden opgehoogd. Als dat niet meer mogelijk is, dienen (vooraf) extra subscriptions te worden ingezet.
Ontwerpregel 23.4	Communicatie tussen de onprem AD en AAD verloopt middels de module Backbone, waarbij connectiviteit met Azure wordt gerealiseerd door de leverancier van de module Backbone.

3.7.3 Topologie infrastructuur

De topologie van de infrastructuur van Azure is in de onderstaande illustratie afgebeeld. Het betreft de hub-and-spoke-topologie die wordt ingezet voor het ROC.



Figuur 4-15: *Hub-and-spoke topologie*

De voordelen van deze topologie zijn onder meer:

- **Kostenbesparingen**
  Door op één locatie (hub) services te centraliseren die kunnen worden gedeeld door meerdere workloads, zoals virtuele netwerkapparaten (NVA's), domain controllers, monitoringsystemen en DNS-servers.
- **Scheiding van domeinen/belangen/verantwoordelijkheden**
  Tussen O,T,A,P-omgevingen (spokes)

Typische toepassingen voor deze architectuur zijn onder meer:

- Workloads die in verschillende omgevingen worden geïmplementeerd, zoals ontwikkeling, test, acceptatie en productie, waarvoor gedeelde services zoals DNS, IDS, NTP of ADDS nodig zijn. Gedeelde services worden in het virtuele hub-netwerk ondergebracht, waarbij iedere omgeving wordt geïmplementeerd in een spoke virtueel netwerk om de isolatie te behouden. Dataverkeer in Azure is standaard niet transitief. Dit wil zeggen, dat dataverkeer tussen spoke en hub mogelijk is, maar standaard niet tussen spokes.
- Workloads die onderling niet met elkaar hoeven te communiceren, maar waarvoor wel toegang tot gedeelde services noodzakelijk is.
- Organisaties die centrale controle over beveiligingsaspecten willen afdwingen, zoals een firewall in de hub-omgeving als DMZ-functie of een gescheiden beheer voor de workloads iedere spoke.

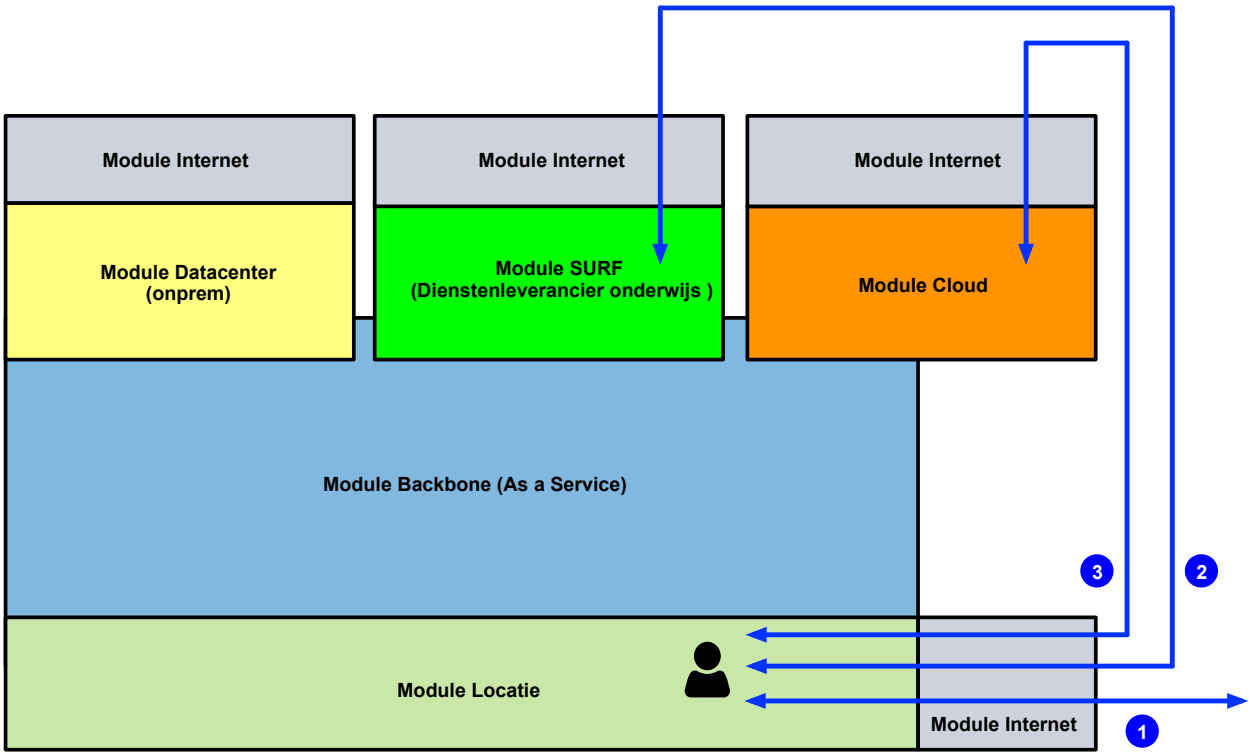
Ontwerpregel 24	**Ontwerpregels Azure/Topologie infrastructuur**
Ontwerpregel 24.1	De topologie van de infrastructuur binnen Azure is gebaseerd op een hub-and-spoke-topologie.
Ontwerpregel 24.2	Shared resources worden centraal ondergebracht in het hub vnet, waarvan de workloads in verschillende spokes gebruik kunnen maken.
Ontwerpregel 24.3	Ieder vnet is opgedeeld in één of meerdere subnets conform het IP Plan van het ROC.
Ontwerpregel 24.4	Communicatie tussen spokes dient te verlopen via het centrale hub vnet.
Ontwerpregel 24.5	Communicatie tussen spokes en het internet dat Azure levert verloopt via de centrale hub.
Ontwerpregel 24.6	De hub met centrale faciliteiten/resources is ondergebracht binnen één ‘generieke’ subscription. De faciliteiten/resources die zijn ondergebracht in de spokes behoren tot andere subscriptions.
Ontwerpregel 24.7	Indien de limieten van de (subscription) van de hub zijn bereikt, dient een nieuwe hub (subscription) te worden aangemaakt met (waar nodig) peering tussen de hubs voor communicatiedoeleinden.
Ontwerpregel 24.8	Binnen iedere subscription dienen resource groups te zijn aangemaakt, waarbinnen de ROC-diensten zijn opgenomen. De te gebruiken classificatie en

	criteria voor opname van ROC-diensten in resource groups dient met stakeholders en diensteigenaren te worden afgestemd. Hierbij dient op z'n minst rekening te worden gehouden met zaken als gezamenlijke LCM van onderdelen, gezamenlijke billing van onderdelen, gezamenlijkheid van functies van onderdelen.

3.8 Use cases/communicatiestromen

3.8.1 Benaderen internet & cloud/SURF-diensten via internet vanaf de module Locatie

Use case 1: Internet browsen en het benaderen van clouddiensten/SURF via internet vanaf de module Locatie



Nr. 1: Internetbrowsen

Gebruikers benaderen het internet middels een local internet breakout op het niveau van de module Backbone. Dit om backhauling van internetverkeer naar de centrale onprem datacenters te voorkomen.

Nr. 2: Diensten SURF aangeboden via internet

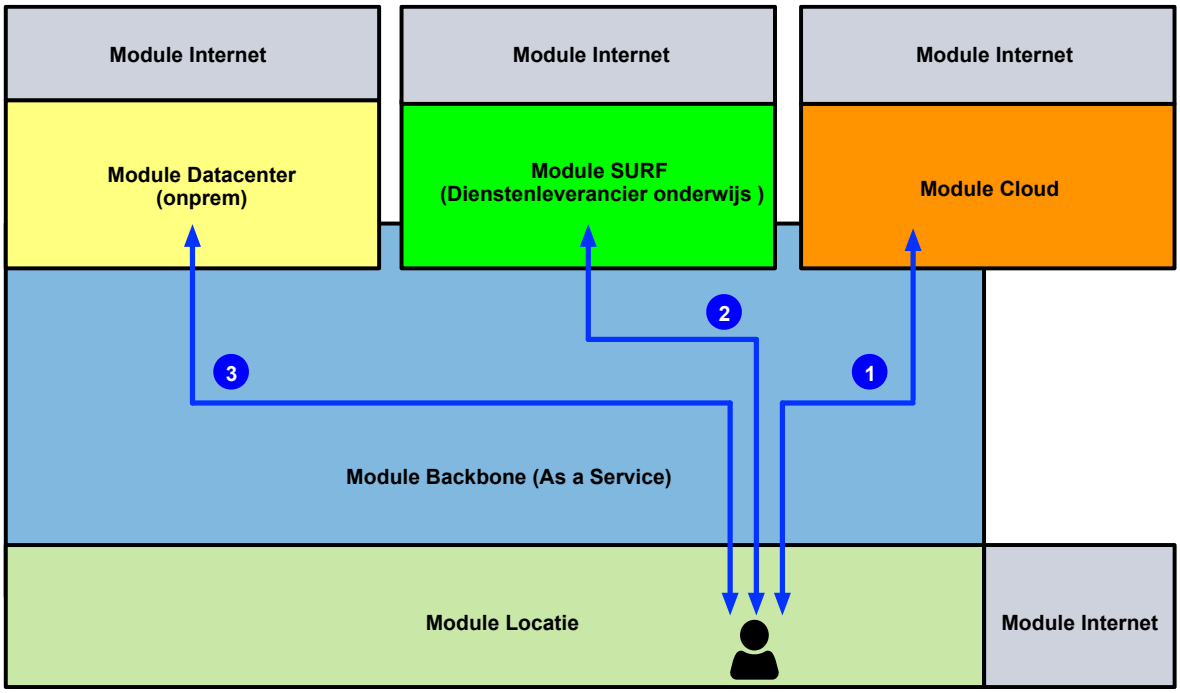
Gebruikers benaderen diensten van SURF middels een local internet breakout op het niveau van de module Backbone. Dit om backhauling van SURF naar de centrale onprem datacenters te voorkomen.

Nr. 3: SaaS-diensten aangeboden via internet

Gebruikers benaderen SaaS-diensten middels een local internet breakout op het niveau van de module Backbone. Dit om backhauling van SaaS-verkeer naar de centrale onprem datacenters te voorkomen.

3.8.2 Benaderen onprem-diensten, cloud/SURF-diensten direct via de module Backbone

Use case 2: Benaderen onprem-diensten, cloud/SURF-diensten via de module Backbone



Nr. 1: Module Cloud

Gebruikers benaderen diensten in het clouddatacenter middels de module backbone. Het clouddatacenter is hierbij direct op de module Backbone aangesloten. SaaS/PaaS-diensten kunnen hierbij ook direct op de module Backbone aangesloten.

Nr. 2: Diensten SURF

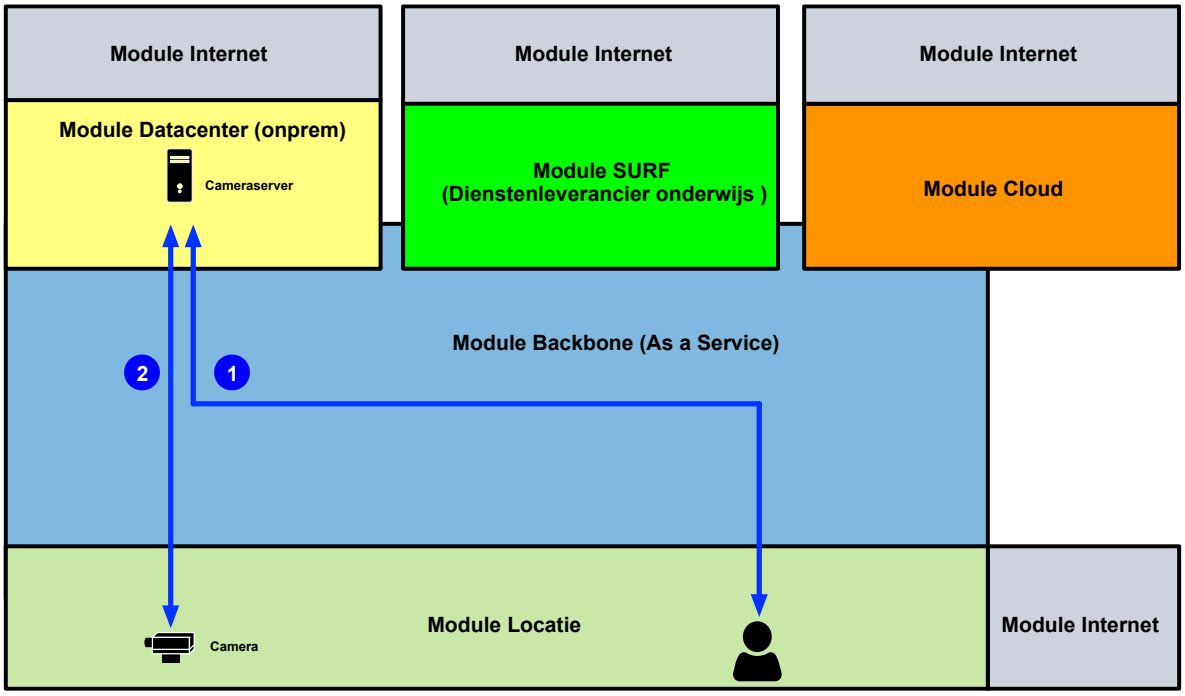
Gebruikers benaderen SURF-diensten direct via de module Backbone. Hierbij is SURF direct op de module Backbone aangesloten.

Nr. 3: Diensten onprem-DC

Gebruikers benaderen diensten in het onprem-DC direct via de module Backbone. De module Datacenter (onprem) is direct op de module Backbone aangesloten.

3.8.3 Opvragen/inzien camerabeelden

Use case 3: Opvragen/inzien camerabeelden



Nr. 1: Camerabeelden

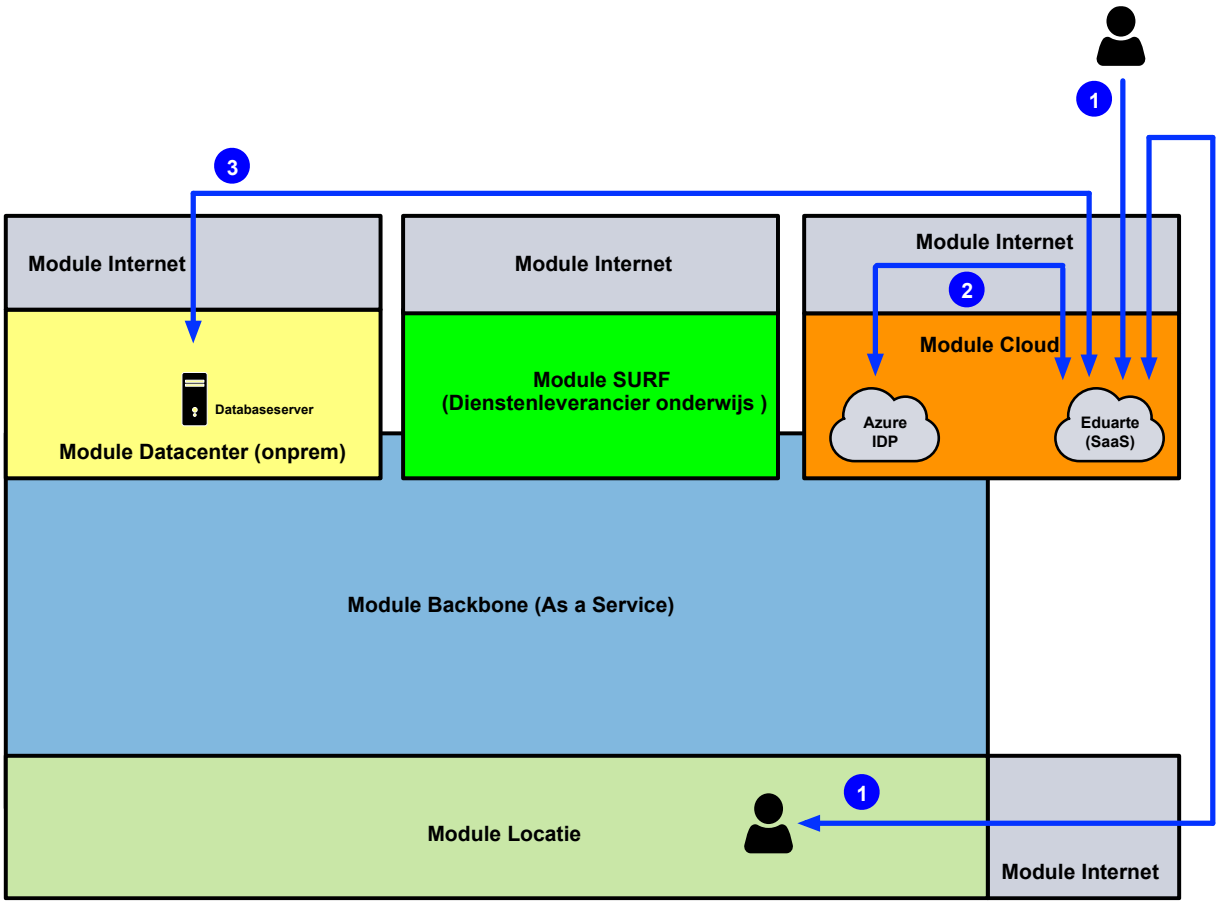
- Een facilitair beheerder bekijkt de live camerabeelden c.q. vraagt oude camerabeelden op vanaf de cameraserver. Dit kan ook de beveiligings-coördinator zijn van de vestiging. Er is geen directe toegang tot de camera's nodig. De gebruikte software heeft alleen toegang tot de cameraserver.
- Een student zit op een centrale locatie en houdt onder toezicht alle camera's van het ROC in de gaten.
- Camera's worden gebruikt in lessituatie, waarbij beelden voor lesdoeleinden gebruikt worden. Hierbij is slechts een klein aantal van de camera's beschikbaar.

Nr. 2: Machine-to-machine-communicatie

Communicatie tussen de camera's en de cameraserver wordt door de module Backbone afgehandeld.

3.8.4 Gebruik Eduarte

Use case 4: Gebruik Eduarte



Nr. 1: Benaderen Eduarte

- Gebruikers binnen de module Locatie benaderen Eduarte middels de local internet breakout die door de module Backbone wordt gefaciliteerd.
- Gebruikers buiten de module Locatie banderen Eduarte middels de 'eigen' internetverbinding.

Nr. 2: Authenticatieverkeer

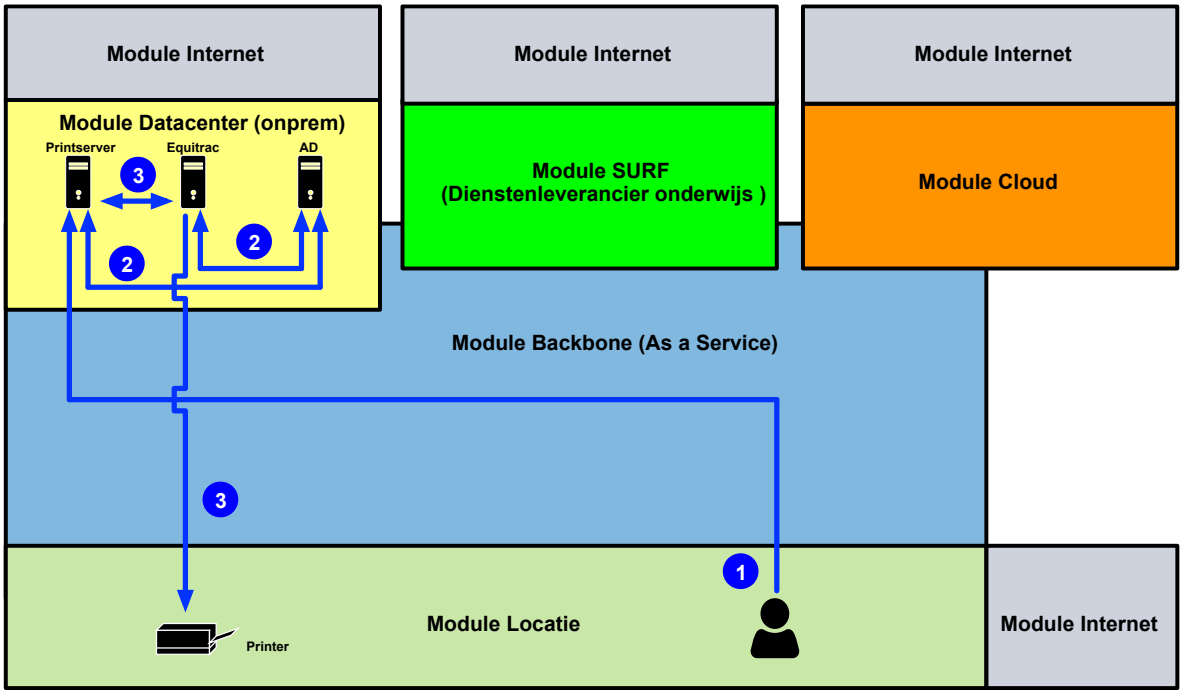
Alvorens toegang te krijgen tot Eduarte dienen authenticaties te worden afgehandeld via de IDP van Azure. Hierbij wordt voor communicatiedoeleinden gebruikgemaakt van de module Internet.

Nr. 3: Replicatieverkeer

Replicatieverkeer in het kader van Eduarte wordt gefaciliteerd door de module Internet, waardoor communicatie mogelijk is tussen Eduarte en de database-server in het onprem datacenter.

3.8.5 Printen

Use case 5: Printen



Nr. 1: Aanvraag printopdracht

Gebruikers in de module Locatie geven een printopdracht waarbij de verkeersstroom door de module Backbone wordt afgehandeld.

Nr. 2: Authenticatieverkeer

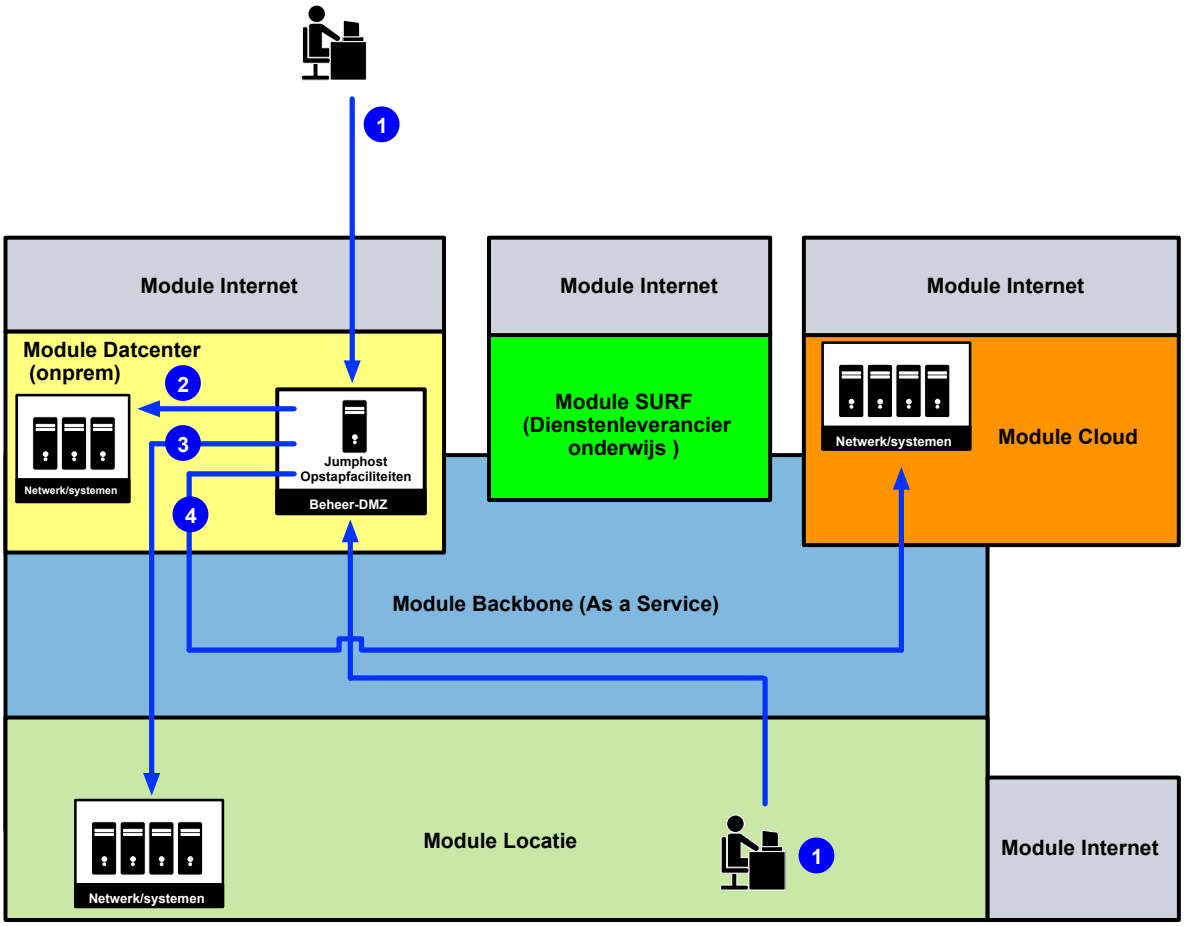
- Authenticatie van de printopdracht dient te worden doorgevoerd op het niveau van de AD in het onprem-DC.
- Authenticatie van de Equitrac-server zelf dient op het niveau van de AD in het onprem-DC te worden doorgevoerd.

Nr. 3 Uitvoering printopdracht

Na authenticaties dient de verkeerstroom m.b.t. de printopdracht door de module Backbone te worden afgehandeld.

3.8.6 Beheer/management (generiek)

Use case 6-1: Beheer/management – Beheerfaciliteiten module Datacenter (onprem scenario)



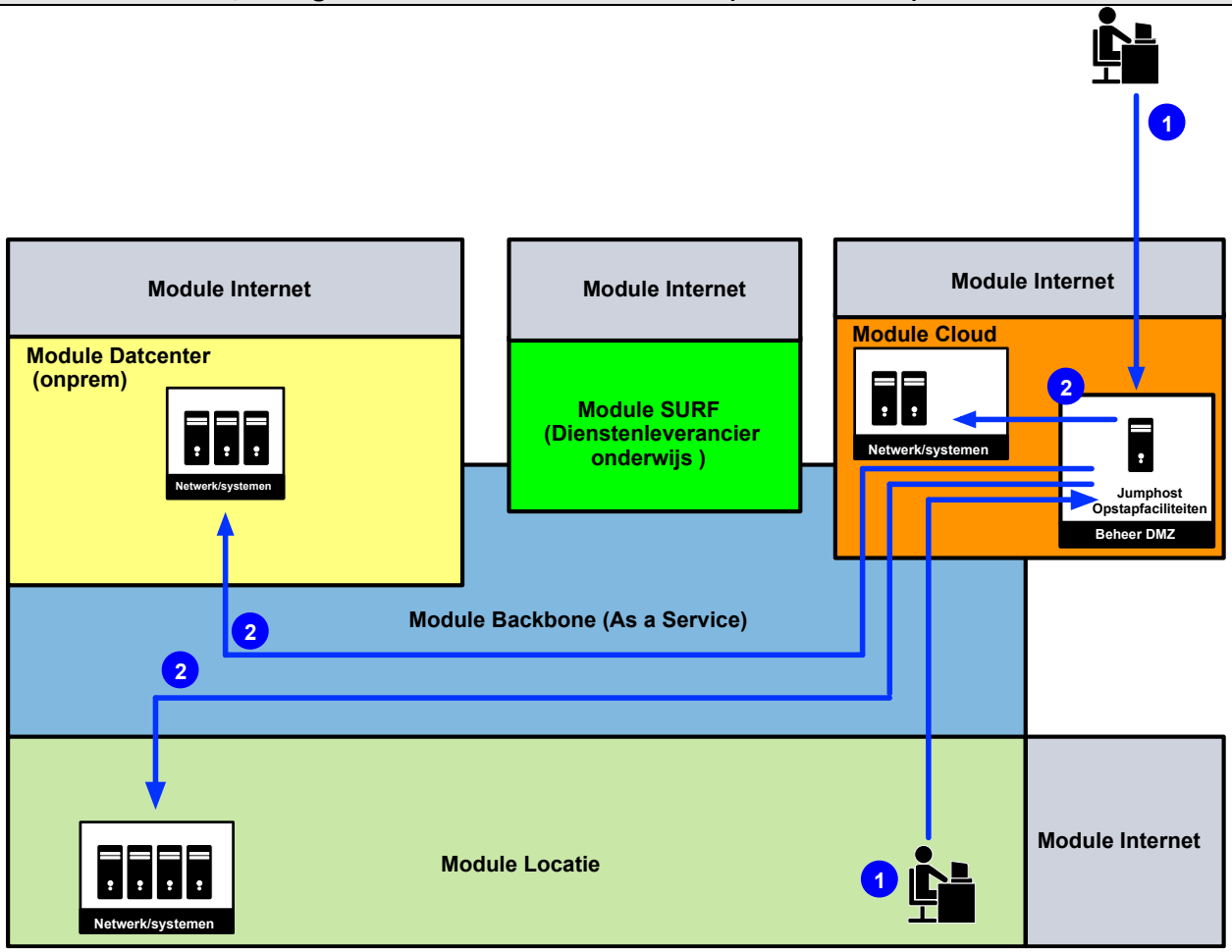
Nr. 1: Benadering managementsystemen

Beheerders benaderen opstapfaciliteiten/jumphost die zich in het functionele domein Beheer DMZ-bevinden binnen het Datacenter (onprem). Beheerders kunnen zich zowel buiten het ROC (via het internet) als binnen het ROC (module Locatie) bevinden. Hierbij dient gebruikgemaakt te worden van 2FA.

Nr. 2: Beheren van netwerksystemen

Vanuit de Beheer-DMZ worden middels de aangewezen tooling/beheerapplicaties/portals de betreffende netwerksystemen benaderd. Alvorens te kunnen inloggen op deze systemen wordt middels het TACACS-protocol geverifieerd of een beheerder rechten heeft om het device te beheren en zo ja, welk autorisatie-niveau daarbij hoort. Na vaststelling van de identiteit en het autorisatieniveau kunnen de betreffende nodes worden beheerd. Let op: Binnen Azure betreft dit nodes van vendoren die appliances bieden via de marktplaats. Cloud native nodes worden in de regel middels de azure-portal beheerd.

Use case 6-2: Beheer/management – Beheerfaciliteiten Cloud (Azure scenario)



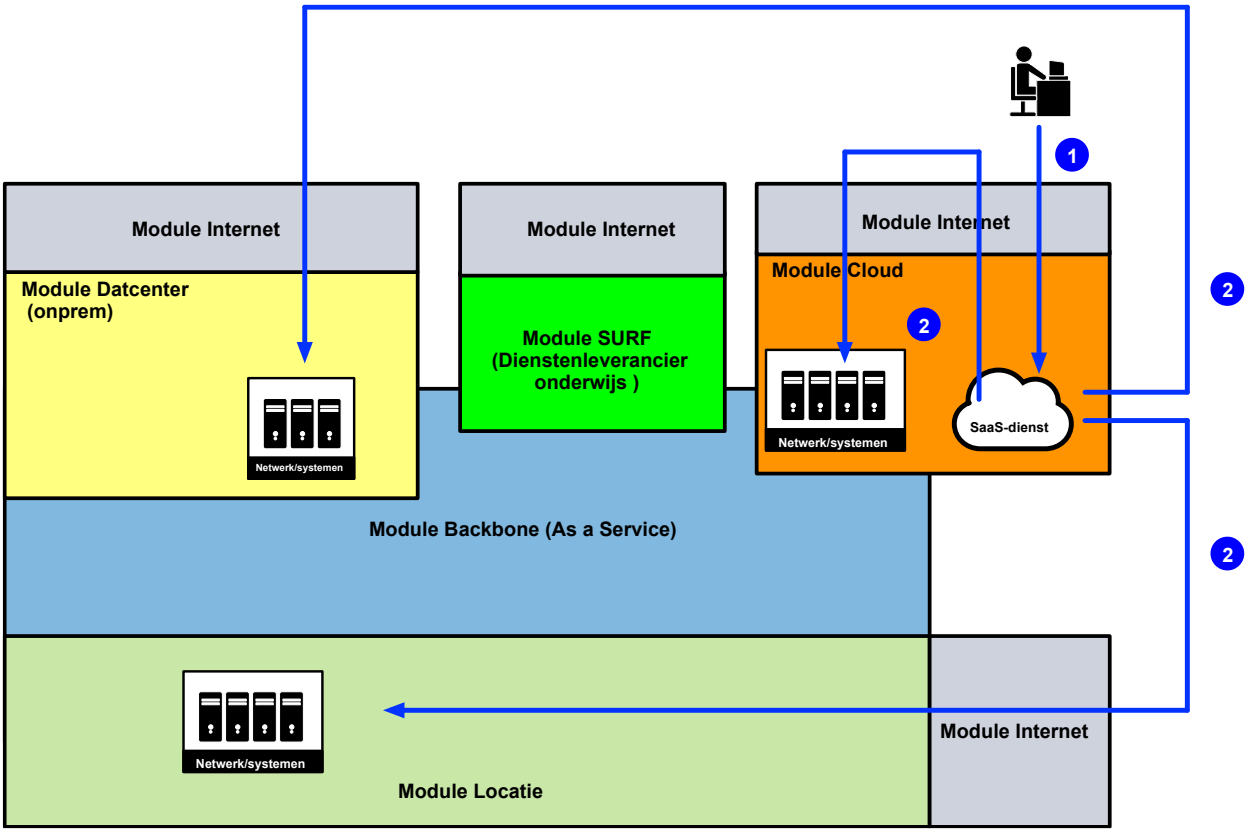
Nr. 1: Benadering managementsystemen

Beheerders benaderen opstapfaciliteiten/jumphost die zich in het functionele domein Beheer DMZ-bevinden binnen Azure. Beheerders kunnen zich zowel buiten het ROC (via het internet) als binnen het ROC (module Locatie) bevinden. Hierbij dient gebruikgemaakt te worden van 2FA.

Nr. 2: Beheren van netwerksystemen

Vanuit de Beheer-DMZ worden middels de aangewezen tooling/beheerapplicaties/portals de betreffende netwerksystemen benaderd. Alvorens te kunnen inloggen op deze systemen wordt middels het TACACS-protocol geverifieerd of een beheerder rechten heeft om het device te beheren en zo ja, welk autorisatie-niveau daarbij hoort. Na vaststelling van de identiteit en het autorisatieniveau kunnen de betreffende nodes worden beheerd. Let op: Binnen Azure betreft dit nodes van vendoren die appliances bieden via de marktplaats. Cloud native nodes worden in de regel middels de azure-portal beheerd.

Use case 6-3: Beheer/management – Beheerfaciliteiten SaaS-dienst



Nr. 1: Benadering managementsystemen (SaaS-dienst)

Beheerders benaderen de SaaS-dienst van waaruit het beheer wordt uitgevoerd. Middels authenticatie (2FA) en autorisatie krijgt de beheer toegangsrechten tot de SaaS-dienst. Let op: Indien een SaaS-dienst in Azure is ondergebracht (e.g. zelf ontwikkeld), behoort deze Azure-dienst ook tot deze use case.

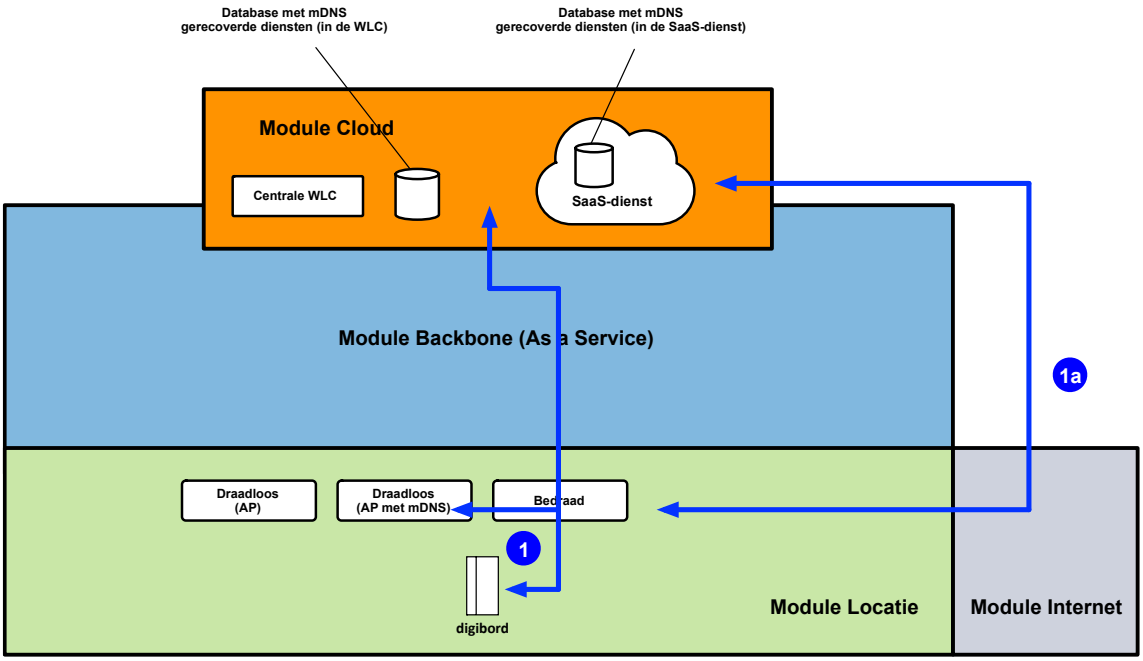
Nr. 2: Beheren van netwerksystemen

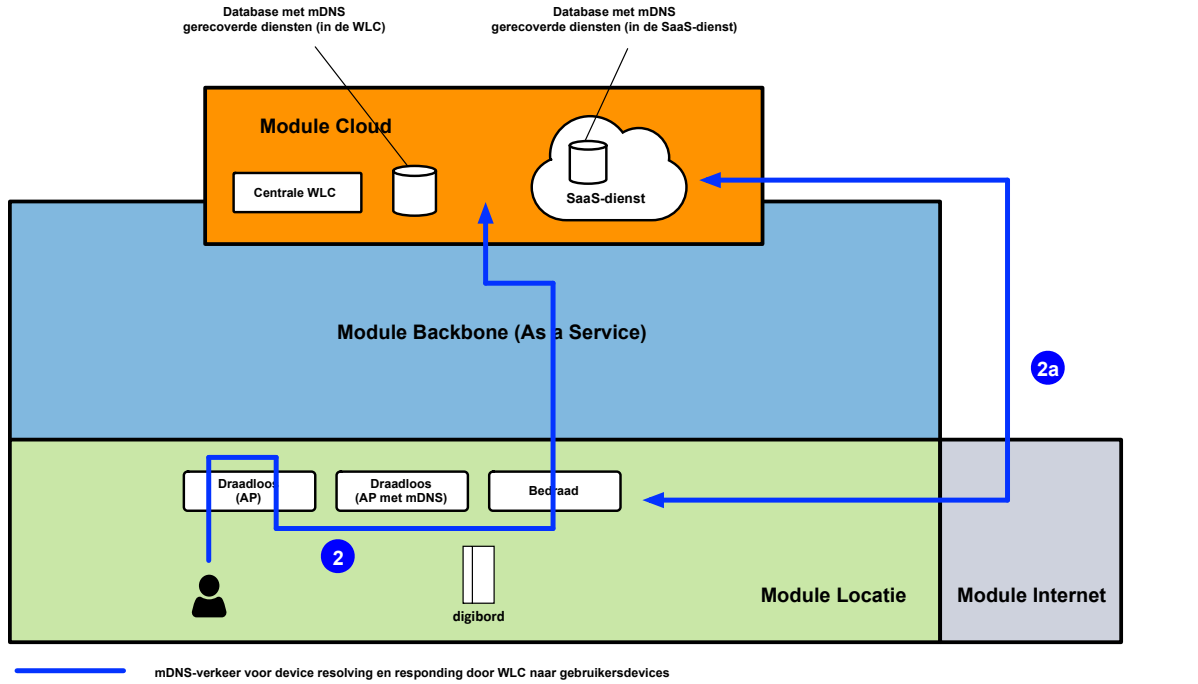
Vanuit de SaaS-dienst worden de systemen benaderd. Aangezien het een SaaS-oplossing betreft, verlopen alle communicatiestromen voor beheer via het internet.

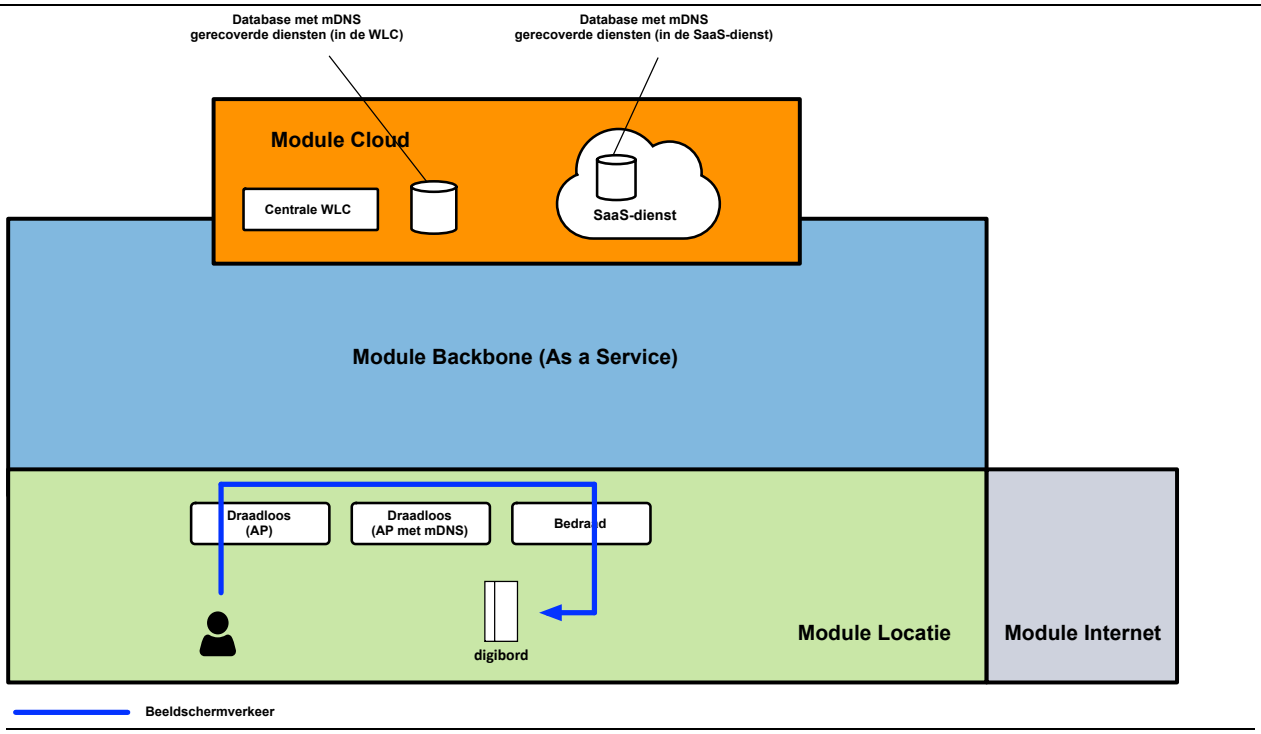
3.8.7 Smartbord

Use case 7: Digibord

In de onderstaande drie figuren is de use case voor Digibord afgebeeld.







Nr. 1: Verzamelen appleplay, chromecast en miracast diensten

Let op: Het ROC staat een 'cloud, tenzij' strategie voor. Dit houdt tevens in, dat de centrale wirelessdienst-verlening vanuit de cloud wordt afgenomen. Dit kan vanuit Azure zijn, maar het kan ook een SaaS-dienst zijn (i.e. communicatiestroom 1a). Communicatiestromen (mDNS resolving & collecting) verlopen naar de clouddienst, tenzij dit door het type dienst/product niet mogelijk is c.q. niet de beste oplossing in de praktijk blijkt te zijn.

Nr. 2: Aanvraag en aanbieden van de appleplay, chromecast en miracast diensten op de wireless netwerken

mDNS-verkeer voor device resolving en responding wordt verstuurd door de WLC naar gebruikersdevices. Indien de WLC als SaaS-dienst wordt afgenomen, verloopt de communicatiestroom via het internet (2a).

Nr 3. Beeldschermverkeer tussen gebruiker en digibord.

Bij voorkeur wordt het beeldschermverkeer lokaal afgehandeld door een local breakout feature, opdat het beeldschermverkeer niet eerst naar de centrale wireless dienstverlening hoeft te worden getransporteerd, waarna het weer wordt teruggestuurd.

3.8.8 IoT-generiek

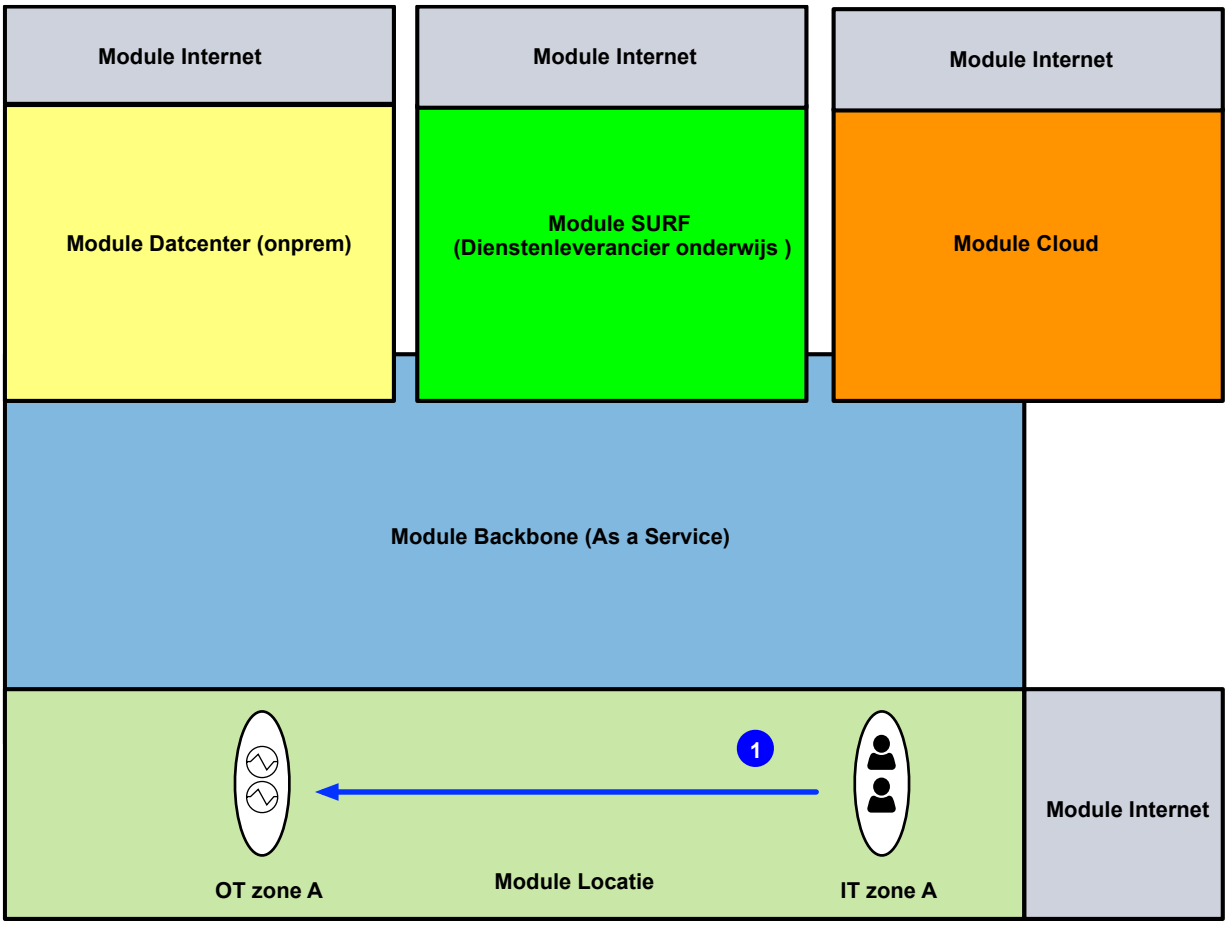
Op deze plaats wordt communicatie in relatie tot IoT apart en generiek behandeld. De IoT-diensten die binnen het ROC gebruikt worden en (mogelijk) zullen worden, zijn hieronder opgesomd.

Domein	Omschrijving
Educatief	• Lasrobots, • Kantbanken, • CNC-banken, • 3d printer, • CNC-snijmachines.
Facilitair/administratief	• Printers, • Labelprinters privasystemen, • Alarmsystemen, • Kluisjes met gebruikers auth, • Kassa's, • Pinautomaten, • Snoepautomaten en andere cateringautomaten. • IP-camera's voor facilitair/beveiliging, • Zonnepanelen, • Windmolen, • Narrowcasting, • Franceermachines, • IP-telefoons.
Educatief ICT	• Camera's voor educatieve doeleinden (beveiligingsopleiding) • Printers, • Apple TV, • Feedtruck app devices. • Kweekkassen, • Nikoservers. • Educatieve homedomotica, • Scheepsimulatoren, • Marifoonsimulatoren, Machinekamersimulatoren '(URK), Educatieve ICT-devices als WiFi-routertjes, switches et cetera (deze hebben vaak tijdelijk wel internet nodig, maar dienen niet als alternatieve internettoegang voor de ICT-studenten).
Toekomst	• Camera's op de digiborden voor het lesgeven via streaming faciliteiten, • Internetradio's,

- Google home et cetera,
- Weerstations.

Voor de begrippen zonering binnen de use cases wordt verwezen naar de technische architectuur-blauwdruk security.

Use case 7-1: IoT-generiek/benaderen IoT device vanuit KA (IT)

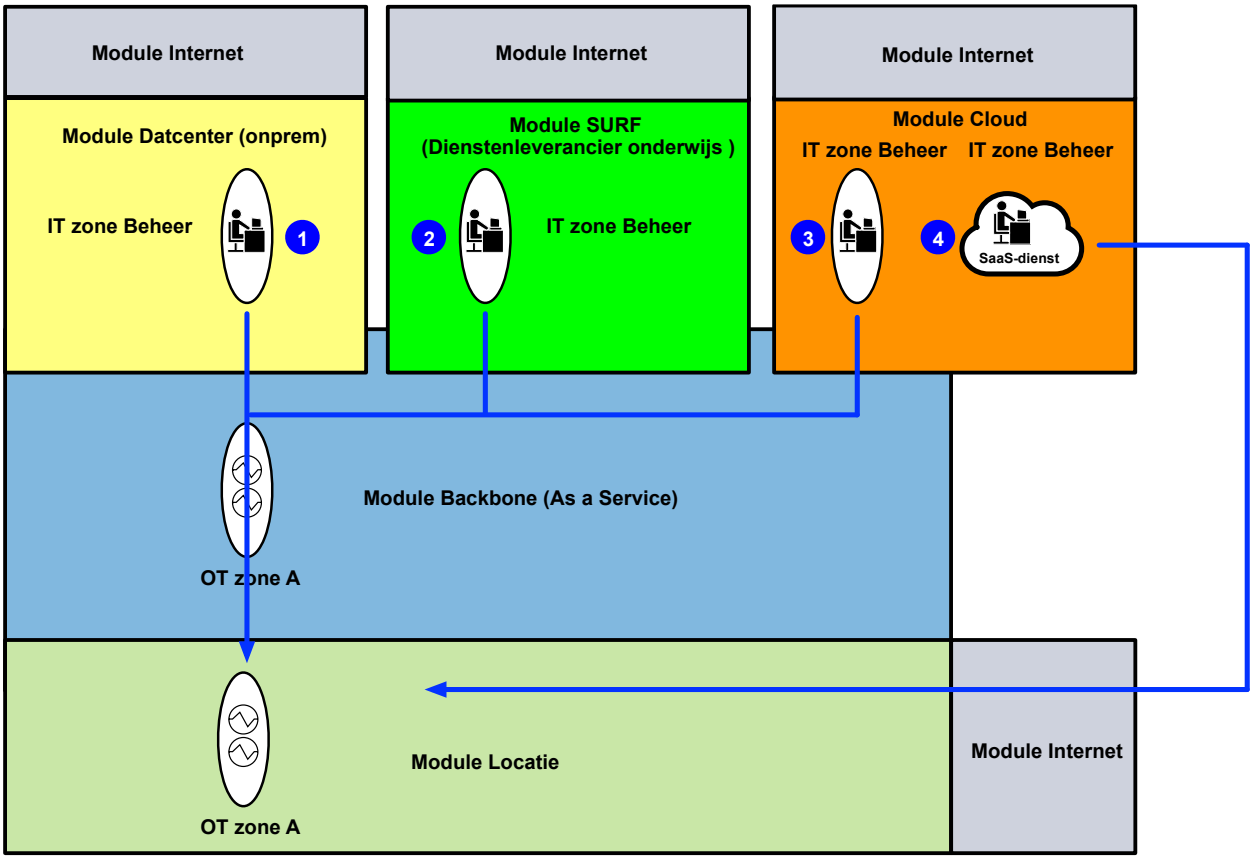


IoT-device

Nr. 1: Benaderen IoT device vanuit KA (IT)

Gebruikers in de module Locatie benaderen vanuit de toegewezen IT-zone de betreffende OT-zone, waarin het specifieke IoT-object is ondergebracht.

Use case 7-2: IoT-generiek/beheer



Nr. 1: Beheer IoT device vanuit module Datacenter (onprem)

IoT-objecten in de OT-zones in de module Locatie worden eveneens vanuit de Beheer DMZ gemanaged.

Nr. 2: Beheer IoT device vanuit module SURF

Het is mogelijk dat SURF een IoT-dienst aanbiedt die vanuit de module SURF wordt aangeboden. Bij voorkeur wordt de beheercommunicatie (die uit een portalfunctionaliteit kan bestaan) gefaciliteerd door de module Backbone zoals afgebeeld in de illustratie, waarbij inter-zoneringsverkeer plaatsvindt. Dit vanwege de mogelijkheid Quality of Service toe te passen op het niveau van de module Backbone en een goed inzicht te hebben van de beheerverkeersstroom. Indien directe communicatie via de module Backbone niet mogelijk blijkt te zijn vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

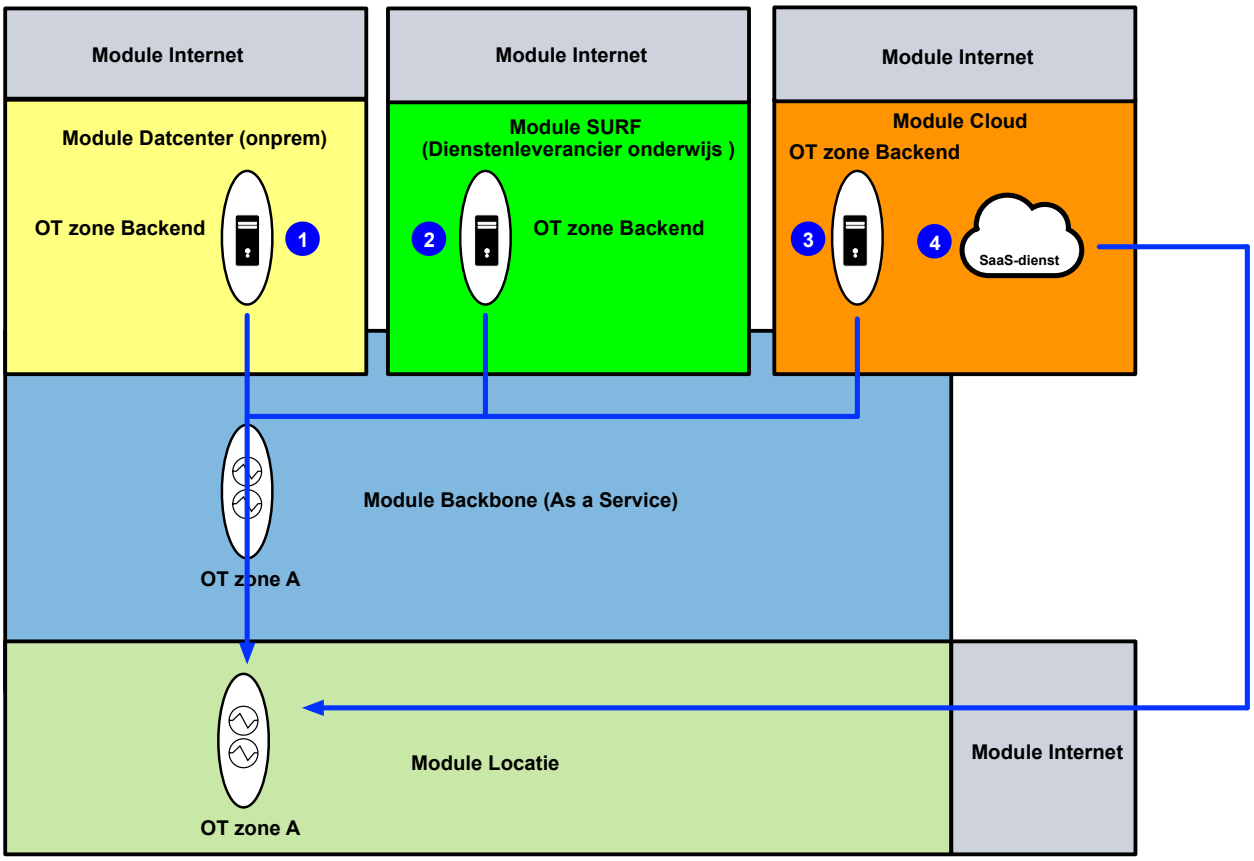
Nr. 3: Beheer IoT device vanuit module Cloud (Azure)

IoT-objecten in de OT-zones in de module Locatie worden eveneens vanuit de Beheer DMZ gemanaged. Bij voorkeur wordt de communicatiestroom gefaciliteerd door de module Backbone in verband met het kunnen toepassen van Quality of Service en vanwege een goed inzicht in de beheer verkeersstroom. Indien

directe communicatie via de module Backbone niet mogelijk blijkt te zijn vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 4: Beheer IoT device vanuit SaaS-dienst
IoT-objecten in de OT-zones in de module Locatie worden via het internet beheerd. De SaaS-dienst-ontsluiting vindt immers via het internet plaats.

Use case 7-3: IoT-generiek/data-overdracht



Nr. 1: Data-overdracht naar module Datacenter (onprem)
IoT-objecten kunnen substantieel veel data verzenden voor bijvoorbeeld data-analyses. Hoewel op grond van het principe 'cloud, tenzij' het niet in de lijn der verwachting ligt, dat in de (nabije) toekomst heel veel van dergelijke data naar het onprem datacenter zal worden verstuurd, dient hier wel rekening mee te worden gehouden.

Nr. 2: Data-overdracht naar module SURF
Op grond van het 'cloud, tenzij' principe zal meer en meer IoT-data verstuurd (gaan) worden naar 'de cloud'. SURF kan in dit kader als dienstenleverancier optreden voor IoT-diensten. De communicatiestroom

vanaf IoT-objecten wordt bij voorkeur gefaciliteerd door de module Backbone in verband met inzicht in verkeersstromen en het toepassen van Quality of Service. Indien verkeer niet via de module Backbone kan worden getransporteerd vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 3: Data-overdracht naar module Cloud (Azure

Op grond van het 'cloud, tenzij' principe zal meer en meer IoT-data verstuurd (gaan) worden naar 'de cloud'. Het clouddatacenter van Azure kan in dit kader worden gebruikt voor dergelijke IoT-diensten. De communicatiestroom vanaf IoT-objecten wordt bij voorkeur gefaciliteerd door de module Backbone in verband met inzicht in verkeersstromen en het toepassen van Quality of Service. Indien verkeer niet via de module Backbone kan worden getransporteerd vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 4: Data-overdracht m.b.t. SaaS-dienst

Via het internet wordt data-overdracht gefaciliteerd naar de SaaS-dienst.

4 Bijlage A: Ontwerpregels Technische Architectuur - architectuurgebied netwerk

4.1 Module Backbone

Ontwerpregel 1	Communicatie modules
1.1	Communicatie tussen: • locaties onderling, • datacenters (onprem) onderling, • locaties en het onprem datacenter, • locaties en het publieke clouddatacenter (onderdeel module Cloud), • locaties en de onderwijsdienstenleverancier SURF, • locaties en PaaS/SaaS-diensten (onderdeel module Cloud) die direct op de Backbone gekoppeld kunnen worden, dient te verlopen via de module Backbone.
1.2	Het is toegestaan de modules Datacenter (onprem) direct aan elkaar te verbinden zonder tussenkomst van de module Backbone. In dit laatste scenario is sprake van een DCI (Datacenter Interconnect).
1.3	De module Backbone dient als fallbackscenario te kunnen worden gebruikt, zodra de DCI-interconnect niet meer functioneert.
1.4	Communicatie tussen publieke clouddatacenters die deel uitmaken van de module Cloud verloopt via de Backbone van de provider van het publieke clouddatacenter).
1.5	Voor zover mogelijk en opportuun dient dataoverdracht tussen modules direct middels de module Backbone te verlopen, waarmee *hairpinning* in het onprem datacenter wordt voorkomen. Dit op grond van trends in het onderwijs, waarbij steeds vaker gebruikgemaakt zal worden van diensten die niet meer geleverd worden vanuit het onprem datacenter.

Ontwerpregel 2	Backbone As A Service
2.1	De Backbone dient als een Service te kunnen worden afgenomen bij een Backbone-provider die connectiviteitsafspraken heeft met leveranciers van clouddatacenters en andere clouddiensten-leveranciers.
2.2	De aansturing, monitoring, provisioning van de Backbone As A Service dient bij voorkeur te worden gereguleerd middels een SaaS-dienst, waarbij het ROC via een portal inzicht heeft in minimaal: • De status van diensten,

	• De status van de overall Backbone, • Trends in de Backbone, waarmee voorspelbaarheid en daardoor beheerbaarheid van de omgeving optimaal kan worden nagestreefd (e.g. O.b.v. ML/AI voorspellende karakteristieken voor bijvoorbeeld capaciteitsmanagement). Hierbij dient het mogelijk te zijn: • Business rules (intelligence) op te nemen via de portal voor alle diensten, waarmee de Backbone op een intelligente en automatische manier invulling kan geven aan de technische vereisten voor de diensten (e.g. thresholds voor metrics als delay, jitter waarbij andere netwerkpaden gebruikt kunnen worden indien thresholds worden overschreden. E.g. gebruik maken van de meest kostenefficiënte onderliggende fysieke dragers, waarbij in geval van overschrijding van bepaalde thresholds (simultaan) een duurdere backup-verbinding kan worden benut). • De Portal locatie-onafhankelijk te kunnen benaderen. • De Backbone te laten doorwerken, indien de onderliggende NMS-systemen (tijdelijk) geen verbinding meer hebben met de module Backbone.
2.3	De backbone dient in een beschikbaarheid te voorzien van 99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
2.4	De geboden service dient de access-nodes of aggregatie-nodes op locaties te ontsluiten conform de ontwerpregels zoals opgesteld in paragraaf 3.3. Hierbij dient het mogelijk te zijn de service te laten ‘meegroeien’ of ‘inkrimpen’ met het type en/of subtype locatie.
2.5	De geboden service dient de aggregatie-nodes in onprem datacenters te ontsluiten conform de ontwerpregels zoals opgesteld in paragraaf 4.3.
2.6	De service dient te voorzien in koppelingen met clouddatacenters en andere clouddiensten die direct op de backbone kunnen worden aangesloten.
2.7	Het ROC dient controle te kunnen uitoefenen op het backbone-netwerk. Toegang is nodig voor: • Het toepassen van security-policies op basis van het vigerende informatiebeveiligingsbeleid van het ROC, • Inzage in de verkeersstromen (Application Visibility & Control) opdat tijdig kan worden bijgestuurd conform de policies van het ROC (e.g. QoS-toepassing/wijziging, bandbreedtewijzigingen et cetera).

Ontwerpregel 3	**Technologie**
De Backbone dient te kunnen worden vormgegeven middels verschillende technologische dragers, waarbij verandering van leverancier en technologie geen of nauwelijks impact mag hebben op het overlay-netwerk van het ROC. Dit overlay-netwerk wordt gevorm door actieve Backbone-nodes die integraal deel uitmaken van de Backbone As A Service.	

Ontwerpregel 4	Functies
4.1	De Backbone dient te voorzien in data-overdracht waarbij het mogelijk is op grond van specifieke business rules/intelligence de Backbone automatisch aan te passen aan de eisen van de applicatie. Indien bijvoorbeeld een normaliter geprefereerd overlay-pad niet optimaal functioneert, dient een ander overlay-pad automatisch te kunnen worden geactiveerd c.q. opgeschaald.
4.2	De Backbone dient te voorzien in foutendetectie en automatisch herstel.
4.3	De Backbone dient te voorzien in Quality of Service.
4.4	De Backbone dient te voorzien in IPv4- en IPv6-functies.
4.5	Redundante uplink/downlinkverbindingen dienen middels linkbundelings-technologie te kunnen worden vormgegeven.
4.6	De Backbone dient automatisch de door de applicatie/dienst gevraagde netwerktopologie te ondersteunen, zijnde: • Any-to-any topologie, • Hub-and-spoke topologie, • Full-mesh topologie, • Point-to-point topologie.
4.7	De Backbone dient te voorzien in traffic-steering-mogelijkheden, waarbij het onprem datacenter als *hub* zoveel als mogelijk wordt ontlast van verkeer dat niet bestemd is voor services die vanuit dit type datacenter worden aangeboden.
4.8	Backbone-nodes dienen te kunnen worden geclusterd, waarbij de beide nodes simultaan verkeer kunnen verwerken afhankelijk van de business rules/intelligentie die worden toegekend aan de betreffende diensten/ applicaties.
4.9	De Backbone dient flexibel te zijn. Met flexibiliteit wordt bedoeld: • Eenvoudig en snel opschaalbaar, • Eenvoudig en snel afschaalbaar, • Eenvoudig en snel leverbaar op locaties waar bijvoorbeeld vaste/bedrade verbindingen niet/nauwelijks en/of niet snel genoeg kunnen worden geleverd. • De implementatie van nieuwe diensten dient snel en zonder tussenkomst van de leverancier te kunnen worden uitgevoerd (snelle *time-to-market*).

4.2 Module Locatie

4.2.1 Traditioneel

Locatietype flexibel:

Ontwerpregel 5	**Traditioneel model: Eigenschappen locatie-type: Flexibel**	
Ontwerpregel 5.1	Aantal personen & systemen	Max. 100
Ontwerpregel 5.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 5.3	Medium tussen nodes accesslaag en nodes module Backbone	Glas, minimaal 1 Gbit/s met opschaalmogelijkheden tot 10 Gbit/s (en vice versa)
Ontwerpregel 5.4	Clustering/stacking	Nodes die deel uitmaken van de accesslaag dienen te kunnen worden geclusterd/gestacked, waarbij iedere node simultaan verkeer kan afhandelen.
Ontwerpregel 5.5	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 1 Gbit/s met opschaal-mogelijkheden tot 10 Gbit/s (haalbaarheid moet worden vastgesteld i.o.m. marktpartij).
Ontwerpregel 5.6	Beschikbaarheid	99,99% -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 5.7	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 5.8	SLA access-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 5.9	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal.
Ontwerpregel 5.10	Toekomstige groei	Bij toekomstige groei dient het type locatie te kunnen doorgroeien naar het locatietype vast. Per geval / situatie dienen hiertoe de mogelijkheden te worden bekeken.

Locatietype vast:

Ontwerpregel 6	Traditioneel model: Eigenschappen locatie-type: Vast	
Ontwerpregel 6.1	Aantal personen & systemen	> 100
Ontwerpregel 6.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 6.3	Medium tussen nodes accesslaag en nodes aggregatielaag	Glas, minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 6.4	Medium tussen nodes aggregatielaag en nodes module Backbone	Glas, minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 6.5	Clustering/stacking	Nodes die deel uitmaken van de accesslaag en aggregatielaag dienen te kunnen worden geclusterd/gestacked, waarbij iedere node simultaan verkeer kan afhandelen.
Ontwerpregel 6.6	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 10 Gbit/s met opschaal-mogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s.
Ontwerpregel 6.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.8	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.9	SLA aggregatie-node	MTTR 8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.10	SLA access-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 6.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal.

Ontwerpregel 6.12	Toekomstige groei/krimp	Bij toekomstige groei dient het type locatie deze groei flexibel te kunnen accommoderen zonder wijzigingen te hoeven aanbrengen in de LAN-topologie. Bij toekomstige krimp dient het type locatie te kunnen afschalen naar het locatietype flexibel.

Generieke kenmerken access-nodes en aggregatie-nodes:

Ontwerpregel 7	**Tradtioneel model: Generieke kenmerken access-nodes en aggregatie-nodes**
Ontwerpregel 7.1	Access-nodes zijn redundant aangesloten op meerdere aggregatienodes, waarbij simultaan gebruikgemaakt kan worden van alle beschikbare paden tussen de beide lagen.
Ontwerpregel 7.2	De access-poorten van een access-node zijn van het type koper 10/100/1000 Mbit/s.
Ontwerpregel 7.3	Access-nodes dienen te voorzien in Power-over-Ethernet-mogelijkheden om Access Points en IP-telefoons van stroom te kunnen voorzien. Hierbij dient per locatie/gebruikssituatie bekeken te worden welk type POE (type 15W, 30W, 60W)
Ontwerpregel 7.4	Access-nodes dienen het gebruik van Wake-on-LAN te ondersteunen.
Ontwerpregel 7.5	Aggregatie-nodes dienen het LAN richting de module Backbone te kunnen ontsluiten op basis van het IP-protocol, waarbij gebruikgemaakt kan worden van open standaarden routeringsprotocollen.
Ontwerpregel 7.6	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 7.7	Nodels dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 7.8	De access-nodes zijn niet voorzien van redundante voedingen, de aggregatienodes wel.
Ontwerpregel 7.9	De nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 7.10	De software-architectuur is bij voorkeur modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien ‘pay as you grow’ kunnen worden ingevuld.
Ontwerpregel 7.11	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de backbone-node, maar in ieder geval binnen de module Locatie.
Ontwerpregel 7.12	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer,

	• gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 7.13	Nodes communiceren met hun omgeving op basis van open standaarden.
Ontwerpregel 7.14	De node(s) van de module Backbone mogen geen deel uitmaken van de aggregatie-laag in verband met: • Het kunnen scheiden van de modules Locatie en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.

4.2.2 SDN

Positie module Backbone binnen het SDN-model:

Ontwerpregel 8	**Positie module Backbone binnen het SDN-model**
Ontwerpregel 8.1	De module Backbone dient separaat en (technologisch) flexibel te zijn in relatie tot het SDN-model op LAN/WLAN-niveau. Dit in verband met de mogelijkheid de module Backbone sourceable te houden door een duidelijk demarcatiepunt tussen de module Backbone en de module Locatie te creëren (dus ook qua technologie indien dit de flexibiliteit en sourceability van de module Backbone ten goede komt).
Ontwerpregel 8.2	Locaties waar SDN-functies worden aangebracht dienen te worden ondergebracht conform het SDN-model type 'multi-site'.
Ontwerpregel 8.3	Communicatie tussen SDN-fabric-sites onderling en communicatie tussen SDN-nodes en de centraal in het datacenter opgestelde SDN-controllers (of SDN-controllers die als SaaS-dienst worden afgenomen) wordt gefaciliteerd door de module Backbone, waarbij het flexibele IP-protocol gebruikt moet kunnen worden.

Locatietype flexibel:

Ontwerpregel 9	**SDN-model: Eigenschappen locatie-type: Flexibel**	
Ontwerpregel 9.1	Aantal personen & systemen	Max. 100
Ontwerpregel 9.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 9.3	Medium tussen nodes SDN-edge-laag en nodes SDN-border-laag	Glas, minimaal 1 Gbit/s met opschaalmogelijkheden tot 10 Gbit/s (en vice versa)

Ontwerpregel 9.4	Medium tussen nodes SDN-border-laag en nodes module Backbone	Glas, minimaal 1 Gbit/s met opschaalmogelijkheden tot 10 Gbit/s (en vice versa)
Ontwerpregel 9.5	Clustering/stacking	De nodes die deel uitmaken van de fabric-site dienen als één logische SDN-wolk te kunnen worden aangestuurd.
Ontwerpregel 9.6	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 1 Gbit/s met opschaal-mogelijkheden tot 10 Gbit/s (en vice versa) (haalbaarheid moet worden vastgesteld i.o.m. marktpartij).
Ontwerpregel 9.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.8	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.9	SLA SDN-border-node	8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.10	SLA SDN-edge-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 9.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal. Zodra meer dan één SDN-border-node wordt ondergebracht, dient het principe van de leaf-spine-architectuur te worden toegepast waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes.
Ontwerpregel 9.12	Toekomstige groei	Bij toekomstige groei dient het type locatie te kunnen doorgroeien naar het locatietype vast. Per geval / situatie dienen hiertoe de mogelijkheden te worden bekeken.

Locatietype vast:

Ontwerpregel 10	SDN-model: Eigenschappen locatie-type: Vast	
Ontwerpregel 10.1	Aantal personen & systemen	> 100
Ontwerpregel 10.2	Afname onderwijskritieke ICT-services	Ja
Ontwerpregel 10.3	Medium tussen nodes SDN-edge-laag en nodes SDN-border-laag	Glas, minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 10.4	Medium tussen nodes SDN-border-laag en nodes module Backbone	Glas, minimaal 10 Gbit/s met opschaalmogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s
Ontwerpregel 10.5	Clustering/stacking	De nodes die deel uitmaken van de fabric-site dienen als één logische SDN-wolk te kunnen worden aangestuurd. Border nodes dienen geclusterd te kunnen worden.
Ontwerpregel 10.6	Ontsluiting nodes module Backbone	Verschillende typen media. Minimaal 10 Gbit/s met opschaal-mogelijkheden tot 100 Gbit/s en afschaalmogelijkheden tot 1 Gbit/s.
Ontwerpregel 10.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.8	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.9	SLA SDN-edge-node	NBD -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.10	SLA SDN-border-node	8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 10.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal. Zodra meer dan één SDN-border-node wordt ondergebracht, dient het principe

		van de leaf-spine-architectuur te worden toegepast waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes.
Ontwerpregel 10.12	Toekomstige groei/krimp	Bij toekomstige groei dient het type locatie deze groei flexibel te kunnen accommoderen zonder wijzigingen te hoeven aanbrengen in de SDN-topologie. Bij toekomstige krimp dient het type locatie te kunnen afschalen naar het locatietype flexibel.

Generieke kenmerken SDN-edge-nodes en SDN-border-nodes:

Ontwerpregel 11	**SDN-model: Generieke kenmerken SDN-edge-nodes en SDN-border-nodes**
Ontwerpregel 11.1	De functies van de SDN-edge-lagen en SDN-border-lagen mogen in één SDN-node zijn ondergebracht indien dit technologisch kan worden doorgevoerd. Deze SDN-node dient dan direct verbonden te worden aan de module Backbone. Indien de functies van SDN-edge- en SDN-border-lagen niet in één SDN-node kunnen worden ondergebracht, geldt het volgende: SDN-edge-nodes zijn redundant aangesloten op één SDN-border-node, tenzij de onderhavige SDN-technologie/systematiek een dergelijke ontsluiting niet toestaat. Indien deze redundante ontsluiting technologisch niet kan worden verwezenlijkt, dient te worden teruggevallen op de leaf-spine-architectuur, waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes. Deze SDN-border-nodes dienen als cluster te kunnen worden aangebracht.
Ontwerpregel 11.2	De access-poorten van een SDN-edge-node zijn van het type koper 10/100/1000 Mbit/s.
Ontwerpregel 11.3	Access-nodes dienen te voorzien in Power-over-Ethernet-mogelijkheden om Access Points en IP-telefoons van stroom te kunnen voorzien. Hierbij dient per locatie/gebruikssituatie bekeken te worden welk type POE (type 15W, 30W, 60W)
Ontwerpregel 11.4	SDN-edge-nodes dienen het gebruik van Wake-on-LAN te ondersteunen.
Ontwerpregel 11.5	SDN-border-nodes dienen te zijn voorzien van de control plane functies die noodzakelijk zijn binnen het SDN-ecosysteem.
Ontwerpregel 11.6	SDN-border-nodes dienen de SDN-fabric-site richting de module Backbone te kunnen ontsluiten op basis van het IP-protocol, waarbij gebruikgemaakt kan worden van open standaarden routeringsprotocollen.
Ontwerpregel 11.7	SDN-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.

Ontwerpregel 11.8	SDN-nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 11.9	De SDN-edge-nodes zijn niet voorzien van redundante voedingen. De SDN-border-nodes zijn wel voorzien van redundante voedingen.
Ontwerpregel 11.10	SDN-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 11.11	De software-architectuur is modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien 'pay as you grow' kunnen worden ingevuld.
Ontwerpregel 11.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de backbone-node, maar in ieder geval binnen de module Locatie. Hiervan kan worden afgeweken, indien bijvoorbeeld: • voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een locatie-overschrijdend OSI Laag 2 pad aan te brengen, • de gekozen technologie in de praktijk dermate anders is c.q. andere inzichten met zich meebrengt dat niet aan dit principe voldaan kan worden.
Ontwerpregel 11.13	SDN-nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 11.14	SDN-nodes communiceren bij voorkeur met hun omgeving op basis van open standaarden, tenzij de voor het ROC gekozen SDN-oplossing alleen middels proprietary protocollen kan worden opgebouwd. Hierbij is het van belang, dat communicatie naar de module Backbone middels open standaarden kan worden gefaciliteerd.
Ontwerpregel 11.15	De node(s) van de module Backbone mogen geen deel uitmaken van de laag SDN-border in verband met: • Het kunnen scheiden van de modules Locatie en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.

4.3 Module Datacenter (onprem)

4.3.1 Traditioneel

Ontwerpregel 12	Traditioneel model: Eigenschappen datatacenter onprem	
Ontwerpregel 12.1	Aanwezigheid onderwijskritieke ICT-services	Ja
Ontwerpregel 12.2	Medium tussen nodes lagen Access en collapsed-core	glas, minimaal 10 Gbit/s
Ontwerpregel 12.3	Medium tussen nodes collapsed core en de module Backbone	glas, minimaal 10 Gbit/s
Ontwerpregel 12.4	Ontsluiting nodes module Backbone	glas, minimaal 10 Gbit/s per connectie
Ontwerpregel 12.5	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.6	SLA backbone-ontsluiting	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.7	SLA access-node	MTTR 8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.8	SLA node collapsed core	MTTR 4 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 12.9	Schaalbaarheid	Accesslaag: horizontale en verticale schaalbaarheid Collapsed core: verticale schaalbaarheid
Ontwerpregel 12.10	Toekomstige groei	In principe geen i.v.m. *cloud, tenzij…*principe.

Generieke kenmerken nodes collapsed core en access:

Ontwerpregel 13	Traditioneel model: Generieke kenmerken nodes collapsed-core
Ontwerpregel 13.1	Redundantie van uplink/downlinkverbindingen dienen middels linkbundelingstechnologie te kunnen worden vormgegeven.

Ontwerpregel 13.2	De chassis' van collapsed-core-nodes dienen te kunnen worden gevirtualiseerd, zodat één logische entiteit/cluster ontstaat. Clustering van collapsed-core-nodes hoeft niet beperkt te worden tot één datacenter en mag derhalve worden toegepast 'over' meerdere datacenters, indien dit in een gebruikssituatie de meest doelmatige oplossing is. Ontsluiting tussen de collapsed-core-nodes dient te zijn gebaseerd op Ethernet 40Gbit/s met de mogelijkheid tot afschaalbaarheid naar 10Gbit/s. Eventuele verbindingen voor heartbeats/ keepalives tussen de nodes mogen met een lagere doorvoersnelheid worden vormgegeven.
Ontwerpregel 13.3	Een collapsed-core-node dient te voorzien in een combinatie van 1 Gbit/s en 10 Gbit/s poorten, waarbij een groei naar 25 Gbit/s of hoger voor het ontsluiten van aanpalende nodes mogelijk dient te zijn indien tijdelijke groei geaccomodeerd dient te worden.
Ontwerpregel 13.4	Uplinks/downlinks zijn dusdanig gepositioneerd dat uitval van één collapsed-core-node in een cluster niet leidt tot een algeheel verlies van connectiviteit met de aanpalende node(s).
Ontwerpregel 13.5	Ontsluiting tussen collapsed-core-nodes en backbone-nodes is gebaseerd op minimaal 20Gbit/s, gebruikmakend van linkbundelingstechnologie.
Ontwerpregel 13.6	Een collapsed-core node voorziet in non-oversubscribed poorten (op elke poort).
Ontwerpregel 13.7	In Service Software Upgrade dient te worden ondersteund.
Ontwerpregel 13.8	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 13.9	Nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 13.10	Nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
Ontwerpregel 13.11	Nodes zijn voorzien van redundante power supplies.
Ontwerpregel 13.12	Nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 13.13	OSI Laag 3 terminatiepunten liggen op bij voorkeur op het niveau van de module Backbone, maar in ieder geval binnen de module Datacenter (onprem). Hiervan kan worden afgeweken, indien bijvoorbeeld voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een DC-overschrijdend OSI Laag 2 pad aan te brengen,
Ontwerpregel 13.14	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.

Ontwerpregel 13.15	Nodes communiceren met hun omgeving op basis van open standaarden.
Ontwerpregel 13.16	De node(s) van de module Backbone mogen geen deel uitmaken van de collapsed-core in verband met: • Het kunnen scheiden van de modules Datacenter onprem en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.
Ontwerpregel 13.17	Access nodes zijn voorzien van redundantie powersupplies
Ontwerpregel 13.18	Access nodes moeten voorzien in modulariteit van 10 Gbit/s UTP, 10 Gbit/s Twinax en combinaties MMF, SMF).
Ontwerpregel 13.19	Access nodes moeten voorzien linkbundelingstechnieken voor uplinks naar de collpased core en naar ontsluitende (server)systemen. Uplinks en downlinks dienen simultaan verkeer te kunnen verwerken.

Communicatie SDN en traditioneel:

Ontwerpregel 14	**Communicatie tussen SDN en traditioneel model**
Communicatie tussen onderdelen die deel uitmaken van het SDN-model en onderdelen die deel uitmaken van de module Backbone of deel uitmaken van services als storage, security verlopen middels border leafs. Communicatie dient te kunnen worden gestandaardiseerd op protocollen die opereren op de niveaus van OSI laag 2 en OSI laag 3.	

4.3.2 SDN

De onderstaande kenmerken gelden voor dit model:

Ontwerpregel 15	**SDN-model-Eigenschappen datatacenter onprem**	
Ontwerpregel 15.1	Aanwezigheid onderwijskritieke ICT-services	Ja
Ontwerpregel 15.2	Medium tussen nodes lagen 'leaf' en collapsed-core	Glas, minimaal 10 Gbit/s
Ontwerpregel 15.3	Medium tussen nodes lagen 'leaf' en 'spine'	Glas, minimaal 10 Gbit/s
Ontwerpregel 15.4	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 15.5	SLA leaf-node	MTTR 4 uren -> (definitieve vaststelling in overleg met de

		markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 15.6	SLA aggregatie-node	MTTR 8 uren -> (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 15.7	Schaalbaarheid	'Leaf-laag': horizontale en verticale schaalbaarheid 'Spine-laag': verticale schaalbaarheid
Ontwerpregel 15.8	Toekomstige groei	In principe geen i.v.m. *cloud, tenzij…*principe. Eventuele groei dient wel te kunnen worden geaccommodeerd in de 'leaf' en 'spine' laag.

Generieke kenmerken leaf en spine nodes:

Het model bevat nodes van het type leaf en spine die generieke kenmerken hebben of kenmerken die dermate overeenkomen dat deze hieronder geroepeerd zijn opgenomen.

Ontwerpregel 16	**SDN-model: Generieke kenmerken leaf en spine nodes**
Ontwerpregel 16.1	Leaf-nodes zijn verbonden met iedere spine-node in de topologie, zodat uitval van een uplinkverbinding of een spine-node niet leidt tot een algeheel verlies van connectiviteit vanaf een leaf-node. Leaf nodes dienen geclusterd te kunnen worden.
Ontwerpregel 16.2	De access-poorten van een leaf-nodes zijn van het type koper of glas met ondersteuning van de interfacesnelheden 1Gbit/s en 10Gbit/s, waarbij een groei naar 25Gbit/s of hoger mogelijk is.
Ontwerpregel 16.3	Leaf-nodes ontsluiten het SDN-model naar de module Backbone, waarbij: • Gebruikgemaakt kan worden van linkbundelingstechnieken, • De ontsluiting gebaseerd is op minimaal 20Gbit/s (modulariteit moet kunnen voorzien in 10 Gbit/s UTP, 10 Gbit/s Twinax en combinaties MMF, SMF). • Meerdere leaf-nodes gebruikt kunnen worden voor de ontsluiting naar de module Backbone ter voorkoming van SPOFs, • Connectiviteit kan worden gerealiseerd op basis van zowel OSI laag 2 als OSI laag 3.
Ontwerpregel 16.4	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.

Ontwerpregel 16.5	Nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
Ontwerpregel 16.6	Spinde-nodes zijn voorzien van redundante power supplies, leaf-nodes niet.
Ontwerpregel 16.7	Nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
Ontwerpregel 16.8	Ontsluiting tussen leaf-nodes en spine-nodes zijn gebaseerd op minimaal 10Gbit/s, waarbij een groei naar 40 Gbit/s of hoger mogelijk dient te zijn.
Ontwerpregel 16.9	De software-architectuur is modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien 'pay as you grow' kunnen worden ingevuld.
Ontwerpregel 16.10	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de module Backbone, maar in ieder geval binnen de module Datacenter. Hiervan kan worden afgeweken, indien bijvoorbeeld voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een datacenter-overschrijdend OSI Laag 2 pad aan te brengen.
Ontwerpregel 16.11	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
Ontwerpregel 16.12	Nodes die deel uitmaken van de SDN-topologie communiceren met nodes buiten deze topologie op basis van open standaarden.

4.4 Module Cloud

Benadering clouddiensten:

Ontwerpregel 17	Benadering van clouddiensten
Ontwerpregel 17.1	Het dient mogelijk te zijn clouddiensten alleen te ontsluiten via de module Backbone waaraan de module Cloud direct is verbonden. Dit indien bepaalde ROC-diensten alleen vanaf de module Locatie via de module Backbone benaderd mogen worden.
Ontwerpregel 17.2	Het dient mogelijk te zijn clouddiensten alleen te ontsluiten via de module Backbone, waarbij gebruikgemaakt wordt van een local-internetbreakout. Tevens kunnen gebruikers die op afstand werken (e.g. mobiel/vanaf huis) de betreffende clouddiensten benaderen.

Generieke ontwerpregels clouddatacenter:

De onderstaande ontwerpregels gelden voor het gebruik van clouddatacenters (e.g. Azure, AWS, GCP).

Ontwerpregel 18	Generieke ontwerpregels clouddatacenter
Ontwerpregel 18.1	ROC-diensten dienen in verschillende availability zones te kunnen worden ondergebracht.
Ontwerpregel 18.2	ROC-diensten dienen in verschillende availability sets te kunnen worden ondergebracht.
Ontwerpregel 18.3	Binnen een clouddatacenter wordt gebruikgemaakt van de door de provider aangeboden default route naar het internet.
Ontwerpregel 18.4	ROC-diensten worden ondergebracht in de regio EER met uitsluiting van de UK.
Ontwerpregel 18.5	Koppeling tussen een clouddatacenter en de module Backbone wordt verzorgd door de leverancier van de module Backbone, waarbij de koppeling met een beschikbaarheid 99,99% wordt aangebracht (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
Ontwerpregel 18.6	Koppeling tussen een clouddatacenter en de module Backbone ondersteunt Quality of Service.
Ontwerpregel 18.7	Koppeling tussen een clouddatacenter en de module Backbone is gebaseerd op minimaal 10Gbit/s, waarbij de afgenomen bandbreedte kan worden afgestemd op het gebruik.
Ontwerpregel 18.8	Zowel IPv4 als IPv6 dienen te worden ondersteund.

4.5 WLAN

Generiek:

Ontwerpregel 19	WiFi generiek
Ontwerpregel 19.1	Bij voorkeur wordt WiFi aangeboden vanuit de module Cloud op grond van het beleidsuitgangspunt van het ROC: c*loud, tenzij*…Dit houdt in dat: • Centrale functies als controller/management vanuit 'de cloud' worden afgenomen, • Management-, provisioning- en beheerportals vanuit 'de cloud' worden afgenomen. Indien de leverancier van de module Backbone geen directe connectiviteits-mogelijkheden heeft met de leverancier van WiFi is het toegestaan connectiviteit aan te brengen vanaf de module Locatie naar de betreffende SaaS-oplossing middels een decentrale internet breakout. Hierbij dient de communicatiestroom echter wel te worden beschermd door protocollen met ingebouwde beveiligingsfuncties (e.g.: IPsec, HTTPS e.d.).
Ontwerpregel 19.2	Access points dienen de standaard IEEE 802.11ax te ondersteunen met extra functionaliteiten voor Bluetooth en Zigbee.
Ontwerpregel 19.3	Access points dienen te voorzien in 4x4 MU-MIMO (Multi-User MIMO) met minimaal 4 spatial streams.
Ontwerpregel 19.4	Access points dienen te voorzien in flexibele radio-instellingen op grond van de RF-omgeving, waarbij deze dual band frequenties (2.4 en 5Ghz) ondersteunt.
Ontwerpregel 19.5	Access points dienen middels PoE van stroom te worden voorzien.
Ontwerpregel 19.6	Access points dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
Ontwerpregel 19.7	Quality of Service dient te worden ondersteund in de draadloze netwerk-faciliteiten.
Ontwerpregel 19.8	Het draadloze netwerk dient multicast te ondersteunen. Het draadloze netwerk dient ook mDNS te ondersteunen in verband met te gebruiken digiborden.
Ontwerpregel 19.9	Het draadloze netwerk dient goede ondersteuning/support te leveren voor 'home oplossingen' als 'hue lampen'. Hierbij dient rekening te worden gehouden met de samenhang tussen het bedrade en draadloze netwerk. Deze lampen vereisen namelijk, dat 'gewerkt' wordt binnen in hetzelfde broadcastnetwerk.
Ontwerpregel 19.10	De managementomgeving/portal van het draadloze netwerk dient goede inzage te geven in 'client-gebruik, 'client-dichtheid', 'client failures', 'AP-failures'. Tevens dient de managementomgeving/portal te beschikken over goede monitoring & troubleshootfuncties.
Ontwerpregel 19.11	'Local breakout' en 'central breakout' moet mogelijk zijn (al dan niet als elkaars fallbackoplossing bij storingen), waarbij authenticatie in alle omstandigheden mogelijk moet blijven.

Ontwerpregel 19.12	Het draadloze netwerk dient dezelfde functionaliteit te bieden als het bedrade netwerk voor dezelfde categorieën devices.

Pre site survey:

Ontwerpregel 20	**Pre site survey**

Alvorens een site survey door te voeren, dienen de onderstaande organisatorische onderdelen te worden aanschouwd/vastgelegd/besproken/beantwoord:

- Vaststellen van de business requirements:
  - Afnemers die gebruik maken van het draadloze netwerk?
  - Typen clients die gebruik maken van het draadloze netwerk?
- Vaststellen van dekking en capaciteit waaraan het draadloze netwerk dient te voldoen:
  - Aantal clients dat een access point accommodeert?
  - Simultaan gebruik van het draadloze netwerk?
  - Groei van het aantal wireless clients dat gebruik zal gaan maken van het draadloze netwerk?
  - De locatie/fysieke plaats waar wireless clients zich bevinden?
  - Piekuren van het gebruik van het draadloze netwerk?
  - Welke wireless devices kunnen interfereren met het draadloze netwerk?
  - Mobility?
  - PoE requirements?
- Analyse van het huidige draadloze netwerk:
  - Vaststellen van problemen met betrekking tot het huidige draadloze netwerk,
  - Welke devices interfereren met het huidige draadloze netwerk?
  - Zijn fysieke locaties/plaatsen aanwezig waar geen of slecht signaalbereik is (‘coverage dead zones’)?
  - Is een Radioplan voorhanden vanuit eerdere site surveys?
  - Welke draadloze apparatuur wordt gehanteerd in de huidige setting?
  - Hoe worden de access points voorzien van stroom?
- Vaststellen huidige bedrade netwerkinfrastructuur:
  - Vaststellen huidige topologie bedrade netwerkinfrastructuur,
  - Waar bevindt/begint de bedrade netwerkinfrastructuur i.v.m. plaatsing van access points?
  - Welk type koper wordt gebruikt?
- Documentatie/rapporten voorhanden?
- Zijn blueprints/oppervlakteschema’s voorhanden?

Site survey:

Ontwerpregel 21	Site survey

De onderstaande technische gegevens zijn van belang in het kader van het uitvoeren van een site survey:

- De site survey dient gebaseerd te zijn op een draadloze netwerkinfrastructuur die wordt gerealiseerd op basis van de meest recente standaard (op het moment van schrijven is dat de IEEE802.11-ax standaard).
- Het vaststellen van de dekking dient te zijn gebaseerd op de principes van zowel een passieve als actieve site survey, waarbij de informatie uit beide surveys met elkaar kunnen worden vergeleken c.q. als aanvulling op elkaar kunnen werken.
- De site survey dient te worden uitgevoerd met apparatuur die representatief is voor de latere implementatie.
- Uitgangspunt qua aantal gelijktijdige wireless clients per gebruiker:
    - Medewerker -> maximaal 3 devices,
    - Studenten -> maximaal 3 devices
    - Docenten -> maximaal 3 devices
- Op grond van:
    - best practices en ervaringen in gelijksoortige omgevingen,
    - huidige gebruikersaantallen en oppervlakten,

  dient een inschatting te worden gemaakt van dekkingsgraden, capaciteitsbehoeften, aantallen access points, aantallen wireless LAN controllers (voorkeur als SaaS-afname) en benodigde licentie(structuren).
- Er dient geen rekening te worden gehouden met ‘backward compatibility’ van wireless devices in het kader van de standaarden IEEE 802.11 a,b,g.
- De draadloze oplossing dient te voldoen aan de wettelijk geldende normen/eisen op het gebied van de maximale elektromagnetische straling.
- Er dient rekening te worden gehouden met een overlap tussen de wireless cellen van 15-20%. Dit in verband met wireless clients waarop voice applicaties kunnen zijn aangebracht.
- ‘Adjacent channel interference’ dient te worden voorkomen door het juist instellen van wireless radio’s op grond van een goed doordacht en berekend RF-plan.
- Indien ‘co-channel interference’ onvermijdelijk blijkt, dient een waarde van 20dB te worden gehandhaafd aan de uiterwaarden van de cellen.
- OSI Layer 2 retransmissions dienen te worden voorkomen. Aandacht dient te worden geschonken aan:
    - Wireless devices die het RF-spectrum interfereren (narrow band interference, wide band interference, all-band interference),
    - ‘Adjacent channel interference’,
    - Lage Signal to Noise Ratio (SNR),
    - Een mismatch in power settings tussen een access point en een wireless client,

- Disproportionele ‘transmit power settings’ tussen verschillende wireless clients (near/far problematiek),
- Hidden node problematiek.

- Roaming dient ‘seamless’ te gebeuren zonder voor gebruikers merkbare onderbreking van verkeersstromen en kwaliteit van de gebruikte diensten. Er dient te worden voldaan aan:
  - Fast roaming, waarbij roaming zowel volgens het principe ‘over-the-air’ als ‘over-the-DS’ mag plaatshebben naar gelang de beste kwaliteit van roaming wordt bereikt,
  - Voor voice applicaties geldt een waarde van -67 dBm (of beter) in de uiterwaarde van een cell met een SNR van 25dB (of beter),
  - Op locaties waar geen voice applicaties gebruikt worden geldt een waarde van -70 dBm (of beter) voor de cell-uiterwaarde met een SNR van 20dB (of beter).

Post site survey:

Ontwerpregel 22	**Post site survey**

Nadat de site survey is doorgevoerd, dienen de onderstaande organisatorische onderdelen te worden aanschouwd/vastgelegd:

- De exacte dekkingsgraad en capaciteitsbehoefte per locatie zal in goed overleg worden afgestemd.
- De volgende deliverables dienen te worden opgeleverd (afzonderlijk of integraal):
  - Statement/doel met requirements als uitgangspunten,
  - Spectrum Analyse met informatie over potentiële bronnen van interferentie,
  - Dekkings Analyse met informatie over alle RF- cellen/uiterwaarden (heating maps),
  - Aanbevelingen voor het positioneren/implementeren van access points, inclusief de oriëntatie van antennes, kanalen, energie settings, installatietechnieken, bekabeling (implementatie-diagrammen).
  - Capaciteit en Performance Analyse met resultaten van ‘application throughput testing’.

4.6 Azure

Ontwerpregel 23	Ontwerpregels Azure: Tenant, management group, subscription
Ontwerpregel 23.1	Het ROC hanteert het één tenantconcept, waarbij één AAD gebruikt wordt.
Ontwerpregel 23.2	Het ROC hanteert het gebruik van management groups voor het centraal kunnen afdwingen van policies/beleid (governance) over alle subscriptions heen.
Ontwerpregel 23.3	Een subscription heeft limieten. Als deze overschreden (kunnen) worden, dienen deze te worden opgehoogd. Als dat niet meer mogelijk is, dienen (vooraf) extra subscriptions te worden ingezet.
Ontwerpregel 23.4	Communicatie tussen de onprem AD en AAD verloopt middels de module Backbone, waarbij connectiviteit met Azure wordt gerealiseerd door de leverancier van de module Backbone.

Ontwerpregel 24	Ontwerpregels Azure/Topologie infrastructuur
Ontwerpregel 24.1	De topologie van de infrastructuur binnen Azure is gebaseerd op een hub-and-spoke-topologie.
Ontwerpregel 24.2	Shared resources worden centraal ondergebracht in het hub vnet, waarvan de workloads in verschillende spokes gebruik kunnen maken.
Ontwerpregel 24.3	Ieder vnet is opgedeeld in één of meerdere subnets conform het IP Plan van het ROC.
Ontwerpregel 24.4	Communicatie tussen spokes dient te verlopen via het centrale hub vnet.
Ontwerpregel 24.5	Communicatie tussen spokes en het internet dat Azure levert verloopt via de centrale hub.
Ontwerpregel 24.6	De hub met centrale faciliteiten/resources is ondergebracht binnen één ‘generieke’ subscription. De faciliteiten/resources die zijn ondergebracht in de spokes behoren tot andere subscriptions.
Ontwerpregel 24.7	Indien de limieten van de (subscription) van de hub zijn bereikt, dient een nieuwe hub (subscription) te worden aangemaakt met (waar nodig) peering tussen de hubs voor communicatiedoeleinden.
Ontwerpregel 24.8	Binnen iedere subscription dienen resource groups te zijn aangemaakt, waarbinnen de ROC-diensten zijn opgenomen. De te gebruiken classificatie en criteria voor opname van ROC-diensten in resource groups dient met stakeholders en diensteigenaren te worden afgestemd. Hierbij dient op z’n minst rekening te worden gehouden met zaken als gezamenlijke LCM van onderdelen, gezamenlijke billing van onderdelen, gezamenlijkheid van functies van onderdelen.

5 Bijlage B: Gebruikte afkortingen

Afkorting	Betekenis
AAD	Azure Active Directory
AD	Active Directory
AI	Artificial Intelligence
AP	Access Point
AWS	Azure Web Services
BSA	Basic Service Area
DC	Datacenter
DCI	Datacenter Interconnect
DS	Distributie System
GCP	Google Cloud Platform
HLD	High Level Design
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IDP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISSU	In Service Software Upgrade
LCM	Life Cycle Management
LLD	Low Level Design
LTE	Long Term Evolution
MU-MIMO	Multi-user multiple-input and multiple-output
ML	Machine Learning
MPLS	Multiple Protocol Label Switching
LAN	Local Area Network
MMF	Multimode Fiber
MTTR	Mean Time To Repair
NBD	Next Business Day
NVA	Network Virtual Appliance
OSI	Open Systems Interconnection
OTAP	Ontwikkel, Test, Acceptatie, Productie
PaaS	Platform As A Service
PEP	Policy Enforcement Point
PoE	Power over Ethernet
POP	Point Of Presence
QoS	Quality of Service

RF	Radio Frequentie
RFP	Request For Proposal
SaaS	Software As A Service
SDN	Software Defined Network
SLA	Service Level Agreement
SMF	Singlemode Fiber
SNR	Signal to Noise Ratio
SPOF	Single Point of Failure
TA	Technische Architectuur
WLAN	Wireless Local Area Network