Afstudeeropdracht: Software Defined Networking

Type document: **Onderzoeksrapport**

Auteur: **Dhr. François Kikken**
Datum: **5 juni 2015**

Afstudeeropdracht:
Software Defined Networking

Type document: Onderzoeksrapport

Format Versie:	**1.0**
Status document:	**Definitief**
Naam van dit document:	**Software Defined Networking - Onderzoeksrapport_V1.0.docx**
Auteur:	**Dhr. François Kikken**
Datum:	**5 juni 2015**

Document versie beheer

Configuratie beheer			
Versie nr.	**Datum**	**Wijzigingen**	**Auteur**
0.1.0	03-03-2015	Opzet template	Dhr. François Kikken
0.2.0	20-04-2015	Invulling Hoofdstuk MAASnet + Opzet hoofdstuk indeling	Dhr. François Kikken
0.3.0	19-05-2015	Hoofdstuk Software Defined Networking	Dhr. François Kikken
0.4.0	20-05-2015	Hoofdstuk Longlist + MoSCoW-prioritering	Dhr. François Kikken
0.5.0	21-05-2015	Invulling MoSCoW-analyse vergelijkingstabel	Dhr. François Kikken
0.6.0	21-05-2015	Hoofdstuk Shortlist + Product explicatie	Dhr. François Kikken
0.7.0	26-05-2015	Hoofdstuk Toepasbaarheid + Eindconclusie + Aanbevelingen	Dhr. François Kikken
0.8.0	28-05-2015	Hoofdstuk Onderzoeksmethode + Managementsamenvatting	Dhr. François Kikken
0.9.0	02-06-2015	Verwerken van feedback uit diverse reviews + Begrippenlijst	Dhr. François Kikken
1.0	05-06-2015	Definitieve versie	Dhr. François Kikken

Tabel 1: Configuratie beheer

Distributie beheer			
Versie nr.	**Datum**	**Wijzigingen**	**Ontvanger**
0.8.0	28-05-2015	Aanlevering ter review	Ing. Daniël Heynen
1.0	10-06-2015	Definitieve inlevering afstudeerportfolio	Bianca Fintelman

Tabel 2: Distributie beheer

Gerelateerde documenten		
Versie nr.	**Naam**	**Functie**
1.0	Software Defined Networking - Project Initiatie Document	Goedkeuring van de start van het project.
1.0	Software Defined Networking - Literatuurstudie	Verzorgen van de benodigde gegevens voor een onderbouwd advies.
1.0	Software Defined Networking - Interviewrapport	Verzorgen van aanvullende informatie voor een onderbouwd advies.

Tabel 3: Gerelateerde documenten

Algemene gegevens

Bedrijfsbegeleider (opdrachtgever)	
Eigenschap	**Gegeven**
Naam	Maastricht University - ICTS Netwerken
Adres	Grote Looierstraat 17, 6211 JH Maastricht
Contactpersoon	Ing. Marc Jonkers

Afstudeerder (opdrachtnemer)	
Eigenschap	**Gegeven**
Naam	Dhr. François Kikken
Adres	Dassenkuillaan 8, 6162 JE Geleen
Telefoon	+31 655 689 801

Schoolbegeleider	
Eigenschap	**Gegeven**
Naam	Zuyd Hogeschool - HBO-ICT
Adres	Nieuw Eyckholt 300, 6419 DJ Heerlen
Telefoon	+31 454 006 060
Contactpersoon	Ing. Daniël Heynen

Projectgegevens	
Eigenschap	**Gegeven**
Documentversie	1.0
Documentsoort	Onderzoeksrapport
Omschrijving	Software Defined Networking – Onderzoeksrapport

Voorwoord

Het afstudeertraject betreft het onderwerp Software Defined Networking (SDN) en is aangedragen door de afstudeerder. Ik ben met dit onderwerp in aanraking gekomen tijdens het bijwonen van een, door Cisco Systems aangeboden, conferentie. Na het bijwonen van deze conferentie zijn bij mij hoge verwachtingen van deze techniek en de bijbehorende interesses ontstaan. Naast mijn interesses op dit gebied, heb ik voor SDN gekozen om mijn kennis m.b.t. dit onderwerp te vergaren.

De keuze voor de bedrijfslocatie is bij mij ontstaan, doordat ik tijdens mijn MBO-stage eerder in aanraking met de universiteit ben gekomen. Echter, heb ik toen der tijd niets met het netwerk of de netwerktechnieken van doen gehad. Dit terwijl de IT-infrastructuur juist de IT-richting is, waar mijn hartstocht ligt. Het lijkt me de ideale situatie om beide aspecten met elkaar te kunnen combineren.

Ten slotte wil ik ICTS (netwerken) en in het bijzonder ing. Marc Jonkers bedanken voor het mede mogelijk te maken en begeleiden van deze opdracht. Tevens wil ik ing. Daniël Heynen bedanken voor het begeleiden van mijn gehele afstudeertraject.

Maastricht, 7 juli 2015

Managementsamenvatting

Aanleiding
Deze opdracht is tot stand gekomen doordat de afstudeerder zijn studietraject dient af te sluiten met een HBO-waardig onderzoek. Tijdens het eerste kennismakingsgesprek tussen ing. Marc Jonkers en dhr. François Kikken is de keuze op Software Defined Networking (SDN) als onderwerp gevallen.

Probleemstelling
Continu verschijnen nieuwe technieken en producten op de markt betreffende de IT-infrastructuur. Om de gebruikservaring van de eindgebruiker optimaal te houden, dient MAASnet mee te gaan met deze constante veranderingen. Echter, voordat een dergelijke verandering doorgevoerd kan worden, dient onderzocht te worden of het aan de eisen en wensen van de afnemer voldoet en tevens toepasbaar is.

Doelstelling
SDN is één van deze nieuwe technieken, waarvoor een weloverwogen advies naar de meerwaarde, de mogelijkheden en de toepasbaarheid nodig is. Dit geheel dient in de context van MAASnet onderzocht te worden. Het doel van dit project luidt dan als volgt: ***"Het onderzoeken of en welke SDN-techniek geschikt is voor gebruik binnen MAASnet."***

Onderzoeksvragen
De bovengenoemde doelstelling wordt beantwoord aan de hand van de onderstaande onderzoeksvraag en de daarbij behorende deelvragen. De opsomming vermeldt als eerste de hoofdvraag en vervolgens zijn de daarbij behorende deelvragen, in het niveau daaronder, terug te vinden.

- Is de SDN-techniek geschikt, en zo ja, welke SDN-methodiek, voor gebruik binnen MAASnet?
  - Wat is Software Defined Networking? (paragraaf 4.5);
  - Welke methodieken bestaan binnen deze techniek? (paragraaf 4.5);
  - Hoe ziet MAASnet eruit op functioneel- en technisch gebied? (paragraaf 3.4);
  - Welke eisen en wensen zijn gesteld aan MAASnet? (paragraaf 3.4);
  - Welke SDN-methodiek is bruikbaar voor MAASnet? (hoofdstuk 9);
  - Voldoet de SDN-methodiek aan de eisen en wensen van MAASnet? (hoofdstuk 9);
  - Wat zijn de voor- en nadelen, met de invalshoek naar MAASnet, van de verschillende SDN methodieken? (hoofdstuk 9);

Methode
Tijdens het afstudeerproject wordt gebruik gemaakt van een open onderzoeksvraag en -deelvragen. Dit betekent dat de doorgaans gebruikte onderzoeksmethode een kwalitatief onderzoek betreft en verantwoordelijk is voor het aandragen van inzicht in de te onderzoeken materie. Echter, vanwege tijdsgebrek om deze onderzoeksmethode te hanteren, wordt een deskresearch gehanteerd.

Conclusie
Software Defined Networking is, op het moment van schrijven, niet geschikt voor implementering binnen MAASnet. Redenen als de onvolwassenheid van-, vele ontwikkelingen binnen deze architecturale benadering, gebrek aan bewijslasten van schaalbaarheid en functionerende implementeringen leiden tot deze conclusie.

Aanbevelingen
Aansluitend op dit afstudeerproject wordt het aanbevolen om vervolgonderzoeken te starten naar de volgende onderwerpen:

- Onderzoek naar Software Defined Networking in een Datacenter netwerkomgeving;
- Onderzoek naar Network Function Virtualisation;
- Onderzoek naar de schaalbaarheidsverschillen van de diverse SDN-modellen;
- Onderzoek naar de business impactanalyse van Software Defined Networking.

Begrippenlijst

Begrippenlijst	
Begrip	**Betekenis**
Abstractie	Een abstractie draagt zorg voor een logische en gesimplificeerde weergave van het netwerk. Hierdoor wordt de gedetailleerde weergave van de netwerkapparatuur verborgen.
Access Control List (ACL)	Een ACL is een beveiligingsmechanisme voor netwerkapparatuur. Dit mechanisme is vooral terug te vinden op routers, firewalls en layer 3 switches en filtert het netwerkverkeer op basis van een vooraf opgestelde lijst met regels. Deze regels kunnen ingesteld worden om verkeer toe te laten of juist te weigeren.
Access layer	De Access layer is onderdeel van het Cisco Three Layered Hierarchical Network Model. Deze laag is verantwoordelijk voor een connectiviteit van alle eindstations. Daarnaast is deze laag veelal in laag 2 van het OSI model uitgevoerd en wordt segmentatie van het netwerkverkeer toegepast.
Access Points (AP)	Een AP is verantwoordelijk voor de connectiviteit van draadloze netwerkapparatuur. Dit apparaat kan in twee verschillende manier functioneren, namelijk aangestuurd door een controller (domme AP) en aangestuurd door zichzelf (slimme AP).
Application Programming Interface (API)	Een application programming interface is een interface die aan de hand van een uniforme programmeertaal kan communiceren met een computerprogramma.
ARP-request	ARP staat voor Address Resolution Protocol en is een protocol binnen de TCP/IP-protocol suite. Aan de hand van dit protocol kan een eindpuntapparaat het laag 2 adres van een ander eindpuntapparaat leren. Een ARP-request is dan eveneens de opvraagmethodiek voor dit adres.
authenticatie-, autorisatie- en accounting- (AAA)	Het AAA-proces wordt gebruikt om elektronische systemen te voorzien van een authenticatie en autorisatie mechanisme voor computernetwerken. Naast het voorzien van een toegangssysteem (authenticatie en autorisatie) worden eveneens de, door de elektronische systemen, uitgevoerde handelingen bijgehouden door het accounting deel van het AAA-proces.
Automatisering	Met behulp van automatisering worden menselijke handelingen (veelal repetitieve taken) uitgevoerd door computersystemen. Binnen netwerkinfrastructuren kan gedacht worden aan het configureren van diverse switches die over dezelfde basisconfiguratie beschikken.
Autonome systemen	Een autonoom systeem, binnen computernetwerken, is een deelnetwerk van het internet en worden aangeduid met een nummer. Deze nummers worden, wereldwijd, toegewezen door de instantie Internet Assigned Numbers Authority (IANA).
BGP-peering	BGP is het protocol wat veelal wordt gebruikt als routingprotocol voor het internet. Met BGP-peering wordt de koppeling tussen twee BGP-eindpunten (in één autonoom systeem) bedoeld.
Border Gateway Protocol (BGP)	BGP is een netwerk routing protocol dat veelal gebruikt wordt voor routering binnen het internet. Het protocol wisselt informatie tussen autonome systemen uit en baseert haar routingbeslissingen op basis van diverse paden, netwerkbeleid en vooraf gedefinieerde regels.

Broadcastdomein	Een broadcastdomein, binnen een computernetwerk, is een gebied waar een datapakket door elk aangesloten apparaat wordt ontvangen. Echter, deze communicatiemanier vindt alleen plaats wanneer gebruik wordt gemaakt van een speciale adressering of wanneer een protocol (bijvoorbeeld een ARP-request) dit vereist.
Broncode	De broncode is de, door de softwareprogrammeur geschreven, leesbare tekst van een computerprogramma. Deze tekst kan in meerdere programmeertalen zijn uitgevoerd en is nog niet door een compiler gehaald.
Cachegeheugen	Het cachegeheugen is een opslagplaats voor tijdelijke data. Daarnaast biedt dit geheugen een dergelijke abstractie dat de oorspronkelijke bron niet zichtbaar is bij het ophalen van deze data.
Cisco Availability (CA)	De Cisco Availability Release is een productversie die alleen voor engineers van Cisco Systems beschikbaar is. Deze productversie wordt veelal gebruikt voor het testen van functionaliteiten van het desbetreffende product.
Cisco Discovery Protocol (CDP)	CDP is een Cisco Systems propriëtair protocol en wordt gebruikt om informatie te verzamelen van rechtstreeks aangesloten Cisco Systems netwerkapparatuur. De informatie wordt iedere 60 seconden via het multicast-adres “01-00-0C-CC-CC-CC” verstuurd en automatisch in de CDP-tabel verwerkt.
Cisco Wireless Service Module (WiSM2)	De Cisco Wireless Service Module is een insteek module voor het Cisco Catalyst 6500 Series Chassis. Deze module is verantwoordelijk voor het aansturen van de diverse Cisco Wireless Access Points.
Control And Provisioning of Wireless Access Points (CAPWAP)	CAPWAP is een protocol dat verantwoordelijk is voor de communicatie tussen de draadloze access points en de draadloze controller. Dit protocol wordt toegepast in een architectuur waar draadloze access point aangestuurd worden door de controller. Het gebruikt UDP poort 5246 voor het controle kanaal en UDP 5247 voor het data kanaal.
Converged network adapter (CNA)	Een CNA is een I/O-apparaat dat de functionaliteiten van een HBA en een NIC combineert tot één enkel hardware-onderdeel of apparaat.
Core layer	Kernlaag uit het Cisco Three Layered Hierarchical Network Model. Deze laag bestaat uit alle fundamentele netwerkapparatuur en is alleen verantwoordelijk voor het doorzetten van de datapakketten.
Darkfiber	Een darkfiber netwerk is een geprivatiseerd glasvezelnetwerk. De bekabeling is gekocht of gehuurd en wordt, in tegen stelling tot het kopen van bandbreedte of leased-line technologie, zelf beheerd.
Distribution layer	Middelste laag uit het Cisco Three Layered Hierarchical Network Model. Deze laag is verantwoordelijk voor het toepassen van alle regels, het routeren, et cetera van de datapakketten.
Domain Name System (DNS)	DNS is een hiërarchisch gedistribueerd benamingssysteem voor apparatuur of services aangesloten op een computernetwerk. Dit computernetwerk kan geprivatiseerd dan wel publiek of een combinatie hiervan zijn. IP-adressen worden gekoppeld aan een DNS-record, waardoor het onthouden van apparaat namen wordt gesimplificeerd.
Dynamic Trunk Protocol (DTP)	DTP is een Cisco Systems propriëtair protocol dat zorg draagt voor het maken van een z.g. trunk verbinding tussen twee VLAN-bewuste switches. Door deze verbinding te creëren kunnen meerdere VLAN’s over dezelfde verbinding worden getransporteerd. DTP kan gebruik maken van de standaarden IEEE 802.1Q of Cisco ISL.

Early Field Trials (EFT)	De Early Field Trials is een term die veelal wordt gebruikt bij het uitvoeren van testen op producten.
East-West API	Een East-West API is een interface die gebruik maakt van een uniforme programmeertaal om federaties tussen diverse SDN-controllers mogelijk te maken.
Enhanced Interior Gateway Routing Protocol (EIGRP)	EIGRP is een Cisco Systems propriëtair protocol dat zorg draagt voor de routering tussen diverse computernetwerken. Dit protocol bepaald de beste route gebaseerd op de kortste afstand en de link-status. Daarnaast stuurt het, in tegen stelling tot andere protocollen, alleen routingupdate wanneer wijzigingen hebben plaatsgevonden.
Error-disabled	Error-disabled is een status van een interface poort op Cisco systems netwerkapparatuur. Bij deze status is de interface hardware matig geactiveerd en software matig gedeactiveerd. Een interface kan deze status krijgen, doordat bijvoorbeeld ingestelde beveiligingsmaatregels worden geschonden.
Extensible Messaging and Presence Protocol (XMPP)	XMPP is een open en op de XML-taal gebaseerd netwerkprotocol. Dit protocol wordt veelal gebruikt voor instant messaging en presence notification.
Federatie	Een federatie is een verband van samenwerkende apparaten die eveneens hun zelfstandigheid behouden. Binnen SDN-omgevingen wordt hiermee gedoeld op SDN-controllers die met elkaar samenwerken.
Fiber Channel over Ethernet (FCoE)	FCoE is een encapsulatie-protocol dat zorg draagt voor het transporteren van Fiber Channel frames over een ethernetverbinding.
Firewall	Een firewall kan zowel software- als hardware matig worden uitgevoerd en draagt de verantwoordelijkheid om informatiesystemen te beschremen.
Framework	Een framework is een geheel aan componenten dat gezamenlijk één functionaliteit beid.
Fysieke servers (VM-hosts)	Een VM-host is een fysieke computer die zijn resources gebruikt voor de ‘rekenkracht’ van de diverse VM’s.
Gateway Load Balancing Protocol (GLBP)	GLBP is een Cisco Systems propriëtair protocol dat de limitatie van een redundant omgeving opheft. Dit wordt bewerkstelligd door het toevoegen van een load-balancing methodiek.
General Availability (GA)	De General Availability release is een productversie die door Cisco Systems wordt gebruikt voor het algemeen beschikbaar maken van een product.
Granulariteit	De term granulariteit is een term afkomstig vanuit datawarehouses en geeft aan in welke mate detail-gegevens van entiteiten aanwezig zijn. Een lagere granulariteit geeft aan dat minder details worden opgeslagen.

Host bus adapter (HBA)	Een HBA is een hardware-onderdeel van een computer en draagt zorg voor de connectiviteit met opslagapparatuur. De connectiviteit kan plaatsvinden aan de hand van glasvezel, External Serial ATA (eSATA) en Small Computer System Interface (SCSI).
Hot Standby Router Protocol (HSRP)	HSRP is een Cisco Systems propriëtair protocol dat zorg draagt voor een redundant en fout-tolerante omgeving.
HyperText Transport Protocol (HTTP)	Het protocol HTTP is een applicatie gebaseerd protocol voor het distribueren van hypermedia informatiesystemen. Deze informatiesystemen worden gebruikt voor het weergeven van webpagina's.
HyperText Transport Protocol Secure (HTTPS)	Het protocol HTTPS is de beveiligde variant van het protocol HTTP.
Hypervisor	Een Hypervisor is een stuk software, hardware of firmware dat verantwoordelijk is voor het aanmaken, bewerken, verwijderen en laten functioneren van een virtuele machine.
IEEE 802.1x	IEEE 802.1x is een standaard en zorgt voor een op poort gebaseerde netwerk toegang. De toegang wordt geauthentiseerd op basis van een authenticatieserver (veelal een RADIUS-server) en vervolgens geautoriseerd door het aansluitende netwerkapparaat.
Instant Messaging (IM)	Instant Messaging is een real-time tekst communicatie middel. De transmissie van de te versturen- en ontvangen tekst vindt plaats over het internet.
Institute of Electrical and Electronics Engineers (IEEE)	IEEE is een non-profit organisatie die verantwoordelijk is voor het standaardiseren van technieken en methodieken die betrekking hebben op computer technologie.
Internet Group Management Protocol (IGMP)	IGMP is een multicast protocol. Het multicast protocol wordt veelal gebruikt wanneer één-naar-veel communicatie benodigd is, zoals video streaming.
Internet Protocol (IP)	Het protocol IP is het belangrijkste communicatie protocol binnen de Internet Protocol Suite. Dit protocol is verantwoordelijk voor het van A naar B transporteren van pakketten en vindt plaats op basis van IP-adressering.
Internet Service Providers (ISP)	Een ISP is een organisatie die services levert om deel te kunnen nemen aan de communicatie op het internet netwerk.
Intrusion Prevention System (IPS)	Een IPS is een netwerkbeveiligingsapparaat dat malafide netwerkverkeer detecteert en blokkeert. Daarnaast wordt tevens, indien zulk verkeer wordt ontdekt, gerapporteerd.
IP versie 4 (IPv4)	IPv4 is de vierde versie van het protocol IP. Binnen dit protocol wordt een adressering van 32-bit gebruikt. Dit komt neer op maximaal 4.294.967.296 adressen.

IP versie 6 (IPv6)	IPv6 is de opvolger van IPv4. Binnen dit protocol wordt een adressering van 128-bit gebruikt. Dit komt neer op maximaal 2^128 (ongeveer 3.4 biljoen) adressen.
Internet Protocol (IP)-adres	Een IP-adres is een uniek adres voor elk apparaat wat connectie maakt met het netwerk. Dit adres is uitgevoerd op laag 3 van het OSI-model en wordt statisch of dynamisch toegekend.
Internet Protocol Suite	Het internet protocol suite is een set van communicatieprotocollen die communicatie over het internet mogelijk maken. Deze set van communicatieprotocollen staat eveneens bekend als TCP/IP.
IP-telefonie	IP-telefonie is het voorzien van communicatie services over het protocol IP.
Lightweight Directory Access Protocol (LDAP)	LDAP is een netwerkprotocol en beschrijft op welke manier gegevens uit een directoryservice benaderd dienen te worden.
Load balancing	Load balancing is een techniek waar de werklast wordt verdeeld over meerdere gelijkwaardige apparaten.
Media Access Control (MAC) adres	Een MAC-adres is een unieke identificatie voor netwerkinterfaces van apparatuur aangesloten op het netwerk. Deze adressen worden gebruikt voor de meeste IEEE 802 standaarden.
Network Function Virtualisation (NFV)	Techniek om netwerkfunctionaliteiten gevirtualiseerd uit te voeren.
Network interface card (NIC)	Een NIC is een hardware-onderdeel van een computer en draagt zorg voor de connectiviteit met het netwerk. De connectiviteit vindt, tegenwoordig, plaats op basis van de ethernet (IEEE 802.3) standaard.
Northbound API	Northbound API's zijn, binnen een SDN-omgeving, uniforme interfaces en dragen zorg voor de communicatie tussen applicaties en de SDN-controller.
Open System Interconnect (OSI)	Het OSI-model is een zeven laags model voor het karakteriseren en standaardiseren van interne functies van een communicatie systeem. Van laag 1 naar laag 7 bestaat dit model uit de lagen: Physical, Data, Network, Transport, Session, Presentation en Application.
Open Virtual Appliance (OVA)	Een OVA is een bestandsformaat bedoeld voor hypervisor onafhankelijke virtuele machines.
OpenFlow	Het meest bekende SDN Southbound protocol.

Open-source	Een broncode die veelal is ontwikkeld door een open-source community (meerdere personen) en geheel vrij van toegang is.
Orkestratie	Orkestratie is een gecentraliseerde manier van aansturen. Binnen computernetwerken wordt de aansturing van de onderliggende netwerkapparatuur bedoeld.
Policy's	Een policy is een lijst met regels en procedures waaraan een systeem of identiteit zich aan dient te houden.
Port Aggregation Protocol (PAgP)	Het protocol PAgP is een Cisco Systems propiëtair protocol dat zorg draagt voor het combineren van meerdere fysieke switchpoorten tot één logische link (eveneens etherchannel genoemd).
Port-based Network Access Control (PNAC)	PNAC is onderdeel van de IEEE 802.1x standaard en draagt zorg voor een op poort gebaseerde netwerktoegang. Zie IEEE 802.1x voor meer informatie.
Power over Ethernet (PoE)	PoE is een methodiek die veelal op de Access laag switches wordt gebruikt. Met behulp van deze methodiek kunnen apparaten, zoals wireless access points en IP-telefoons, worden voorzien van een stroomvoorziening over de ethernet bekabeling.
Programmeertalen	Een programmeertaal is een taal met vocabulaire syntaxis dat wordt gebruikt voor het samenstellen van een computerprogramma.
Quality of Service (QoS)	QoS is een methodiek die gehanteerd wordt om inzicht en controle te krijgen over de datapakketten van een computernetwerk. Met behulp van deze methodiek kan dataverkeer worden opgedeeld in groepen. Deze groepen krijgen vervolgens een bepaalde prioriteit toegekend om bijvoorbeeld voorrang op ander verkeer te krijgen.
RADIUS	RADIUS is een protocol dat aan de hand van het AAA-mechanisme netwerkconnectie voor gebruikers beheerd.
Rapid Per VLAN Spanning Tree Plus (RPVST+)	RPVST+ is een variant uit de Spanning Tree protocolsuite. Met behulp van Spanning Tree worden switching-loops voorkomen (zie switching-loop). Bij de RPVST+ variant is het mogelijk om per VLAN een Spanning Tree sessie op te zetten. Daarnaast biedt deze variant een lagere convergentietijd dan zijn PVST+ variant.
Request for change (RFC)	Een RFC is, volgens de ITILv2 en v3 methodiek, een formele aanvraag voor een wijziging in de IT-infrastructuur of elk ander aspect van een IT-service.
Reverse Proxy	Een reverse proxy is een proxyserver die datastromen initieert vanaf externe apparaten. Deze datastroom doet zich vervolgens voor alsof deze van de proxyserver afkomstig is.
Routed network	Binnen een gerouteerd netwerk kunnen diverse netwerksegmenten (over laag 3 van het OSI-model) met elkaar communiceren.

Scriptingtalen	Een script is een combinatie van meerdere losstaande commando's voor het (in één keer) uitvoeren van diverse opdrachten. Met de talen van een script wordt gedoeld op de taal die een applicatie ondersteund voor het uitvoeren van losstaande commando's.
Service Set Identifier (SSID)	Een SSID is de menselijk leesbare naam van het MAC-adres van het wireless access point (eveneens Basic service set identification (BSSID) genoemd).
Session Initiation Protocol (SIP)	Het protocol SIP is verantwoordelijk voor het signaleren en de beheersing van multimedia communicatie sessies, zoals IP-telefonie.
Simple Network Management Protocol (SNMP)	Het protocol SNMP is verantwoordelijk voor het managen van apparaten op een IP-netwerk. Het protocol wordt veelal gebruikt voor het uitlezen van condities van het netwerk en haar apparatuur. Echter, dit protocol biedt tevens functionaliteiten voor het beheren van de netwerkapparatuur.
Southbound API's	Southbound API's zijn, binnen een SDN-omgeving, uniforme interfaces en dragen zorg voor de communicatie tussen de diverse netwerkapparaten en de SDN-controller.
Storage Area Network (SAN)	Een SAN is een netwerkarchitectuur voor dataopslagapparaten.
Switching	Switching is het expediëren van, op laag 2 van het osi model gebaseerde, datapakketten.
Switching-loop	Een switching-loop ontstaat in een computernetwerk wanneer meer dan één layer 2 connectie bestaat tussen twee switches. Een switch stuurt, indien de eindbestemming niet bekend is, een datapakket over alle poorten (op de ontvangende poort na) naar buiten. Hierdoor blijft, in het geval van meer dan één layer 2 connectie, het datapakket oneindig op het netwerk circuleren.
Tenants	Een tenant is een gebruikersgroep die een gedeelde toegang heeft tot een softwarepakket. De rechten- en beveiligingsscheidingen vinden niet op het netwerk, maar binnen het softwarepakket plaats.
Unix	Unix is een op open-source gebaseerd besturingssysteem.
Virtual Desktop Interface (VDI)	Een VDI is een bureaubladgeoriënteerde omgeving en bevindt zich op een remote VM-host. Deze techniek maakt gebruik van een remote-display protocol, waardoor een apparaat onafhankelijke situatie ontstaat.
Virtual Local Area Networks (VLAN)	Met behulp van een VLAN kan een fysiek layer 2 netwerk worden opgedeeld in meerdere virtuele layer 2 netwerken. Door van deze techniek gebruik te maken, kunnen netwerkomgevingen van elkaar worden gescheiden en zich toch op hetzelfde fysieke netwerk bevinden.
Virtual Private Network (VPN)	Een VPN-verbinding is een methodiek om de functionaliteiten van een privénetwerk te verlengen naar aansluitpunten buiten de fysieke netwerkaansluitingen van dat netwerk. De verbinding wordt bewerkstelligd met een tunnel over het publieke internet heen.

Virtual Router Redundancy Protocol (VRRP)	Het protocol VRRP is verantwoordelijk voor het creëren van een redundant default-gateway. Binnen dit protocol worden twee layer 3 capabel apparaten met elkaar gekoppeld en voorzien van één IP-adres. Hierdoor kan, wanneer R1 defect raakt, bijvoorbeeld R1 het routeren van R2 overnemen.
Virtual Switching System (VSS)	VSS is een technologie die meerdere Cisco Catalyst 6500 Series Switches met elkaar combineert tot één logische virtuele switch.
Virtualisatie	Virtualistatie is een techniek die het mogelijk maakt om hardware onderdelen te verplaatsen naar software. Ter adstructie kan worden gedacht aan het een computersysteem (combinatie van diverse hardware onderdelen). Met behulp van virtualisatie kan een dergelijk systeem, door een softwareapplicatie, worden nagebootst.
Virtuele machine (VM)	Een VM is een software matige emulatie van een computersysteem. Door van een dergelijke VM gebruik te maken, kunnen de resources efficiënter worden gebruikt.
Virtuele Overlays	Binnen computernetwerken wordt, met een virtueel overlay netwerk, geduid op een logisch deel van het complete computer netwerk. Aan de hand van een dergelijk overlay netwerk wordt alleen de netwerkapparatuur getoond wat daadwerkelijk gebruikt wordt.
VLAN Trunking Protocol (VTP)	Het Cisco System propriëtair protocol VTP maakt het mogelijk om VLAN-databases op één enkele switch aan te maken en deze vervolgens automatisch te laten verspreiden naar de resterende switches in hetzelfde VTP-domein.
WAN-accelerators	Een WAN-accelerator is een hardware matige oplossing die de gebruikerservaring op Wide Area Networks vergroot.
Weighted Random Early Detection (WRED)	WRED is een queuemechanisme om congestie te voorkomen. Het is een extensie op Random Early Dectection (RED). Bij dit mechanisme buffert het netwerkapparaat, zolang de buffer niet vol is, pakketten. Bij een volle buffer worden pakketten weggegooid.

Tabel 4: Begrippenlijst

Inhoudsopgave

Inleiding

Dit rapport wordt geschreven om inzicht te tonen in de beantwoording van zowel de onderzoeksvraag als de daarbij behorende deelvragen. Daarnaast geeft dit rapport eveneens inzicht in de gebruikte methodes en de achtergrondinformatie van het afstudeerproject. Het rapport wordt geschreven door de afstudeerder (dhr. François Kikken) en is zowel gericht aan de bedrijfsbegeleider (ing. Marc Jonkers) als de schoolbegeleider (ing. Daniël Heynen). De distributie hiervan vindt plaats op de woensdag van de 16e week samen met het gehele afstudeerdossier.

De opdracht omvat de SDN-techniek en is bedoeld om de meerwaarde van deze techniek, binnen het netwerk van Maastricht University (MAASnet), aan te tonen. Een meer gedetailleerde doelstelling is in het Project Initiatie Document (Kikken, Software Defined Networking - Project Initiatie Document, 2015) terug te vinden.

Ieder hoofdstuk beschrijft een ander deel van het afstudeerproject. Onderwerp zoals achtergrondinformatie, methode, MAASnet, Software Defined Networking, Longlist, MoSCoW-prioritering, Shortlist, productexplicatie, toepasbaarheid, eindconclusie en aanbevelingen maken onderdeel uit van de diverse hoofdstukken in dit rapport. De hoofdstukken MAASnet, Software Defined Networking en toepasbaarheid beantwoorden aan het einde van het desbetreffende hoofdstuk één of meerdere deelvragen. Met behulp van al deze antwoorden wordt de onderzoeksvraag, in het hoofdstuk eindconclusie, beantwoord. Ten slotte worden eventuele vervolgonderzoekonderwerpen besproken in het hoofdstuk aanbevelingen.

1 Achtergrondinformatie

Dit hoofdstuk is bedoeld om een beeld in het afstudeerproject te geven. Onderwerpen zoals de projectaanleiding, opdrachtomschrijving, probleemstelling en doelstelling behoren tot de, binnen dit hoofdstuk, beschreven materie.

1.1 Aanleiding

Deze opdracht is tot stand gekomen doordat de afstudeerder zijn studietraject dient af te sluiten met een HBO-waardig onderzoek. Tijdens het eerste kennismakingsgesprek tussen ing. Marc Jonkers en dhr. François Kikken is de keuze op Software Defined Networking als onderwerp gevallen.

1.2 Opdrachtomschrijving

Met behulp van dit project wordt het concept SDN en zijn toepasbaarheid binnen MAASnet inzichtelijk gemaakt. Dit wil zeggen dat de alternatieven binnen de SDN-techniek vergeleken en naast de eisen en wensen van MAASnet geconsidereerd worden. Hieruit ontstaat een doordacht en onderbouwd advies over welke SDN-methodiek en of deze überhaupt geschikt is voor gebruik binnen MAASnet. Hierbinnen wordt rekening gehouden met o.a. een bekabeld- en draadloos netwerk, een studenten- en medewerkers omgeving, de noodzakelijke netwerkbeveiligingseisen en de volwassenheid van de techniek.

1.3 Probleemstelling

Continu verschijnen nieuwe technieken en producten op de markt betreffende de IT-infrastructuur. Om de gebruikservaring van de eindgebruiker optimaal te houden, dient MAASnet mee te gaan met deze constante veranderingen. Echter, voordat een dergelijke verandering doorgevoerd kan worden, dient onderzocht te worden of het aan de eisen en wensen van de afnemer voldoet en tevens toepasbaar is.

1.4 Doelstelling

SDN is één van deze nieuwe technieken, waarvoor een weloverwogen advies naar de meerwaarde, de mogelijkheden en de toepasbaarheid nodig is. Dit geheel dient in de context van MAASnet onderzocht te worden. Het doel van dit project luidt dan als volgt: ***"Het onderzoeken of en welke SDN-techniek geschikt is voor gebruik binnen MAASnet."***

De bovengenoemde doelstelling wordt beantwoord aan de hand van de onderstaande onderzoeksvraag en de daarbij behorende deelvragen. De opsomming vermeldt als eerste de hoofdvraag en vervolgens zijn de daarbij behorende deelvragen, in het niveau daaronder, terug te vinden.

- Is de SDN-techniek geschikt, en zo ja, welke SDN-methodiek, voor gebruik binnen MAASnet?
  - Wat is Software Defined Networking?
  - Welke methodieken bestaan binnen deze techniek?
  - Hoe ziet MAASnet eruit op functioneel- en technisch gebied?
  - Welke eisen en wensen zijn gesteld aan MAASnet?
  - Welke SDN-methodiek is bruikbaar voor MAASnet?
  - Voldoet de SDN-methodiek aan de eisen en wensen van MAASnet?
  - Wat zijn de voor- en nadelen, met de invalshoek naar MAASnet, van de verschillende SDN-methodieken?

2 Methode

Dit hoofdstuk geeft inzicht in de gebruikte werkwijze tijdens het afstudeerproject. De onderzoeksmethode, projectfasering, productanalyse, aanpak en kwaliteitswaarborging zijn de besproken onderwerpen van dit hoofdstuk.

2.1 Onderzoeksmethode

Tijdens het afstudeerproject wordt gebruik gemaakt van een open onderzoeksvraag en -deelvragen. Dit betekent dat de doorgaans gebruikte onderzoeksmethode een kwalitatief onderzoek betreft en verantwoordelijk is voor het aandragen van inzicht in de te onderzoeken materie. Echter, vanwege tijdsgebrek om deze onderzoeksmethode te hanteren, wordt een deskresearch gehanteerd (Hoogers, 2015) (InfoNu, 2015).

2.2 Aanpak en Kwaliteitsborging

Goede projectmanagement- en kwaliteitsborgingsmethodes zijn essentieel voor het succesvol afronden van het afstudeerproject. Gedurende de levenscyclus van dit afstudeerproject is gebruik gemaakt van PRINCE2 als projectmanagementmethode en zowel de MoSCoW- als de Deming-methode voor het waarborgen van de kwaliteit van de diverse producten (Kikken, Software Defined Networking - Project Initiatie Document, 2015) (Kikken, Software Defined Networking - Prestatieplan, 2015).

2.3 Projectfasering

De gehele levenscyclus van het afstudeerproject is opgedeeld in een vijftal faseringen t.w. een oriëntatie-, onderzoeks-, analyse-, advies- en een realisatiefase. Deze faseringen zijn verantwoordelijk voor zowel een gestructureerd als een goed verloop van het afstudeerproject. Elke fase heeft een andere relatie met het afstudeerproject. Zo is de oriëntatiefase verantwoordelijk voor het juist formuleren van de opdracht, onderzoeksvraag en de daarbij behorende doelstellingen. In de onderzoeksfase wordt aan de hand van een literatuurstudie, diverse interviews en een deskresearch informatie geworven. De verworven informatie wordt vervolgens in de analysefase geanalyseerd en gefuseerd tot bruikbare gegevens. Deze gegevens worden in de adviesfase verwerkt tot de beantwoording van de onderzoeksvraag en de daarbij behorende deelvragen. Ten slotte is de realisatiefase verantwoordelijk voor het aantonen van een werkende SDN-omgeving. Een gedetailleerde takenplanning van de diverse fases is terug te vinden in het Project Initiatie Document (Kikken, Software Defined Networking - Project Initiatie Document, 2015).

2.4 Productanalyse

Het mogelijk te adviseren product ontstaat door gebruik te maken van een combinatie tussen een Long-/Shortlist en de MoSCoW-prioritering. De Longlist is een eerste select van mogelijk toepasbare producten en wordt, in het kader van het afstudeerproject, gebaseerd op een tweetal bronnen met beschikbare producten voor het Enterprise Campus netwerk. De Longlist wordt vervolgens met de prioriteringseisen van de MoSCoW-methode geverifieerd en verwerkt tot de Shortlist. De Shortlist bestaat hierdoor uit maximaal twee mogelijk toepasbare producten. Informatie over de producten in de Shortlist worden vervolgens verder uitgewerkt naar de productexplicatie en dient als fundering voor de beantwoording van de diverse deelvragen. Deze beantwoording draagt uiteindelijk zorg voor een wel of niet te adviseren product.

3 MAASnet

MAASnet is het data- en telecommunicatienetwerk van Maastricht University (UM) en wordt geleverd door het ICT Servicecentrum (ICTS). Het netwerk verzorgt o.a. diverse netwerkservices, connectiemogelijkheden voor zowel bekabelde- als draadloze apparatuur, connectie met SURFnet en onderlinge communicatie tussen de 40+ verschillende universiteitsgebouwen. De aangesproken doelgroep van het netwerk is, op het moment van schrijven, circa 15.000 studenten en 4.000 medewerkers (Maastricht University, 2013)[1]. Met behulp van dit hoofdstuk wordt een duidelijker beeld van MAASnet en de gestelde eisen hieraan gecreëerd.

3.1 Netwerkopbouw

Het huidige MAASnet is volledig opgebouwd uit Cisco apparatuur en is ontworpen volgens het Cisco Traditional Hierachical Network Design Model. Dit betekent dat het netwerk opgedeeld is uit drie lagen, namelijk: core-, distribution- en access layer. Door het netwerk op deze manier in te delen, kan aan elke laag een andere functie worden toegewezen.

3.1.1 Core layer

De core laag wordt gezien als de kern, eveneens backbone genoemd, van het netwerk. Deze laag is verantwoordelijk voor een snelle- en betrouwbare afhandeling van pakketten. Dit wordt bewerkstelligd met behulp van een routeringsprotocol dat op basis van het 3e niveau van het Open System Interconnect (OSI) model de bestemming bepaalt. Dit niveau wordt de 'network' laag, eveneens layer 3, genoemd en selecteert op basis van het Internet Protocol (IP) adres. Doordat de core laag verantwoordelijk is voor een snelle- en betrouwbare afhandeling van pakketten, worden pakketten op deze laag tevens niet gemanipuleerd. Onder het manipuleren van pakketten wordt o.a. labellering en filtering verstaan. Routering daar in tegen vindt wel plaats op deze laag.

Binnen MAASnet is deze laag opgebouwd uit een zestal Cisco Catalyst 6500 Series switches. Deze switches zijn uitgevoerd met de Virtual Switching System (VSS) technologie, waardoor gebundelde switches als één switch worden gezien. Hierdoor worden protocollen als Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) en Gateway Load Balancing Protocol (GLBP) overbodig geacht. Daarnaast wordt op deze laag het protocol Enhanced Interior Gateway Routing Protocol (EIGRP) gebruikt. Dit protocol is verantwoordelijk voor het juist routeren van de pakketten.

De Cisco Catalyst 6500 Series switch is een modulaire switch bestaande uit een chassis en losse modules. De modules binnen deze switches dragen zorg voor het aansturen van het draadloos netwerk en haar draadloze Access Points (AP) – besproken in paragraaf 3.1.7 – , de connectie naar het internet en de connectie naar de switches op de distribution layer. De connectie met SURFnet en de distribution layer switches is redundant uitgevoerd en wordt bewerkstelligd met behulp van gebundelde darkfiber lijnen. Deze gebundelde lijnen variëren, afhankelijk van de benodigde doorvoersnelheidseisen, in doorvoersnelheden. Waar nodig, zoals de connectie naar SURFnet of het datacenter, worden 10Gbp/s bundels gebruikt. De bundeling van deze lijnen vindt plaats op basis van het protocol Port Aggregation Protocol (PAgP).

Wat de protocollen betreft, wordt binnen deze laag gebruik gemaakt van het protocol Cisco Discovery Protocol (CDP). Met behulp van dit protocol kunnen routers en switches hun naburige Cisco apparatuur om apparaat informatie vragen. Het Simple Network Management Protocol (SNMP) draagt zorg voor een makkelijke overdracht van managementinformatie van de netwerkapparatuur. Netwerk queuing gebeurt op deze laag met behulp van de Weighted Random Early Detection (WRED) techniek. Hierbinnen wordt een prioriteit op het spraakverkeer gesteld en krijgt dit verkeer voorrang op het overig verkeer. Het voice verkeer wordt bewerkstelligd met behulp van het protocol Session Initiation Protocol (SIP). Ten slotte wordt het Internet Group Management Protocol (IGMP) gebruikt voor het multicastverkeer.

[1] Bron is afkomstig van het intranet (niet publiek toegankelijk) van de universiteit.

3.1.2 Distribution layer

De distribution laag is verantwoordelijk voor de demarcatie tussen de core- en de access laag. Deze laag differentieert zich van de core, doordat pakketten binnen deze laag wel gemanipuleerd worden. Naast het manipuleren, worden o.a. routes samengevoegd, beveiligingsmaatregels toegepast en tussen Virtual Local Area Networks (VLAN) gerouteerd.

Binnen MAASnet is deze laag opgebouwd uit een negental (DIST1 t/m DIST9) distributiewolken en zijn verdeeld over de verschillende locaties van de UM. De Cisco Catalyst 4500 Series switches worden voor deze laag gebruikt en hebben veelal 1Gbp/s glasvezelverbindingen naar de Access laag.

Wat de gebruikte protocollen betreft, wordt op deze laag gebruik gemaakt van o.a. EIGRP, CDP, IGMP, SNMP, SIP, Quality over Service (QoS), Access Control List (ACL), VLAN Trunking Protocol (VTP), Dynamic Trunk Protocol (DTP), en Rapid Per VLAN Spanning Tree Plus (RPVST+). Het protocol Quality of Service (QoS) voorziet het verkeer van een prioriteit. Hierdoor krijgt bijvoorbeeld voice- voorrang op data verkeer. De ACL's en het doel hiervan wordt in paragraaf 3.1.10 beschreven. VTP draagt zorg voor het verspreiden van de VLAN-database naar de Access layer switches. Dit gebeurt met behulp van tien verschillende domeinen. Iedere distributiewolk heeft een apart domein. Om het VTP-verkeer naar de Access switches te versturen en tevens verschillende VLAN's over de desbetreffende verbinding te laten verlopen, wordt gebruik gemaakt van het protocol DTP. Dit protocol wordt statisch op de desbetreffende verbindingen ingesteld. Ten slotte maakt MAASnet, binnen deze laag, gebruik van het protocol RPVST+. Met behulp van dit protocol kunnen zogenaamde switching loops worden voorkomen.

3.1.3 Access layer

De Access layer draagt zorg voor de connectiviteit van de eindgebruiker. Daarnaast is deze laag veelal, in tegenstelling tot de core- en distribution laag, op het 2e niveau van het OSI-model uitgevoerd. Dit niveau wordt de 'data link' laag, eveneens layer 2, genoemd en transporteert het netwerkverkeer op basis van het Media Access Control (MAC) adres. Ten slotte wordt de Access laag voorzien van beveiligingsmaatregels om de netwerkapparatuur te beschermen en het verkeer wordt gesegmenteerd met behulp van VLAN's.

Binnen MAASnet bestaat deze laag uit een 154-tal switches bestaande uit een samenstelling van Cisco Catalyst 3560 Series- en de Cisco Catalyst 4500 Series switches. De Cisco Catalyst 4500 Series is een modulaire switch en is gevuld met diverse modules. De Cisco Catalyst 3560 Series switches daar in tegen is een niet modulair en wordt, indien nodig, via een glasvezel verbinding met elkaar verbonden. Daarnaast is het merendeel van deze switches of modules uitgevoerd met de Power over Ethernet (PoE) technologie. Hierdoor kan netwerkapparatuur worden voorzien van stroom over de ethernetbekabeling.

Wat de op deze laag gebruikte protocollen betreft, wordt gebruik gemaakt van RPVST+, CDP, SNMP, QoS, VTP, DTP en SIP. Voor VTP wordt gebruik gemaakt van de modus cliënt. Hierdoor kan vanuit de Access laag geen aanpassingen naar de VLAN-database gemaakt worden. Ten slotte is het protocol DTP, tevens op deze laag, statisch ingesteld.

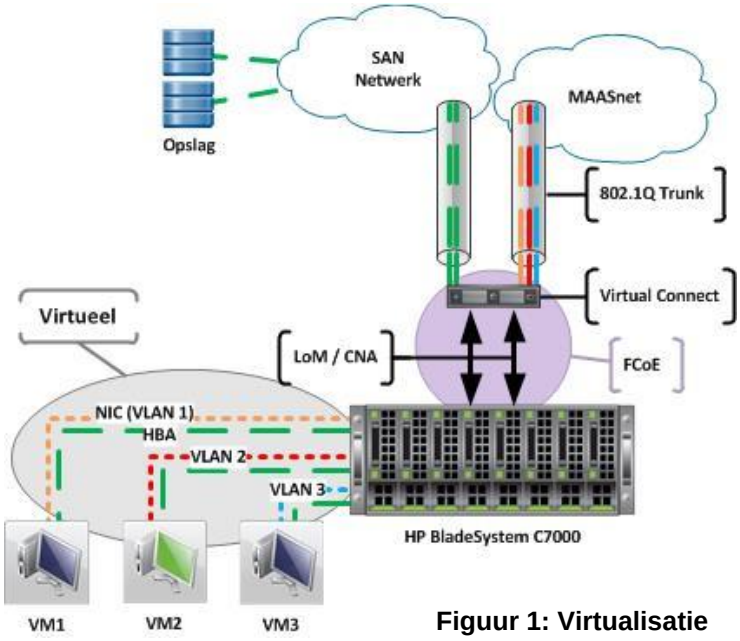
3.1.4 Internetconnectie

De UM maakt gebruik van twee verschillende Internet Service Providers (ISP), namelijk SURFnet en Ziggo. De internetconnectie via Ziggo wordt gebruikt om de bezoekers van de UM, bij speciale activiteiten zoals opendagen, te voorzien van een internetconnectie. Door deze werkwijze te hanteren, is het niet noodzakelijk om voor elke gebruiker een tijdelijk account te maken. De connectie met SURFnet wordt gebruikt om het gehele MAASnet te voorzien van een internetconnectie. Deze connectie is met behulp van een primary- en secondary- 10Gbp/s glasvezelverbinding aangesloten op de core laag. De verbindingsaansluiting vindt plaats op laag 3 van het OSI-model en gebruikt het protocol Border Gateway Protocol (BGP) voor routering naar het internet. Daarnaast wordt een internetverbinding voor de gelieerde bedrijven verzorgd. Deze verbinding heeft eveneens een aansluiting naar SURFnet. Echter, de verbindingsaansluiting vindt plaats op laag 2 van het OSI-model. In alle bovenstaande gevallen, die connectie met SURFnet maken, wordt gebruik gemaakt van de Cisco Catalyst 3560 Series switch om de internetconnectie mogelijk te maken.

3.1.5 Serverfarm

Het serverfarm van de UM bestaat uit een collectie virtuele servers (VM) en worden beheerd met behulp van een VMware vSphere Hypervisor. Daarnaast wordt gebruik gemaakt van F5 Load Traffic Manager (LTM) modules om op een veilige manier het netwerkverkeer over meerdere servers te verdelen. De achterliggende hypervisorarchitectuur wordt op twee verschillende manieren, afhankelijk van het doeleinde hiervan, bewerkstelligd. Zo wordt gebruik gemaakt van VM's met lokale opslag en VM's die een Storage Area Network (SAN) als opslagmedium benutten. De VM's met lokale opslag bieden functionaliteit om nieuwe technieken en methodieken te testen. De VM's met SAN-opslag worden gebruikt voor daadwerkelijke productie applicaties, zoals SAP, Exchange, et cetera. De 'rekenkracht' van de VM's wordt bewerkstelligd met een aantal fysieke servers (VM-hosts). Deze servers zijn geplaatst in een viertal, twee per geografische gescheiden locatie, HP BladeSystem C7000 Chassis.

Om connectiviteit met de SAN-opslag en MAASnet te maken, is ieder HP BladeSysteem C7000 Chassis voorzien van een tweetal 10Gbit/s Virtual Connect modules. Deze modules maken, via LAN on Motherboard (LoM), verbinding met de verschillende VM-hosts. Dit is een converged network adapter (CNA) direct aangesloten op het moederbord van het HP BladeSysteem C7000 Chassis. Een CNA combineert de connectiefunctionaliteiten van een host bus adapter (HBA) – gebruikt voor aansluiting met het SAN-netwerk – en een network interface card (NIC) – gebruikt voor netwerkconnecties – tot één enkele connectiemethodiek. Het protocol dat voor deze methodiek wordt gebruikt, is Fiber Channel over Ethernet (FCoE). De connectie tussen de VM-host en de diverse VM's vindt geheel virtueel plaats. Hierdoor worden instellingen, zoals bandbreedte, VLAN-toewijzing, MAC-adressering, et cetera gecoördineerd door de Hypervisor. Figuur 1 geeft een duidelijker beeld hoe de virtuele omgeving met SAN-opslag in elkaar zit.



Figuur 1: Virtualisatie

3.1.6 Connectiemogelijkheden

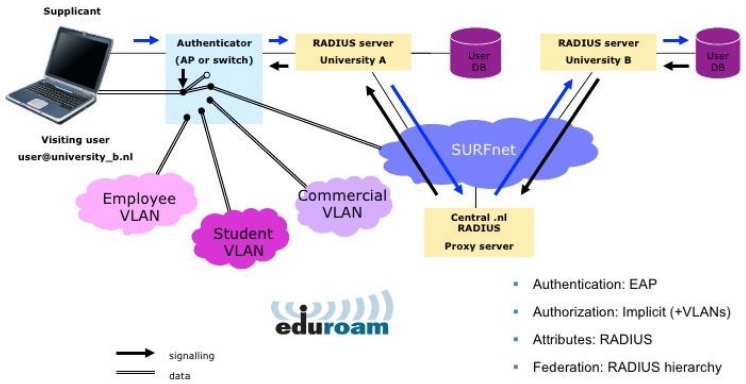
Gebruikers en apparatuur kunnen op diverse manieren een connectie maken met MAASnet, namelijk via een bekabelde MAASnet aansluiting, een draadloze verbinding en een Virtual Private Network (VPN) verbinding. Een connectie via een bekabelde MAASnet aansluiting is echter gelimiteerd tot een drietal apparaten. De connectiepoorten maken namelijk gebruik van de techniek port-security. Met behulp van deze techniek worden de, op de poort aangesloten, MAC-adressen op de switch bijgehouden. In geval van een overschrijding van het maximaal aantal MAC-adressen, wordt de poort in een error-disabled modus geplaatst en toegang tot het netwerk geblokkeerd. Een connectie via het draadloze netwerk kan daar in tegen wel meerdere apparaten bevatten. De connectie via dit middel is afhankelijk van de eindgebruikersdoelgroep en de daarbij behorende Service Set Identifier (SSID). Paragraaf 3.1.7 geeft een verduidelijking welke eindgebruikersdoelgroep bij welke SSID hoort en hoe deze dit draadloos netwerk is opgebouwd. Ten slotte bestaat de mogelijkheid om via een VPN-verbinding een connectie met MAASnet te maken. Echter, deze verbinding vindt niet op een van de fysieke locaties van de UM plaats. Deze connectie wordt bewerkstelligd met een gecodeerde tunnel over het publieke internet.

3.1.7 Draadloos

Het draadloos communicatienetwerk wordt bewerkstelligd door een viertal Cisco Wireless Service Modules (WiSM2) en circa 1100 – diverse modellen – Cisco AP's. De WISM2's zijn geplaatst in het chassis van de Cisco Catalyst 6500 Series switches op de Core laag en zijn in een high availability pair uitgevoerd. De diverse AP's daar in tegen zijn aangesloten op de Access laag. Deze worden tevens, door de op de access switches ingestelde PoE-techniek, voorzien van stroomtoevoer. Door gebruik te maken van een WISM2 worden AP's centraal beheerd en stroomt al het dataverkeer door de controller heen. Het protocol Control And Provisioning of Wireless Access Points (CAPWAP) wordt gebruikt voor de control- en datacommunicatie tussen beide apparaten.

De connectiviteit wordt bewerkstelligd met een drietal verschillende draadloze netwerken, ieder corresponderend aan een andere eindgebruikersdoelgroep, bijbehorend(e) SSID('s) en VLAN('s). De verschillende SSID's zijn: UMnet, UMguest en eduroam. UMnet en UMguest zijn initiatief van de UM en zijn bedoeld voor de connectiviteit van medewerkers (UMnet) en gasten (UMguest). Voor authenticatie en autorisatie wordt gebruik gemaakt van de Institute of Electrical and Electronics Engineers (IEEE) 802.1x standaard en is bedoeld voor Port-based Network Access Control (PNAC). Deze standaard maakt het mogelijk om, aan de hand van een domeinaccount en wachtwoord, de toegangsrechten tot het netwerk te bepalen. Studenten aan de UM maken gebruik van eduroam.

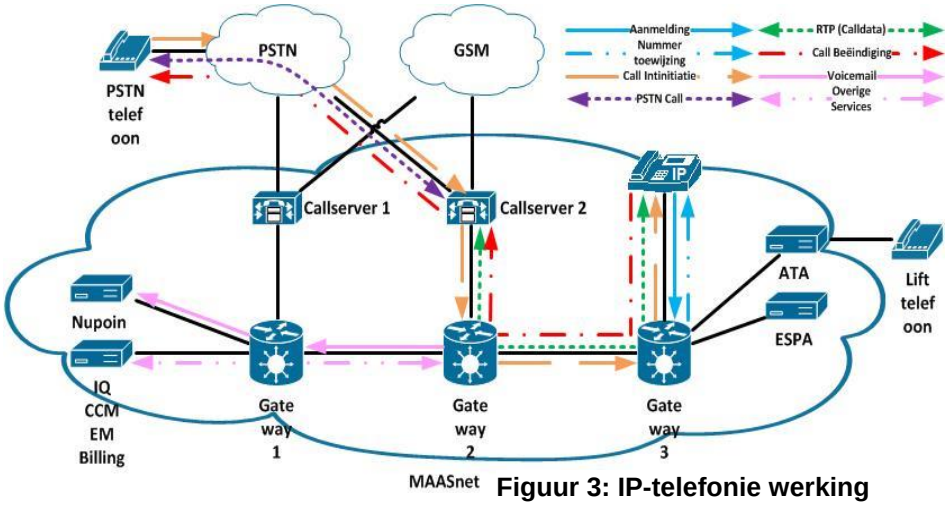
Eduroam is een initiatief van SURFnet en is bedoeld om medewerkers en studenten van onderwijs- en onderzoeksinstellingen te voorzien van een internetconnectie op alle, aan SURFnet, aangesloten instellingen. De connectie hiervan gebeurt geheel met inloggegevens van de eigen instelling. De gebruiker wordt dus geauthentiseerd door zijn eigen instelling en geautoriseerd door de instelling waar hij connectie met eduroam maakt. Hierdoor kan de eindgebruiker, vanuit het gebruikersperspectief gezien, zijn eigen apparatuur gebruiken alsof hij binnen zijn eigen instelling aan het werk is. Om dit mogelijk te maken, wordt gebruik gemaakt van de IEEE 802.1x standaard met een Remote Authentication Dial In User Service (RADIUS) federatie hiërarchie. Figuur 2 geeft een duidelijker beeld hoe het authenticatie- en autorisatie proces werkt.



Figuur 2: eduroam (Cisco Systems, 2012)

3.1.8 Telefonie

De gehele UM maakt gebruik van IP-telefonie. Met behulp van deze techniek wordt het mogelijk gemaakt om telefoonverkeer over het datanetwerk te transporteren. Het protocol dat hiervoor gebruikt wordt, is het protocol SIP. De apparatuur die hiervoor benodigd is, bestaat uit o.a. Mitel Mxe Server, Mitel Mxe Gateway, Mitel Nupoint, Mitel IQ/CCM/EM, ATA-connector en een SIP - ESPA convertor. De onderstaande sub paragrafen geven een verduidelijking in welk apparaat welke functie vervult. Daarnaast geeft figuur 3 een verduidelijking in de werking van een IP-telefoniegesprek.



Figuur 3: IP-telefonie werking

3.1.8.1 Mxe Server

De Mxe server, eveneens call server genoemd, is het belangrijkste apparaat binnen een SIP IP-telefonie architectuur. Deze server is verantwoordelijk voor het initiëren en verbreken van de spraakcommunicatieverbinding. De verbinding zelf wordt bewerkstelligd met het protocol Realtime Transport Protocol (RTP) en is daardoor niet afhankelijk van de call server. Verder verzorgt deze server de connectie met het public switched telephone network (PSTN)-[2] en het Global System for Mobile Communications (GSM)[3] netwerk. Hierdoor is de call server verantwoordelijk voor het transleren van PSTN- en GSM- naar IP-telefonie verkeer. Binnen MAASnet is deze server redundant uitgevoerd op een fysiek gescheiden locatie en ontstaat, zelfs bij calamiteiten, een high-available situatie.

3.1.8.2 Mxe Gateway

De Mitel Mxe Gateway is eveneens een fysiek apparaat en is verantwoordelijk voor connectie tussen de diverse apparatuur, het routeren van gesprekken en het uitdelen van telefoonnummers. Daarnaast is dit het connectiepunt waar gebruikers, via hun telefoontoestel, inloggen. Binnen MAASnet is dit apparaat drie maal uitgevoerd, elk op een fysiek gescheiden locatie.

3.1.8.3 Nupoint

Mitel Nupoint is een apparaat verantwoordelijk voor voicemail services. Dit apparaat is, binnen MAASnet, fysiek uitgevoerd en enkel op één locatie aanwezig. Indien een gebruik als niet beschikbaar wordt geacht, wordt het gesprek naar dit apparaat herleid. De persoon, die het gesprek geïnitieerd heeft, krijgt hier de mogelijkheid om een bericht achter te laten of de verbinding te verbreken. Indien een bericht achter gelaten is, krijgt de gespreksontvanger een melding hiervan.

3.1.8.4 IQ/CCM/EM

Dit apparaat bestaat, binnen MAASnet, uit een fysieke server met diverse virtuele machines. Deze machines vervullen iedere een andere functie, zoals Intelligence Queue (IQ), contact center management (CCM), Enterprise Messaging (EM) en kostenregistratie. Zo zijn IQ en CCM hulpmiddelen voor het callcenter en is EM verantwoordelijk voor de opslag van alle voicemail berichten.

3.1.8.5 ATA-connector

Aan de hand van dit apparaat wordt het mogelijk gemaakt om ‘oudere’ PSTN-apparatuur (lifttelefoons, modems, faxen, et cetera) aan te sluiten op het IP-telefonie netwerk.

3.1.8.6 SIP - ESPA

Het vertalen van signalen afkomstig van brandmeld- en beveiligingssystemen, wordt bewerkstelligd met dit apparaat. Het analoge signaal wordt vertaald naar een signaal dat met het protocol SIP afgehandeld kan worden.

[2] PSTN: Netwerk bedoeld voor de communicatie via analoge telefonie.
[3] GSM: Netwerk bedoeld voor de communicatie via mobiele telefonie.

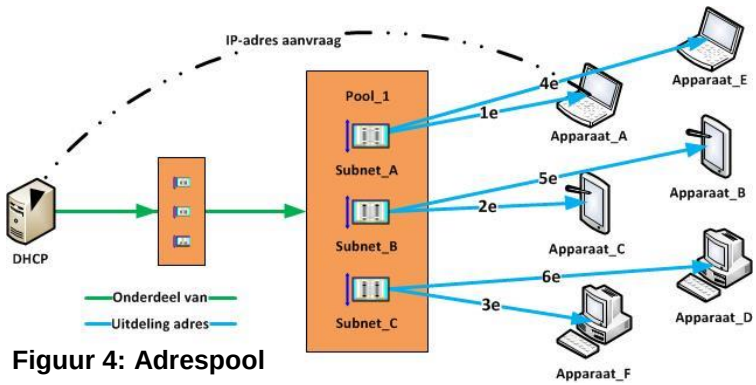
3.1.9 Adressering

Binnen MAASnet worden de netwerkapparaten van een IP-adres en het netwerkverkeer van een VLAN-ID voorzien. Hiermee wordt het mogelijk gemaakt om netwerkapparatuur met elkaar te laten communiceren en tevens juiste beveiligingsmaatregels te treffen. Met behulp van de onderstaande sub paragrafen wordt de gebruikte adressering voor IP-adressen en VLAN-toewijzing inzichtelijk gemaakt.

3.1.9.1 IPv4

SURFnet levert een publieke IP versie 4 (IPv4) adressering van 137.120.0.0 met een subnet van 16 aan de UM. Dit wil zeggen dat de IP-adressen 137.120.0.1 t/m 137.120.255.254 gebruikt worden voor adrestoewijzing. Dit komt neer op 65.536 adressen. Om beveiliging, bandbreedte en beheermogelijkheden binnen deze adresseringsrange te verbeteren, worden de adressen opgedeeld in diverse subnetten. De eerste verdeling vindt plaats op de diverse distributiewolken. Deze krijgen, afhankelijk van de grootte en het verwachtte groeipatroon, een blok IP-adressen toegewezen. Deze blokken worden vervolgens verder onderverdeeld in subnetten voor de VLAN's binnen de desbetreffende distributiewolk. Doordat de grootte en het verwachtte groeipatroon meespelen in de bepaling van het formaat, is van consistentie binnen de subnetten geen sprake. Zo zijn bijvoorbeeld de eerste 32 subnetten gereserveerd voor adressering van de servers en worden 30 subnetten, van ieder 512 adressen, voor de adressering van het draadloos netwerk gebruikt.

De uitdeling van adressen gebeurt met behulp van Infoblox apparatuur (te weten: Infoblox Trinzic DDI 1420 en Infoblox GRID). Deze apparatuur is gespecialiseerd op het managen en identificeren van IP-adressen en Domain Name System (DNS) verwijzingen. De uitdeling van distributiewolk overlappende VLAN's, zoals het VLAN voor het draadloos netwerk, gebeurt aan de hand van zo genaamde adrespools. Hoe deze uitdeling werkt, wordt met behulp van figuur 4 inzichtelijk gemaakt. Binnen deze afbeelding hebben de nummers 1e t/m 6e betrekking op de aanvraagvolgorde van een IP-adres en de oranje vlakken betrekking op softwarematige instellingen. Door het gebruik van deze techniek, worden de adressen en tevens de daarop aansluitende bandbreedte van de diverse VLAN's gelijkmatig verdeeld. Deze techniek is echter wel alleen van toepassing op apparaten die connectie maken met een overlappend VLAN niet tot zeer specifiek VLAN behoren. Verder worden adrespools ontworpen op basis van geografische locaties. Zo is bijvoorbeeld een adrespool voor de locaties in de binnenstad en een pool voor de locaties in Randwyck gemaakt.



Figuur 4: Adrespool

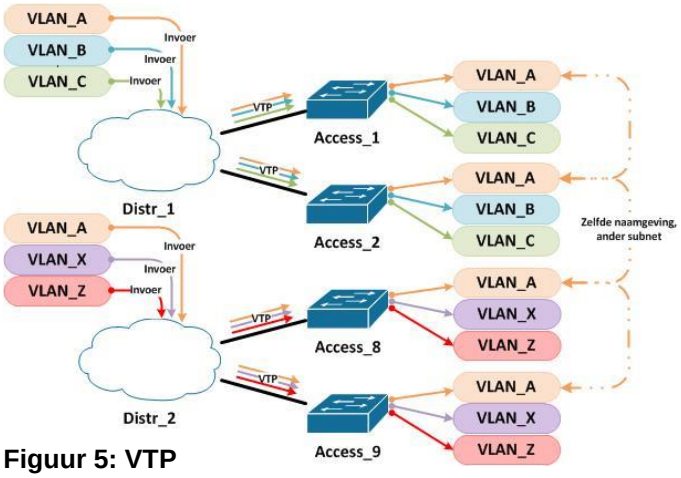
Ten slotte wordt, naast de publieke IPv4 adressering, gebruik gemaakt van een tweetal privé IPv4 adresseringsplannen. Eén van deze adresseringsplannen heeft betrekking op de apparatuur die geen internetconnectie vereist, zoals printers, camerasystemen, et cetera. De hiervoor gebruikte adressering bestaat uit adressen uit de 10.x.y.0 range met elk een subnet van 24 en betekent dat, per subnet, 254 adressen beschikbaar worden gesteld. Daarnaast geeft 'x' aan op welke distributiewolk en 'y' op welk VLAN dit subnet betrekking heeft. Het andere adresseringsplan heeft betrekking op het open draadloos netwerk wat de connectiviteit verzorgt naar de internetconnectie van Ziggo. De hiervoor gebruikte adressenrange bedraagt 172.16.0.0 met een subnet van 16 en komt neer op 65.536 beschikbare adressen.

3.1.9.2 IPv6

MAASnet maakt, op het moment van schrijven, nog geen gebruik van een IP versie 6 (IPv6) adressering. Het adresseringsplan is daar in tegen wel al ontworpen en toegekend door SURFnet. De adresseringsrange 2001:0610:0190:: met een subnet van 48 wordt aangeleverd door SURFnet en komt neer op 1.208.925.819.614.629.174.706.176 beschikbare adressen.

3.1.9.3 VLAN

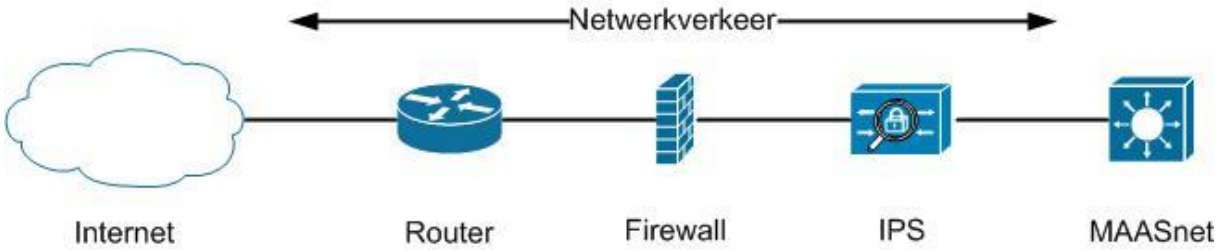
Binnen MAASnet worden VLAN's gebruikt om netwerkverkeer van elkaar te scheiden en tevens een duidelijke structuur hierin te behouden. Zo is bijvoorbeeld een scheiding tussen bekabeld- en draadloos-, studenten- en medewerkers-, server- en voice netwerverkeer aanwezig. Dit verkeer wordt weliswaar al opgedeeld door subnetten. Door de combinatie met VLAN's te maken, wordt een duidelijke structuur gecreëerd en kunnen verschillende netwerken – naast elkaar – op hetzelfde broadcastdomein functioneren. Daarnaast is het toepassen van beveiligingsmaatregels veel overzichtelijker met behulp van VLAN's. De VLAN-databases, vanuit de distribution- naar de access laag switch, verstuurd met het protocol VTP. De instellingen die daarmee gepaard gaan, zijn 'server' op de distribution-, 'client' op de access laag en het domein waarin beide opereren. Hierdoor worden de databases aangemaakt, gewijzigd en verwijderd op de distribution laag. Hoe deze techniek werkt, wordt aan de hand van figuur 5 verduidelijkt. MAASnet maakt, per distributiewolk, gebruik van een ander domein om de databases naar de access laag switches te verspreiden. Overlappende VLAN's – zoals in figuur 5 weergegeven – hebben dezelfde naamgeving, maar behoren tot een ander subnet.



Figuur 5: VTP

3.1.10 Beveiliging

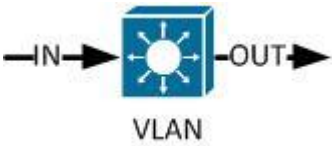
MAASnet wordt beveiligd met behulp van hardware appliance firewalls, ACL's en een Intrusion Prevention System (IPS). Figuur 6 maakt inzichtelijk hoe dit wordt bewerkstelligd. De ACL's bevinden zich op diverse distribution layer switches binnen de verschillende distributiewolken.



Figuur 6: Netwerkbeveiliging

Al het netwerkverkeer afkomstig van- of met een bestemming buiten MAASnet, dient door de firewalls en IPS'en heen te gaan. De firewalls binnen MAASnet zijn zodanig ingesteld dat al het inkomende verkeer, op een aantal veel gebruikte protocollen na, wordt geblokkeerd (default deny mentaliteit). Al het, op een aantal protocollen na, uitgaande verkeer kan daar in tegen zonder enig probleem het netwerk verlaten (default permit mentaliteit). Daarnaast wordt gebruik gemaakt van stateful packet inspection. Deze techniek zorgt ervoor dat uitgaande connecties worden bijgehouden en het daarbij behorende inkomende verkeer wordt toegelaten tot MAASnet. De IPS'en zijn verantwoordelijk voor het monitoren van zowel het inkomend- als het uitgaand verkeer. Indien de IPS malafide verkeer ontdekt, voert deze (afhankelijk van de ingestelde policy) een actie uit. Daarnaast wordt deze ongeoorloofde activiteit gerapporteerd naar de beheerders.

Het netwerkverkeer binnen MAASnet wordt gesegmenteerd met behulp van VLAN's en vervolgens voornamelijk bij de server VLAN's gefilterd met ACL's. Door het gebruik van segmentatie kunnen diverse netwerken binnen MAASnet gescheiden blijven, nochtans van alle functionaliteiten genieten. De ACL's bevinden zich, zoals eerder in deze paragraaf beschreven, op de distribution layer switches binnen de diverse distributiewolken en worden toegepast op de VLAN-interfaces. Dit zijn virtuele interfaces op een switch of router en hebben betrekking op het desbetreffende aansluitend VLAN. De ACL's filteren het inkomende- en uitgaande verkeer (figuur 7 geeft hier verduidelijking in) en hebben voornamelijk betrekking op de VLAN's waarin de servers van elke faculteit zich bevinden. De regels binnen de ACL's zijn per VLAN verschillend en kunnen aan de hand van een request for change (RFC) ticket worden gewijzigd.

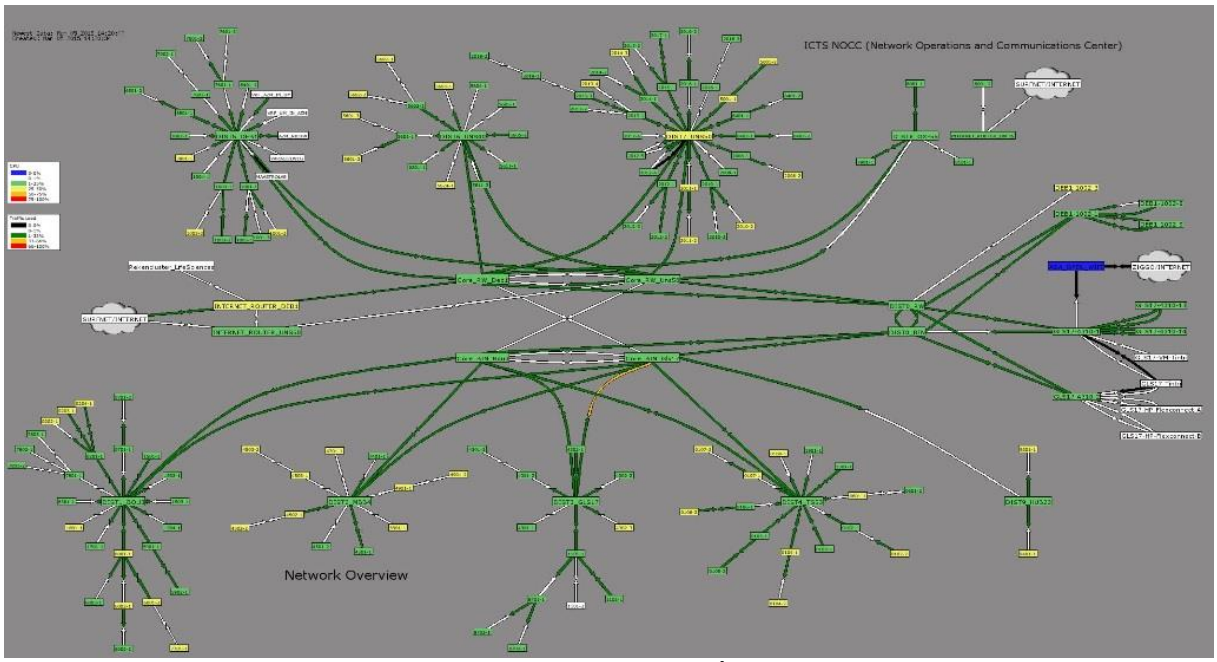


Figuur 7: VLAN ACL

Wat de beveiliging van fysieke netwerkaansluitingen betreft, wordt gebruik gemaakt van best practice methodes. Deze methodes zijn ontstaan door eerder gerapporteerde incidenten van diverse leveranciers van IT-infrastructuur. Vervolgens worden de oplossingen m.b.t. de incidenten getest en de oplossingen gepubliceerd door de fabrikant van de netwerkapparatuur. DHCP-snooping, port-blocking, niet gebruikte poorten uitgeschakeld, BPDU-guard, et cetera maken o.a. onderdeel uit van deze methode. (Cisco Systems, 2008)

3.1.11 Topologie

In figuur 8 is een visuele weergave van MAASnet terug te vinden. Deze afbeelding is van een dusdanig formaat gemaakt, zodat de tekstuele eigenschappen binnen deze afbeelding niet leesbaar zijn.



Figuur 8: Netwerkoverzicht (Maastricht University, 2015)[4]

[4] Bron is afkomstig van het intranet (niet publiek toegankelijk) van ICTS-Netwerken.

3.2 Eisen

ICTS streeft om een betrouwbaar- en stabiel netwerk te leveren aan de UM. Om dit te bewerkstellen zijn een aantal aspecten in een Service Level Agreement (SLA) opgenomen. De aspecten zijn hierdoor onderdelen waaraan het netwerk moet voldoen. De belangrijkste aspecten hiervan worden in deze paragraaf opgenomen.

MAASnet dient continu – dan wel 24 uur per dag, 7 dagen per week, 365 dagen per jaar – beschikbaar te zijn voor haar gebruikers. De garandeerde beschikbaarheid bedraagt 95% en komt neer op een maximale uitvaltijd van 18,25 dagen per jaar. Daarnaast mogen gebruikers, tijdens het gebruik van MAASnet, geen vertragingen of wachttijden te ondervinden. De onderstaande opsomming geeft een overzicht van de opgestelde maximale verbindingscapaciteit aan de bekabeling en apparatuur van MAASnet.

- 100 Mbit/s - 1 Gbit/s per aansluitpunt;
- 2 Gbit/s per distributie punt;
- 20 Gbit/s MAASnet core;
- 54 Mbit/s aansluitpunt draadloos netwerk[5];
- 10 Gbit/s aansluiting met SURFnet.

Verder dient MAASnet uit een bekabelde- en een draadloze infrastructuur, met hierbinnen een opdeling tussen een medewerkers- en studenten omgeving, te bestaan. Deze infrastructuur biedt daarnaast functionaliteiten, zoals ontsluiting met het internet (SURFnet), externe MAASnet toegang (VPN), internet adresseringen, IP-telefonie, connectie tot diverse applicatieservers en connectie tot print- en scanfaciliteiten.

Ten slotte dient MAASnet van optimale beveiligingsmaatregels te genieten. Dit wordt bewerkstelligd met behulp van IPS'en, ACL's en firewalls. (Kooij, 2013)

3.3 Wensen

Op het moment van schrijven zijn enkele pilots, binnen MAASnet, in bedrijf. Een pilot is een project dat zich in een testfase bevindt en is daardoor niet zeker van integratie. De pilots worden in deze categorie meegenomen en hierdoor in acht gehouden bij het uiteindelijk advies. De pilots hebben betrekking op de onderwerpen Surfdrive, Unified Communications en Virtual Desktop Infrastructure (VDI).

SURFdrive is een initiatief van SURFnet en in nauwe samenwerking met CvDUR (ICT-directeuren van de aangesloten universiteiten) gerealiseerd. SURFdrive is ontstaan door de vraag naar functionele voordelen van een cloudopslagdienst te combineren met Nederlandse en Europese privacywetgeving. Veel commerciële cloudopslagdiensten kunnen deze combinatie niet garanderen of leveren. Daarnaast wordt de data, op een veilige en bekende locatie, in Nederland opgeslagen en nooit aan derden verstrekt. (SURFnet, 2015)

Unified Communications is een concept waarbij diverse communicatieservices met elkaar worden gecombineerd. Onder communicatieservices vallen o.a. Instant Messaging (IM), IP-telefonie, video conferentie, voicemail en bureaublad deling. Door deze services met elkaar te combineren worden communicatieservices beter te beheren, apparaat onafhankelijker en gebruiksvriendelijker voor de eindgebruiker. (Wikipedia, 2015)

Een VDI-omgeving is een bureaublad-georiënteerde service en draagt zorg voor een bring-your-own-device-concept. Dit concept wordt bewerkstelligd, doordat de bureaubladomgeving van de eindgebruiker zich op een VM-host bevindt. De verwerking van de bureaubladomgeving en de daarbij behorende data vindt, in zijn geheel, plaats op deze VM-host. Om de omgeving te kunnen benaderen wordt gebruik gemaakt van een remote-display protocol en een connection-broker service. Door deze combinatie te maken keert de eindgebruiker, bij het verliezen van connectiviteit, terug naar zijn juiste omgeving en is de verbinding apparaat-onafhankelijk.

[5] Gebaseerd op de maximale snelheid van het laagst aangeboden protocol (IEEE 802.11g).

3.4 Conclusie

De deelvraag ***"Hoe ziet MAASnet eruit op functioneel- en technisch gebied?"*** kan met behulp van de bevindingen in paragraaf 3.1 worden beantwoord. MAASnet is een complex computernetwerk dat de verschillende faculteiten van de universiteit voorziet van zowel data- als telefonieverkeer. Dit verkeer vindt zowel intern (binnen de gehele universiteit), extern (over het internet), draadloos als bekabeld plaats en beschikt over een gebruikersaantal van circa 19.000 personen. Het gebruikersaantal is opgebouwd uit ongeveer 15.000 studenten en 4.000 medewerkers.

Alle netwerkapparatuur binnen MAASnet is afkomstig van de fabrikant Cisco System en bestaat uit een productencatalogus van zowel de Catalyst 6500-, Catalyst 4500-, Catalyst 3560 series, WISM2, diverse Aironet Access Point series als de ASA 5585-X Adaptive Security Appliance. De internetconnectie (geleverd door SURFnet en Ziggo) en het IPS-systeem worden verzorgd door een drietal Catalyst 3560E-12D-E switches met IPS software. Naast de Cisco Systems apparatuur maakt MAASnet gebruik van Mitel MiVoice-, Infoblox DDI- en F5 LTM apparatuur voor het creëren van zowel een IP-telefonie omgeving als het beheren van netwerkadresseringen.

De onderstaande opsomming geeft een overzicht van de functionaliteiten die met behulp van deze apparatuur wordt bewerkstelligd.

- Netwerksegmentatie aan de hand van VLAN's en subnets;
- Netwerkroutering met behulp van de protocollen EIGRP en BGP;
- Netwerkfiltering aan de hand van ACL's, IPS-systemen en firewalls;
- Netwerktoegang met behulp van de IEEE standaard 802.1X;
- Externe netwerktoegang aan de hand van VPN-techniek
- Netwerkprioritering aan de hand van QoS en WRED;
- IP-telefonie met behulp van het protocol SIP en Mitel MiVoice apparatuur;
- Netwerk adresseringsmanagement met behulp van Infoblox apparatuur;
- Stroomvoorzieningen met behulp van de PoE-techniek.

Ten slotte bestaat het serverfarm van MAASnet uit een collectie virtuele servers die vanuit een VMware vSphere Hypervisor worden beheerd. De hiervoor gebruikte achterliggende architectuur wordt op twee verschillende manieren, afhankelijk van het doeleinde hiervan, bewerkstelligd. Zo wordt gebruik gemaakt van VM's met lokale opslag en VM's die een Storage Area Network (SAN) als opslagmedium benutten. De VM's met lokale opslag bieden functionaliteit om nieuwe technieken en methodieken te testen. De VM's met SAN-opslag worden gebruikt voor daadwerkelijke productie applicaties, zoals SAP, Exchange, et cetera. De 'rekenkracht' van de VM's wordt bewerkstelligd met een aantal fysieke servers (VM-hosts). Deze servers zijn geplaatst in een viertal, twee per geografische gescheiden locatie, HP BladeSystem C7000 Chassis

Met behulp van de bevindingen uit de paragrafen 3.1, 3.2 en 3.3 wordt beantwoording van de deelvraag ***"Welke eisen en wensen zijn gesteld aan MAASnet?"*** mogelijk gemaakt. Wat de eisen betreft dient MAASnet, voor zowel de bekabelde- als de draadloze netwerkinfrastructuur, over een continue netwerksegmentatie van de medewerkers- en studenten omgeving te beschikken. Naast segmentatie tussen deze omgevingen dient segmentatie op o.a. faculteiten, afdelingen, zowel gebruikers- als apparaat groepen en netwerkfunctionaliteiten (bijv. VPN-verkeer, IP-telefonieverkeer, et cetera) eveneens plaats te vinden. Verder dient MAASnet continu – dan wel 24 uur per dag, 7 dagen per week, 365 dagen per jaar – beschikbaar te zijn voor haar gebruikers. De garandeerde beschikbaarheid bedraagt 95% en komt neer op een maximale uitvaltijd van 18,25 dagen per jaar. Daarnaast mogen gebruikers, tijdens het gebruik van MAASnet, geen vertragingen of wachttijden te ondervinden. De onderstaande opsomming geeft een overzicht van de opgestelde maximale verbindingscapaciteit aan de bekabeling en apparatuur van MAASnet.

- 100 Mbit/s - 1 Gbit/s per aansluitpunt;
- 2 Gbit/s per distributie punt;
- 20 Gbit/s MAASnet core;
- 54 Mbit/s aansluitpunt draadloos netwerk[6];
- 10 Gbit/s aansluiting met SURFnet.

[6] Gebaseerd op de maximale snelheid van het laagst aangeboden protocol (IEEE 802.11g).

Wat de wensen van MAASnet betreft, worden een drietal pilots meegenomen naar het uiteindelijke toepasbaarheidsadvies. Dit drietal pilots bestaat uit het SURFdrive-, Unified Communications- en het VDI-project.

4 Software Defined Networking

Dit hoofdstuk draagt zorg voor een verduidelijking van het concept SDN en de werking hiervan. Echter, om een goed beeld van de werking van SDN te krijgen, is kennis van de werking van traditionele netwerken essentieel. Het vergaren van deze benodigde kennis – indien niet aanwezig – kan aan de hand van de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 12-14) geschieden. Naast zowel het concept als de werking hiervan worden de diverse SDN-modellen en -uitvoeringen in dit hoofdstuk beschreven.

4.1 Wat is Software Defined Networking?

Software Defined Networking is, op het moment van schrijven, een nieuw architecturaal netwerk design. Binnen dit concept wordt het controle- van het data (forwarding) draagvlak gescheiden en op een centrale locatie binnen het netwerk geplaatst. Daarnaast worden forwarding besluiten gebaseerd op flows en policy's. Deze aanpak draagt zorg voor een gesimplificeerd, gecentraliseerd en programmeerbaar computernetwerk.

SDN heeft bij iedere belanghebbende partij een andere definitie. Doordat Open Network Foundation (ONF) helemaal is toegewijd aan SDN en één van de eerste SDN-communicatie standaarden (t.w. OpenFlow) heeft voorgesteld, wordt de definitie van ONF als leidraad in dit document gebruikt. (Open Networking Foundation , 2015) benoemd de definitie als volgt:

> *Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.* (p.1)

Door de grote hoeveelheid verschillende definities – meerdere SDN-definities zijn terug te vinden in de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015, p. 15) – en interpreteringen van SDN kan verwarring ontstaan of een product nu wel of geen SDN-product is. Deze verwarring wordt opgeheven door een zestal eigenschappen op te stellen. Om tot de categorie SDN-producten te behoren, dient een product aan deze eigenschappen te voldoen. De eigenschappen zijn: draagvlak splitsing, simplificeerde apparatuur, gecentraliseerd beheer, openheid en zowel netwerkautomatisering als netwerkvirtualisatie (Göransson & Black, 2014).

4.1.1 Draagvlak scheiding, gecentraliseerd beheer en simplificeerde apparatuur

De eerste drie eigenschappen (te weten: Draagvlak scheiding, gecentraliseerd beheer en simplificeerde apparatuur) kunnen als één eigenschap worden gezien. Deze drie eigenschappen sluiten op elkaar aan en zijn logische vervolgstappen van elkaar. Als eerste wordt een scheiding tussen het controle- en data (forwarding) draagvlak toegepast. De doelstelling en functionaliteiten van de verschillende draagvlakken is in (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 13-14) beschreven. Door deze scheiding toe te passen is het mogelijk om de intelligentie van het netwerkapparaat (t.w. het controledraagvlak) te verplaatsen naar een gecentraliseerde locatie en ontstaat een gecentraliseerde locatie om het netwerk te beheren. Door deze verplaatsing hoeft het netwerkapparaat geen complexe berekeningen meer uit te voeren om een overzicht van het netwerk te creëren en ontstaat een gesimplificeerd netwerkapparaat.

4.1.2 Netwerk- automatisering en virtualisatie

Binnen de softwareprogrammeringswereld heeft Barbara Liskov de 2008 Turning Award gekregen voor het object-georiënteerd programmeringstaalontwerp. Zij zei: *"Modularity based on abstraction is the way things get done"* (Shenker, 2011) over Computer Wetenschappen. Volgens Shenker is abstractie binnen een SDN-netwerk eveneens van groot belang. Hij benoemde de abstracties van een gedistribueerde staat, van forwarding en van configuratie als de drie vereisten van een SDN-netwerk. Aan de hand van deze abstracties wordt een globaal netwerkoverzicht gecreëerd, waarbij geen kennis van de onderliggende netwerkapparatuur nog de diverse configuraties benodigd is. De abstractie ontstaan door het toepassen van een SDN-controller met de daarbij behorende Application Programming Interface (API)'s (zie paragraaf 4.2 voor meer informatie over de diverse API's). Deze API's dragen zorg voor één of meerdere gestandaardiseerde communicatieprotocollen en programmeertalen waardoor automatisering en virtualisatie mogelijk wordt.

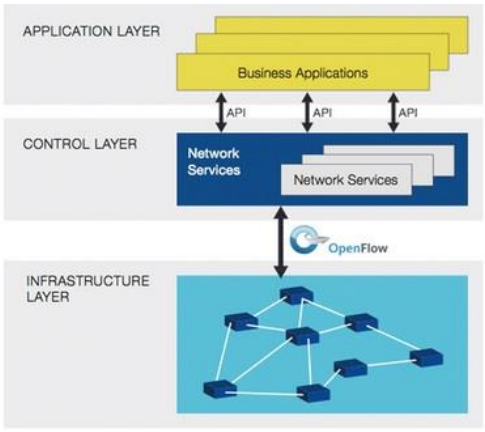
4.1.3 Openheid

De laatste eigenschap van een SDN-netwerk is de openheid van de API's en broncodes van de diverse controllers. Door deze openheid krijgen onderzoekers en engineers de mogelijkheid om te innoveren naar nieuwe methodieken op het gebied van netwerk- en beheerstechnieken. Deze API's, broncodes en innovaties dienen echter wel goed gedocumenteerd te zijn (Göransson & Black, 2014) (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 15-16).

4.2 SDN-framework

Hoewel meerdere variaties op het SDN-concept bestaan, is de basis van het framework veelal hetzelfde. Het SDN-framework bestaat uit een 4-tal basiselementen, namelijk een SDN-controller, Southbound API's, Northbound API's en een East-West API. Figuur 9 geeft een weergave van een dergelijk SDN-framework.

De SDN-controller, eveneens het brein van het netwerk genoemd, is een logisch gecentraliseerde netwerkentiteit die de verantwoording heeft over (1) het vertalen van SDN-applicatie eisen naar de onderliggende infrastructuur, (2) SDN-applicaties voorzien van een abstract netwerkoverzicht, (3) SDN-applicaties voorzien van eventmeldingen en statistieken van het netwerk, (4) netwerkadministrators voorzien van de mogelijkheid om te kunnen participeren in de flow van datapakketten en (5) het programmeren van forwarding entries. Daarnaast zijn de diverse API's tevens terug te vinden op de SDN-controller.

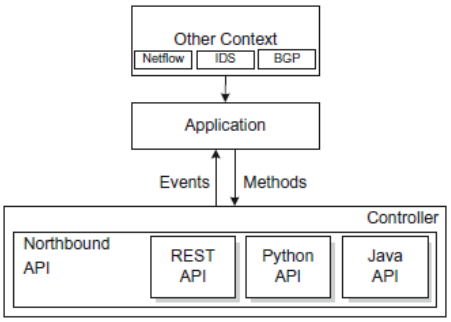


Figuur 9: SDN-Framework (Open Networking Foundation , 2015)

De Southbound API's zijn verantwoordelijk voor de communicatie tussen de SDN-controller en de diverse netwerkapparatuur. Binnen figuur 9 wordt gebruik gemaakt van het protocol OpenFlow om deze communicatie te bewerkstelligen. Echter, om deze communicatie te bewerkstelligen kunnen – afhankelijk van de implementatiemethode – meerdere protocollen worden gebruikt. De literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 24-25) geeft meer duidelijkheid in de deze protocollen. Daarnaast kunnen de huidige CLI's en het protocol SNMP eveneens voorzien worden van de Southbound-API naamgeving.

De East-West API is verantwoordelijk voor communicatie tussen groepen of federaties van SDN-controllers. Synchronisatie tussen de SDN-controllers wordt aan de hand van deze API bewerkstelligd en wordt het single point of failure principe opgeheven. Daarnaast ontstaat door deze API de mogelijkheid om meerdere en diverse SDN-controllers, binnen hetzelfde netwerk, te implementeren.

De Northbound API's zijn verantwoordelijk voor de communicatie tussen de diverse SDN-applicaties en de SDN-controller. SDN-applicaties kunnen bestaan uit netwerkservices (t.w. switching- en routingprotocollen, firewall-, loadbalancing oplossingen, et cetera) en applicaties (t.w. applicaties voor automatisering, orkestratie, monitoring, hypervisor, et cetera) die het netwerkverkeer manipuleren of als informatiebron gebruiken. De communicatie tussen de controller en SDN-applicaties bestaat uit events (netwerkinformatie) en methodes (flowmodificaties).
Met behulp van figuur 10 wordt hier een verduidelijking in gecreëerd. Daarnaast kunnen de API's in een low- of high-level worden uitgevoerd. Bij een low-level API is de SDN-applicatie bewust van de diverse onderliggende individuele netwerkapparatuur. Echter, de verschillen tussen de diverse apparaten zijn afgeschermd. Bij een high-level API wordt het bewustzijn van de diverse onderliggende individuele netwerkapparaten extra afgeschermd. Hierdoor ontstaat alleen een globaal beeld van het netwerk. In tegenstelling tot de Southbound API's zijn, op het moment van schrijven, nog geen standaarden voor de Northbound API's ontwikkelt. Hierdoor worden de meest gangbare scripting- en programmeertalen door deze API ondersteund. ONF heeft tegen het einde van 2013 een werkgroep opgericht voor het standaardiseren van een Northbound API protocol. Echter, tot op heden is daar nog geen standaardiseringsverzoek uit ontstaan (SDxCentral, 2015) (Göransson & Black, 2014).



Figuur 10: Northbound API (Göransson & Black, Software Defined Networks: A Comprehensive Approach, 2014)

Naast de meest gangbare scripting- en programmeertalen kan Representational state transfer (REST) eveneens als Northbound API worden gebruikt. REST is een architecturale methode om communicatie van- en naar een grote diversiteit aan softwarefunctionaliteiten te bewerkstellen. REST is opgebouwd uit een zestal architecturale randvoorwaarden en levert – wanneer aan deze randvoorwaarden is voldaan – meer schaalbaarheid, onafhankelijkheid en comptabiliteit naar de API's. De onderstaande opsomming geeft een overzicht van de zes verschillende randvoorwaarden en wat hiermee wordt bedoeld.

1. **Client-Server**[7] - Door de userinterface- van de data storage zorgen te scheiden, worden de userinterfaces platformonafhankelijk en ontstaat meer schaalbaarheid. Binnen SDN betekent dit dat zowel verschillende applicaties als programmeertalen van dezelfde functionaliteiten, binnen de REST API, kunnen genieten.
2. **Stateless** - Een stateless client-server connectie draagt ervoor zorg dat, wanneer een client een request aan de server doet, het verzoek alle informatie bevat om de opdracht te begrijpen. Door gebruik te maken van een stateless connectie ontstaat een efficiënter gebruik van de API en SDN-controller.
3. **Caching** - De prestatie en schaalbaarheid van de API wordt vergroot door de veel gebruikte informatie in een lokaal kopie op de client op te slaan. Door aan de server kant te definiëren of een lokaal kopie is toegestaan, wordt een extra beveiliging toegevoegd.
4. **Layered System** - Door een gelaagd systeem toe te passen is de client in staat te communiceren met alle, op die laag aangelegen, servers en niet verder. Voor SDN betekent dit dat de applicatie alleen met de controller en niet met de onderliggende architectuur kan communiceren.
5. **Uniform Interface** - Het toepassen van een uniforme interface draagt zorg dat alle informatie, ongeacht afkomst of gebruikte taal, op dezelfde manier wordt weergegeven. Wat de REST API (binnen een SDN omgeving) betreft, vindt deze weergave veelal plaats op basis van de programmeertaal XML of JSON.
6. **Code-on-Demand** - Via code-on-demand ontstaat de mogelijkheid om, bij een request, een functionaliteit volledig op de server uit te voeren. Deze voorwaarde is optioneel en wordt gebruikt als de API's niet naar behoren (en wel juist geconfigureerd zijn) functioneren.

[7] De servers (binnen de opsomming) staan in verband met de SDN-applicaties en de clients in verband met de SDN-controller.

De meest gebruikte protocollen binnen deze REST API is het protocol HyperText Transport Protocol (HTTP) en de beveiligde variant HyperText Transport Protocol Secure (HTTPS). Deze protocollen maken gebruik van gestandaardiseerde methodes om informatie weer te geven, te manipuleren en te verwijderen. De methodes zijn zowel 'GET', 'HEAD', 'POST', 'PUT', 'DELETE', 'TRACE' als 'CONNECT' en staan beschreven in IETF RFC 2616 (IETF, RFC 2616, 1999). Met behulp van deze uniforme methodes kunnen applicaties eenvoudig zogenaamde CRUD-acties, tegen de SDN-controller aan, uitvoeren. CRUD is een acroniem voor 'Create', 'Read', 'Update' en 'Delete' (James, 1983) (Fielding R. , 2000) (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 21-22).

4.3 SDN-Modellen

Binnen een SDN-omgeving kan, op het moment van schrijven, het controledraagvlakmechanisme op twee manieren worden uitgevoerd. Deze manieren betreffen zowel een imperatief- als een declaratief model en beschrijven hoe de onderliggende netwerkapparatuur datapakket afhandelingen uitvoert.

Binnen het imperatieve model functioneert de SDN-controller als het centrale zenuwcenter van een SDN-omgeving. Zoals in paragraaf 4.2 beschreven staat, ontvangt de controller – vanuit de Northbound API's – applicatieverzoeken en vertaalt deze naar flows. Deze flows worden vervolgens via de Southbound API's naar het data (forwarding) draagvlak van de onderliggende netwerkapparatuur verzonden. Daarnaast benadert de onderliggende netwerkapparatuur, wanneer datapakket afhandelingsopties onbekend zijn, de SDN-controller voor verdere afhandelingsinstructies. Door deze werkwijze te hanteren, blijft alle intelligentie binnen de SDN-controller(s) (SDxCentral, 2015).

Het flowververkeer – binnen het imperatieve SDN-model – kan gereguleerd worden aan de hand van drie verschillende methodieken, namelijk proactief-statisch, proactief-dynamisch en reactief. Bij een proactief-statische methode is de netwerkbeheerder geheel verantwoordelijk voor het netwerkverkeer. Om dit verkeer te bewerkstellen, dient de netwerkbeheerder alle mogelijke datapakketflows handmatig in de SDN-controller te programmeren. Gebruik van wildcards is mogelijk, maar verlaagt de granulariteit van de forwardingtabel. Deze methodiek is vergelijkbaar met het gebruik van statische routes binnen een traditioneel netwerk. Door de volledig statisch aard is deze methodiek de meest veilige, maar tevens de meest tijdrovende oplossing. De proactief-dynamische methode is een dynamische oplossing. Bij deze methode is de SDN-controller bewust van de individuele aangesloten eindpuntapparaten. De bewustheid ontstaat, hetzelfde als bij traditionele netwerken, doordat het aangesloten eindpunt apparaat – bij de eerste connectie met het netwerk – een ARP-request verzendt. De SDN-controller gebruikt deze gegevens om vervolgens de netwerktopologiedatabase te vullen en de kortste paden bij deze locatie te berekenen. De flowtabellen worden na de berekening, bij beide proactieve methodes, naar het geheugen van de onderliggende netwerkapparaten gestuurd. Hierdoor hoeft niet elk datapakket naar de controller te worden gestuurd en ontstaat een efficiënter gebruik van zowel de SDN-controller als de onderliggende netwerkarchitectuur. De reactieve methode, daarin tegen, dient wel alle datapakketen via de SDN-controller naar de eindbestemming te versturen. Hierdoor worden geen flowtabelgegevens in het cachegeheugen van de onderliggende netwerkapparatuur opgeslagen. Naast het feit dat – bij deze methode – zowel de SDN-controller als de onderliggende netwerk apparatuur minder efficiënt wordt benut, is het netwerk tevens onbruikbaar bij een controller failure (Klebanov, 2013).

Het declaratieve model draagt zorg voor een SDN-omgeving met meer gedistribueerde intelligentie. Dit model wordt eveneens het 'wat / hoe' model genoemd. Binnen dit model vertaalt de SDN-controller applicatieverzoeken naar policy's (wat). Deze worden onderverdeeld in deel policy's en vervolgens naar de controledraagvlakken van de netwerkapparatuur verstuurd. Door deze werkwijze te hanteren, verneemt de onderliggende netwerkapparatuur wat wel en niet is toegestaan. De methodes om deze regels te hanteren, daarin tegen, worden door de netwerkapparatuur zelf bepaald (hoe) (SDxCentral, 2015) (Kikken, Software Defined Networking - Literatuurstudie, 2015, p. 23).

4.4 SDN-Uitvoeringen

Naast de onderscheiding tussen de twee SDN-modellen kan een SDN-omgeving in een viertal uitvoeringen worden gecategoriseerd. Deze categorieën zijn zowel Classic SDN, Hybrid SDN, Virtuele Overlays als Policy gericht en geven weer op welke manier een SDN-omgeving wordt ingevoerd. Figuur 12 geeft een visueel beeld in de diverse categorieën. Binnen deze afbeelding worden de Classic- en Hybrid SDN samengevoegd tot één categorie.

4.4.1 Classic SDN

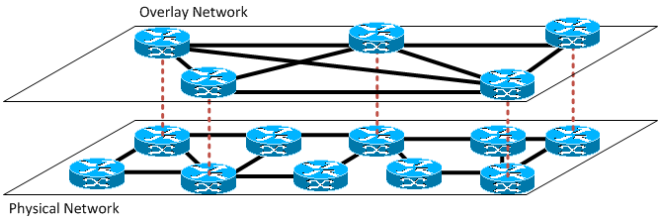
Classic SDN is een implementatiemethode waarbij een duidelijke scheiding tussen het controle- en het data (forwarding) draagvlak is te herkennen. De SDN-controller is volledig verantwoordelijk voor het beheren van de onderliggende netwerkapparatuur en de daarbij behorende forwarding tabellen. Door de gecentraliseerde geaardheid en de volledige controllerverantwoording valt deze uitvoering onder het imperatieve SDN-model. Deze SDN-uitvoering is de uitvoering die ONF oorspronkelijk voor SDN heeft bedoeld.

4.4.2 Hybird SDN

De Hybrid SDN implementatiemanier maakt gebruik van een gecombineerde netwerkomgeving architectuur. Een deel van de netwerkomgeving wordt bewerkstelligd aan de hand van de Classic SDN-uitvoering en is afhankelijk van een gecentraliseerde SDN-controller. Het andere deel van de netwerkomgeving is opgebouwd uit de huidige traditionele netwerk architectuur en is volledig gedecentraliseerd. Door deze combinatie te maken kan een SDN-omgeving gefaseerd worden ingevoerd.

4.4.3 Virtuele Overlays

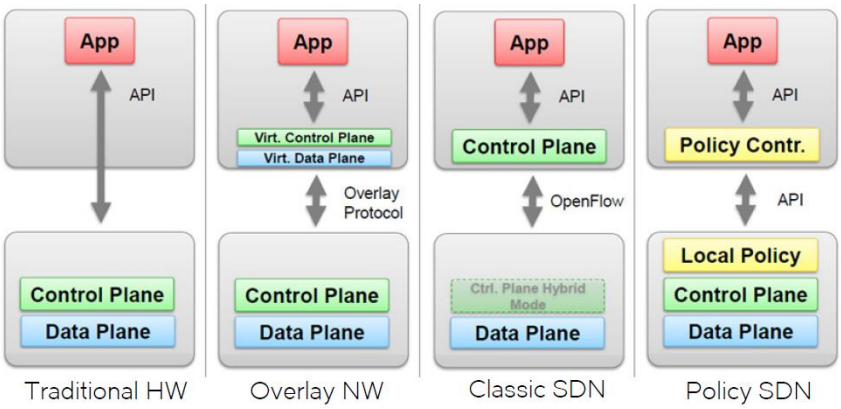
Een virtuele overlay is een virtuele laag bovenop de fysieke netwerkapparatuur. Deze virtuele laag wordt gezien als een apart gescheiden netwerk. Echter, de virtuele netwerk laag is wel afhankelijk van de onderliggende fysieke netwerkapparatuur. Figuur 11 geeft hier een visuele verduidelijking in. Hoewel deze virtuele overlays niet aan alle SDN-definiëringseisen voldoen, wordt deze uitvoering toch meegenomen als SDN-uitvoering. Deze uitvoering kan binnen bepaalde netwerkdelen (zoals datacenter omgevingen) een waardevolle toevoeging zijn.



Figuur 11: Virtuele Overlays (Elsen, 2013)

4.4.4 Policy gericht

De laatste categorie van SDN-uitvoeringen is een policy gerichte uitvoering. Deze uitvoering is ontstaan, doordat – aldus de SDN-visie van Cisco System: *"Many solutions suffer from scalability and performance limitations that result from the use of a centralized, rather than a distributed, control plane."* (Cisco Systems, 2015) – een imperatief SDN-model niet schaalbaar is voor de huidige datacenternetwerken. Deze uitvoering wordt bewerkstelligd met een SDN-controller die gebruik maakt van het declaratieve SDN-model en draagt zorg voor een gecentraliseerde netwerkarchitectuur met gedeeltelijk gesimplificeerde apparatuur (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 23-24).



Figuur 12: SDN-uitvoeringen (Laarhoven, 2015)

4.5 Conclusie

De deelvraag ***"Wat is Software Defined Networking?"*** kan met behulp van de bevindingen uit de paragrafen 4.1 en 4.2 worden beantwoord. Software Defined Networking is – op het moment van schrijven – een nieuwe architecturale benadering om computernetwerken te ontwerpen, construeren en beheren. Binnen deze architecturale benadering wordt het huidig gedecentraliseerde controledraagvlak – eveneens bekend als de intelligentie van de netwerkapparatuur – van de onderliggende netwerkapparatuur afgezonderd en naar een centrale controller verplaatst. Door deze benadering toe te passen ontstaat een gesimplificeerd, gecentraliseerd en programmeerbaar computernetwerk. Daarnaast is een netwerkomgeving – door het toepassen van zowel open-source broncodes als -protocollen en het gebruik van uniforme application programming interfaces – niet meer aan één netwerkapparatuur fabrikant gebonden. Om – aldus de oorspronkelijke bedoeling van de bedenkers van het SDN-concept – tot een volwaardig SDN-product te behoren dient een product aan een zestal eigenschappen te voldoen. De onderstaande opsomming geeft een overzicht van deze eigenschappen:

- Draagvlak scheiding;
- Gecentraliseerd beheer;
- Gesimplificeerde apparatuur;
- Netwerk automatisering;
- Netwerk virtualisatie;
- Openheid van apparatuur en broncode.

De deelvraag ***"Welke methodieken bestaan binnen deze techniek?"*** kan met behulp van de bevindingen uit de paragrafen 4.3 en 4.4 worden beantwoord. Een SDN-omgeving is in eerste instantie onderverdeeld in twee verschillende modellen, namelijk het imperatieve- en declaratieve model. Beide modellen hebben betrekking op het afhandelen van de communicatie tussen de netwerkapparatuur en de controller. Het grootste verschil tussen deze modellen is terug te vinden in de regulatie van het netwerkverkeer. Bij het imperatieve model wordt het netwerkverkeer gereguleerd aan de hand netwerkflows, terwijl het netwerkverkeer bij het declaratieve model aan de hand van policy's wordt gereguleerd. Hierdoor is binnen het imperatieve model de SDN-controller verantwoordelijk voor de complete afhandeling van het netwerkverkeer, terwijl de controller binnen een declaratief model alleen aangeeft welk netwerkverkeer mag plaatsvinden. De onderliggende netwerkapparatuur bepaalt vervolgens hoe deze regels worden toegepast. Het declaratieve model wordt daardoor eveneens het wat/hoe model genoemd.

De tweede onderverdeling heeft alleen betrekking op het imperatieve model. Dit model kan aan de hand van twee verschillende uitvoeringen worden geïmplementeerd, namelijk Classic- en Hybrid SDN. De Classic SDN uitvoering is een implementatiewijze waarbij de onderliggende netwerkapparatuur volledig gebruik maakt van de SDN-controller. Deze implementatiewijze wordt eveneens als een volledige SDN-omgeving gecategoriseerd. De Hybrid SDN-uitvoering daarin tegen is een implementatiewijze waarbij een combinatie van zowel het traditioneel- als het SDN-netwerkdesign wordt gebruikt. Een – SDN-controller afhankelijke – protectie laag tussen deze combinatie architectuur bepaald welk verkeer wordt afgehandeld door welke netwerkarchitectuur. Deze SDN-uitvoering draagt zorg voor een gefaseerde SDN-implementatie.

5 Longlist

Dit hoofdstuk geeft een weergave van de longlistselectie die tijdens de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015, p. 26) is ontstaan.

Een longlist is bedoeld om een eerste (grove) selectie te maken uit de mogelijk toepasbare oplossingen. Deze lijst is ontstaan door zowel (SDxCentral, 2015) als (Network Computing Editors, 2015) te raadplegen en hieruit een selectie te maken op basis van volledig Enterprise geschikte oplossingen. Daarnaast is deze lijst – door de grote hoeveelheid start-ups en de onvolwassenheid van SDN – opgebouwd uit alleen de bekende traditionele netwerkapparatuur fabrikanten. Ten slotte is declaratieve SDN- (ter vergelijking op het imperatieve model) en een volledig open source (als eis van de opdrachtgever) oplossing meegenomen naar deze lijst. De onderstaande opsomming geeft een overzicht van de mogelijk toepasbare oplossingen:

- Cisco Application Policy Infrastructure Controller;
- Cisco Application Policy Infrastructure Controller - Enterprise Module;
- Cisco Open SDN Controller (voormalig Cisco Extensible Network Controller);
- HP Virtual Applcation Networks (VAN) Controller;
- Brocade Vyatta Controller;
- Extreme Networks OneController;
- NEC ProgrammableFlow Controller;
- Floodlight.

In Bijlage I: Longlist SDN-Controllers is een gedetailleerde tabel over de SDN-controller eigenschappen, SDN-definiëring en typering terug te vinden.

6 MoSCoW-prioritering

Dit hoofdstuk beschrijft de eigenschap categorisering van de bevindingen van het onderzoek naar MAASnet en de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015). Deze categorisering wordt bewerkstelligd aan de hand van de MoSCoW-methodiek en fungeert als input voor de MoSCow-analyse vergelijkingstabel (zie Bijlage II: MoSCoW-analyse SDN-controllers).

6.1 Must-haves

De eigenschappen binnen deze categorie zijn minimaal benodigd voor een goed functionerend netwerk en zijn gebaseerd op de bevindingen van hoofdstuk 3. De (onderstaand) benoemde eigenschappen dragen namelijk zorg voor het, binnen een SDN-omgeving, bieden van dezelfde functionaliteiten zoals deze momenteel binnen MAASnet worden aangeboden. De onderstaande opsomming geeft een weergave van de diverse must-haves eigenschappen:

- Netwerkapparatuur (t.w. Catalyst 3560-, 4500 en 6500 series) compatibiliteit;
- Netwerksegmentatie;
- Netwerkverkeer prioritering;
- Netwerkverkeer filtering gebaseerd op laag 2 en 3 van het OSI-model (ACL's);
- Netwerkapparatuur en -verkeer identificering (AAA / 802.1X);
- Netwerkverkeer monitoring en tracering;
- BGP-peering voor ontsluiting met de Internet Service Provider.

6.2 Should-haves

De eigenschappen binnen deze categorie zijn zeer gewenst, maar niet vereist voor een goed functionerend netwerk. Deze (onderstaand) genoemde eigenschappen zijn voornamelijk gebaseerd op hoofdstuk 4 en hebben betrekking op de definiëring van een SDN-omgeving. Door de onvolwassenheid van- en de vooralsnog vooruitstrevende ontwikkelingen binnen deze netwerkbenadering, kan het voorkomen dat mogelijk geschikte oplossingen niet aan alle eigenschappen voldoen. De benoeming van de compatibiliteit met de WISM2 Wireless LAN Controller wordt binnen deze categorie genoemd, doordat geen directe koppeling tussen de SDN-controller en de WISM2 is vereist. Deze Wireless LAN Controller kan eveneens, afhankelijk van de implementatiewijze, als netwerkeindstation (geswitchte poort) worden gezien. De onderstaande opsomming geeft een overzicht van de diverse eigenschappen binnen deze MoSCoW-categorie:

- Netwerkapparatuur (t.w. WISM2) compatibiliteit;
- Draagvlak scheiding;
- Gecentraliseerd beheer;
- Gesimplificeerde apparatuur;
- Netwerkautomatisering;
- Netwerkvirtualisatie;
- Openheid;
- SDN-controller federatie.

6.3 Could-haves

De eigenschappen binnen deze categorie zijn niet essentieel voor een goed functionerend product, maar hebben wel toegevoegde waarde. Daarnaast hebben de eigenschappen binnen deze categorie een lagere prioriteit dan de eigenschappen in de Should-haves categorie. De (onderstaand) genoemde eigenschappen hebben voornamelijk betrekking op de, in paragraaf 3.3 benoemde, pilots van MAASnet. De onderstaande opsomming geeft een weergave van de diverse eigenschappen:

- Hypervisor (t.w. VMware ESXi) koppeling;
- Unified Communications koppeling.

6.4 Won't-haves

De eigenschappen binnen deze categorie worden gedurende de looptijd van dit project niet meegenomen. Echter, deze eigenschappen kunnen dienen als hoofdonderwerp voor- of een waardevolle toevoeging zijn op toekomstige projecten. De (onderstaand) beschreven eigenschappen hebben voornamelijk betrekking op de, in het Project Initiatie Document (Kikken, Software Defined Networking - Project Initiatie Document, 2015, p. 13) benoemde, projectgrenzen van het afstudeertraject. Daarnaast zijn de aan een SDN-omgeving aansluitende bevindingen eveneens in deze categorie opgenomen. De onderstaande opsomming geeft een overzicht van de diverse eigenschappen:

- Nework Function Virtualisation (NFV);
- Software Defined Networking voor het Datacenter;
- Het aansluitend netwerk, met de daarbij behorende wensen en eisen, van het Academisch Ziekenhuis Maastricht (AZM).

7 Shortlist

Dit hoofdstuk beschrijft de shortlist van de onderzoeksresultaten. Een shortlist fungeert als lijst met de meeste passende oplossingen en wordt gecreëerd aan de hand van een eigenschap vergelijkingsanalyse. Deze eigenschap vergelijkingsanalyse is gebaseerd op de, in hoofdstuk 6 besproken, prioriteringscategorieën en is terug te vinden in Bijlage II: MoSCoW-analyse SDN-controllers.

De MoSCoW-analysetabel toont aan dat de Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) de enige mogelijk toepasbare SDN-Controller oplossing is. Deze controller voldoet namelijk aan alle eigenschappen van de MoSCoW Must-haves categorie en kan daardoor alle basisfunctionaliteit van MAASnet vervullen. Hierdoor is dit eveneens de enige oplossing wat terug te vinden is in de zogenaamde shortlist. De resterende controllers vallen af op de hardware compatibiliteitseisen van MAASnet.

De categorieën Could- en Would-haves, binnen deze tabel, hebben voornamelijk betrekking op zowel de classificering van een SDN-product als de in acht name van de pilotprojecten van MAASnet. De, binnen deze categorieën benoemde, eigenschappen hebben geen invloed op de basisfunctionaliteiten van MAASnet nog de uitkomst van de vergelijkingsanalyse.

8 Productexplicatie

Dit hoofdstuk beschrijft de eigenschappen van het, uit hoofdstuk 7 afkomstige, product. De controlleruitvoering, Roadmap van ontwikkeling, een aantal mogelijkheden van deze SDN-controller en de toekomstplannen zijn o.a. onderdeel van dit hoofdstuk.

8.1 Cisco Application Policy Infrastructure Controller Enterprise Module

De Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) is een SDN-achtige oplossing die de, oorspronkelijk voor het datacenter bedoelde, Application Centric Infrastructure (ACI) architectuur naar het Enterprise Campus netwerk haalt. De APIC-EM SDN-controller wordt hierdoor gezien als aanvulling op de APIC SDN-controller (SDN-controller variant voor het datacenter). Beide controllers zijn gebaseerd op een Cisco System propriëtair geschreven broncode en maken gebruik van het declaratief SDN-model.

Op het moment van schrijven verkeert dit product in een bèta-testfase, waardoor het verkrijgen van specifieke en gedetailleerde informatie moeizaam verloopt. De bevindingen van het interview met dhr. Joep Remkes (Kikken, Software Defined Networking - Interviewrapport, 2015, pp. 5-9) en de Release Notes van deze bètaversie (Cisco Systems, 2015) worden hierdoor als hoofdzakelijke bron gebruik voor de explicatie van dit product.

8.1.1 SDN-definiëring

In Tabel 7: MoSCoW-analyse SDN-Controllers 2/2 is terug te zien dat de SDN-oplossing van Cisco Systems niet aan alle zes oorspronkelijk SDN bedoelde eigenschappen (t.w. draagvlak scheiding, gecentraliseerd beheer, gesimplificeerde apparatuur, netwerk virtualisatie, netwerk automatisering en openheid) voldoet. Deze oorspronkelijk bedoelde SDN-omgeving is aldus Cisco Systems niet voldoende schaalbaar voor een Datacenter- of Enterprise Campus netwerkomgeving. Dhr. Remkes (Remkes, SDN-Discussie, 2015) benoemt hiervoor de reden

> ***Een 10 jaar geleden zijn wij op de markt gekomen met de Catalyst 5000 series. Deze switch beschikte al over de FlowBased Switching techniek. De application-specific integrated circuit (ASIC) werden toentertijd geprogrammeerd met flowtabellen en bij het ontstaan van het SQL Slammer virus liepen we tegen schaalbaarheidsissues aan.***

(Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.2 Controller uitvoering en specificaties

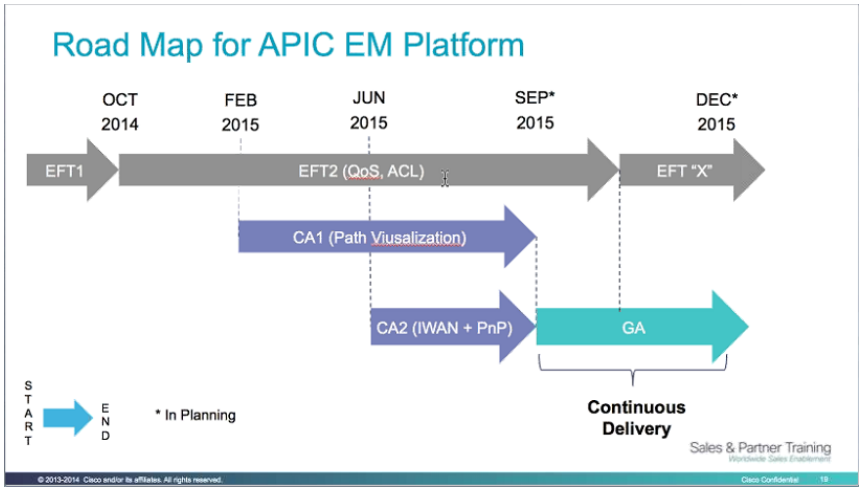
De APIC-EM SDN-controller wordt, op het moment van schrijven, alleen in een softwarematige variant uitgevoerd en kan alleen worden geïnstalleerd op een virtuele machine. Daarnaast dient deze virtuele machine minimaal aangestuurd te worden door een VMware vSphere v5.1 hypervisor. De controller wordt hierdoor als een voor geconfigureerde Open Virtual Appliance (OVA) aangeleverd. De onderstaande opsomming geeft een overzicht van de minimale systeem eisen voor deze OVA:

- Server – 64-bit x86 architectuur;
- vCPU – 4 Cores, ingesteld op een snelheid van 2.4 Ghz;
- Geheugen – 64 Gigabytes;
- Browser – Google Chrome v28.0;
- Hypervisor – VMware vSphere v5.1;
- Opslag – 150 Gigabytes (direct aangesloten opslag of op een SAN gebaseerde opslag[8]);
- Netwerk adapter – 1x;
- Web toegang vereist (Cisco Systems, 2015).

De afhankelijkheid van de specifieke hypervisor bestaat uit het feit, dat de APIC-EM OVA gebruik maakt van Grapevine (zie paragraaf 8.1.4 voor meer informatie) om schaalbaarheid van netwerkservices toe te passen (Kikken, Software Defined Networking - Interviewrapport, 2015) (Remkes, SDN-Discussie, 2015).

[8] Bij een SAN-opslag wordt het echter wel aangeraden om de logic unit number (LUN) voor te programmeren met een minimum van 300 input/output operations per second (IOPS).

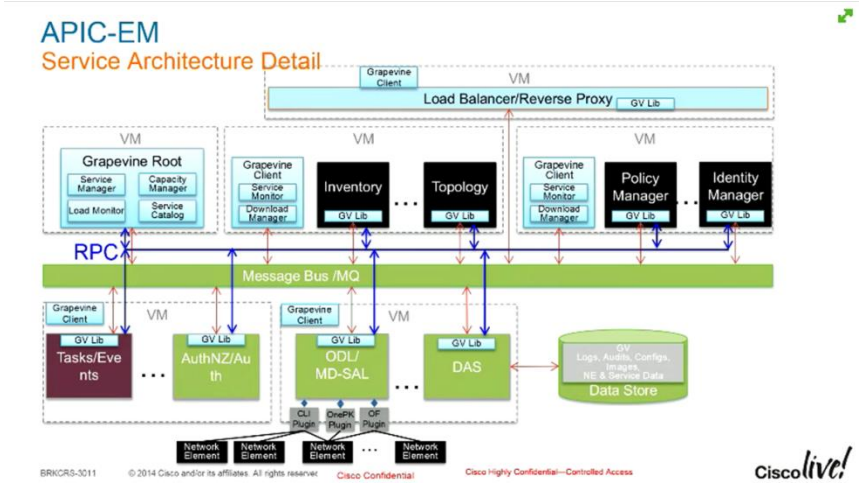
8.1.3 APIC-EM Roadmap



Figuur 13: Roadmap APIC-EM (Kikken, Software Defined Networking - Interviewrapport, 2015)

De ontwikkelingscyclus van APIC-EM SDN-Controller wordt aan de hand van figuur 13 verduidelijkt. In dit figuur is sprake over meerdere Early Field Trials (EFT), Cisco Availability (CA) releases en een General Availability (GA) release. De diverse EFT's zijn ontwikkelde testen om werking de toegevoegde functionaliteiten te conformeren. De GA-release wordt de eerste, voor klanten beschikbare, definitieve versie van de APIC-EM SDN-Controller. Deze release staat gepland voor september 2015 en wordt continu aangevuld met nieuwe functionaliteiten. Deze functionaliteiten kunnen, naar wens van de netwerkarchitecten en business formuleringen, zowel geautomatiseerd als manueel worden toegevoegd. Verder staat het in de planning om in de toekomst van de virtuele omgeving afhankelijkheid af te stappen en de productencatalogus aan te vullen met een hardware matige APIC-EM oplossing (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.4 Grapevine

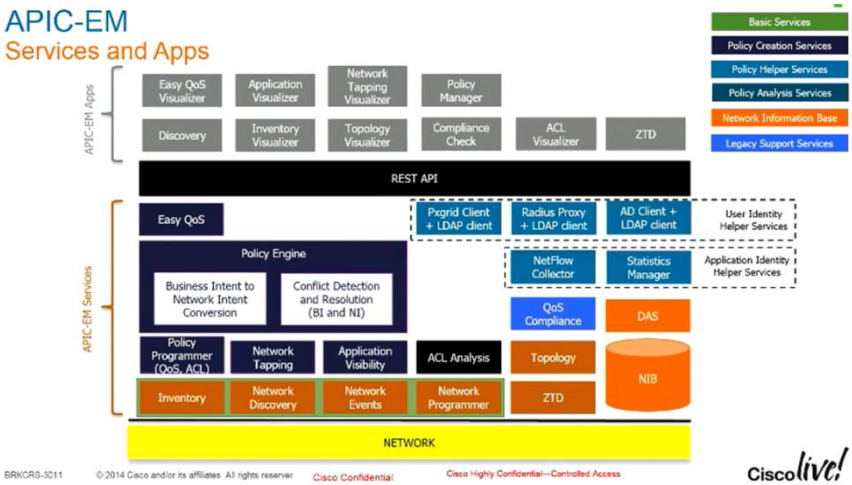


Figuur 14: Grapevine Service Architecture Detail (Cisco Systems, 2015, p. 49)

Grapevine is een door Cisco System eigen ontworpen- en op Unix gebaseerd product dat verantwoordelijk is voor het orkestreren van diverse virtuele machines wat gebruik worden voor de verschillende netwerkservices (t.w. topologie service, database service, graphical user interface service, et cetera). Dit product bestaat uit minimaal één Grapevine Root, diverse Grapevine Clients en een Load Balancer/Reverse Proxy. De Grapevine Root draagt de verantwoordelijkheid om de diverse Grapevine Clients, naar aanleiding van de vraag van de diverse netwerkservices, te orkestreren. De Grapevine Clients verzorgen de diverse netwerkservices en bestaan uit allemaal individuele virtuele machines. Hierdoor is elke virtuele machine (Grapevine Client) verantwoordelijk over een eigen netwerkservice en kunnen deze eenvoudig worden geschaald naar de vraag ervan. Door deze dynamische schaalbaarheidsoplossing is, op het moment van schrijven, de koppeling met de specifieke hypervisor vereist. De Grapevine Root dient namelijk, naar aanleiding van de vraag, Grapevine Clients aan te kunnen maken, bewerken en verwijderen. Ten slotte is de Load Balancer/Reverse Proxy verantwoordelijk voor alle communicatie van- en naar het Grapevine product. Dit Grapevine aspect is het enige onderdeel dat is voorzien van een IP-adres. De resterende Grapevine aspecten communiceren aan de hand van een interne Message Bus (VMware vSwitch), via de Load Balancer/Reverse Proxy, met elkaar. Figuur 14 geeft een visuele weergave in deze Grapevine Service Architectuur (Cisco Systems, 2015) (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.5 APIC-EM Controller architectuur

Figuur 15 geeft een visueel overzicht van de APIC-EM Controller architectuur en de standaard meegeleverde SDN-applicaties. In deze afbeelding komt duidelijk naar voren dat de SDN-controller van het declaratieve SDN-model gebruik maakt. Daarnaast is terug te zien dat een koppeling met identiteitsservices kan worden bewerkstelligd. De protocollen zowel Lightweight Directory Access Protocol (LDAP) als RADIUS maken deze koppeling mogelijk en verlengen het declaratieve SDN-model naar de Active Directory Domain Services (AD DS). Hierdoor kunnen SDN-policy bijvoorbeeld aan gebruikers(groepen), computeraccounts of andere AD DS aspecten worden gekoppeld. Deze functionaliteit is echter, op het moment van schrijven, in ontwikkelfase. Ten slotte is in de afbeelding terug te vinden dat SDN-applicaties zoals QoS, ACL Visualisatie, Network Tapping, Policy Manager, et cetera deel uit maken van de standaard APIC-EM Controller functionaliteiten (Kikken, Software Defined Networking - Interviewrapport, 2015).



Figuur 15: APIC-EM Controller (Cisco Systems, 2015, p. 48)

8.1.6 Southbound API

De connectie tussen de APIC-EM SDN-Controller en de onderliggende netwerkapparatuur (southbound API) wordt bewerkstelligd aan de hand van de Cisco Systems propriëtair CLI's. Door deze keuze te maken, kan een huidige infrastructuur (brownfield) eenvoudig worden aangevuld met SDN-functionaliteiten. (Remkes, SDN-Discussie, 2015) zegt hier het volgende over:

> ***Het gebruik van CLI is verreweg van ideaal, maar hierdoor ontstaat wel de mogelijkheid om het toe te passen binnen een bestaande infrastructuur. In de tussentijd zijn we wel aan het kijken naar een geschikt protocol om in de toekomst van CLI af te stappen. Vanuit Cisco Systems gezien zijn wij niet kapot van het protocol OpenFlow, aangezien dit protocol gebruik maakt van FlowBased Switching.***

(Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.7 Dynamische QoS

De APIC-EM SDN-Controller is standaard uitgerust met een QoS-applicatie die het onderliggende netwerk voorziet van prioriteringspolicy's. Echter, deze policy's worden alleen geactiveerd wanneer deze vereist zijn en vervolgens verwijderd wanneer deze niet meer nodig zijn. Ter adstructie wordt een voicecall aan de hand van het protocol Extensible Messaging and Presence Protocol (XMPP) gebruikt. Dit protocol stuurt, bij het opzetten van een dergelijke verbinding, een gespreksinformatiebericht naar de SDN-controller. Deze controller reageert hierop door een QoS-policy voor de desbetreffende, in aanmerking komende, netwerkapparatuur te versturen. Na de beëindiging van dit gesprek, wordt door de SDN-controller een QoS-policy verwijderingsconfiguratie verstuurd (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.8 Zero-Touch Deployment

De CA2-release van de APIC-EM SDN-Controller wordt uitgerust met de zogenaamde 'zero-touch deployment' techniek. Aan de hand van deze techniek ontstaat de mogelijkheid om vooraf geconfigureerde configuratiebestanden op de SDN-controller klaar te zetten. Nieuwe netwerkapparatuur kan vervolgens (zonder configuratie) op het netwerk worden aangesloten en maakt via een toegevoegde DHCP-optie connectie met de SDN-controller. Deze controller voorziet de netwerkapparatuur daaropvolgend van de vooraf ingestelde configuratie (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.9 ACL Tracering en Analyse

De APIC-EM SDN-Controller is uitgerust met een uitgebreide ACL-management applicatie. Deze applicatie raadpleegt de ACL's op de onderliggende netwerkapparatuur en analyseert deze op regel tegenspraak, -verband en onnodige -redundantie. Hierdoor heeft de netwerkbeheerder een actueel overzicht van de juist- en onjuist geconfigureerde ACL's. Daarnaast geeft de applicatie de mogelijkheid ACL's, vanuit het oogpunt van een netwerkeindstation (bijv. werkstation, laptop, et cetera), te testen (Cisco Systems, 2015).

8.1.10 Policy Manager

De policy manager van de APIC-EM SDN-Controller draagt zorg voor een gesimplificeerd en abstract beheer van netwerkpolicy's. Binnen deze controller worden netwerkpolicy's op business niveau ingevoerd en door de controller vertaald naar het niveau van de onderliggende netwerkapparatuur. De policy's kunnen op basis van o.a. tijd, type gebruiker, -bekabeling, et cetera worden ingeschakeld. Hierdoor ontstaan dynamische netwerkpolicy's die geen gedetailleerde kennis van netwerkapplicaties en de daarbij behorende -protocollen vereisen (Cisco Systems, 2015).

8.1.11 Netwerk topologie visualisatie

De APIC-EM SDN-Controller is uitgerust met een netwerk topologie visualisatie applicatie. Met behulp van deze applicatie worden netwerkentiteiten automatisch gevonden en toegevoegd aan de visuele topologie weergave. Hierdoor wordt het vinden en oplossen van incidenten eenvoudiger (Cisco Systems, 2015).

8.1.12 Toekomst plannen

Tijdens het interview met dhr. Remkes (Remkes, SDN-Discussie, 2015) zijn een aantal aspecten als toekomstplannen naar voren gekomen. De onderstaande sub paragrafen (8.1.12.1 t/m 8.1.12.5) beschrijven deze aspecten in meer detail.

8.1.12.1 Hardware matige controller

De bevindingen van paragraaf 8.1.2 beschrijven dat op het moment van schrijven alleen een software matige uitvoering van de controller beschikbaar is. Tijdens het interview (Remkes, SDN-Discussie, 2015) is echter naar voren gekomen dat Cisco Systems bezig is met de ontwikkeling van een hardware matige uitvoering van deze controller. Deze hardware matige uitvoering dient zorg te dragen voor het afschaffen van de specifieke hypervisor eis. Binnen de hardware matige SDN-Controller wordt het Grapevine product vervangen door linux container systemen. Dit zijn kleine virtuele omgevingen gecreëerd naar de eisen van een desbetreffende applicatie. Hierdoor worden, in tegenstelling tot normale virtuele omgevingen, alleen de benodigde services en niet een volledige omgeving virtueel uitgevoerd. Producten zoals Docker en LVC zijn hier een voorbeeld van (Kikken, Software Defined Networking - Interviewrapport, 2015) (Docker, Inc, 2015).

8.1.12.2 Federatie van controllers

Uit het interview met dhr. Remkes (Remkes, SDN-Discussie, 2015) blijkt dat Cisco Systems een toekomstgedachte heeft met betrekking tot de toevoeging van een APIC-EM SDN-Controller federatiemogelijkheid. Echter, uit dit interview blijkt eveneens dat Cisco Systems nog geen visie heeft over wanneer of hoe deze oplossing wordt bewerkstelligd (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.12.3 Policy's gebaseerd op AD-gebruikers(groepen)

In paragraaf 8.1.5 is sprake over een koppeling tussen de APIC-EM SDN-Controller en AD DS-systemen. Deze koppeling draagt, op het moment van schrijven, alleen zorg voor het bewerkstellen van een authenticatiesysteem aan de hand van bijvoorbeeld de protocollenstandaard 802.1X. Echter, de netwerkpolicy's kunnen nog niet worden gebaseerd op AD-gebruikers(groepen). Uit het interview met dhr. Remkes (Remkes, SDN-Discussie, 2015) blijkt dat de koppeling tussen AD-gebruikers(groepen) en netwerkpolicy's wel onderdeel uitmaakt van de toekomstplannen (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.12.4 Nieuwe segmentatie oplossingen

Zodra de ontwikkeling en implementatie van de koppeling tussen netwerkpolicy's en AD-gebruikers(groepen) is voltooid, wordt segmentatie op een geheel andere manier bewerkstelligd. Segmentatie gebeurt dan aan de hand van protocollen zoals VXLAN, LISP, et cetera en draagt zorg voor een multi-tenant netwerkomgeving. Daarnaast ontstaat hierdoor tevens de mogelijkheid om nieuwe netwerkoplossingen en -methodes te testen in een productieomgeving. Een toevoegingsdatum of versie is voor deze mogelijkheden echter nog niet bekend (Kikken, Software Defined Networking - Interviewrapport, 2015).

8.1.12.5 Uniform Southbound-API protocol

Uit het interview met dhr. Remkes (Remkes, SDN-Discussie, 2015) blijkt dat de CLI als Southbound-API protocol niet de meest ideale oplossing is. Een nieuw uniform Southbound-API protocol is daardoor eveneens een onderdeel van de toekomstvisie van Cisco Systems (Kikken, Software Defined Networking - Interviewrapport, 2015).

9 Toepasbaarheid

Dit hoofdstuk heeft betrekking op de toepasbaarheid van een SDN-omgeving binnen MAASnet. Met behulp van dit hoofdstuk worden de laatste drie deelvragen (t.w. ***"Welke SDN-methodiek is bruikbaar voor MAASnet?"***, ***"Voldoet de SDN-methodiek aan de eisen en wensen van MAASnet?"*** en ***"Wat zijn de voor- en nadelen, met de invalshoek naar MAASnet, van de verschillende SDN-methodieken?"***) beantwoord.

Voor de beantwoording van de deelvraag ***"Welke SDN-methodiek is bruikbaar voor MAASnet?"*** kunnen de bevindingen van zowel tabel 6 uit Bijlage II: MoSCoW-analyse SDN-controllers als hoofdstuk 7 en 8 worden gebruikt. Uit de bevindingen van tabel 6 blijkt dat de APIC-EM SDN-Controller van Cisco Systems de enige SDN-controller is die aan alle aspecten voldoet om de basisfunctionaliteiten van MAASnet te vervullen. De bevindingen van hoofdstuk 8 geven weer dat deze SDN-Controller gebruik maakt van het declaratieve (policy gericht) SDN-model. Aan de hand van de combinatie van bovenstaande bevindingen kan worden geconcludeerd dat het declaratieve SDN-model (op technisch gebied) bruikbaar is voor MAASnet.

De deelvraag ***"Voldoet de SDN-methodiek aan de eisen en wensen van MAASnet?"*** kan met behulp van de bevindingen uit hoofdstuk 3, 4 en 8 worden beantwoord. De – in paragraaf 3.2 beschreven – eisen van MAASnet hebben voornamelijk betrekking op hoe het netwerk dient te functioneren (t.w. netwerkverkeer segmentatie, -distributie, -filtering, -prioritering, -monitoring, -tracering en zowel netwerkverkeer als -apparatuur identificering), terwijl paragraaf 4.1 aangeeft dat SDN een nieuwe architecturale benadering van het ontwerpen van een computernetwerk is. Dit betekent dat hypothetisch gezien zowel het imperatieve als het declaratieve SDN-model aan deze functionaliteiten voldoen en tevens daardoor aan de eisen van MAASnet voldoen. Echter, de hardware compatibiliteit van het imperatieve model wordt – op het moment van schrijven – nog niet door alle netwerkapparatuur ondersteund. Dit draagt zorg dat momenteel alleen het declaratieve SDN-model volledig toepasbaar is. Deze conclusie kan worden geverifieerd aan de hand van tabel 6 uit Bijlage II: MoSCoW-analyse SDN-controllers.

Verder wordt het declaratieve SDN-model, aldus de bevindingen in paragraaf 4.3, het 'wat/hoe' model genoemd. Dit betekend dat de SDN-controller verantwoordelijk is voor het bepalen welk netwerkverkeer (wat) mag plaatsvinden en de onderliggende netwerkapparatuur verantwoordelijk is voor hoe deze regels worden bewerkstelligd (hoe). Hierdoor blijft de intelligentie van de netwerkapparatuur gedeeltelijk gedecentraliseerd. Daarnaast kan de Enterprise Module van de APIC SDN-Controller worden toegepast op een bestaande netwerkarchitectuur (brownfield), waardoor een aantal basis netwerkfunctionaliteiten – t.w. netwerkverkeersegmentatie en -distributie – hetzelfde blijven functioneren.

Wat de wensen van MAASnet betreft, hebben deze voornamelijk betrekking op programma's en protocollen die gebruik maken van een netwerkverbinding. Deze programma's en protocollen herkennen geen verschil tussen een Software Defined- of een traditioneel netwerk en functioneren daardoor naar behoren op beide architecturale netwerkontwerpen.

De deelvraag ***"Wat zijn de voor- en nadelen, met de invalshoek naar MAASnet, van de verschillende SDN-methodieken?"*** kan aan de hand van de bevindingen uit hoofdstuk 8 en zowel paragraaf 1.10 als paragraaf 1.11 uit de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015, pp. 26-31) worden beantwoord. Daarnaast wordt bij beantwoording van deze deelvraag onderscheid gemaakt tussen zowel de twee verschillende SDN-modellen (t.w. imperatief en declaratief) als de overkoepelende voor- en nadelen. Doordat de technisch toepasbare SDN-oplossing een declaratief SDN-model is, wordt zowel het declaratieve model als de overkoepelende voor- en nadelen benadrukt.

Imperatief
De onderstaande opsomming geeft een overzicht van de voordelen die betrekking hebben op MAASnet in combinatie met het imperatieve SDN-model:

- Overzichtelijkere doelgroep segmentatie (doelgroep segmentatie);
- Mogelijkheid tot testen in een productieomgeving (Testen in Live-omgeving).

De bovenstaande voordelenopsomming is in de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015) in meer detail beschreven. De nadelen van het imperatieve model zijn gelijk aan de nadelen die bij het overkoepelende deel staan beschreven.

Declaratief
De onderstaande opsomming geeft een overzicht van de voordelen die betrekking hebben op MAASnet in combinatie met het declaratieve SDN-model:

- Dynamische QoS;
- Zero-Touch Deployment;
- Eenvoudiger beheer van ACL's (ACL Tracering en Analyse);
- Eenvoudiger beheer van netwerkpolicy's (Policy Manager);
- Visualisatie van netwerktopologie (Netwerk topologie visualisatie).

De bovenstaande voordelenopsomming is in paragraaf 8.1.7 t/m 8.1.11 gedetailleerder beschreven. De nadelen van het declaratieve model zijn gelijk aan de nadelen die bij het overkoepelende deel staan beschreven.

Overkoepelend
De onderstaande opsomming geeft een overzicht van de voordelen die betrekking hebben op MAASnet in combinatie met zowel het declaratieve- als het imperatieve SDN-model:

- Reducering in de CapEx en OpEx;
- Meer tijd beschikbaar voor andere werkzaamheden (innovatie);
- Kortere doorlooptijd van IT-projecten (time-to-market);
- Betere samenwerking tussen IT-afdelingen (ontschotting IT-afdelingen);
- Hogere betrouwbaarheid;
- Gesimplificeerd beheer;
- Automatisering.

De onderstaande opsomming geeft een overzicht van de nadelen die betrekking hebben op MAASnet in combinatie met zowel het declaratieve- als het imperatieve SDN-model:

- Single-point-of-failure;
- Kwetsbaarheden in het onderliggende besturingssysteem/hypervisor.

Zowel de bovengenoemde voor- als nadelen zijn in de literatuurstudie (Kikken, Software Defined Networking - Literatuurstudie, 2015) gedetailleerder beschreven.

10 Eindconclusie

Dit hoofdstuk beschrijft de beantwoording van de onderzoeksvraag ***"Is de SDN-techniek geschikt, en zo ja, welke SDN-methodiek, voor gebruik binnen MAASnet?"***. De bevindingen van de diverse deelvragen, binnen dit onderzoeksrapport, vormen de basis voor deze beantwoording.

De bevindingen van zowel hoofdstuk 9 als de bevindingen uit paragraaf 3.4 en 4.5 maken duidelijk dat het declaratieve model, op het moment van schrijven, het enige SDN-model is dat aan zowel alle functionele- als niet-functionele aspecten voldoet om MAASnet op een identieke wijze te laten functioneren. Dit SDN-model wordt momenteel binnen een tweetal SDN-controllers toegepast, namelijk de APIC en de APIC-EM van Cisco Systems. De APIC SDN-Controller is bedoeld voor het Datacenter gedeelte van het computernetwerk en de APIC-EM SDN-Controller voor het gehele Enterprise Campus netwerk. Hierdoor is de APIC-EM de enige mogelijk toepasbare SDN-Controller voor het Enterprise Campus netwerk van Maastricht University. Echter, de bevindingen uit zowel paragraaf 8.1 als het interview met dhr. Remkes van Cisco Systems (Remkes, SDN-Discussie, 2015) geven weer dat deze controller – op het moment van schrijven – in een bèta-testfase verkeerd en de eerste release-versie voor september 2015 gepland staat.

Verder blijkt uit tabel 7 uit Bijlage II: MoSCoW-analyse SDN-controllers dat beide declaratieve SDN-Controllers niet aan alle, oorspronkelijk door ONF bedoelde, SDN-categoriseringseigenschappen (t.w. draagvlak scheiding, gecentraliseerd netwerkbeheer, gesimplificeerde netwerkapparatuur, netwerk automatisering, -virtualisatie en openheid) voldoen. De categoriseringseigenschappen draagvlak scheiding, openheid en gesimplificeerde netwerkapparatuur zijn niet tot gereduceerd terug te vinden binnen deze declaratieve SDN-controllers. Dit heeft echter te maken met de onvolwassenheid van SDN en de relatief veel ontwikkelingen die binnen deze nieuwe architecturale netwerkdesign benadering plaatsvinden. De Gartner Hype Cycle for Networking and Communications 2014 (zie figuur 16 in Bijlage III: Gartner Hype Cycle for Networking and Communications 2014) voorspelt dat deze ontwikkelingsfase nog circa vijf tot 10 jaar voortduurt.

Alles bijeengenomen is SDN, op het moment van schrijven, niet geschikt voor een effectuering binnen MAASnet. Redenen als de onvolwassenheid van-, vele ontwikkelingen binnen deze architecturale benadering, gebrek aan bewijslasten van schaalbaarheid en gerealiseerde omgevingen voor het Enterprise Campus netwerk leiden tot deze conclusie.

11 Aanbevelingen

Dit hoofdstuk beschrijft een overzicht van aanbevelingsonderwerpen die in acht genomen dienen te worden bij eventuele vervolgonderzoeken.

11.1 SDN-Datacenter

Gedurende het onderzoek is duidelijk geworden dat het grootste deel van SDN-ontwikkelingen binnen het Datacenter netwerkgedeelte plaatsvinden. Binnen dit netwerkgedeelte zijn, in tegenstelling tot het Enterprise Campus gedeelte, meer case studies van functioneerde implementaties en daardoor meer referentiemodellen beschikbaar. Daarnaast verhuist de grote bulk van het netwerkverkeer, door de integratie van bijvoorbeeld Cloud- en VDI-oplossingen, naar dit gedeelte van het netwerk. Aan de hand van deze aspecten is het raadzaam, alvorens de implementatie van SDN in het Enterprise Campus netwerk, een onderzoek naar SDN in het Datacenter uit te voeren.

11.2 Network Function Virtualisation

Network Function Virtualisation (NFV) is een architecturaal netwerkconcept dat bundels van netwerkapparatuur, met behulp van virtualisatie techniek, als één apparaat weergeeft. Daarnaast kunnen hardware matige oplossingen zoals firewalls, load balancers, WAN accelerators, intrusion prevention en detection systemen op een virtuele server worden uitgevoerd. Het NFV-netwerkconcept draagt hierdoor, eveneens als een SDN-omgeving, zorg voor een gesimplificeerd netwerk en is daardoor een zeer waardevolle aanvulling op SDN. Door deze waardevolle aanvulling is het aan te raden een vervolgonderzoek naar NFV uit te voeren (SDxCentral, 2015).

11.3 Schaalbaarheidsverschillen

Hoofdstuk 10 beschrijft dat, op het moment van schrijven, een gebrek aan Use-Cases van functionerende omgevingen en daardoor een gebrek aan schaalbaarheidsbewijslasten tussen de twee verschillende SDN-modellen aanwezig is. De netwerkapparatuur van MAASnet voldoet, weliswaar, momenteel niet aan de hardware compatibiliteitseisen van het imperatieve SDN-model. Dit blijft echter niet het geval. Hierdoor is het aan te raden om een vervolgonderzoek uit te voeren naar de schaalbaarheidsverschillen tussen de twee SDN-modellen.

11.4 Business impactanalyse

De grote achterliggende gedachtes van een SDN-omgeving hebben betrekking op een gesimplificeerd- en geautomatiseerd computernetwerk. Hierdoor krijgen de netwerkbeheerders, hypothetisch gezien, meer tijd innovatie van nieuwe ontwikkelingen. Verder kan de op software gerichte aard van een SDN-omgeving zorgdragen voor een fusie van de diverse IT-afdelingen of andere werkzaamheden creëren. Ten slotte kan de eis tot het verwerven van veel nieuwe kennis ontstaan. Al deze aspecten kunnen een behoorlijke impact op de business hebben en is het raadzaam om, alvorens implementatie, een business impactanalyse uit te voeren.

Tabellenlijst

Figurenlijst

Bibliografie

Alcatel-Lucent. (2015, 05 01). *Software Defined Networks: Optimizing Your Environment*. Retrieved from Alcatel-Lucent Enterprise: http://enterprise.alcatel-lucent.com/?innovation=NewThinking&page=SoftwareDefinedNetworks

Brocade. (2015, 05 01). *Software-Defined Networking (SDN)* . Retrieved from Brocade: http://www.brocade.com/solutions-technology/technology/software-defined-networking/index.page

Cisco Systems. (2008, 05 21). *Campus Network for High Availability Design Guide*. Retrieved from Campus Network for High Availability Design Guide: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

Cisco Systems. (2015). BRKCRS-3011 - Advanced - APIC-EM - SDN in the Enterprise. *BRKCRS-3011 - Advanced - APIC-EM - SDN in the Enterprise* (p. 129). Milaan: Cisco Live.

Cisco Systems. (2015, 04 15). *Cisco Application Centric Infrastructure*. Retrieved from OpFlex: An Open Policy Protocol: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731302.html

Cisco Systems. (2015, 05 15). *Data Sheet*. Retrieved from Cisco Application Policy Infrastructure Controller Enterprise Module: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-enterprise-module/datasheet-c78-730594.pdf

Cisco Systems. (2015, 05 26). *Policy Analysis*. Retrieved from APIC - Enterprise Module Sandbox: https://sandboxapic.cisco.com/policy/analysis?q=40&device=cceaf2fe-c3d9-4d37-bf14-fba071c27d6e&acl=dea7a366-4cdd-4006-ad51-27f0a0b2fb40

Cisco Systems. (2015). *Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module.* San Jose, CA, USA: Cisco Systems.

Docker, Inc. (2015, 05 26). *What is Docker?* Retrieved from Docker: https://www.docker.com/whatisdocker/

Fielding, R. (2000). *Architectural Styles and the Design of Network-based Software Architectures.* Irvine, CA, USA: University of California.

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (1999). *IETF, RFC 2616.* Internet Engineering Task Force.

Göransson, P., & Black, C. (2014). In S. Elliot, *Software Defined Networks: A Comprehensive Approach* (p. 15). Waltham: Morgan Kaufmann (an imprint of Elsevier).

Haleplidis, E., Pentikousis, K., Denazis, S., Hadi Salim, J., Meyer, D., & Koufopavlou, O. (2015). *IETF, RFC 7426.* Internet Engineering Task Force.

Hoogers, R. (2015, 05 29). *Onderzoeksmethoden*. Retrieved from InfoNu: http://wetenschap.infonu.nl/onderzoek/86838-onderzoeksmethoden.html

InfoNu. (2015, 05 29). *Kenmerken: Kwalitatief & Kwantitatief onderzoek*. Retrieved from InfoNu: http://wetenschap.infonu.nl/onderzoek/106079-kenmerken-kwalitatief-kwantitatief-onderzoek.html

James, M. (1983). Create, read, update and delete. In M. James, *Managing the database environment* (p. 381). Englewood Cliffs, NJ, USA: Prentice-Hall.

Juniper Networks. (2015, 05 01). *SDN*. Retrieved from Juniper Networks: http://www.juniper.net/us/en/dm/sdn/

Kikken, F. (2015). *Software Defined Networking - Interviewrapport.* Maastricht: Maastricht University.

Kikken, F. (2015). *Software Defined Networking - Literatuurstudie.* Maastricht: Maastricht University.

Kikken, F. (2015). *Software Defined Networking - Prestatieplan.* Maastricht: Maastricht University.

Kikken, F. (2015). *Software Defined Networking - Project Initiatie Document.* Maastricht: Maastricht University.

Klebanov, D. (2013, 09 16). *An alternate method of SDN network programmability*. Retrieved from NetworkWorld: http://www.networkworld.com/article/2169967/tech-primers/an-alternate-method-of-sdn-network-programmability.html

Kooij, J. v. (2013). *SLA_MAASnet_0.5.pdf.* Maastricht: Maastricht University.

Laarhoven, W. v. (2015). SDN-uitvoeringen. *SDN From a Brocade Point of View* (p. 85). Heerlen: Brocade.

Maastricht University. (2013, 03 04). *MAASnet*. Opgehaald van MAASnet: https://myum.unimaas.nl/irj/portal?NavigationTarget=ROLES://portal_content/DEEPLINK/nl.ifa.pages.DeeplinkPage&deepLink=https%3A%2F%2Fintrassl.myum.unimaas.nl%2Fweb%2FICTS2%2FICTSProductenEnDienstencatalogus%2FMAASnet.htm

Maastricht University. (2015, 03 18). *Network Overview*. Retrieved from Network Overview: http://- IP-adres -/

Munch, B., & Lassman, J. (2014). *Hype Cycle for Networking and Communications, 2014.* Stamford, CT, USA: Gartner, Inc.

Network Computing Editors. (2015, 03 03). *SDN Controller Handbook*. Retrieved from Network Computing: Connecting the infrastructure community: http://www.networkcomputing.com/networking/sdn-controller-handbook/d/d-id/1319300?page_number=1

Open Networking Foundation . (2015, April 08). *Software-Defined Networking (SDN) Definition*. Retrieved from What is SDN?: https://www.opennetworking.org/sdn-resources/sdn-definition

Oracle. (2015, 05 01). *Oracle SDN*. Retrieved from Oracle: http://www.oracle.com/us/products/networking/virtual-networking/sdn/overview/index.html

Remkes, J. (2015, 04 29). RE: OpenFlow Support. Maastricht, Limburg, Nederland.

Remkes, J. (2015, 05 01). SDN-Discussie. (F. Kikken, Interviewer)

SDxCentral. (2015, 04 24). *Comprehensive List of SDN Controller Vendors & SDN Controllers*. Retrieved from SDxCentral: https://www.sdxcentral.com/resources/sdn/sdn-controllers/sdn-controllers-comprehensive-list/

SDxCentral. (2015, 04 15). *SdxCentral*. Retrieved from What is Cisco OpenFlow?: https://www.sdxcentral.com/resources/cisco/cisco-openflow/

SDxCentral. (2015, April 09). *Software-Defined Networking*. Retrieved from What are SDN Northbound APIs?: https://www.sdxcentral.com/resources/sdn/north-bound-interfaces-api/

SDxCentral. (2015, 05 28). *What is NFV – Network Functions Virtualization?* Retrieved from SDxCentral: https://www.sdxcentral.com/resources/nfv/whats-network-functions-virtualization-nfv/

SDxCentral. (2015, 04 28). *What's Software-Defined Networking (SDN)?* Retrieved from SDxCentral: https://www.sdxcentral.com/resources/sdn/what-the-definition-of-software-defined-networking-sdn/

Shenker, S. (2011). The Future of Networking, and the Past of Protocols. *Open Networking Summit* (p. 11). Stanford, CA, USA: ONS. Retrieved from http://opennetsummit.org/archives/oct11/shenker-tue.pdf

SURFnet. (2015, 02 23). *SURFdrive*. Retrieved from SURFdrive: https://www.surf.nl/diensten-en-producten/surfdrive/surfdrive.html

Wikipedia. (2015, 01 31). *Unified communications*. Retrieved from Unified communications: http://en.wikipedia.org/wiki/Unified_communications

Bijlage I: Longlist SDN-Controllers

Naam	Cisco Application Policy Infrastructure Controller (APIC)	Cisco APIC - Enterprise Module (EM)	Cisco Open SDN Controller (XNC)	Brocade Vyatta Controller	HP Virtual Applcation Networks (VAN)	Extreme Networks OneController	NEC Programmable Flow Controller	Floodlight
SDN-controller eigenschappen								
Fabrikant	Cisco Systems	Cisco Systems	Cisco Systems	Brocade	Hewlett-Packard	Extreme Networks	NEC	Project Floodlight community
Type controller	Appliance	Software / Appliance	Software	Software	Software	Fysiek- / Virtueel Appliance	Appliance	Software
Source code afkomstig van	n.v.t. (eigen bron)	n.v.t. (eigen bron)	OpenDayLight	OpenDayLight	n.v.t. (eigen bron)	OpenDayLight	OpenDayLight	Eigen source
South protocol	OpFlex, L4-7 Scripting API	CLI	OpenFlow v1.3, OnePK API	OpenFlow v1.3, NETCONF, YANG, OVSDB	OpenFlow v1.3	OpenFlow v1.3, NETCONF, OVSDB	OpenFlow v1.3	OpenFlow
North protocol	REST	REST	OSGi, REST	REST	REST	REST	REST	REST
Status	Operationeel	Aangekondigd	Operationeel	Operationeel	Operationeel	Operationeel	Operationeel	Operationeel
SDN-definitie normering								
Draagvlak scheiding	Nee	Nee	Ja	Ja	Ja	Ja	Ja	Ja
Gesimplificeerde apparatuur	Gedeeltelijk	Gedeeltelijk	Ja	Ja	Ja	Ja	Ja	Ja
Gecentraliseerd management	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Mogelijkheid tot automatisering	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Netwerk abstractie (virtualisatie)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Openheid	Sourcecode: Ja Hardware: Nee	Sourcecode: Nee Hardware: Nee	Sourcecode: Ja Hardware: Ja	Sourcecode: Ja Hardware: Ja	Sourcecode: Nee Hardware: Ja	Sourcecode: Ja Hardware: Ja	Sourcecode: Ja Hardware: Ja	Sourcecode: Ja Hardware: Ja
SDN-typering								
SDN-uitvoering	Declaratief	Declaratief	Imperatief	Imperatief	Imperatief	Imperatief	Imperatief	Imperatief
SDN-type	Policygericht	Policygericht	Classic-, Hybrid SDN	Classic-, Hybrid SDN	Classic-, Hybrid SDN	Classic-, Hybrid SDN	Classic-, Hybrid SDN	Classic SDN
Omgeving	Datacenter	Enterprise	Enterprise	Enterprise, Datacenter	Enterprise	Enterprise, Datacenter	Enterprise, Datacenter	Enterprise, Datacenter
Overig								
Customerservice	Support via fabrikant	Support via fabrikant	Support via fabrikant	Support via fabrikant	Support via fabrikant	Support via fabrikant	Support via fabrikant	Support via Open Source Community
Opmerkingen	-	-	-	-	≥ 50 OF-apparaten	Virtueel uitgevoerd via servicecontract	≥ 100 OF-apparaten	-

Tabel 5: SDN-Controller vergelijking

Bijlage II: MoSCoW-analyse SDN-controllers

Naam	Cisco Application Policy Infrastructure Controller (APIC)	Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)	Cisco Open SDN Controller	Brocade Vyatta Controller	HP Virtual Applcation Networks (VAN)	Extreme Networks OneControlle r	NEC Programmabl e Flow Controller	Floodlight
MoSCoW Must-haves								
Compatibiliteit Catalyst 3560 Series	Nee	Ja	Nee*	Nee*	Nee*	Nee*	Nee*	Nee*
Compatibiliteit Catalyst 4500 Series	Nee	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Compatibiliteit Catalyst 6500 Series	Nee	Ja	Nee**	Nee**	Nee**	Nee**	Nee**	Nee**
Mogelijkheid voor netwerksegmentatie	Ja	Ja	Ja	Ja	Ja^	Ja	Ja	Ja^
Mogelijkheid voor netwerkverkeer prioritering	Ja	Ja	Ja^	Ja^	Ja^	Ja^	Ja^	Ja^
Mogelijkheid voor netwerkverkeer filtering	Ja	Ja	Ja	Ja	Ja^	Ja	Ja	Ja^
Netwerkapparatuur en -verkeer identificering	Ja	Ja	Ja	Ja	Ja^	Ja	Ja	Ja^
Mogelijkheid voor netwerkverkeer monitoring en tracering	Ja	Ja*****	Ja	Ja	Ja	Ja	Ja	Ja
Mogelijkheid voor BGP-peering	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

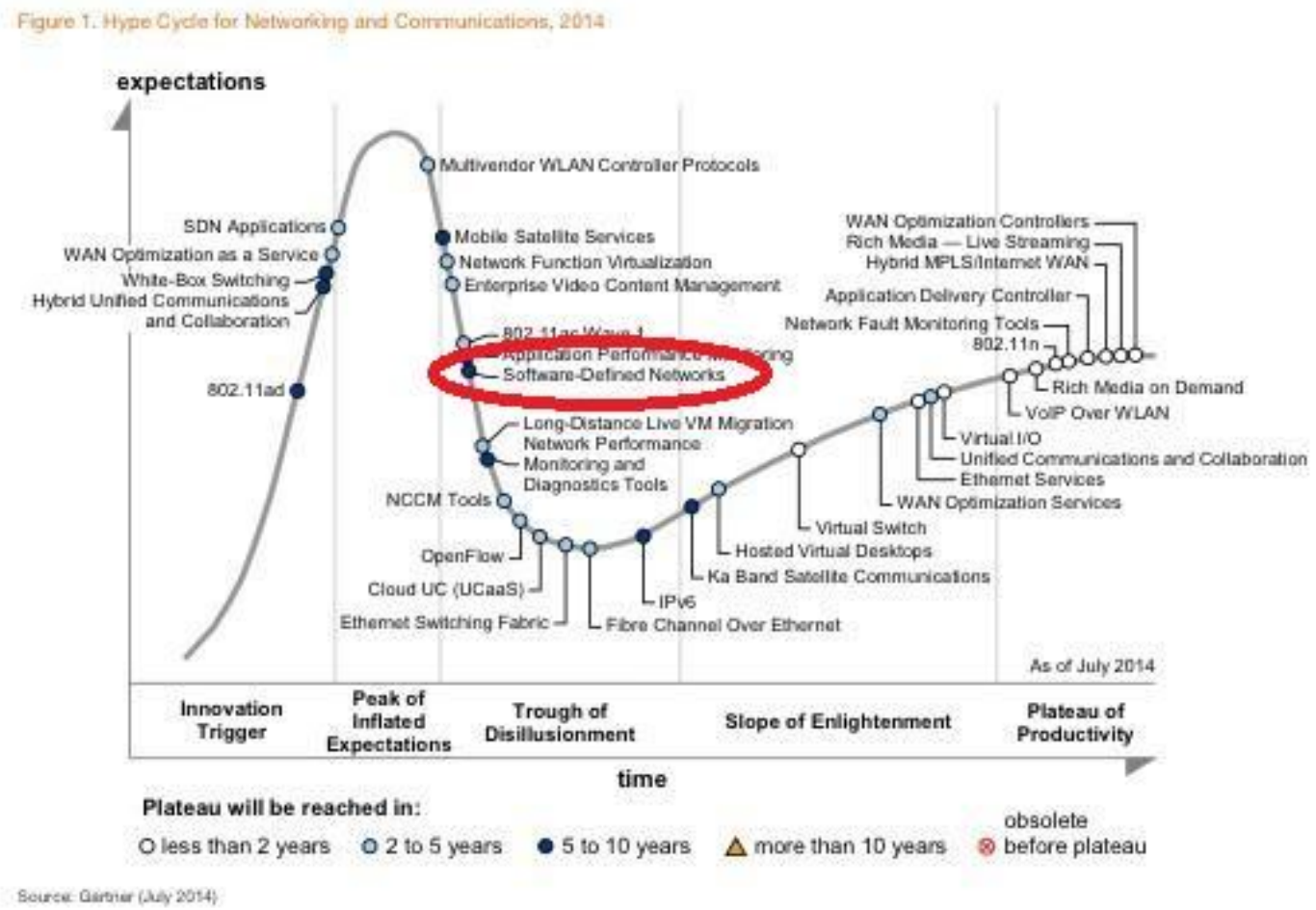
Tabel 6: MoSCoW-analyse SDN-Controllers 1/2

Naam	Cisco Application Policy Infrastructure Controller (APIC)	Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)	Cisco Open SDN Controller	Brocade Vyatta Controller	HP Virtual Applcation Networks (VAN)	Extreme Networks OneControlle r	NEC Programmabl e Flow Controller	Floodlight
MoSCoW Should-haves								
Compatibiliteit WISM2	Nee	Ja	Ja^^	Ja^^	Ja^^	Ja^^	Ja^^	Ja^^
Draagvlak scheiding	Nee	Nee	Ja	Ja	Ja	Ja	Ja	Ja
Gecentraliseerd netwerkbeheer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Gesimplificeerde netwerkapparatuur	Gedeeltelijk	Gedeeltelijk	Ja	Ja	Ja	Ja	Ja	Ja
Netwerk automatisering	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Netwerk virtualisatie	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Openheid	Nee	Nee	Ja	Ja	Gedeeltelijk	Ja	Ja	Ja
SDN-controller federatie	Ja	Nee	Ja	Ja	Ja	Ja	Ja	Nee
MoSCoW Could-haves								
VMware ESXi integratie	Ja	Ja***	Ja	Nee	Ja	Ja	Nee	Ja
Unified-Communications koppeling	Ja****	Ja****	Nee	Nee	Ja^	Nee	Nee	Nee

Tabel 7: MoSCoW-analyse SDN-Controllers 2/2

* = De beschikbaarheid van OpenFlow op het image van de Cisco Catalyst 3560 series is pas beschikbaar vanaf het vierder kwartaal van 2015 (Remkes, RE: OpenFlow Support, 2015).
** = De beschikbaarheid van OpenFlow op het image van de Cisco Catalyst 6500 series is nog niet bekend (Remkes, RE: OpenFlow Support, 2015).
*** = Afhankelijk van de implementatiewijze.
**** = Gebaseerd op het protocol XMPP.
***** = Afhankelijk van gebruikte SDN-Controller versie en netwerkapparatuur.
^ = Via SDN-applicatie.
^^ = Via aangesloten netwerkpoort(en). De Wireless LAN Controller wordt als netwerkeindstation gezien.

Bijlage III: Gartner Hype Cycle for Networking and Communications 2014



Figuur 16: Gartner Hype Cycle for Networking and Communications 2014 (Munch & Lassman, 2014)