Polytechnic College
Instituut voor hoger beroepsonderwijs in Suriname

Elektrotechniek

Studiejaar: 2013/2014

Onderzoek naar de mogelijkheid van cloud computing binnen Telesur

Afstudeerverslag ter verkrijging van de graad van
Bachelor of Applied Technology (BTech.)
in de studierichting Elektrotechniek

D. Tsen You 10402

Paramaribo, 3 februari 2014

Polytechnic College
Instituut voor hoger beroepsonderwijs in Suriname

Elektrotechniek

Studiejaar: 2013/2014

Onderzoek naar de mogelijkheid van cloud computing binnen Telesur

Afstudeerverslag ter verkrijging van de graad van

Bachelor of Applied Technology (BTech.)

in de studierichting Elektrotechniek

Student + studentenreg.nr:	David Tsen You 10402
Docent-begeleider:	D. Ramlakhan MSc.
Bedrijf:	Telesur
Bedrijfsbegeleider:	S.Tjitrotaroeno MBA, BSc.

Paramaribo, 3 februari 2014

Inhoudsopgave

Voorwoord

Ter afronding van de opleiding aan het Polytechnic College (PTC) dient iedere student middels een afstudeerproject aan te tonen dat hij/zij voldoende kennis heeft opgedaan om in de praktijk technische problemen kritisch te analyseren en mogelijke oplossingen aan te dragen. De titel die de student behaalt na het afstudeerproject met goed gevolg te hebben afgerond is Bachelor of Applied Technology (BTech.). Onder begeleiding en door grotendeels zelfwerkzaamheid heb ik naast mijn werk bij het Telecommunicatiebedrijf Suriname, Telesur, mijn studie Elektrotechniek met als specialisatie Informatietechniek mogen voltooien.

Vanwege de snelle groei van internetdiensten, zouden ook in Suriname deze diensten geïmplementeerd kunnen worden zonder gebruik te maken van buitenlandse providers. Ik lever mijn bijdrage om een van deze diensten, namelijk cloud computing binnen Suriname mogelijk te maken.

Mijn dank gaat uit naar mijn begeleiders, de heer S. Tjitrotaroeno MBA, BSc. van Telesur, de heer D. Ramlakhan MSc en mw. G. Long Him Nam van het Polytechnic College voor hun kritische en deskundige begeleiding bij de uitvoering en de vastlegging van mijn afstudeerproject. Ik spreek dank uit aan de afdelingen DCD, MIS en IMD van Telesur die een bijdrage hebben geleverd aan de totstandkoming van dit verslag. Ten slotte bedank ik mijn familie voor de morele ondersteuning die ik heb mogen ontvangen gedurende de periode waarin ik het afstudeerproject heb uitgevoerd.

Paramaribo, 3 februari 2014
David Tsen You

Samenvatting

Telesur is een telecommunicatiebedrijf dat de afgelopen tien jaren zich heeft beziggehouden met datacommunicatie en internetdiensten. Om de steeds veranderende technologie bij te houden is het ook belangrijk om na te gaan wat voor nieuwe internetdiensten er zijn die voor zowel de eindgebruiker(klant) als voor het bedrijf Telesur van belang zou kunnen zijn.
Cloud computing is al geruime tijd een populaire service die vaak meer internationaal gebruikt wordt door klanten. Vandaar dat er voor deze scriptie als opdracht gekozen is te onderzoeken wat de mogelijkheden zijn voor Telesur om cloud computing als dienst te leveren. Cloud computing is een virtuele omgeving die in de ICT wordt voorgesteld als een wolk (cloud) waar via de computer-, tablet-, smartphone- en laptop hardware, software en informatie op aanvraag beschikbaar zijn via het internet.
Uit het onderzoek blijkt dat er drie typen cloud computing bekend zijn, elk met zijn voor- en nadelen. Deze drie typen zijn: Public cloud, Private cloud en Hybrid cloud. Public cloud is via het internet aangeboden of verkregen service, Private cloud is een lokaal gebouwde cloud waarover de provider volledig beheer heeft en een Hybrid Cloud is een combinatie van Public en Private Cloud. Binnen cloud computing kan ook een aantal services aangeboden worden zoals Software As A Service(SAAS), Platform As A Service(PAAS), Infrastructure As A Service(IAAS). SAAS biedt de mogelijkheid software aan te bieden aan de klant via de cloud waarbij PAAS de mogelijkheid geeft software te laten ontwikkelen en als laatst hebben wij IAAS die infrastructuur biedt aan de klant, zoals meer opslagruimtemogelijkheden, bijvoorbeeld voor het maken van back-ups. Er zijn ook heel wat beveiligingstechnieken aangehaald die een cloud provider kan gebruiken om de betrouwbaarheid voor de klant te vergroten. Cloud computing wordt als service vanuit een datacenter geleverd. Een datacenter is een gebouw of faciliteit waar bedrijfskritische ICT-apparatuur (bijvoorbeeld servers) kan worden ondergebracht. Een datacenter wordt grotendeels gebruikt door bedrijven als een database voor het opslaan van informatie.
Bij een datacenter zijn er heel wat kenmerken en standaarden waarmee men rekening moet houden.

De probleemstelling luidt:
In hoeverre is het mogelijk binnen Telesur cloud computing als internetservice te implementeren?

Doelstelling: implementeren van cloud computing als internet service voor de eindgebruiker binnen de huidige situatie van Telesur.

Het onderzoek is uitgevoerd op de afdeling Data Communicatie Diensten van Telesur. Uit informatie verkregen vanuit het internet, het raadplegen van rapporten en literatuur blijkt dat bij de implementatie van cloud computing Telesur twee mogelijkheden zou hebben. Telesur zou zelf een datacenter kunnen bouwen en van daaruit zijn cloud diensten uitvoeren. Daarnaast zou Telesur ook de mogelijkheid hebben een datacenter van het buitenland te gebruiken door een bepaalde ruimte te reserveren en deze verder te verkopen aan zijn klanten.

Lijst van afkortingen

ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
API	Application Program Interface
CENELEC	European Committee for Electro technical Standardization
EDA	Equipment Distribution Area
ENI	External Network Interface
EVDO	Enhanced Voice-Data Optimized
GSM	Global System for Mobile communication
HDA	Horizontal Distribution Area
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IAAS	Infrastructure as A Service
ICT	Information and Communication Technology
IP	Internet Protocol
IPL	International Private Line
LDP	Local Distribution Point
MDA	Main Distribution Area
NICE	Network Information Communication Entertainment
PAAS	Platform as A Service
POTS	Plain Old Telephone Service
PTP	Point to Point
SAAS	Software As A Service
SHDSL	Symmetrical High-speed Digital Subscriber Line
TIA	Telecommunications Industry Association
UPS	Uninterruptible Power Supply
VDSL	Very High bit-rate Digital Subscriber Line
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access

Lijst van figuren

Lijst van tabellen

1 Inleiding

Telesur is in 1995 begonnen met het implementeren van internet in Suriname met het bekende "Dial Up" systeem. Hierdoor kon de klant op het internet gaan door in te bellen naar Telesur. Door de jaren heen is in Suriname de vraag naar een veel beter en snellere toegang tot het internet gaan groeien. Telesur heeft dit kunnen realiseren met de toepassing van Asymmetric Digital Subscriber Line (ADSL). In 2003 is Telesur met zijn ADSL-dienst begonnen. Binnen de telecommunicatie is ALL IP (Internet Protocol) een "hot item" waarin het mogelijk wordt gebruik te maken van een of meerdere diensten zoals bellen, film kijken en internet allemaal vanuit één apparaat. De gebruikers worden in staat gesteld zelf te kiezen op welke wijze, wanneer en waar ze communiceren. Cloud computing is één technologie die door middel van IP (Internet Protocol) ook als dienst uitgevoerd zou kunnen worden. Hierbij heeft de gebruiker de mogelijkheid op afstand zijn software te besturen via een virtueel opgestelde omgeving (ook wel cloud genoemd) alsook zijn data overal beschikbaar te hebben via een cloud. Telesur zou gebruik kunnen maken van cloud computing om cloud- diensten aan te bieden aan de Surinaamse samenleving met als gevolg een uitbreiding van zijn diensten over het internet.
De opdracht is om na te gaan hoe cloud computing technisch geïmplementeerd zou kunnen worden als een dienst in het Telesurnetwerk en welke diensten aangeboden kunnen worden in Suriname.

Het doel is om binnen Telesur's huidige situatie cloud computing met de nodige services te implementeren.
De probleemstelling luidt:
In hoeverre is het mogelijk binnen Telesur cloud computing als internetservice te implementeren?

Om aan te geven hoe cloud computing geïmplementeerd kan worden moet er rekening worden gehouden met de volgende aspecten:

- De typen cloud computing
- De services binnen cloud computing
- De nodige elementen voor het implementeren van cloud services
- De implementatie binnen het huidige Telesurnetwerk.

De kern van dit verslag bestaat uit vijf hoofdstukken. In hoofdstuk 2 wordt beschreven wat cloud computing allemaal inhoudt en wat de noodzaak is van een datacenter. In hoofdstuk 3 is dieper ingegaan op wat een datacenter is. In hoofdstuk 4 wordt beschreven hoe het huidige net-werk van Telesur eruitziet en hoe de gewenste situatie eruit zal moeten zien.

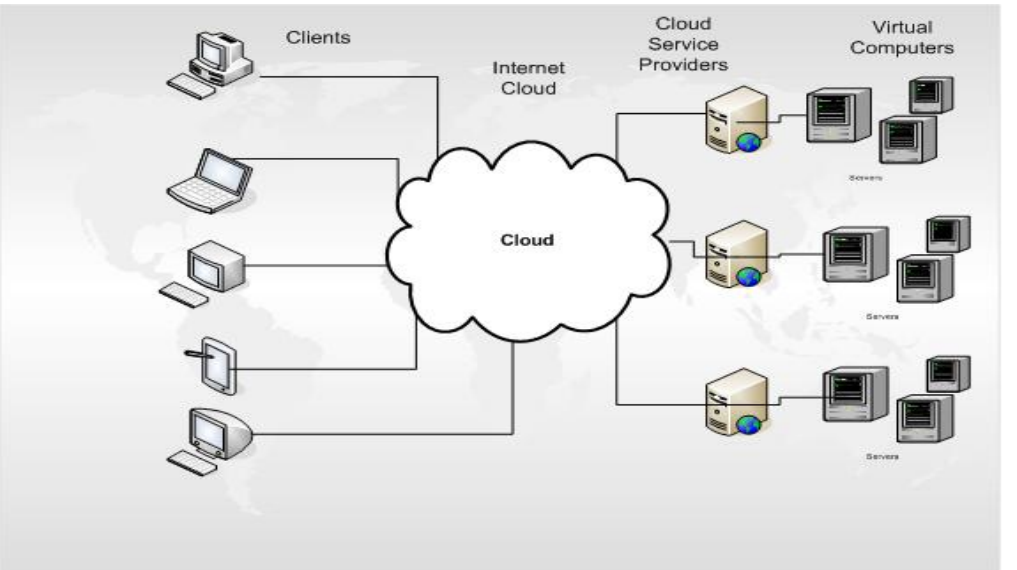
Belangrijkste bronnen: http://www.datacenter.rdm.com/global/en/data-center-solutions/data-center-standards.html Escalante, A., Borko,F.(2010). *Handbook of Cloud computing*, Springer, Boca Raton/Florida USA .

2 Cloud computing

In dit hoofdstuk wordt beschreven wat cloud computing is (2.1) en wat cloud computing allemaal inhoudt zoals welke typen er zijn met hun voor- en nadelen (2.2), wat voor services er aangeboden kunnen worden(2.3) en wat voor type beveiliging voor cloud computing aangeboden zou kunnen worden(2.4).
Bron: Escalante, A., Borko,F.(2010). *Handbook of Cloud computing*, Springer, Boca Raton/ Florida USA .

2.1 Wat is cloud computing ?

Cloud computing is het via het internet op aanvraag beschikbaar stellen van hardware, software en gegevens. De term is afkomstig uit de schematechnieken uit de informatica waar een groot, decentraal netwerk (zoals het internet) met behulp van een wolk wordt aangeduid.
De cloud staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt. Met elke dienst hebben wij altijd een provider en een eindgebruiker, beide met hun eigen rol en verantwoordelijkheden; dat is het geval ook bij cloud computing. De cloud provider is het bedrijf of organisatie die cloud - diensten aan de eindgebruikers biedt. De eindgebruiker weet niet op welke computer de software, hardware en gegevens beschikbaar zijn. De eindgebruiker hoeft op deze manier geen eigenaar meer te zijn van de gebruikte hard- en software en is niet verantwoordelijk voor het onderhoud.



Figuur 1: Cloud computing (http://www.brownbagradio.net/)

2.2 Cloud computing types

De verschillende typen clouds zijn:

1. Private cloud
2. Public cloud
3. Hybrid cloud

Ad 1 Private cloud

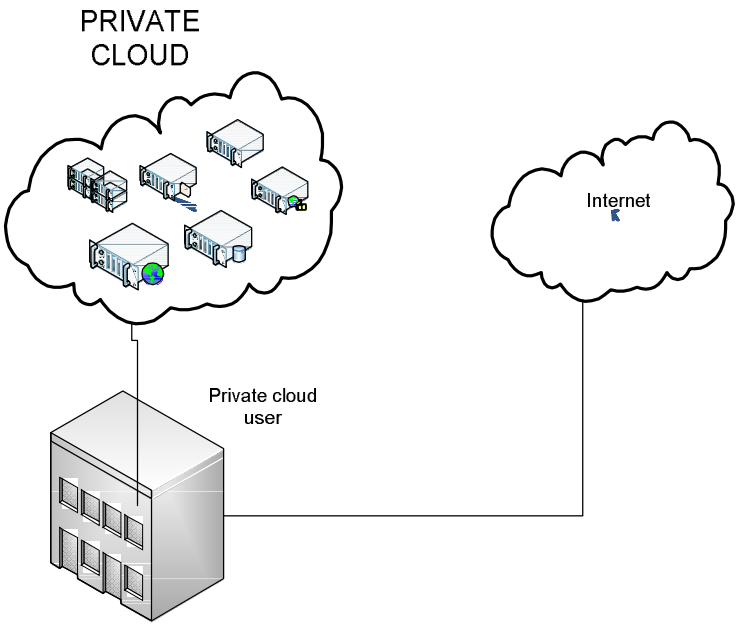
Een private cloud die ook een local cloud is, is een cloud die in een privéomgeving gebouwd is (zie figuur 2). Dit betekent dat die zelf is opgezet of dat er speciale apparatuur wordt gescheiden van de rest van het cloud netwerk voor een klant waarbij de klant alleen toegang heeft tot de resources van de gebruikte apparatuur. De infrastructuur van de private cloud wordt niet verdeeld. Een private cloud wordt gebruikt als er een hoge mate van beveiliging nodig is voor specifieke data. Connecties naar een private cloud worden via transportmethoden uitgevoerd die niet over het internet hoeven te geschieden zoals point to point(ptp), virtual private networks(vpn) ,of international private lines(ipl) connecties. Het gebruiken van een private cloud heeft zijn voor- en nadelen.

Voordelen:

- Betere beveiliging van data
- Betere controle over verstuurde data
- Het vol gebruik van capaciteit van de servers in de private cloud

Nadelen:

- Hoge kosten door gebruik te maken van eigen servers voor het opzetten van een private cloud
- Het gebruiken van overbodige capaciteit van de servers voor doelen die heel weinig capaciteit nodig hebben.



Figuur 2: Private Cloud

Ad 2 Public cloud

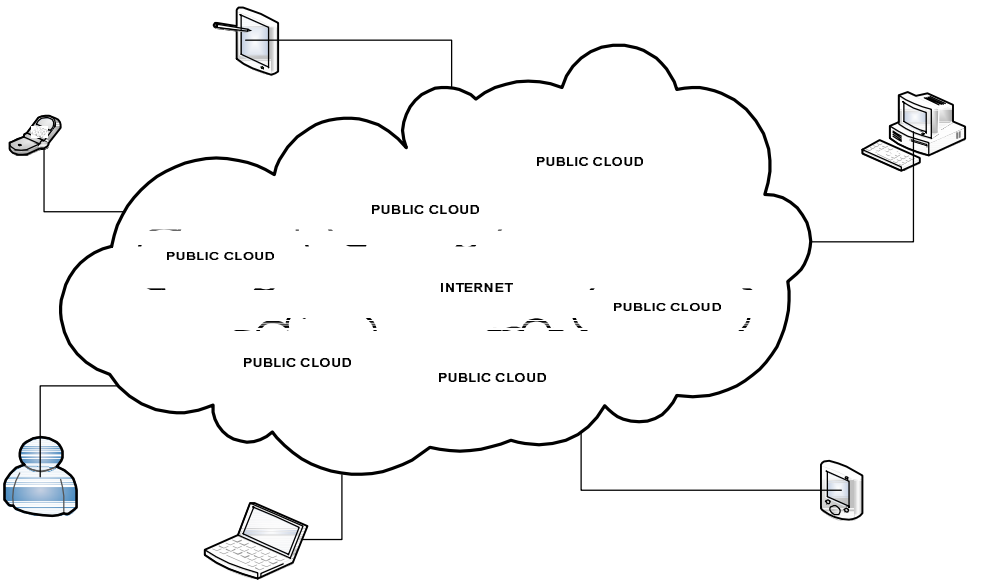
Een public cloud is een cloud die over het internet toegankelijk is en waarvan meerdere klanten gebruik kunnen maken (zie figuur 3). Een public cloud wordt door een cloud provider opgezet die niet in het land gevestigd hoeft te zijn. Verder worden alle services zoals dataopslag, software en hardware allemaal via het internet aangevraagd. Beveiliging voor gebruikers van een public cloud is niet volledig gegarandeerd vanwege de enige connectiemethode die hier beschikbaar is, namelijk het internet.

Voordelen:

- Minder kosten vanwege weinig nodige hardware
- Betalen waarvoor je het gebruikt
- Toegankelijkheid zolang er internet is

Nadelen:

- Minder beveiligd
- Niet - betrouwbaar
- Weinig controle over data



Figuur 3: Public Cloud

Ad 3 Hybrid cloud

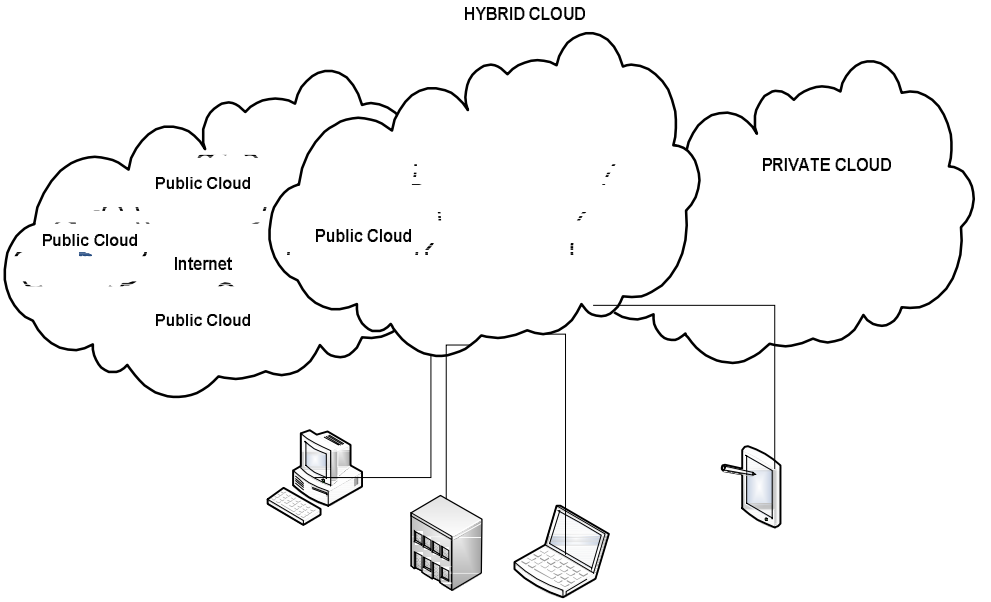
Een hybrid cloud is een mix van public cloud en een private cloud (zie figuur 4). Een goed voorbeeld hiervan is om een private cloud te gebruiken om data op te slaan en een public cloud voor software of applicaties die gebruikmaken van deze data en die toegankelijk te maken via het internet.

Voordelen:

- Minder kosten dan bij private cloud
- Data kunnen op locatie gehouden worden of ergens anders.
- Ingeval van extra opslag en processing kan dat aangekocht worden voor de tijd, dat het nodig is.

Nadelen:

- Beveiliging van data
- Geen vaste kosten uitgaven
- Afhankelijk van cloud provider voor enkele diensten.

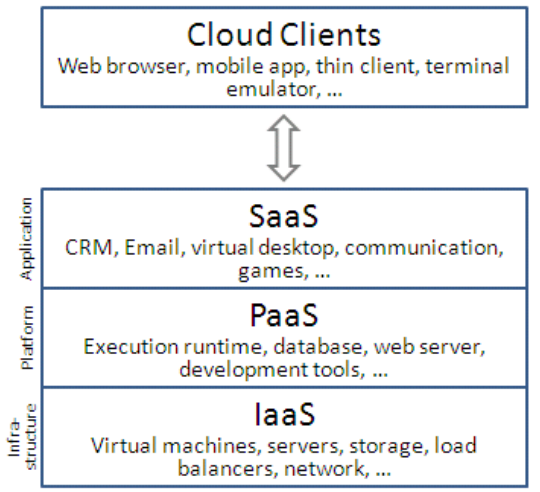


Figuur 4: Hybrid Cloud

2.3 Cloud computing services

Nu wij hebben gezien wat voor typen cloud er zijn is het goed te weten wat voor diensten er vanuit de cloud mogelijk zijn. Elke dienst binnen de cloud wordt onderverdeeld (zie figuur 5) in:

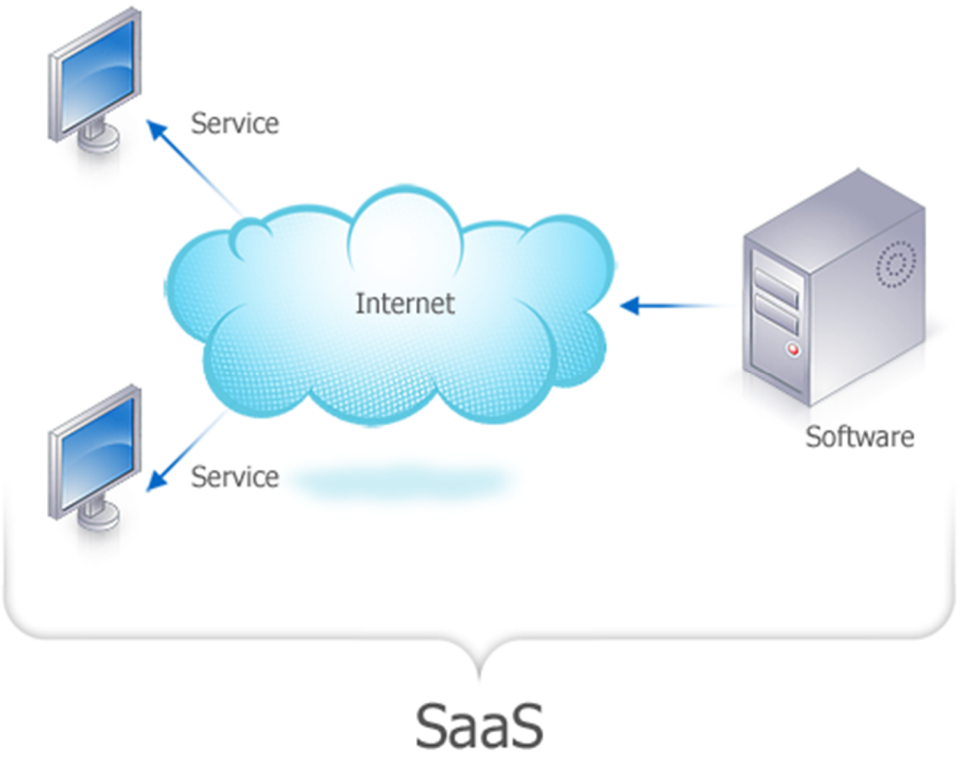
1. Software As A Service (SAAS)
2. Platform As A Service (PAAS)
3. Infrastructure As A Service (IAAS)



Figuur 5: Cloud -diensten

2.3.1 SAAS

Bij software as a service (SAAS) biedt de dienstaanbieder eindapplicaties aan via de cloud. Deze applicaties kunnen van allerlei soort zijn, bijvoorbeeld e-mail, klantenbeheer, personeelsbeheer, videoapplicaties. De dienstaanbieder heeft de volledige controle over de applicaties, maar de klant of een derde partij die het beheer uitvoert voor de klant, kan in veel gevallen wel de applicatie configureren en functioneel beheren. In veel gevallen zijn de SaaS-applicaties te gebruiken via een webbrowser op een computer. Hierbij wordt er doorgaans gebruikgemaakt van moderne technologieën zoals Ajax en HTML5 om een interactieve functionaliteit te verkrijgen die vergelijkbaar is of beter is dan die van traditionele client software. Veel SaaS-applicaties werken ook met mobiele apparaten zoals smartphones en tabletcomputers. Ook is er soms een specifiek stuk client software vereist en/of is de applicatie te gebruiken via een technische interface (API). Enkele voorbeelden van applicaties zijn Webmail, Skype, Facebook en Microsoft Office 365.

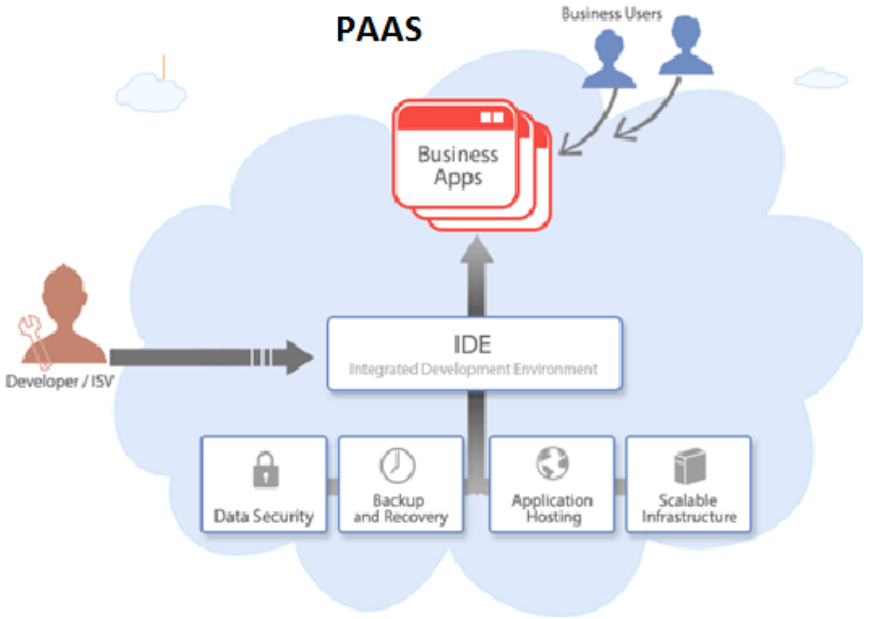


Figuur 6: SAAS (http://www.teamwox.com/en/groupware/articles/60/saas-online-collaboration-system)

2.3.2 PAAS

De PAAS biedt een aantal diensten bovenop de infrastructuur die SAAS -aanbieders de mogelijk geven hun toepassingen op een gestructureerde en geïntegreerde wijze aan te bieden.

Voorbeelden van diensten in deze service zijn toegangsbeheer, identiteitsbeheer, portaalfunctionaliteiten en integratiefaciliteiten. De klant van PAAS- diensten is een professionele, technische partij die voor het uitoefenen van zijn rol dan ook de nodige vrijheidshandelingen moet hebben, binnen vastgelegde grenzen. In dit systeem worden het framework en de infrastructuur beheerd door de dienstverlener en kan de gebruiker verder instaan voor de applicaties. Er is dikwijls ook sprake van faciliteiten voor de ontwikkeling. Hier wordt vaak gewerkt met een ontwikkelingstaal of framework zoals Python, .NET of Java waarin men functionaliteiten kan definiëren. Enkele voorbeelden van de aanbieders van de PAAS zijn PayPal, Google Apps Engine, Amazon S3, Rackspace Cloud Sites en Windows Azure.

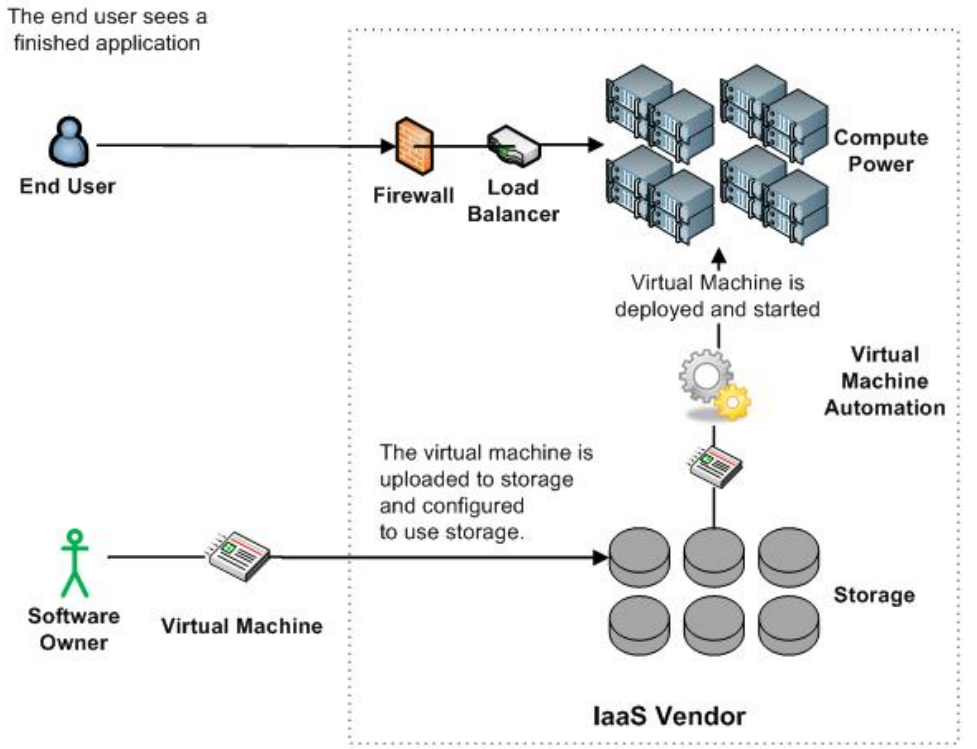


Figuur 7: PAAS (http://www.zoho.com/creator/paas.html)

2.3.3 IAAS

In deze service wordt de infrastructuur aangeboden via een virtualisatie van hardware-integratie. In deze service vindt men de servers, netwerken, opslagcapaciteit en andere infrastructuur. Dit geeft de gebruiker volledige vrijheid over de hardware.

De cloud server kan dan ook vanaf een externe locatie door meerdere personen worden bediend. Enkele voorbeelden van de aanbieders van de IAAS zijn Amazon, CloudWatch, en GoGrid .



Figuur 8: IAAS (http://cloudtimes.org/2011/02/27/what-to-consider-before-choosing-an-iaas-provider/)

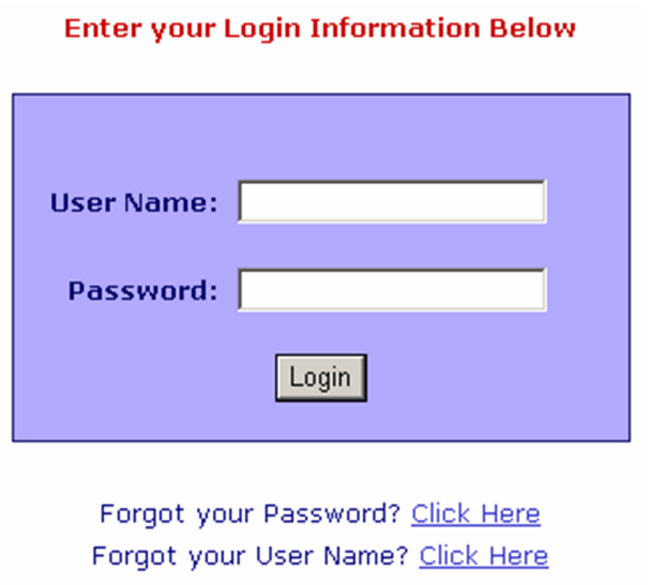
2.4 Beveiliging van cloud computing

De beveiliging is een heel moeilijk onderwerp omdat die van beide kanten afhankelijk is. De cloud provider kan heel veel security inbouwen maar als er bij de klant heel slecht wordt omgegaan met de security gegevens van de cloud provider dan kan de cloud provider geen garantie daarop geven. Zo zijn er ook privacy- overeenkomsten getekend door verschillende instanties ten aanzien van cloud computing voor de bescherming van privégegevens van klanten. De provider kan heel wat methoden toepassen ten aanzien van beveiliging.

Deze zijn:

1. Authenticatie:

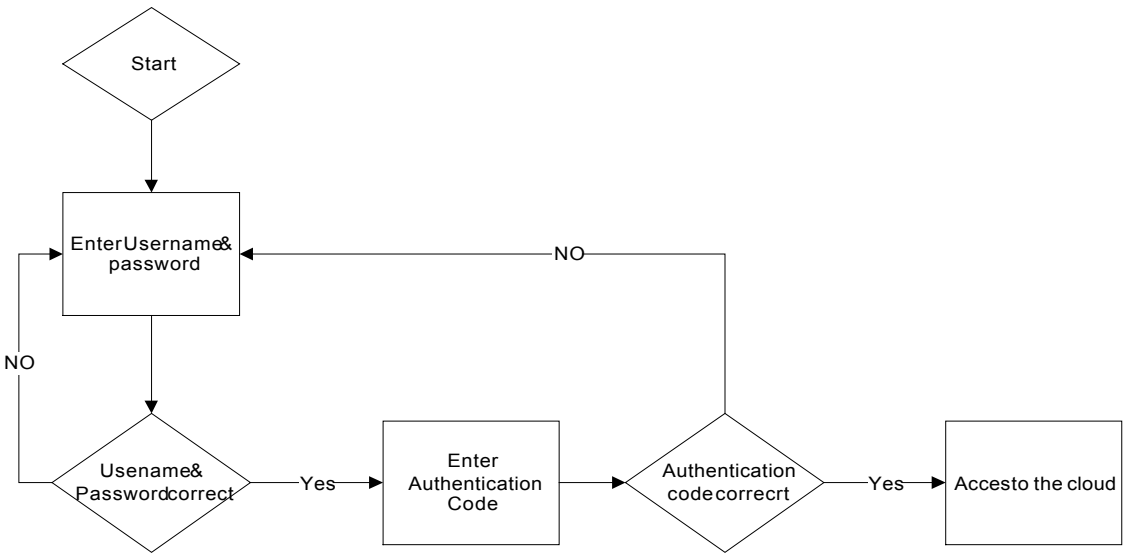
   De eindgebruiker kan door middel van de bekende username en passwordmethode toegang krijgen tot de dienst, zie figuur 9. Hiervoor zal wel een formulier met gewenste gegevens ingevoerd moeten worden.



Figuur 9: Authenticate (http://www.carlisle-local.k12.oh.us/Progress_Book.htm)

2. Autorisatie:

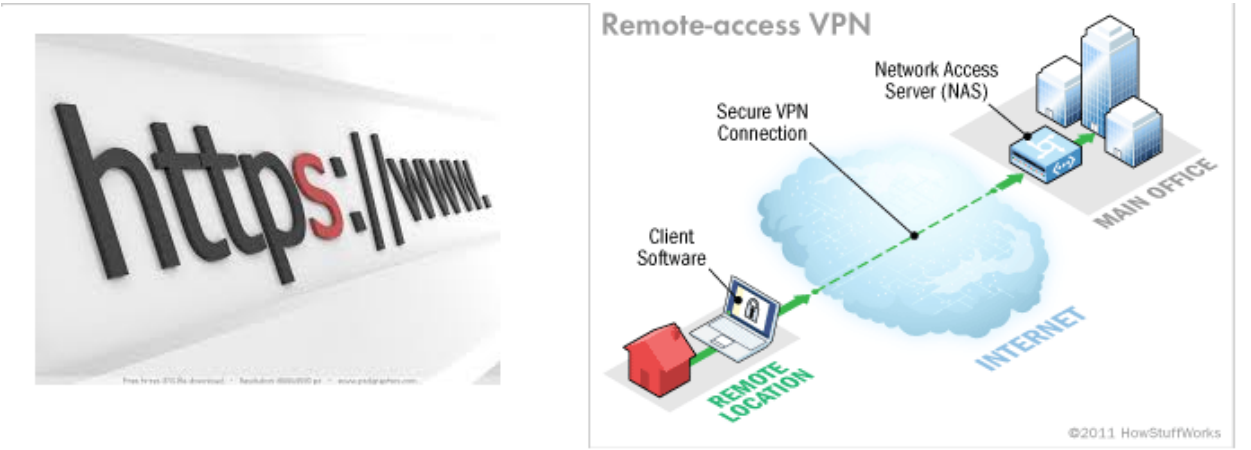
   Om als extra beveiliging te dienen kan er om autorisatie gevraagd worden aan de eindgebruiker. Dit kan op heel wat manieren gebeuren. |Een voorbeeld is om tijdens de registratie om een telefoonnummer te vragen waarnaar er bij elke login een code verstuurd wordt voor autorisatie, zie figuur 10.



Figuur 10: Flowchart van autorisatie

3. Encryptie:

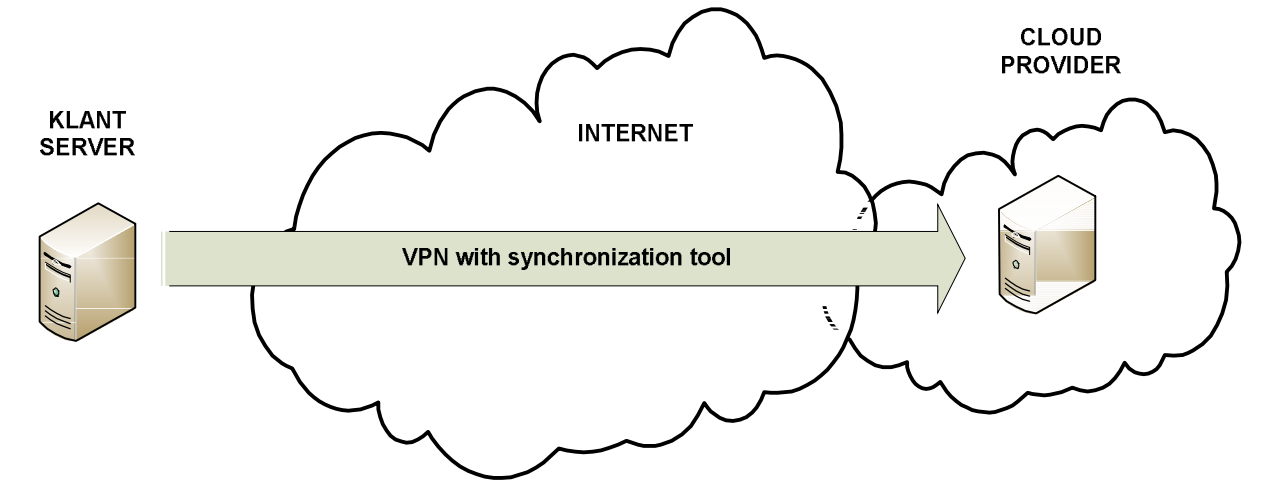
   De verbinding met de cloud-dienst is te allen tijde versleuteld. Dit kan door gebruik te maken van een https- (Hypertext Transfer Protocol Secure) pagina of door gebruik te maken van een VPN- (Virtueele Privé Netwerk) connectie.



Figuur 11: https en VPN solution.(http://facebooksecurity.blogspot.com, http://www.howstuffworks.com/vpn.htm/printable)

4. Gebruikersbeheer:

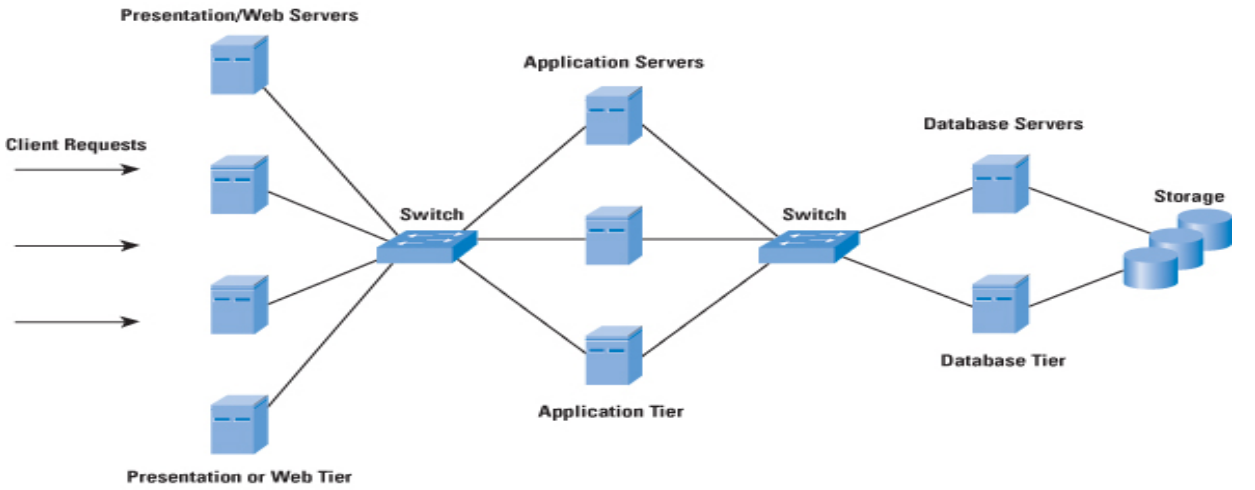
   De cloud provider biedt een synchronisatie tool aan die een secure toegang heeft tot de gegevens van de klant en die automatisch updates uitvoert tussen klant en provider.
   De secure connectie kan ook via een VPN gebeuren.



Figuur 12: Secure connectie met synchronisatietool

2.6 Cloud computing architectuur

Nu er al gezien is wat cloud computing allemaal inhoudt moeten wij ook weten wat er in het algemeen nodig is om cloud computing op te zetten. Figuur 13 geeft aan hoe een standaard cloud architectuur eruitziet volgens Cisco.



Figuur 13: Cloud computing architectuur volgens Cisco
(http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_12-4/124_cloud2.html)

Omdat klanten zelf geen servers zullen aanschaffen betekent het dat deze servers aangekocht moeten worden door de cloud provider om de klanten de nodige hardwarediensten aan te bieden. In figuur 13 zien wij dat vanaf het begin de cloud- structuur al bestaat uit webservers voor toegang naar je cloud, daarna application servers voor het leveren van softwarediensten en op de achtergrond hebben wij databaseservers voor capaciteit- en processing power doeleinden en als laatste storage voor opslag. Aan de hand van welke dienst er geleverd wordt zal de structuur veranderen of de hoeveelheid aangepast worden. Verder zou de cloud provider een dedicated internetverbinding moeten hebben om alle cloud -diensten zonder enig probleem te kunnen leveren. Bij het leveren van cloud -diensten moet de provider zich aanpassen om duizenden klanten te voorzien van cloud - diensten aangezien ze een internetdienst zijn. Om zo een groot aantal klanten te voorzien zullen er grote aantallen servers aan elkaar verbonden moeten worden zoals te zien is in figuur 13. Om zo een groot aantal servers te faciliteren zal er gebruik moeten worden gemaakt van een datacenter.

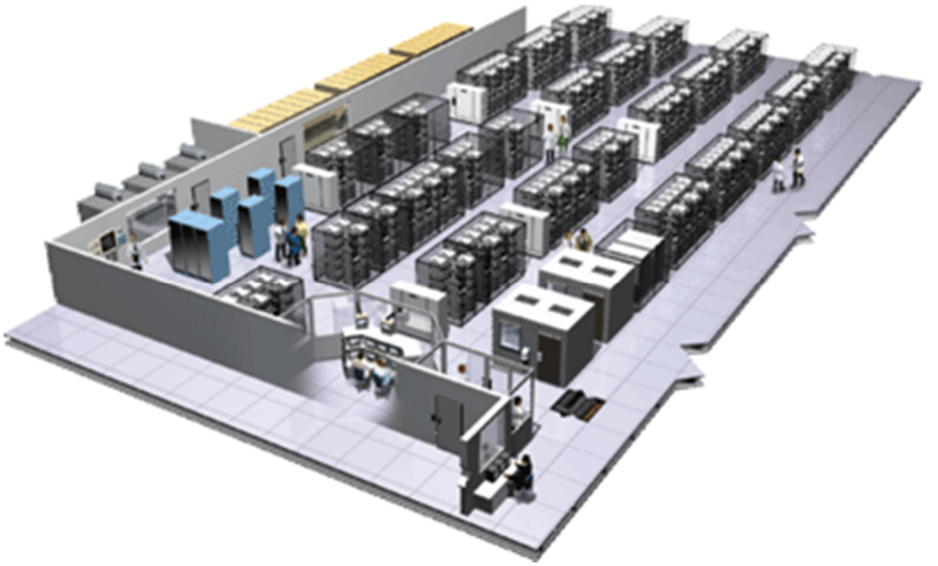
3 Datacenter

In dit hoofdstuk wordt beschreven wat een datacenter is (3.1), wat de kenmerken van een datacenter zijn(3.2) en welke standaarden er gebruikt worden voor een datacenter(3.3).
Bron: http://www.datacenter.rdm.com

3.1 Wat is een datacenter?

Een datacenter is een gebouw of faciliteit waar bedrijfskritische ICT-apparatuur (bijvoorbeeld servers) kan worden ondergebracht (zie figuur 14). Een datacenter is uitgerust met diverse voorzieningen, waaronder klimaatbeheersing door middel van airconditioning, geavanceerde automatische brandblussystemen en back-upstroomvoorzieningen. Kortom, een datacenter is een afgesloten ruimte met diverse voorzieningen om servers zo optimaal mogelijk te laten draaien.
Zo heeft een datacenter een aantal kenmerken:

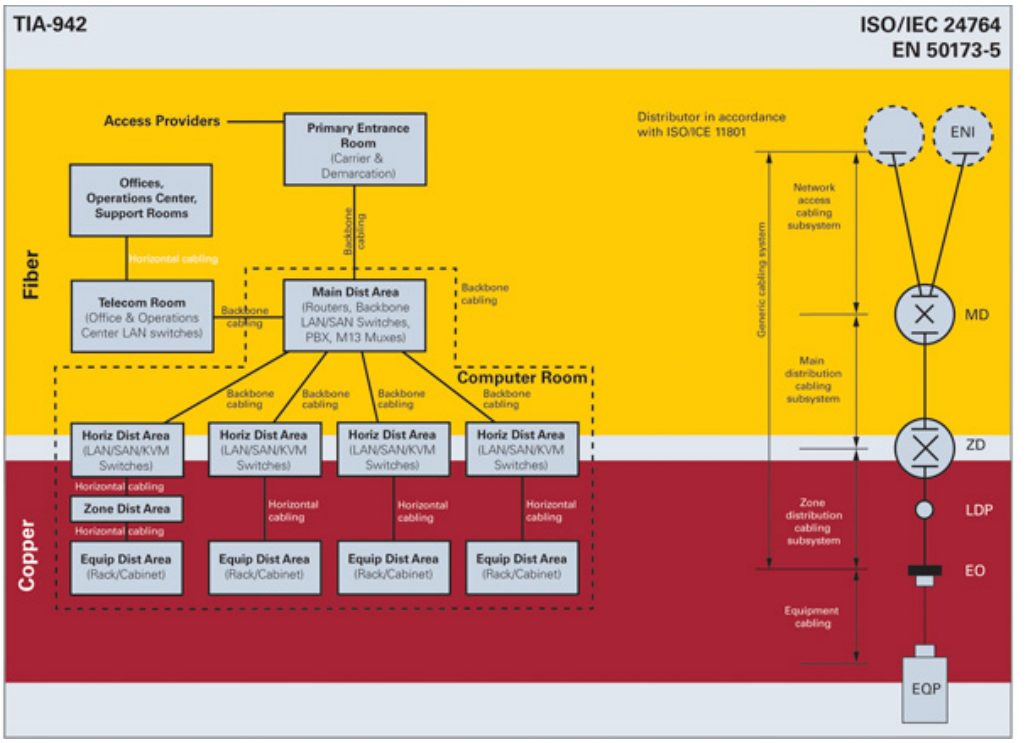
1. Airconditioning
2. Netwerkverbindingen
3. Noodstroomvoeding, ook wel UPS genoemd
4. Verhoogde vloeren
5. Redundantie
6. Brandblussysteem



Figuur 14: Datacenter (http://www.quintis.com/dtc_home.aspx)

3.2 Standaarden van een datacenter

Het bouwen van een datacenter moet aan internationale standaarden voldoen. Zo hebben wij instanties die daarvoor zorgen, namelijk de de American National Standards Institute (ANSI) en European Committee for Electrotechnical Standardization (CENELEC). De ANSI is volgens Amerikaanse standaarden en CENELEC volgens Europese standaarden. De beide organisaties hebben hun eigen standaardcodes: voor ANSI is het de TIA en voor CENELEC is het EN.
De Telecommunications Industry Association (TIA) is geaccrediteerd door de American National Standards Institute (ANSI) om standaarden te ontwikkelen voor een aantal Information and Communication Technologies (ICT) producten. Enkele zijn : private radio equipement, cellular towers, van het bedrijf zelf, satellites, telephone terminal equipment, accessibility, VoIP devices, structured cabling, datacenters, mobile device communications, multimedia multicast, vehicular telematics, healthcare ICT, machine-to-machine communications en smart utility networks. Voor datacenters wordt de TIA-942 en de EN50173-5 standaard toegepast. Volgens de TIA-942 en de EN50173-5 standaard geldt voor het bouwen van een datacenter het volgende. Zie figuur 15.



Figuur 15: Datacenter standards (http://www.datacenter.rdm.com/global/en/data-center-solutions/data-center-standards.html)

TIA-942:

1. One or more entrance rooms
2. Main Distribution Area (MDA)
3. One or more Horizontal Distribution Areas (HDA)
4. Equipment Distribution Area (EDA)
5. Backbone and Horizontal cabling

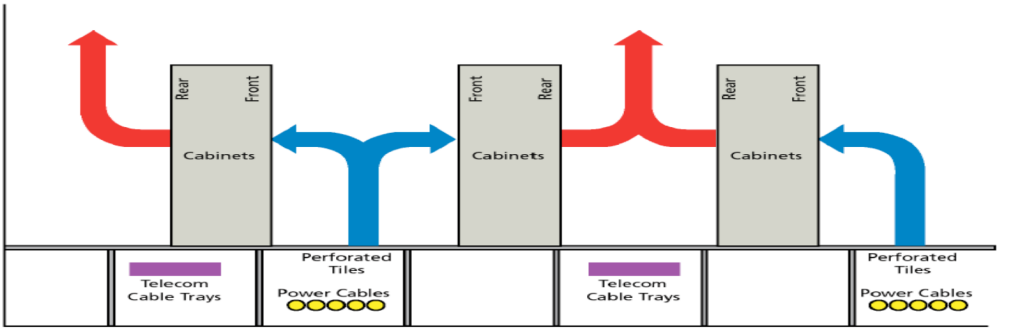
EN 50173-5:

1. ENI: External Network Interface
2. MD: Main Distributor
3. ZD: Zone Distributor
4. LDP: Local Distribution Point

TIA-942 en EN 50173-5 gebruiken andere namen voor hun opbouw maar de structuur blijft het-zelfde. Hoewel TIA-942 zich concentreert op de opbouw van een datacenter, houdt EN 50173-5 zich grotendeels bezig met de bekabeling. Dus een combinatie van de twee is ideaal voor elke datacenter.

3.3 Koeling van een datacenter

Hier worden de kenmerken airconditioning en verhoogde vloeren beschrijven. Binnen een datacenter zal er met een grote hoeveelheid ICT- apparatuur gewerkt worden. ICT- apparatuur moet heel koel blijven om optimale performance en langdurigheid te garanderen. Verder zal de hoe-veelheid stroom die voor deze ICT- apparatuur verbruikt wordt ook voor verhoogde temperatu-ren zorgen. Zo is het ook belangrijk om een datacenter in omgevingen te bouwen waar de tem-peratuur zo laag mogelijk gehouden zou kunnen worden. Indien een geschikte plek niet gevon-den kan worden zal er heel veel aan de koelinstallaties gedaan moeten worden. Zo heeft de TIA-942 standaard een oplossing voor een heel goed koelsysteem dat gebruikt kan worden binnen de datacenter. Door gebruik te maken van verhoogde vloeren kan de gekoelde lucht ook van onder de apparaten geschieden. Voor de koeling heeft men een opzetstandaard voor unitruimte, beka-beling en stroomdistributie, zie figuur 16.



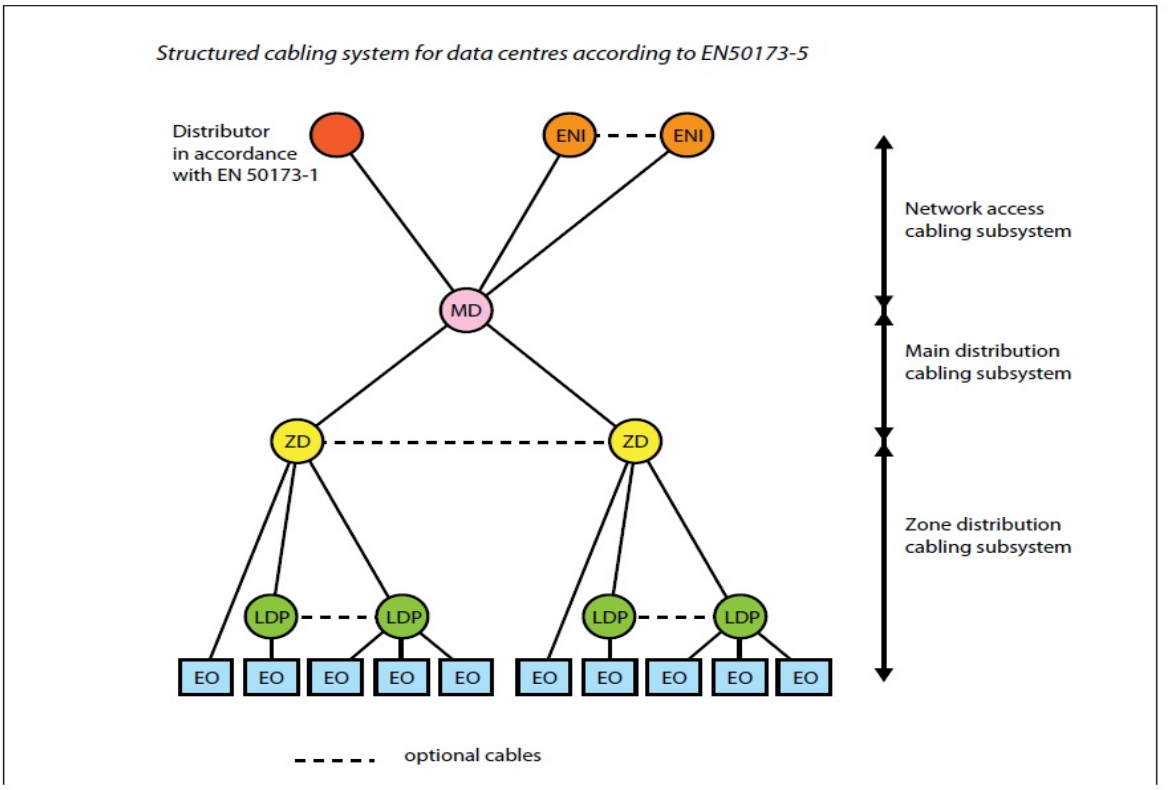
Figuur 16: Koelingstandaard

3.4 Bekabeling van een datacenter

De bekabeling van een datacenter is heel belangrijk bij het opzetten van een datacenter. Bekabeling zorgt voor de communicatie tussen alle ICT- apparatuur binnen de datacenter. Verder moet men ook weten welk type kabel er gebruikt zal moeten worden voor het opzetten van de datacenter. Om een betere uitleg te geven van de bekabeling zal er gebruikgemaakt worden van de standaard EN 50173-5. Volgens EN 50173-5 standaard zijn er drie bekabelingssystemen binnen een datacenter, zie figuur 17.

Deze zijn:

1. Network acces cabling subsystem
2. Main distribution cabling subsystem
3. Zone distribution cabling subsystem



Figuur 17: Bekabeling structuur volgens EN 50173-5

Naast het kabelsysteem is het ook belangrijk te weten wat voor typen kabels er nodig zijn en wat de mogelijkheid is van elk type kabel. In tabel 2 is dit allemaal te zien waarbij snelheid, afstand en kabeltype allemaal een verhouding met elkaar hebben.

Tabel 1: Kabeltypen

Ethernet Protocols IEEE 802.3 (maximum values)	Application Area Copper (m)				Application Area Fiber Optic (m)			
	Cat. 5e	Cat. 6	Cat. 6 Real10*	Cat. 6_A	OM1/2	OM3	OM4	OS2
100 Gbit/s	–					125	150	
40 Gbit/s	–					125	150	
10 Gbit/s	–		100	100	82	300	550	40000
1 Gbit/s	100	100	100	100	500	750	750	
100 Mbit/s	100	100	100	100	550	550	550	

3.5 Redundantie van een datacenter

Redundantie heeft te maken met de bereikbaarheid en beschikbaarheid van alle ICT-apparatuur binnen de datacenter. Om de beschikbaarheid te garanderen wordt de spanning in de meeste gevallen dubbel uitgevoerd indien er spanningsproblemen zouden kunnen optreden. Voor de bereikbaarheid worden ook de netwerkverbindingen dubbel uitgevoerd. Onder dubbele uitvoering verstaat men dat de ICT -apparatuur vanuit twee verschillende bronnen gevoed wordt en ook vanuit twee verschillende bronnen connecties heeft. Bij een datacenter wordt de mate van redundantie dienodig is, verdeeld onder Tier levels. Volgens de TIA-942 standaard zijn er vier Tier levels(zie tabel 2). Tiers zijn niets meer dan een gestandaardiseerde methodologie om de uptime van een datacenter te defineren. De beschikbaarheid van elke Tier level is :

1. Tier 1: Gegarandeerd 99.671% beschikbaarheid.
2. Tier 2: Gegarandeerd 99.741% beschikbaarheid.
3. Tier 3: Gegarandeerd 99.982% beschikbaarheid.
4. Tier 4: Gegarandeerd 99.995% beschikbaarheid.

Tabel 2: TIA-942 Tier model

Criticality	Business characteristics	Effect of system design
1. (Lowest)	•Typically small businesses •Mostly cash-based •Limited online presence •Low dependence on IT •Perceive downtime as a tolerable inconvenience	•Numerous single points of failure in all aspects of design •No generator if UPS has 8 minutes of backup time •Extremely vulnerable to inclement weather conditions •Generally unable to sustain more than a 10 minute power outage
2.	•Some amount of online revenue generation •Multiple servers •Phone system vital to business •Dependent on email •Some tolerance to scheduled downtime	•Some redundancy in power and cooling systems •Generator backup •Able to sustain 24 hour power outage •Minimal thought to site selection •Vapor barrier •Formal data room separate from other areas
3.	•World-wide presence •Majority of revenue from online business •VoIP phone system •High dependence on IT •High cost of downtime •Highly recognized brand	•Two utility paths (active and passive) •Redundant power and cooling systems •Redundant service providers •Able to sustain 72-hour power outage •Careful site selection planning •One-hour fire rating •Allows for concurrent maintenance
4. (Highest)	•Multi-million dollar business •Majority of revenues from electronic transactions •Business model entirely dependent on IT •Extremely high cost of downtime	•Two independent utility paths •2N power and cooling systems •Able to sustain 96 hour power outage •Stringent site selection criteria •Minimum two-hour fire rating •High level of physical security •24/7 onsite maintenance staff

3.6 Beveiliging binnen een datacenter

De beveiliging binnen een datacenter kan verder verdeeld worden in:

1. beveiliging van de datacenter zelf
2. beveiliging van de informatie binnen een datacenter.

Beveiliging van de datacenter zelf ligt meer aan hoe men toegang tot de datacenter zal geven en verder hoe men de handelingen die men uitvoert binnen de datacenter zal controleren. Hiervoor kan men beperkte toegang geven aan een bepaald groep van personeel, verder een camerasysteem installeren als ook zwaardere eisen voor toegang eisen, een vingerafdrukscanner of misschien wel een retinascanner plaatsen voor toegang tot de datacenter. Verder kan het beveiligen van informatie binnen de datacenter tot stand gebracht worden door gebruik te maken van kleurencoderingen voor kabels als ook plugs en verder door middel van labels waardoor beveiligde connecties gemaakt kunnen worden die geen problemen veroorzaken.

3.7 Lokaliseren van een datacenter

De inhoud van de datacenter is heel belangrijk maar om een datacenter goed op te zetten zal de locatie ook een heel grote rol spelen in het geheel. Een datacenter kan niet op elk gebied geplaatst worden: er is een aantal randvoorwaarden waaraan het gebied moet voldoen.
Deze randvoorwaarden zijn:

1. De verbindingen of connecties met de klanten en internet
2. De energievoorziening
3. Milieu
4. Kwaliteit

4 Telesur

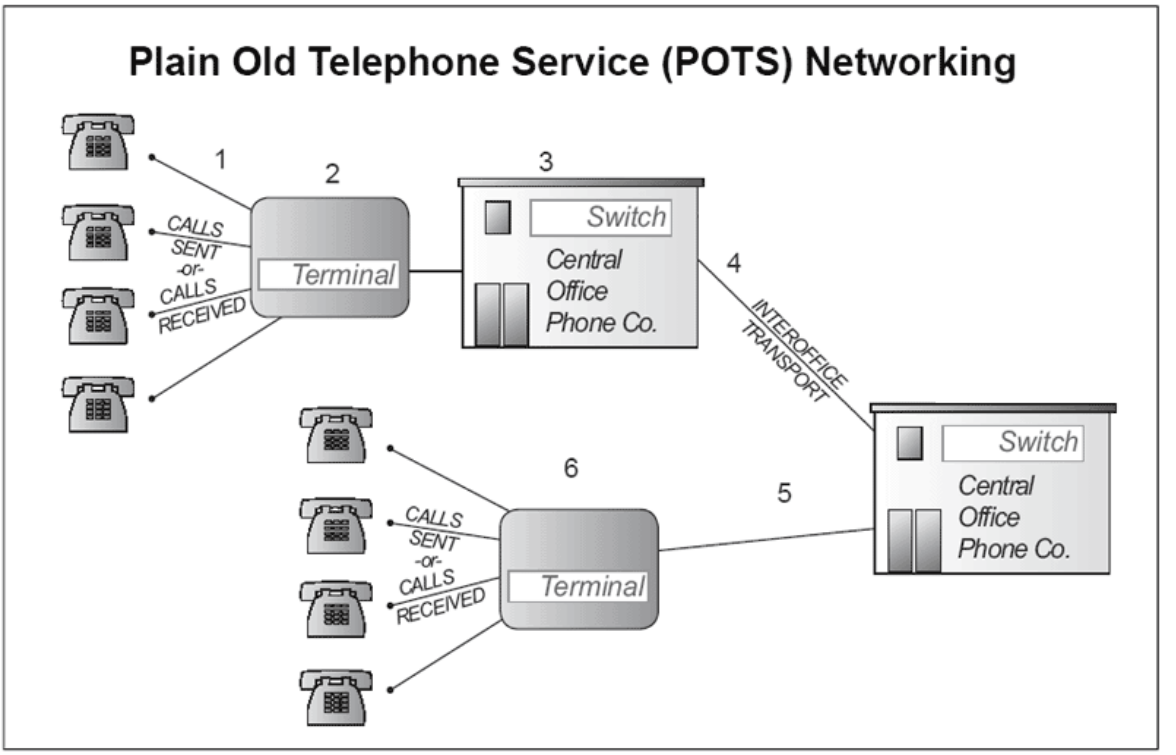
In dit hoofdstuk wordt beschreven hoe de huidige situatie van Telesur eruitziet (4.1), hoe wij Telesur willen hebben gecombineerd met cloud computing (4.2) en wat de mogelijke impact zal zijn als cloud computing geïmplementeerd wordt (4.3).
Bron: Afdeling Data Communicatie Diensten Telesur
http://www.mackinac.org

4.1 Huidige situatie Telesur

Telesur is een telecommunicatiebedrijf dat binnen Suriname al gedurende een heel lange periode telecomdiensten aanbiedt zoals huistelefoon en cellulair. Met de groeiende technologische ontwikkelingen is Telesur ook internetdiensten gaan aanbieden binnen Suriname waar er ook een core netwerk geïmplementeerd moest worden zodat alle aansluitingen via het core netwerk moeten geschieden. Een core netwerk is het hoofdnetwerk binnen een bedrijf waarvan alle datadiensten afkomstig zijn. Het zorgt ook voor communicatie tussen kleinere subnetwerken binnen een bedrijf of organisatie.
De huidige aansluitingen die Telesur biedt zijn:

1. Telefoon- of POTS- aansluitingen
2. Cellulaire of GSM- aansluitingen
3. Internetaansluitingen

Ad 1 POTS- aansluitingen
Telefoonaansluitingen zijn de bekende POTS- (Plain Old Telefoon System) aansluitingen die wij allemaal kennen van onze huisaansluitingen (zie figuur 18).



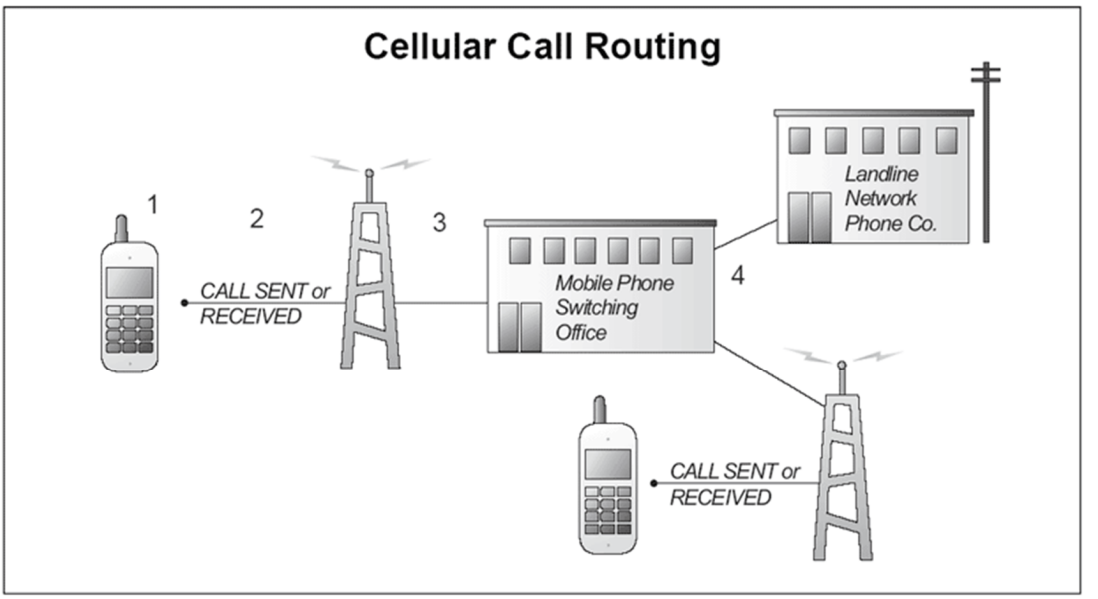
Figuur18: Werking van een POTS (http://www.mackinac.org/images.aspx?ID=6765)

Om een beter beeld te krijgen van de werking van zo een POTS -systeem zullen wij de nummering vanuit figuur 18 volgen:

1. Klant pleegt een call via zijn huistelefoon.
2. De gepleegde call maakt eerst connectie met de terminal van het gebied. Dit wordt meestal gezien als rechthoekige witte kasten aan de zijkant van de weg.
3. De terminal is in verbinding met de hoofdcentrale van het gebied en zal vanuit de centrale nagaan waarnaar toe de klant zijn call wenst te plegen.
4. Indien de gepleegde call zich in een ander centraal gebied bevindt zal die verder verstuurd worden naar de hoofdcentrale verantwoordelijk voor dat gebied.
5. De hoofdcentrale maakt verbinding met de terminal die verantwoordelijk is de call verder te versturen.
6. De call komt aan bij de desbetreffende persoon.

Ad 2 GSM- verbindingen

Cellulaire aansluitingen zijn onze bekende GSM- (Global System for Mobiles) aansluitingen, (figuur 19). Vanuit zijn GSM- netwerk draait Telesur zijn bekende services zoals de Blackberry, 2G en 3G. Services als 2G en 3G vallen onder internetverbindingen maar op het GSM- netwerk.



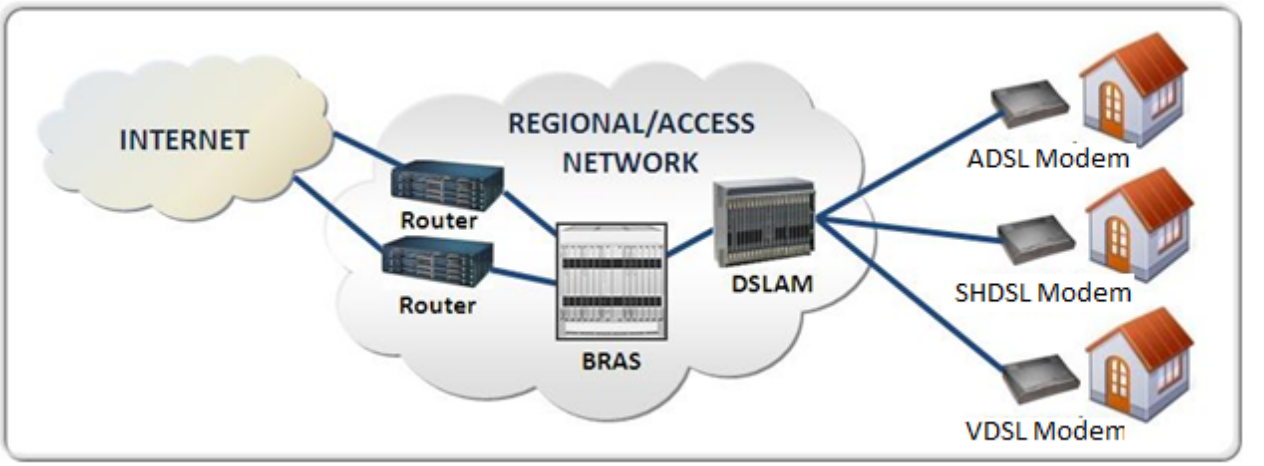
Figuur19: Structuur van GSM- netwerk.(http://www.mackinac.org/images.aspx?ID=6765)

Net zoals bij de POTS doen wij hetzelfde voor GSM:

1. De klant pleegt een GSM- call
2. Er wordt hierna verbinding gemaakt door middel van radiogolven met de dichtstbijzijnde basisstation die verder gekoppeld is met de hoofdcentrale van dat gebied.
3. Er wordt nu gecontroleerd binnen de hoofdcentrale of de klant naar een ander GSM- toestel heeft gebeld of naar een huistelefoon.
4. Verder wordt deze verder verstuurd naar de gewenste verbinding

Ad 3 Internetaansluitingen

Internetverbindingen worden grotendeels geleverd door middel van Telesurs koper infrastructuur waarvan onze telefoonaansluiting ook gebruik maakt. Om internet te leveren aan de klanten wordt er gebruikgemaakt van een aantal methodieken zoals Asymmetric digital subscriber line (ADSL), Single-pair high-speed digital subscriber line (SHDSL) en Very-high-bit-rate digital subscriber line (VDSL)(zie figuur 20).



Figuur20: Bekende internetverbindingen

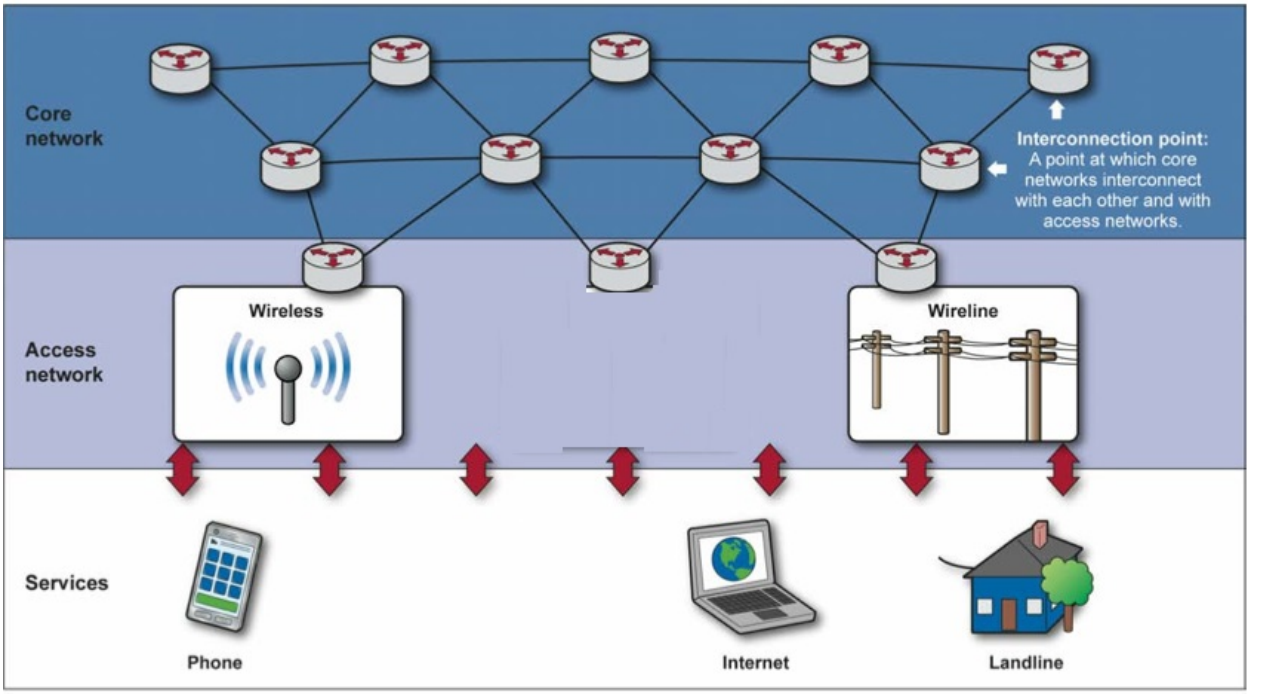
Elke internetverbinding heeft ook zijn maximale bandbreedte die hij kan leveren, zie tabel 3.

Tabel 3: Banbreedte tabel

Family	ITU	Name	Ratified	Maximum Speed capabilities
ADSL	G.992.1	G.dmt	1999	7 Mbps down 800 kbps up
ADSL2	G.992.3	G.dmt.bis	2002	8 Mb/s down 1 Mbps up
ADSL2plus	G.992.5	ADSL2plus	2003	24 Mbps down 1 Mbps up
ADSL2-RE	G.992.3	Reach Extended	2003	8 Mbps down 1 Mbps up
SHDSL (updated 2003)	G.991.2	G.SHDSL	2003	5.6 Mbps up/down
VDSL	G.993.1	Very-high-data-rate DSL	2004	55 Mbps down 15 Mbps up
VDSL2 -12 MHz long reach	G.993.2	Very-high-data-rate DSL 2	2005	55 Mbps down 30 Mbps up
VDSL2 - 30 MHz Short reach	G.993.2	Very-high-data-rate DSL 2	2005	100 Mbps up/down

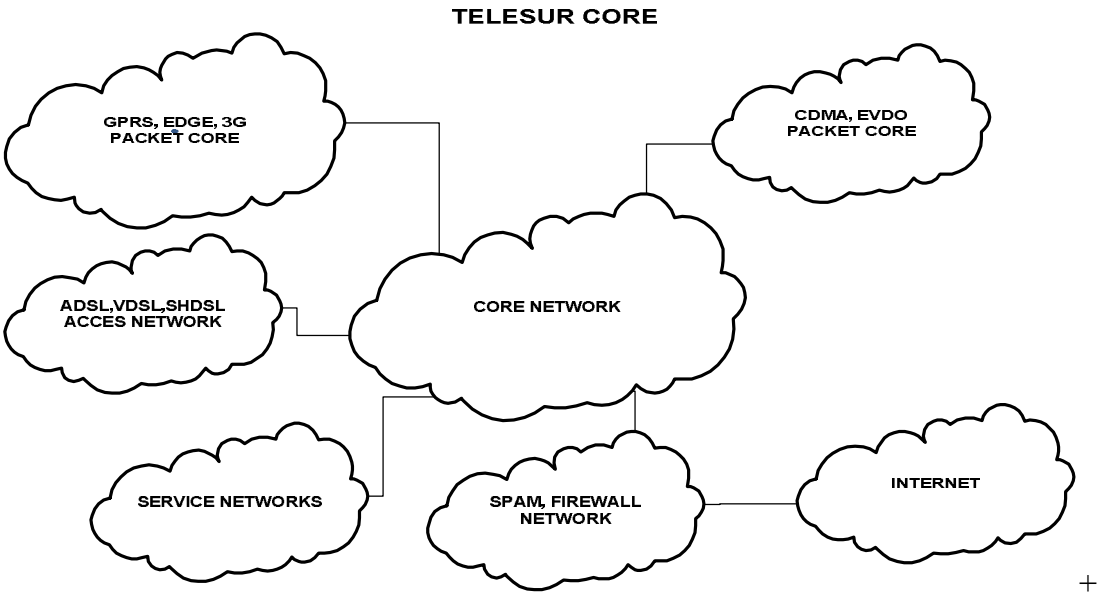
Andere internetverbindingen die geen gebruikmaken van de koper infrastructuur zijn de WCDMA- en EVDO- verbinding. EVDO en WCDMA werken volgens hetzelfde principe als een GSM- toestel, alleen op een andere golflengte.

Bij de introductie van internetverbindingen aan de samenleving heeft Telesur binnen zijn POTS- en GSM- netwerk een data core netwerk gebouwd dat voor het totale datanetverkeer zorgt voor zowel het gehele Telesurbedrijf als voor de klanten verbonden bij Telesur.
Het huidige netwerk is momenteel opgebouwd uit drie lagen, te weten :de core laag, access of distributielaag en service of toegangslaag (zie figuur 21)



Figuur 21: Drielagenmodel

Het huidige core netwerk met alle bijbehorende services ziet er als volgt uit (figuur 22):



Figuur 22:Huidig core netwerk

4.2 Gewenste situatie Telesur

De huidige situatie biedt al internet-, gsm- en telefoondiensten aan de klanten van Telesur maar met de voortgang van technologie in de wereld moet Telesur meegaan met wat er internationaal gebruikt wordt en bewijzen dat het ook lokaal mogelijk is. Cloud computing wordt veelal overal in de wereld gebruikt door grote bedrijven zoals Google, Amazon, Apple, Cisco en Microsoft en deze bieden dezelfde diensten die zij zelf gebruiken aan klanten wereldwijd. Telesur zou net als deze grote bedrijven ook cloud computing kunnen introduceren om aan te geven dat ook lokaal deze diensten verkrijgbaar zijn en dat dit niet alleen internationaal mogelijk is. Telesur heeft twee mogelijkheden waarbij het zich kan aanpassen aan cloud computing. Deze zijn:

1. Telesur gebruikt de infrastructuur van buitenlandse cloud providers door de gewenste capaciteit en services in te huren.
2. Telesur creëert zijn eigen cloud infrastructuur door een datacenter op te zetten met een ervaren cloud vendor bijvoorbeeld, VMware, IBM, HP. Hierdoor wordt Telesur zijn eigen cloud provider.

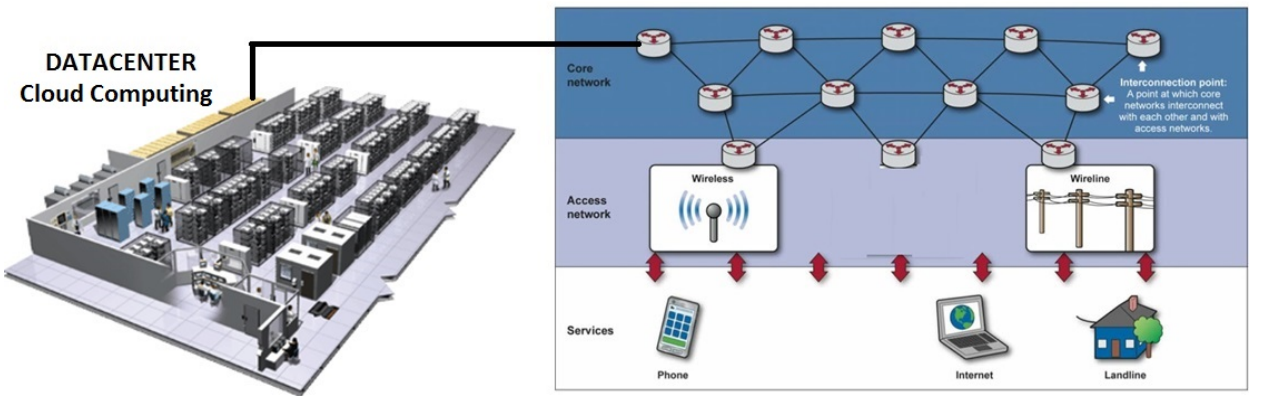
4.2.1 Telesur met buitenlandse cloud provider

Telesur kan zijn gewenste cloud diensten uitbesteden aan externe cloud providers zoals Google, Amazon, Apple, Cisco of Microsoft. Het voordeel dat Telesur hier aan kan hebben is kostenbe-

sparing. Kostenbesparing kan men verder onderverdelen in: het minder gebruikmaken van apparatuur, geen extra personeel voor beheer en onderhoud van systemen.
Nadeel voor Telesur is dat alle data en services via het buitenland opgeslagen en beheerd worden. Telesur is afhankelijk van de bereikbaarheid en beschikbaarheid van zijn buitenlandse cloud provider.

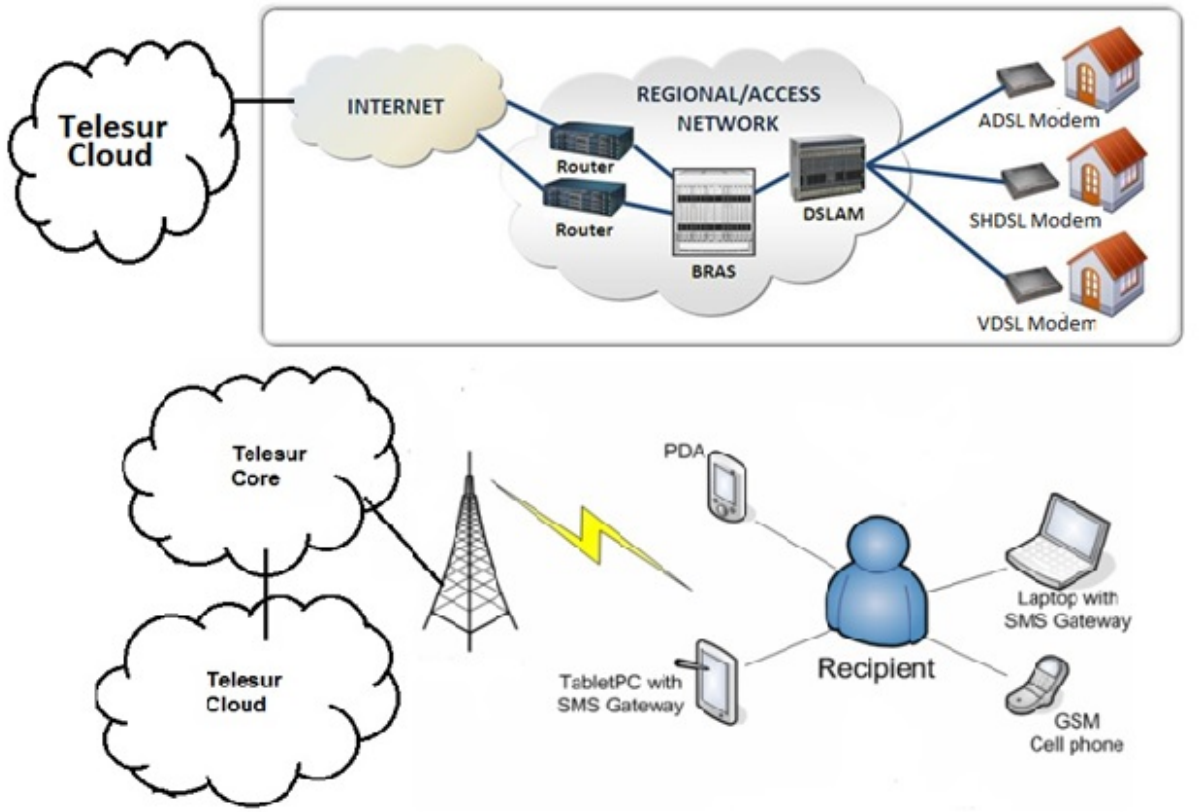
4.2.2 Telesur als lokale cloud provider

Bij het implementeren van cloud computing lokaal zal Telesur een datacenter moeten opzetten, dat zal moeten voldoen aan de internationale standaarden en voorwaarden(zie paragraaf 3.2, Standaarden van een datacenter). Deze datacenter zal dan een koppeling maken met Telesurs huidige data core netwerk om deze te implementeren in het geheel (figuur 23).



Figuur 23: Datacenter gecombineerd met het data core netwerk.

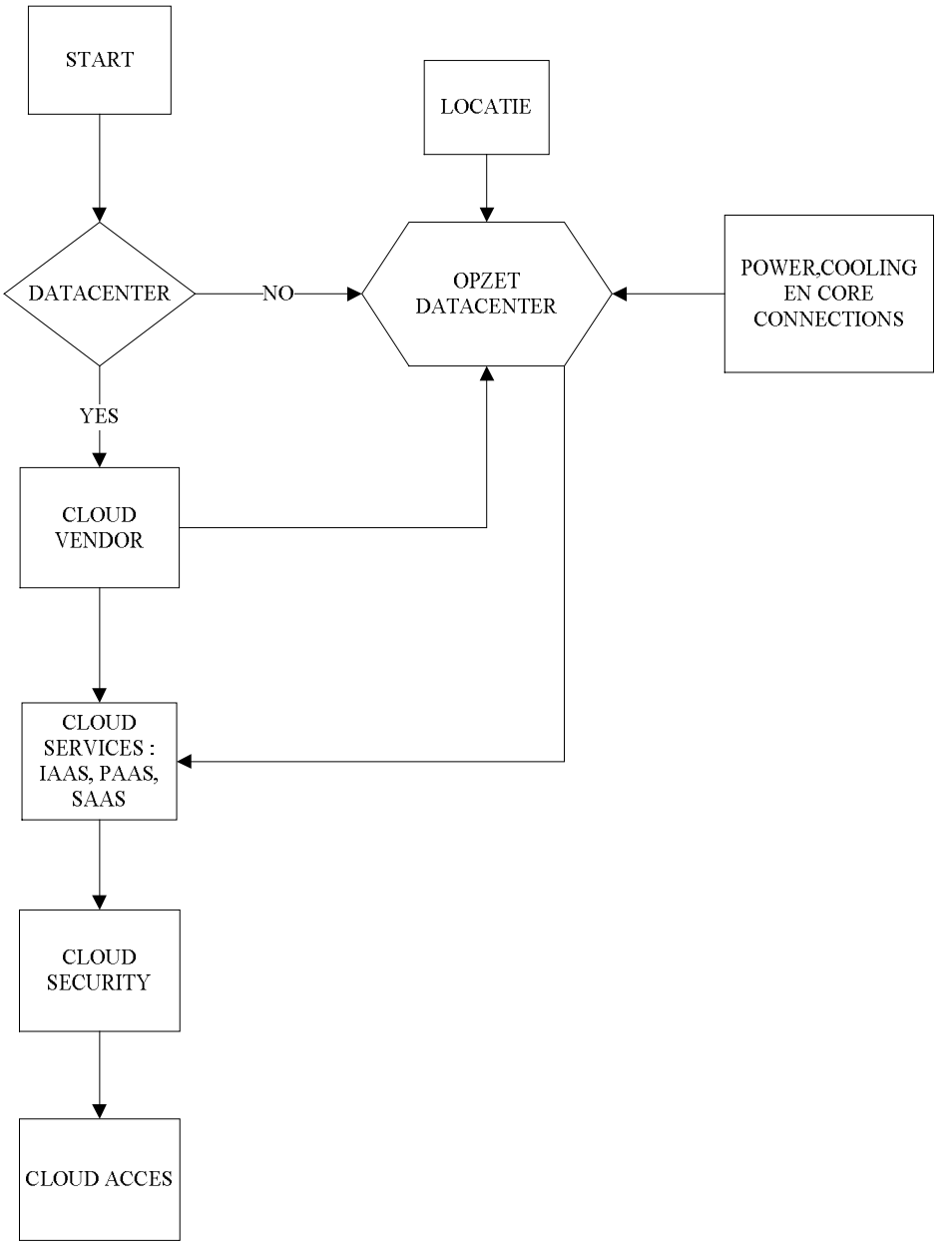
Klanten zullen gebruikmaken van onze huidige internetverbindingen om toegang te krijgen tot Telesur cloud (figuur 24). Cloud computing is afhankelijk van je internetconnectie en de bandbreedte speelt ook een grote rol bij het bieden van een goede cloud service. Grote bedrijven die heel veel gebruik zouden willen maken van zo een service zullen heel veel bandbreedte ter beschikking moeten krijgen waarvan de huidige koper infrastructuur van Telesur heel verouderd is.



Figuur 24: Toegang tot de cloud

Bij het opzetten van de datacenter zullen er database servers aangeschaft moeten worden voor het maken van back-ups en het opslaan van data. Om aan de eisen van cloud computing te voldoen zal er met een cloud vendor afgestemd moeten worden of de huidige servers voldoen of dat er andere aangekocht moeten worden. De mogelijkheid bestaat ook om de database samen met de cloud vendor te installeren waarbij de software al aanwezig zal zijn. Aangezien een datacenter wordt gebruikt voor het maken van back-ups en het opslaan van data kan Telesur alvast voldoen aan het bieden van storage als een service die deel uitmaakt van IAAS. De overige services zoals SAAS en PAAS kunnen in de toekomst als service aangenomen worden. Dit vanwege externe invloeden zoals het hebben van additionele software en expertise om deze services uitgevoerd te krijgen.

Hoe de implementatie zal geschieden, zal duidelijk gemaakt worden met de volgende flowchart, zie figuur 25.



Figuur 25: Flowchart technische implementatie

4.3 Impact van implementatie van cloud computing

In het strategische plan 2006 - 2016 wordt aangegeven dat Telesur marktleider wil zijn van NICE-diensten (Network Information Communication Entertainment). Als we naar de letters N en I kijken die staan voor network en information dan voldoet cloud computing voor het uitbreiden van deze typen diensten. Het biedt de klant de mogelijkheid zijn netwerk uit te breiden door middel van het verkrijgen van meer opslag zonder dat de apparatuur hiervoor aangeschaft hoeft te worden. Verder kan men de vergrote opslagruimte gebruiken voor het opslaan van voldoende informatie, Aangezien de technologische ontwikkelingen niet stilstaat, zullen er heel veel spelers

zijn die cloud computing als service zouden willen aanbieden om hun dienstenpakket te vergroten.

Enkele voordelen en nadelen voor Telesur zijn:
Voordelen voor Telesur:

1. Minder kosten intern voor zowel het bedrijf als extern voor de klanten.
2. Informatie toegankelijk op elke locatie waar er een internetconnectie aanwezig is.
3. Nieuwe dienstenmogelijkheden naar klanten toe.
4. Toename van aantal nieuwe klanten die gebruik willen maken van cloud diensten
5. Mogelijkheid om in de toekomst diensten internationaal uit te breiden omdat de cloud via het internet werkt.
6. Nationaal opgezette datacenter zodat de data niet over het internet getransporteerd hoeven te worden.

Nadeel voor Telesur:

1. Hoge kosten bij het opzetten van de datacenter
2. Het bijhouden van nieuwe cloud diensten en het trainen van personeel
3. Grote concurrentie met grote buitenlandse bedrijven als Google, Amazon, Dropbox,etc

De klanten zullen hiervan ook genieten als de voorwaarde voor het gebruik van cloud computing is een werkende laptop, pc of smartphone te hebben die toegang heeft tot het internet.

5 Conclusies en aanbevelingen

Conclusies

1. Binnen het huidige netwerk van Telesur kunnen er momenteel geen cloud diensten en services aangeboden worden.
2. Telesur kan cloud diensten inkopen en als wederverkoper fungeren.
3. Telesur kan cloud diensten bieden maar er moet eerst een datacenter gebouwd worden.
4. Grote bedrijven zullen meer bandbreedte nodig hebben om cloud diensten te draaien.
5. Verouderde koper infrastructuur kan een beperking zijn voor sommige klanten.

Aanbevelingen

1. Telesur zou zijn datacenter voor het leveren van zijn cloud service liever lokaal moeten draaien zodat hij meer beheer heeft over apparatuur, die aangeschaft wordt alsook de informatie die erin opgeslagen wordt. Beheer is belangrijk voor het beter beveiligen van bedrijfsgevoelige informatie die niet door derden afgehandeld wordt. Verder kunnen wij lokaal veel hogere bandbreedte aanbieden zodat de klant tevreden zal kunnen zijn met de service.
2. Cloud computing is slechts een dienst die een datacenter kan bieden . Er zijn heel veel andere methoden en diensten die een datacenter kan bieden dus meer dienstenopties voor toekomstige klanten
3. De beveiliging van een datacenter is heel belangrijk vanwege de grote hoeveelheid informatie van het bedrijf zelf die opgeslagen zal worden, alsook voor zijn toekomstige klanten. Hiervoor moeten heel strenge maatregelen genomen moeten worden om de klant gerust te stellen over zijn opgeslagen informatie.
4. Als start-up voor Telesur zouden wij kunnen beginnen met IAAS waarbij er capaciteit en infrastructuur aangeboden zal worden. Capaciteit is heel makkelijke aan te bieden omdat capaciteit alleen de cloud software nodig heeft om aangeboden te worden. SAAS zou ook als service optie aangeboden kunnen worden omdat softwareaankoop ook een van de meestgebruikte onderdelen binnen het bedrijfsleven is. Hiervoor zou Telesur een studie moeten doen wat de meest gebruikte software is binnen Suriname, deze moeten aanschaffen en verder distribueren naar zijn klanten.

5. Indien er lokaal meer bandbreedte aangeboden wordt en de verouderde koper infrastructuur een beperking zou kunnen veroorzaken lijkt verglazen van de koper infrastructuur een heel goede oplossing hiervoor te zijn.

Literatuurlijst

Geraadpleegde boeken:

- Escalante, A., Borko,F.(2010). an book of lou computing, Springer, Boca Raton/Florida USA.
- Kroenke, M.D. (2007). atabases, Beginselen, Ontwerp en Implementatie, Pearson Education Benelux.
- Marks, A.E., Lozano, B. (2010). ecutive s ui e to lou computing, John Wiley & Sons, Inc, Hoboken, New Jersey.
- Rittinghouse,W.J., Ransome, F.J. (2010). lou computing, mplementation anagement an ecurity, Taylor & Francis group, Boca Raton/ Londen New York.

Geraadpleegde rapporten

- Good-Engelhardt, Regina. ata entre tan ar -
- TIA-942 Datacenter Standards Overview

Onlinedocument

- www.previder.nl: White paper datacenter
-

Website

- http://www.datacenter.rdm.com/global/en/
- http://www.mackinac.org/images.aspx?ID=6765

Bijlage 1: Datacenters wereldwijd