AFSTUDEERRAPPORT

ADTS ICT B.V. - NL - Capelle aan den IJsel

Video over IP

Auteur	:	Maurice Rutenfrans
Studentnummer	:	10001468
Document	:	Afstudeerrapport – Haagse Hogeschool
Studie		Technisch Informatica
Releasedatum	:	08 Jan. 15
Versie	:	1.0
Status	:	Definitief

Referaat

Titelbeschrijving

Maurice Rutenfrans, “Video over IP”, Afstudeerrapport opleiding Technische Informatica, Haagse Hogeschool 2015

Samenvatting

Het wordt meer gebruikelijk om een collegezaal of vergaderruimte binnen te lopen, waarbij iedereen live een spreker of presentatie op een externe locatie volgt. Dit wordt o.a. mogelijk gemaakt door video over IP. In deze afstudeeropdracht wordt hier onderzoek naar gedaan en een proof of concept gerealiseerd. Dit afstudeerverslag beschrijft het traject dat is doorlopen bij het uitvoeren van de afstudeeropdracht.

Descriptoren

- Video over IP
- Videoconferencing
- Telepresence

Aanvullende informatie

Begeleidende examinator:	Jan Dirk Schagen
Tweede examinator:	Madelon Nieuwland
Afstudeerperiode:	25 augustus t/m 9 januari 2015

Organisatie:	ADTS ICT B.V.
Adres:	Cypresbaan 38
Postcode:	2908 LT
Plaats:	Capelle aan den IJssel
Telefoon:	+31 10 310 13 00
Bedrijfsmentor:	Bernhard van der Linde

Documenthistorie

Versie	omschrijving	Datum
0.1	Start afstudeerverslag	29 Aug. 14
0.2	Organisatiebeschrijving gemaakt	5 Sep. 14
0.3	Afstudeeropdracht beschreven	12 Sep. 14
0.4	Hoofdstuk voorbereidingsfase geschreven	26 Sep.14
0.5	Deel hoofdstuk onderzoeksfase geschreven	24 Okt. 14
	Concept klaar voor eerste review	26 Nov. 14
0.51	Feedback eerste review verwerkt	27 Nov. 14
0.6	Deel hoofdstuk ontwerpfase geschreven	5 Dec. 14
0.7	Hoofdstuk ontwerpfase afgerond	15 Dec. 14
0.8	Hoofdstuk implementatiefase geschreven	23 Dec. 14
0.9	Hoofdstuk testfase geschreven	30 Dec. 14
1.0	Afstudeerverslag afgerond	8 Jan. 15

Distributielijst

Versie	Datum	Ontvanger	Email
0.5	25 Nov. 14	Jan Dirk Schagen	J.D.Schagen@hhs.nl
1.0	9 Jan.15	Jan Dirk Schagen	J.D.Schagen@hhs.nl
1.0	9 Jan.15	Madelon Nieuwland	m.w.h.nieuwland@hhs.nl

Relevante documenten

Versie	Datum	Auteur	Document
1.0	05 sep. 14	Maurice Rutenfrans	Plan van aanpak
1.0	16 sep. 14	Maurice Rutenfrans	Onderzoeksplan
1.0	01 dec. 14	Maurice Rutenfrans	Onderzoeksrapport
1.0	01 dec. 14	Maurice Rutenfrans	Business case
1.0	15. dec.14	Maurice Rutenfrans	Ontwerprapport
1.0	24 dec. 14	Maurice Rutenfrans	Testrapport

Voorwoord

Na vier jaar studeren kijk ik terug op een periode van hard werken en veel leren. Als eerste wil ik Rick Hoevenaar bedanken die mij als Operational manager heeft begeleid en mijn documenten van feedback heeft voorzien. Bernhard van der Linde wil ik graag bedanken voor het aanbieden van de afstudeeropdracht en het goed uitvoeren van zijn rol als opdrachtgever. Daarnaast gaat mijn dank ook uit naar vele studenten en docenten die mij geholpen hebben tijdens mijn studie Technische Informatica aan de Haagse Hogeschool.

Rotterdam, januari 2015
Maurice Rutenfrans

Inhoudsopgave

1. Inleiding

Het doel van dit afstudeerrapport is om inzage te verschaffen in het verloop van mijn afstudeerperiode bij ADTS ICT B.V. Het project is begonnen op 25 augustus 2014 en heeft 20 weken geduurd tot 9 januari 2015.

Het verslag is geschreven voor mijn onderwijsinstelling de Haagse Hogeschool, om mijn begeleidend examinator Jan Dirk Schagen en twee examinator Madelon Nieuwland inzicht te geven in mijn afstudeerproces. Dit document staat ook wel bekend als afstudeerverslag, procesverslag of scriptie. Met dit verslag toon ik aan dat de afstudeeropdracht projectmatig is aangepakt, welke keuzes gemaakt zijn en tot slot evalueer ik de producten en het proces.

In het tweede en derde hoofdstuk is de organisatieomschrijving en afstudeeropdracht terug te lezen. In de organisatieomschrijving wordt het bedrijf waar ik afstudeer beschreven en waar ik daarbinnen sta. In de afstudeeropdracht wordt de opdrachtsomschrijving, aanpak en proces omschreven.

Het belangrijkste onderdeel van dit verslag zijn de daaropvolgende vijf hoofstukken. Elk hoofdstuk behandelt een fase van het project en verdiept zich hierin. Ik zal daarin uitleggen wat mijn handelingen waren tijdens de verschillende werkzaamheden, waarom ik gekozen heb voor bepaalde onderdelen, of hiervoor alternatieven beschikbaar waren en wat het resultaat van die beslissingen waren.

Tot slot zal er een evaluatie plaats vinden over mijn afstudeerperiode bij ADTS ICT B.V. Tijdens deze evaluatie wordt er, achteraf, gekeken naar de kwaliteit van het geleverde werk.

2. Organisatiebeschrijving

2.1 ADTS Groep B.V.

ADTS Groep B.V. is opgericht in 1994 en is gevestigd in Capelle aan den IJsel. Dit familiebedrijf met internationale expertise bestaat uit drie divisies:

1) ADTS Consultancy B.V.
2) ADTS Projects B.V.
3) ADTS ICT B.V.

Sinds 1994 is ADTS Consultancy B.V., als zelfstandig ingenieurs- en detacheringsbureau, werkzaam in de Civiele Techniek. De specialisten van ADTS Consultancy kunnen elk moment worden ingezet bij projecten op het gebied van risico- en projectmanagement, enginering, deskundigenrapportage, nulmetingen en kwaliteitszorg. Er wordt voornamelijk aan overheden en landelijke adviesbureaus deskundigheid en expertise geleverd.

De tweede business unit van ADTS Groep B.V. is ADTS Projects B.V. Deze business unit combineert techniek en marketing tot een geïntegreerd werkend geheel. Specialisten op het gebied van R&D (research and development) en trendwatchers werken nauw samen met technici en marketeers. Onlangs hebben ze de DEi (Diesel Engine Injection) op de markt gebracht. Dit is een computergestuurd gasinjectiesysteem, dat zowel het dieselbrandstofverbruik als uitstoot van schadelijke stoffen reduceert en de werking van de dieselmotor optimaliseert.

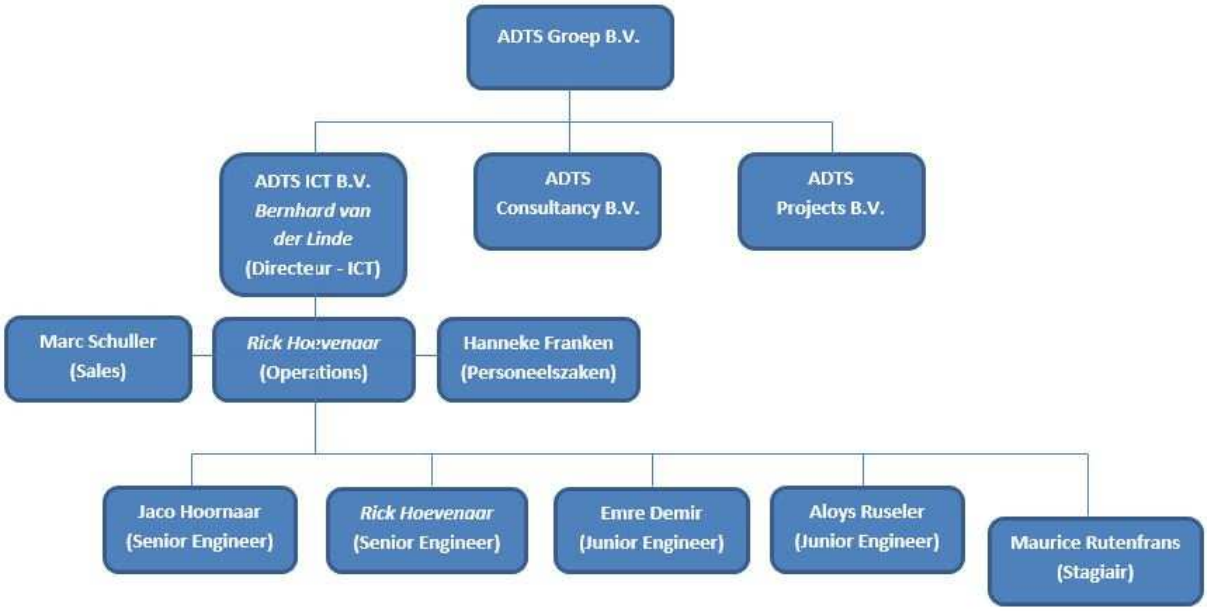
ADTS ICT B.V. is de derde business unit van ADTS Groep B.V. Vanaf september 2007 zijn er ICT werkzaamheden aan de huidige activiteiten van de ADTS Groep toegevoegd. ADTS ICT is een gespecialiseerde leverancier van hoogwaardige ict-infrastructuurproducten en diensten. Ze richt zich volledig op connectiviteit en is op een hoog niveau gecertificeerd partner van o.a. CISCO, Microsoft, VMware en NetApp. De bedrijfsvisie is het leveren van “maatwerk” voor elke oplossing, omdat iedere aanvraag en opdracht andere eisen en wensen heeft. Data, Voice, Security en Wireless worden met elkaar geïntegreerd.

De werkzaamheden van ADTS ICT B.V. zijn:

- Ontwerp van data- & voiceinfrastructuren
- Implementatie van data- & voiceinfrastructuren
- Routing & switching
- Security & Wireless
- Unified Communications
- (Remote) beheer van data- & voiceinfrastructuren
- Installatie en onderhoud servers & applicaties
- Datacenter oplossingen

2.2 Mijn plaats binnen ADTS Groep B.V.

De organisatie is hiërarchisch opgebouwd met een formele werksfeer. In het organogram hieronder (figuur 1) wordt er verder ingezoomd op ADTS Groep B.V. Om ervoor te zorgen dat deze overzichtelijk en doelgericht blijft, verdiept deze zich alleen op ADTS ICT. Tijdens mijn afstudeerstage heb ik onderdeel uit gemaakt van de Operations afdeling van ADTS ICT. De personen die van belang waren tijdens mijn afstudeerdopdracht zijn cursief aangegeven. Dat zijn Rick Hoevenaar (Operational Maganer), hij is mijn aanspreekpunt en bedrijfsmentor binnen ADTS ICT. Bernhard van de Linde (Directeur) vervult de rol als opdrachtgever.



Figuur 1: Organogram ADTS Groep B.V.

3. Afstudeeropdracht

3.1 Opdrachtsomschrijving

Dit hoofdstuk is deels overgenomen uit het plan van aanpak (zie Bijlage B) en beschrijft kort wat de initiële afstudeeropdracht inhoudt.

Probleemstelling

De stijgende behoefte om o.a. werk en privé flexibel te kunnen combineren leidt tot een groeiende vraag bij klanten naar video over IP. Ook willen steeds meer bedrijven een bijdrage leveren aan de duurzaamheid van hun leefomgeving. Daarnaast liggen de kosten op lange termijn lager dan de reizenkosten. Echter staat deze snel groeiende technologie, die ervoor moet zorgen dat klanten waar dan ook ter wereld op afstand kunnen samenwerken en communiceren, nog in de kinderschoenen binnen ADTS ICT B.V.

Doelstelling

Het doel van deze opdracht is het onderzoeken van video over IP en de achterliggende architectuur, zodat de klanten van ADTS ICT B.V. in de toekomst een op maat gemaakte oplossing kunnen krijgen. Dit onderzoek wordt ondersteund door een lab-opstelling waarin het onderzoek in de praktijk zal worden getest en gedemonstreerd.

Benodigdheden

- Werkplek met Microsoft Office.
- Toegang internet en literatuur.
- Microsoft Visio voor het realiseren van netwerkontwerpen.
- Hardware/apparatuur voor de demonstratie.
- Lab ruimte voor demonstratie.

Scope

- Onderzoek naar video over IP.
- Onderzoek wordt gedaan met producten van Cisco, Microsoft, Polycom en Vydeo.
- Een van de mogelijkheden van video over IP wordt toegepast op een fictieve netwerk infrastructuur (Demonstatie van video over IP).
- Realiseren van een sales presentatie.

Resultaat

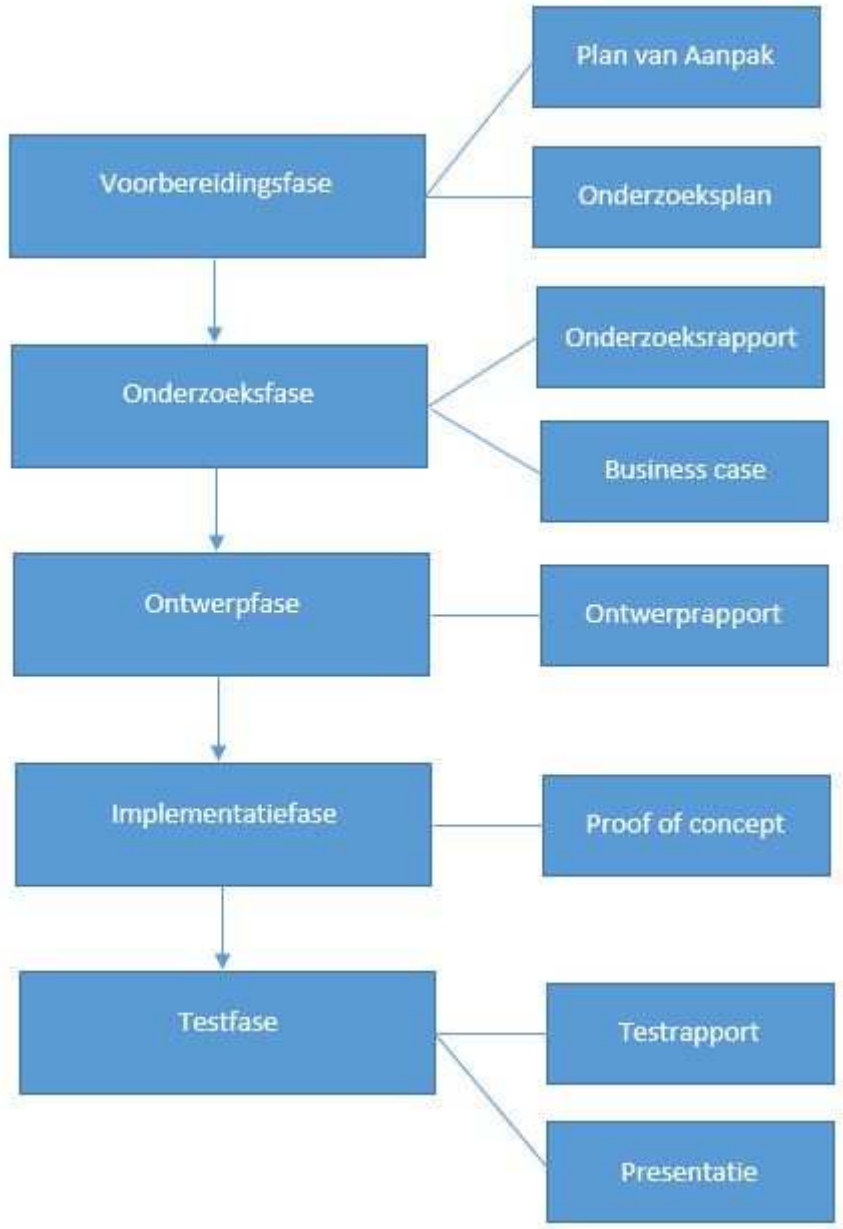
Het resultaat van deze opdracht is een onderzoekrapport over video over IP waarin onder andere de benodigde apparatuur, netwerk designs, protocollen, netwerk impact etc. beschreven worden en wat de voor- en nadelen hiervan zijn. Dit dient bewezen te worden aan de hand van een proof of concept. Daarnaast wordt deze proof of concept ondersteunt met een presentatie die gebruikt kan worden door ADTS ICT B.V. voor de sales.

3.2 Aanpak

Voor het starten van de afstudeeropdracht zijn de uit te voeren werkzaamheden en mijlpaalproducten samen met de begeleidende examinator vastgelegd in het afstudeerplan. Vervolgens zijn deze ook nog een keer vastgelegd in het plan van aanpak samen met de bedrijfsmentor en opdrachtgever. Het project zal volgens de watervalmethode doorlopen worden

(keuze wordt in de voorbereidingsfase nader toegelicht) en is zo afgebakend dat dit individueel uitgevoerd kan worden.

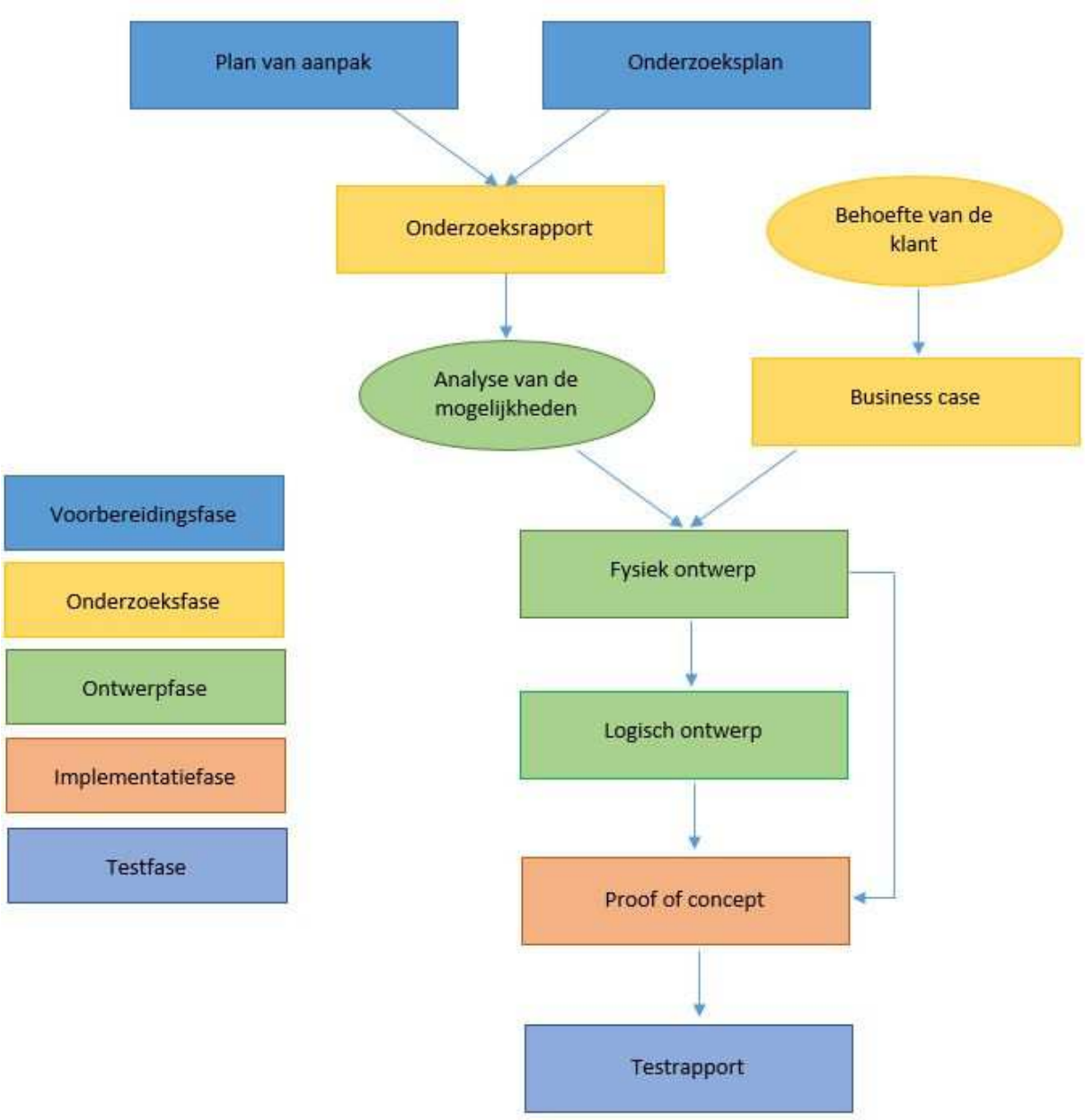
De uit te voeren werkzaamheden van dit project zijn in vijf fases ingedeeld: Voorbereidings-, onderzoeks-, ontwerp-, implementatie- en testfase. De voorbereidingsfase wordt gebruikt voor het verhelderen, plannen en inrichten van de afstudeeropdracht. De onderzoeksfase wordt gebruikt voor het vergaren en vastleggen van informatie met betrekking tot video over IP en de van te voren vastgelegde leveranciers. Daarnaast worden ook de behoeftes voor de proof of concept vastgelegd in een business case. Vervolgens wordt het fysieke en logische ontwerp in de ontwerpfase gerealiseerd. Daarna vindt de implementatie van het ontwerp plaats en wordt de proof of concept gemaakt. Tot slot wordt deze op de proef gesteld. Figuur 2 geeft een schematische weergaven van de fases en de bijbehorende producten die opgeleverd moeten worden.



Figuur 2: Fases en bijbehorende producten (watervalmethode).

3.3 Proces

De kern van dit afstudeerrapport is ingedeeld op basis van de achtereenvolgende fases die doorlopen zijn. Om een duidelijk beeld te geven hoe alles samenhangt, is in figuur 3 het proces te volgen zoals die doorlopen is. De producten en werkzaamheden zijn ingekleurd naar de fases van de projectmethode. Ook wordt er aangegeven waar het verslag zich bevond tijdens de tussentijdse assessment.



Figuur 3: Overzicht ontwikkelingsproces.

4. Voorbereidingsfase

De voorbereidingsfase beschrijft het proces wat doorlopen is tijdens het verhelderen, plannen en inrichten van de afstudeeropdracht. In dit hoofdstuk wordt op chronologische volgorde alle producten en keuzes die daarbij gemaakt zijn beschreven. Het resultaat van deze fase is het plan van aanpak (Bijlage B) en het onderzoeksplan (Bijlage C). In het plan van aanpak zijn de volgende onderdelen terug te vinden Opdrachtsomschrijving, Achtergrond en opdrachtgever, Project aanpak, Planning, Project organisatie en Risicoanalyse. In het onderzoeksplan zijn het Theoretisch kader, Reden onderzoek, Het onderzoek, Planning en Inventarisatie hardware opgenomen.

4.1 Plan van aanpak

In het plan van aanpak is de opdrachtsomschrijving van het afstudeerplan samen met de opdrachtgever verder aangescherpt en de scope bepaalt. Een belangrijk onderdeel hierbij was het vaststellen van een aantal leveranciers die interessant zijn voor ADTS ICT B.V., waarvan ze de producten aan hun klanten kunnen aanbieden. Na een oriëntatie heb ik de volgende zes leverancier uitgekozen, omdat deze de grootste en meest innoverend zijn binnen deze markt:

- Cisco
- Lifesize
- Microsoft
- Polycom
- Vidyo
- Sony

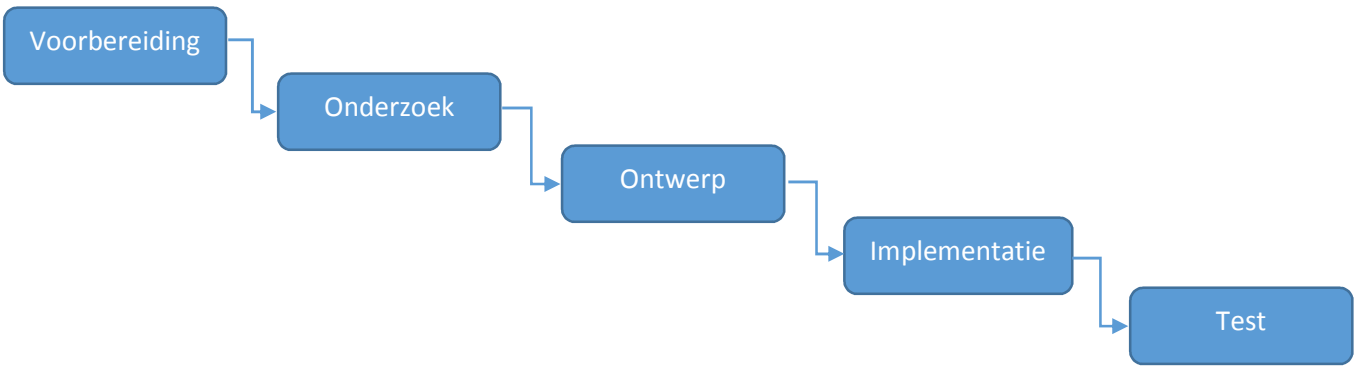
Deze zijn tijdens een gesprek met de opdrachtgever besproken en verminderd tot vier leveranciers. Er is gekozen om dit te verminderen, om de grote van de opdracht te beperken. De volgende vier leveranciers zijn gekozen om verder uit te werken en onderzoeken (figuur 4):

- Cisco
- Microsoft
- Polycom
- Vidyo.

Figuur 4: Leveranciers.

Bovenstaand leveranciers zijn voor verschilleden redenen gekozen. Cisco is gekozen, omdat veel klanten van ADTS ICT B.V. alleen maar Cisco apparatuur gebruiken. Microsoft biedt standaard Lync (videoconferencing software) aan in Office 365 en steeds meer klanten zullen dit dus in bezit krijgen. Polycom is gekozen omdat het zeer groot is in Nederland en Vidyo, omdat ze innovatief zijn met hun “VidyoRouter architectuur”.

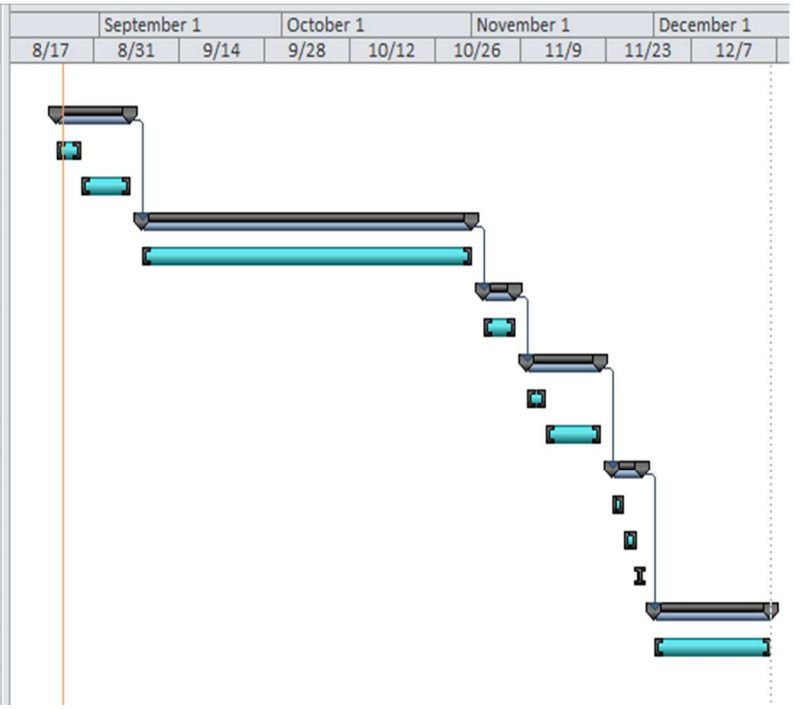
Naast het verhelderen van de opdracht is ook de aanpak gedefinieerd en vastgelegd. Met behulp van deze aanpak is het mogelijk om de opdracht goed te kunnen plannen en inrichten. Tijdens deze afstudeeropdracht zal de watervalmethode toegepast worden, want er hoeven geen aanpassing gedaan te worden in fases die zijn afgesloten (Figuur 5).



Figuur 5: Watervalmethode.

Na verhelderen van de opdracht en vastleggen van de projectmethode is de volgende planning gemaakt (Figuur 6). De officiële startdatum is 25-08-2014 en de uiterlijke opleverdatum 09-01-2015. In deze planning zijn extra data zoals het bedrijfsbezoek en tussentijdse assessment niet verwerkt.

	Task Mod	Task Name	Duration	Start
1				
2		**Voorbereidingsfase**	**10 days**	**Mon 8/25/14**
3		Plan van Aanpak	4 days	Mon 8/25/14
4		Onderzoeksplan	6 days	Fri 8/29/14
5		**Onderzoeksfase**	**40 days**	**Mon 9/8/14**
6		Onderzoeksrapport	40 days	Mon 9/8/14
7		**Ontwerpfase**	**5 days**	**Mon 11/3/14**
8		Ontwerpdocument	5 days	Mon 11/3/14
9		**Implementatiefase**	**10 days**	**Mon 11/10/14**
10		Demonstratie opbouwen	3 days	Mon 11/10/14
11		Demonstratie configureren	7 days	Thu 11/13/14
12		**Testfase**	**5 days**	**Mon 11/24/14**
13		Testplan	2 days	Mon 11/24/14
14		Testrapport	2 days	Wed 11/26/14
15		Presentatie	1 day	Fri 11/28/14
16		**Afrondingsfase**	**15 days**	**Mon 12/1/14**
17		Afstudeerscriptie	15 days	Mon 12/1/14



Figuur 6: Planning (Bijlage B).

Tot slot ben ik geëindigd met een risicoanalyse. De risicoanalyse is tot stand gekomen komen met de opgedane ervaring van andere projecten en met feedback van mijn bedrijfsmentor. De twee risico's die invloed kunnen hebben op het afstudeerproject zijn: "Geen of onvoldoende hardware voor de demonstratie" en "Deadlines niet behalen". Het eerste risico (tabel 1) kan resulteren in (deels) onuitvoerbare implementatie- en testfase. Het tweede risico (tabel 2) kan erin resulteren dat het project niet op tijd af is voor de eindbeoordeling. Daarom zijn deze risico's opgenomen in het plan van aanpak.

Risico: Geen of onvoldoende hardware voor de demonstratie	
Beschrijving	Indien er geen of onvoldoende hardware aanwezig is kunnen sommige fases niet uitgevoerd worden. Dit heeft tot gevolg dat de implementatie- en testfase deels of niet doorlopen kunnen worden en de demonstratie niet uitgevoerd kan worden.
Kans	Groot, indien de benodigde apparatuur (deels) niet aanwezig is en te laat besteld/geleverd wordt.
Kans vermindering	Onderzoek snel starten, zodat het eerder duidelijk wordt of er extra hardware nodig is en op tijd besteld kan worden.
Impact	Groot.
Impact vermindering	Door een duidelijke scope stellen en een goede planning te maken waar het mogelijk is om bij deze fases uit te kunnen lopen.
Plan B	Als het mogelijk is gebruik maken van een remote lab van Cisco of de emulator GNS3.

Tabel 1: Risico 1: Geen of onvoldoende hardware (bijlage B).

Risico: Deadlines niet behalen	
Beschrijving	Er zijn verschillende redenen waardoor de deadlines niet gehaald kunnen worden. Dit kan bijvoorbeeld komen door ziekte of het verkeerd inschatten van de grootte van de opdracht.
Kans	Groot
Kans vermindering	De kans wordt verminderd door wekelijks een voortgang gesprekken te hebben met de stagebegeleider binnen ADTS ICT B.V.
Impact	Middelmatig
Impact vermindering	Achterstanden kunnen ingehaald worden buiten werkuren in de weekenden en op doordeweekse avonden.
Plan B	In overleg met de stagebegeleiders, van zowel ADTS ICT B.V. als van de HHS, de opdracht verkleinen.

Tabel 2: Risico 2: Deadlines niet behalen (Bijlage B).

4.2 Onderzoeksplan

In het onderzoeksplan wordt als eerste het theoretisch kader beschreven. Dit is het vooronderzoek dat ik heb uitgevoerd. Hierin is de basis over video over IP terug lezen (Bijlage C) [1] [2]:

- Geschiedenis
- Basisprincipes
- Codec
- Frame types
- Videocompressie
- IP verkeer
- Leveranciers

Vervolgens is de reden voor het onderzoek uitgewerkt. Dit vond ik zelf zeer belangrijk om nog eens te achterhalen wat er van mij verwacht wordt en te achterhalen hoe de markt er nu en voor de toekomst uit ziet.
“Cisco voorspelt [3] dat het gebruik van video over IP over de komende jaren sterk blijft toenemen. Volgens dit onderzoek zal video 84% van al het internetverkeer voor zijn rekening nemen, dit is een toename van 6% in vier jaar tijd (2014-2018).”

Ook is hierin de richting van het onderzoek en daarbij van de afstudeerdopdracht bepaalt, want video over IP is zeer breed en je kan er veel kanten mee op. Dit is eerst verkleind naar videoconferencing over IP, omdat dit het meest aantrekkelijk is voor ADTS ICT B.V. en ook de meeste kansen liggen. Vervolgens is er een hoofdvraag opgesteld in samenwerking met de opdrachtgever en die luidt als volgt:

“Hoe zet je een zo optimaal mogelijke videoconferencing over IP netwerk op voor Ampelmann?”.

Hierbij is Ampelmann een klant van ADTS ICT B.V. die zeer geïnteresseerd is een video oplossing, omdat ze wereldwijd opereren. Meer informatie over Ampelmann wordt in het volgende hoofdstuk gegeven. Bij deze hoofdvraag zijn ook bijbehorende deelvragen gedefinieerd, waarmee uiteindelijk antwoord gegeven kan worden op de hoofdvraag. Deze heb ik opgedeeld in drie categorieën: Algemeen, Implementatie en Veiligheid.

Algemeen

1) Hoe werkt videoconferencing over IP?
    a. Wat is videoconferencing over IP en wat zijn de voor- en nadelen ervan?
    b. Welke apparatuur is er nodig voor videoconferencing over IP?
    c. Welke protocollen worden gebruikt voor videoconferencing over IP?
    d. Is er een minimale resolutie nodig?
    e. Wat is de invloed van de bandbreedte op de kwaliteit?

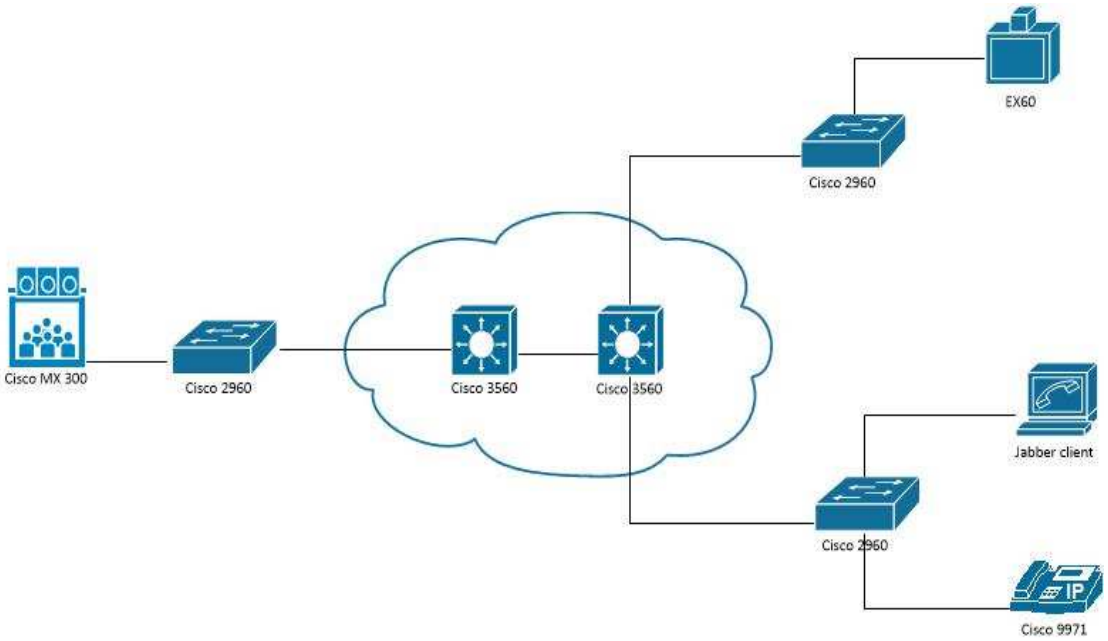
Implementatie

2) Wat zijn de grootste videoconferencing over IP implementatie problemen?
    a. Wat zijn de Quality of Service eisen voor video over IP?
    b. Welk netwerk architectuur kan het beste toegepast worden?
    c. Wat zijn de Multipoint bridging mogelijkheden?
    d. Wat voor impact heeft video over IP op de netwerk performance?

Veiligheid

3) Hoe veilig is video over IP?
    a. Hoe wordt de data beveiligd?
    b. Zijn extra beveiligingstechnieken zoals firewall, natting en VPN mogelijk?

Het onderzoeksplan ben ik geëindigd met het inventariseren van de hardware die al aanwezig is binnen ADTS ICT B.V. en dat eventueel gebruikt kan worden voor de proof of concept. Met deze hardware heb ik ook alvast een mogelijk ontwerp (figuur 7) gemaakt, om te laten zien hoe deze hardware eventueel gebruikt kan worden. De Cisco 3560 layer 3 switches kunnen hierbij gebruikt worden om het internet te simuleren. Aan het “internet” zijn verschillende locaties gekoppeld, in dit voorbeeld zijn dit er drie. Deze worden gesimuleerd met de Cisco 2960 layer 2 switches. Op elke locatie wordt er van verschillende videoconferencing oplossingen gebruik gemaakt. In dit ontwerp zijn dit Cisco MX 300 G2, EX60, Cisco 9971 en een PC met jabber client (softphone).



Figuur 7: Mogelijk ontwerp (Bijlage C).

5. Onderzoeksfase

De onderzoeksfase beschrijft het proces dat doorlopen is tijdens het vergaren en vastleggen van informatie met betrekking tot video over IP en de van te voren vastgelegde leveranciers. In dit hoofdstuk wordt op chronologische volgorde de deelvragen en keuzes die daarbij gemaakt zijn beschreven. Het resultaat van deze fase is het onderzoeksrapport (Bijlage D). Tijdens deze fase is ook de business case voor Ampelmann Operations opgesteld (Bijlage E).

5.1 Onderzoek

5.1.1 Deelvraag 1: Algemeen

a) Wat is videoconferencing over IP en wat zijn de voor- en nadelen ervan?

Videoconferencing over IP maakt gebruik van audio- en videotelecommunicatie om personen op verschillende locaties bij elkaar te brengen voor een ontmoeting. Dit kan een ontmoeting zijn tussen twee personen die zich elk op een andere locatie bevinden (point-to-point), of een ontmoeting met meerdere personen in grote ruimten op meerdere locaties (point-to-multipoint). Naast het verzenden van audio en video kunnen er ook documenten en informatie op whiteboards gedeeld worden. Videoconferencing over IP is ook bekend als videocommunicatie, visual collaboration of net als bij spraak VoIP.
Om de data te verzenden moet deze eerst gedigitaliseerd en gecomprimeerd worden door middel van een codec. De resulterende digitale stroom van enen en nullen wordt onderverdeeld in gelabelde pakketten, die vervolgens worden verstuurd over een digitaal netwerk. Voor de overdracht van deze data kan er gebruik gemaakt worden van het IP protocol. Hierdoor is het mogelijk om te videoconference vanaf elke plek met internet.

De minimale benodigdheden voor videoconferencing over IP zijn:

- Video input: Videocamera of webcam.
- Audio input: Microfoon.
- Video output: Beeldscherm, televisie of projector.
- Audio output: Luidsprekers of telefoon.
- Digitaal netwerk: LAN of internet.
- Computer: Data processing unit die alles met elkaar verbindt.

Nog niet lang geleden was videoconferencing in een redelijke resolutie met werkbaar geluid behoorlijk prijzig. Echter heeft videoconferencing over IP grote vooruitgang geboekt en is het een stuk voordeliger geworden. Er zijn verschillende voor- en nadelen die overwogen moeten worden voor het overstappen op videoconferencing over IP [4][5][6].

Voordelen:

- Tijdwinst, men hoeft minder te reizen.
- Kostenbesparing, de aanschaf van videoconferencing apparatuur is zeer prijzig, maar liggen op lange termijn lager dan de reis- en telefoonkosten.
- Snel face-to-face contact, er kan direct bijeengekomen worden indien dit nodig is, waardoor niet iedereen zich op een centrale plek hoeft te verzamelen.
- Samenwerking, het bevorderd de samenwerking binnen bedrijven.
- Gemak, in plaats van verre reizen of een vergadering in drukke schama's te plannen kan dit op elk moment van de dag gedaan worden.
- Schaalbaarheid, overal waar internet is kan het gebruikt worden en is dus eenvoudig uit te breiden.
- Milieuvriendelijk, vermindering van CO2 uitstoot door minder te reizen.

Nadelen:

- Persoonlijk contact, bij binnenkomst wordt er geen hand meer gegeven en tijdens de lunch of koffiepauze vindt er geen small talk meer plaats.
- Technische problemen, de techniek kan op kritische momenten falen door bv. een stroomstoring bij de provider of een overbelast netwerk overbelast.
- Afhankelijkheid, de kwaliteit hangt ook af van de apparatuur (netwerk backbone) van de andere partij.
- Kosten, de kosten voor de aanschaf van goede apparatuur liggen hoog.
- Veiligheid, indien slecht geconfigureerd kan het door hackers gesaboteerd worden.

Voor de meeste bedrijven is het terugdringen van reiskosten de belangrijkste drijfveer. Bij internationale bedrijven is het haalbaar gebleken om 75% van de reiskosten te besparen. Grote organisaties zien hun zakelijk reisverkeer zelden helemaal verdwijnen, omdat persoonlijk contact zeer belangrijk blijft en niet onderschat mag worden. Een directeur kan door deze techniek bijvoorbeeld zeer modern, maar ook zeer afstandelijk over komen.

b) Welke apparatuur is er nodig voor videoconferencing over IP?

Om te achterhalen welke apparatuur er nodig is voor videoconferencing over IP en wat elke leverancier voor producten te bieden heeft, is er gekozen om de benodigde apparatuur op te delen in 2 categorieën. Deze twee categorieën zijn gekozen, omdat niet elke leverancier dezelfde standaard hanteert:

- Eindpunten
- Platform

Om de lijst met componenten te beperken is er in overleg met de opdrachtgever voor gekozen om niet in te gaan op accessoires/randapparatuur. De eindpunten omvat alles wat de gebruiker te zien krijgt en platform de achterliggende apparatuur. Ook de eindpunten zijn opgedeeld in drie categorieën:

- Personal video conferencing systems, onafhankelijk werkende apparatuur voor persoonlijk gebruik. Bijvoorbeeld een videotelefoon of een geïntegreerd systeem.
- Room-based videoconferencing systems, apparatuur geschikt voor een groep.
- Immersive videoconferencing systems, compleet systeem en omgeving. Hierbij zijn naast het systeem ook aanpassing aan de omgeving nodig voor de beste kwaliteit.

De tabellen die tijdens deze vraag gerealiseerd zijn, zijn terug te vinden in bijlage D. Tijdens het beantwoorden van deze vraag ben ik tot de conclusie gekomen dat er in de hardware niet veel verschillen zijn tussen de leveranciers. Ze leveren allemaal HD video kwaliteit met de beste compressietechnieken die er zijn. Daarnaast zeggen ze allemaal “award winning” te zijn. Waar ik wel verschillen ben tegen gekomen is bij compatibiliteit. Daarom heb ik ervoor gekozen het algemene onderdeel van het onderzoek uit te breiden met twee deelvragen (groen aangeduid hieronder):

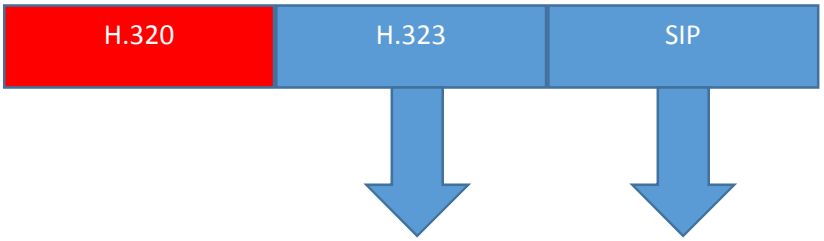
Algemeen

1) Hoe werkt videoconferencing over IP?
    a. Wat is videoconferencing over IP en wat zijn de voor- en nadelen ervan?
    b. Welke apparatuur is er nodig voor videoconferencing over IP?
    c. Welke protocollen worden gebruikt voor videoconferencing over IP?
    d. Is er een minimale resolutie nodig?
    e. Wat is de invloed van de bandbreedte op de kwaliteit?
    f. Wat is het verschil tussen de leveranciers en zijn ze onderling compatibele?

g. Is integratie met telefonie, computers, mobiel en software mogelijk?

Deze vraag is essentieel voor het onderzoek, maar heeft veel tijd gekost. Hij had sneller beantwoord kunnen worden als deze later in het onderzoek voorkwam. Sub vraag c behandelde bijvoorbeeld de protocollen van videoconferening over IP. Die kennis had het lezen van de datasheets en het bepalen wat relevant is veel makkelijker gemaakt.

c) Welke protocollen worden gebruikt voor videoconferencing over IP?
In de derde sub vraag zijn de drie bekendste videoconferencing standaarden uitwerkt: H.320, H.323 en SIP. Na het globaal inlezen van deze standaard viel H.320 af, omdat deze gebruikt wordt voor ISDN en niet voor IP.



Vervolgens zijn de protocollen die onder H.323 en SIP vallen uitgewerkt. Om binnen deze vele termen en protocollen een beter overzicht te krijgen, zijn deze gegroepeerd in de volgende categorieën:

- Audio: G.711, G.722, G.723.1, G,726, G.728, G.729, AAC-LD
- Video: H.264 High Profile, H.264, H.264 SVC, H.263, H.261
- Data: H.239
- Control: H.225, H.245, H.460
- Transport: TCP, UDP, RTP

Meer informatie over bovenstaande protocollen is terug te lezen in Bijlage D.

d) Is er een minimale resolutie nodig?
De vierde sub vraag (d) vond ik tijdens het beantwoorden ervan niet goed gesteld, want die verwijst naar wat de klant acceptabel vindt en is zeer subjectief. Kortom dit is voor elk bedrijf en elk persoon binnen dat bedrijf verschillend. Daarom is besloten om deze aan te passen en te richten op hoe je de beste kwaliteit voor elke situatie kunt bepalen.

d. Hoe wordt de resolutie bepaald die nodig is?

De kwaliteit van een videoconferentie maakt of breekt de werkbaarheid van een video oplossing. Twee primaire factoren die de videoconferencing kwaliteit beïnvloeden zijn resolutie en framerate, en zijn direct verbonden met de hoeveelheid bandbreedte die nodig is. Het verhogen van de resolutie of framerate levert dus meer netwerkverkeer op. Hoewel compressie technieken de benodigde bandbreedte drastisch vermindert, kan dit ook maar tot een bepaalde hoogte (tabel 3) [7].

Schermgrootte	Resolutie	Framerate	Benodigde bandbreedte (H.264)	Benodigde bandbreedte (H.264 High Profile)
CIF	352 x 288	30 fps	128 kbps	64 kbps
4CIF	704x576	30 fps	256 kbps	128 kbps
HD720	1280x720	30 fps	1024 kbps	512 kbps
HD720	1280x720	60 fps	1512 kbps	832 kbps
HD1080	1920x1080	30 fps	2048 kbps	1024 kbps

Tabel 3: Resolutie en benodigde bandbreedte na compressie (Bijlage D).

Een belangrijke bevinding van dit onderdeel is dat een betere resolutie niet vanzelfsprekend een betere beeld kwaliteit betekent. Samengevat hangt de resolutiekeuze af van de volgende aspecten:

- De omgeving en hoeveel personen tegelijk deelnemen.
- Framerate, indien de bandbreedte gelimiteerd is.
- Content sharing, waarvoor wordt het gebruikt.
- De grote van het scherm.

e) Wat is de invloed van de bandbreedte op de kwaliteit?
Sub vraag e is een aanvulling op de vorige vraag, waar framerate en resolutie behandeld zijn. De kwaliteit van de video wordt ook beïnvloed door andere factoren zoals latency en packet loss [8].

Latency beïnvloed de kwaliteit door eventuele netwerk vertraging, want de data moet van A naar B verzonden worden. Om bijvoorbeeld een afstand van 4000km te overbruggen met glasvezel duurt 20 milliseconden (4000km / 200000km/s). In de praktijk is deze tijd groter, omdat het door verschillende netwerk componenten verwerkt wordt en die zorgen op hun beurt voor nog meer vertraging. Er zal dus altijd een vertraging in het verzenden en ontvangen van data zitten. In dit geval maakt het verhogen van de bandbreedte niet uit, want een bit kan zich niet sneller verplaatsen. Het maakt het alleen mogelijk meer data parallel te verzenden.
In een videoconferentie is een vertraging van minder dan 100 ms gedoogd, omdat dit kleine verschil door de meeste mensen niet wordt waargenomen. Boven de 200 ms begint de aandacht van de deelnemers af te nemen en zullen ze na korte tijd vermoeidheid ervaren. Als de vertraging groter wordt dan 300 milliseconden, wordt het voor gebruikers vervelend om te videoconferencen en zal dit uiteindelijk resulteren in een onhandig gesprek waarbij iedereen door elkaar praat.

Naast latency hebben zelfs de best ontworpen IP netwerken een kleine hoeveelheid pakketten die verloren gaat, dit heet packet loss. Fouten in pakketten worden door veel professionele oplossing opgevangen door een foutcorrectie mechanisme, zodat de video alsnog gereconstrueerd kan worden ondanks dat er enkele pakketten verloren zijn gegaan. Het opnieuw verzenden van pakketten is bij video geen optie, door de sequentiële aard van een video signaal en zou dan veel te laat aankomen. Het effect van packet loss is een schok- en blokkerig beeld in combinatie met wegvallend geluid.

f) Wat is het verschil tussen de leveranciers en zijn ze onderling compatibele?
g) Is integratie met telefonie, computers, mobiel en software mogelijk?
Sub vraag f en g zijn tijdens het onderzoek bijgevoegd, omdat er geconcludeerd is dat er hardwarematig niet veel verschillen zijn tussen de leveranciers. Hierin is er gekeken naar Interoperabiliteit tussen leveranciers en integratie.

De beste videoconferentie systemen zijn zo goed als de mogelijkheid om met andere eindpunten te kunnen verbinden, ongeacht van welke leverancier ze afkomstig zijn. Interoperabiliteits problemen zijn dus ook niet minimaal in de ogen van een klant

Jaren lang was de interoperabiliteit tussen videoconferencing platformen een groot probleem, maar over de laatste jaren is dit aan het verbeteren. Interoperabiliteit tussen de leveranciers kan op twee manieren gerealiseerd worden. Door ingebouwde/standaard ondersteuning of door het gebruiken van software oplossingen, genaamd “gateways”. Dit zorgt vaak wel voor mindere kwaliteit en/of een onacceptabele latency

Bedrijven zijn op zoek naar interoperabiliteit met een naadloze gebruikerservaring die:

- Hen instaat stelt te profiteren van nieuwe innovaties.
- Samenwerkt met (eventueel) bestaande en toekomstige investeringen.
- Extern werkt in verschillende omgevingen.

Alle leveranciers zorgen voor backward compatibiliteit, zodat hun klanten eerder aangeschafte product kunnen blijven gebruiken. Daarnaast is de interoperabiliteit tussen leveranciers verbeterd bij grote leveranciers. In het tabel hieronder is de interoperabiliteit tussen de leveranciers weergegeven (tabel 4), waarbij drie categorieën gehanteerd worden: groen (goed), oranje (matig) en rood (niet).

	Cisco	Vidyo	Polycom	Microsoft
Cisco				
Vidyo				
Polycom				
Microsoft				

Tabel 4: Interoperabiliteit tussen leveranciers (Bijlage D).

Bij Polycom zitten er voornamelijk knelpunten in verouderde systemen en codec’s die nog steeds ondersteund moeten worden en die voor problemen kunnen zorgen. Vidyo is door het gebruik van H.264 SVC gelimiteerd, omdat dit nog geen standaard is en dus met derde partijen compatibiliteit problemen kan veroorzaken. Microsoft Lync wordt daarentegen door elke leveranciers ondersteunt en is bij sommige zelf geïntegreerd. Cisco heeft hun TIP protocol vrijgegeven en die wordt ook al door Polycom gebruikt. Daarnaast richten zich ook al op de toekomst met H.265.

Naast onderlinge interoperabiliteit is er ook gekeken naar de integratie met telefonie, computers, mobiel, applicaties en browsers (tabel 5). Deze lijst is tot stand gekomen door een oriënterend onderzoek en een gesprek met de opdrachtgever. Er worden drie categorieën gehanteerd: groen (goed), oranje (matig) en rood (niet).

		Cisco	Vidyo	Polycom	Microsoft
Telefonie	Voice	x	-	x	x
	Voicemail	x	-	x	x
Computers (OS)	Linux	x	x	-	-
	Mac	x	x	x	x
	Windows	x	x	x	x
Mobiel (OS)	iOS	x	x	x	x
	Blackberry OS	x	-	-	-
	Microsoft Phone	x	-	-	x
	Android	x	x	x	x
Software	MS office	x	x	x	x
	Active directory	x	x	x	x
Browsers	Internet Explorer	x	x	x	x
	Chrome	x	x	x	-
	Firefox	x	x	x	x
	Safari	x	x	x	x

Tabel 5: Integratie vergelijking (Bijlage D).

5.1.2 Deelvraag 2: Implementatie

a) Wat zijn de Quality of Service eisen voor video over IP?

Real time netwerkverkeer zoals videoconferencing en VoIP zijn gevoeliger ten opzichte van ander verkeer zoals e-mail en file transfers. Quality of Service (QoS) is een netwerk term die verwijst naar de intelligentie in het netwerk om een netwerk performance te garanderen voor bepaald verkeer, zodat bv. spraak en video data voorrang krijgt en een minimale vertraging en verlies oploopt. Bij video over IP netwerken is het doel: het behouden van zowel essentiële data in het bijzijn van spraak en video, en het behouden van spraak en video kwaliteit in de aanwezigheid van onregelmatig data verkeer. Parameters die gebruikt worden voor het beschrijven van de QoS zijn de al eerder behandelde: Bandbreedte, Latency en packet loss.

Er zijn drie manieren om QoS in een netwerk in te regelen [9].

1. Provisioning, is het verzorgen van voldoende bandbreedte voor zowel spraak, video en data applicaties die van het netwerk gebruik maken. Bijvoorbeeld door gebruik te maken van een 100Mbps ethernet netwerk i.p.v. een 10Mbps. Er moet altijd rekening gehouden worden met een 20% verhoging van de bandbreedte door IP overhead.
2. Classifying (CoS), betekend het geven van een classificatie aan pakketten die gebaseerd is op hun prioriteit. Spraak pakketten krijgen de hoogste prioriteit, omdat deze het gevoeligst zijn voor vertraging. Video krijgt vaak een iets lager prioriteit en email pakketten krijgen bijvoorbeeld de laagste prioriteit.
3. Queuing, refereert naar een proces dat plaats vindt in routers en switches waarbij verschillende buffers (queues) worden vastgesteld voor de verschillende classificaties. Hiermee kan bijvoorbeeld een buffer gebruikt worden voor latency of packet loss gevoelig verkeer.

Om dit probleem voor video over IP op te lossen zijn twee fases nodig, zodat er geen bottlenecks meer aanwezig zijn. De kwaliteit is zo goed als het zwakste punt in het netwerk.

1. Garanderen van een QoS binnen een specifiek (gecontroleerd intranet) netwerk.
2. Garanderen van een QoS tussen verschillende locaties (WAN).

Er zijn vier grote QoS initiatieven [10]:

- 802.1p
- IP Precedence
- DiffServ (Differentiated Services)
- RSVP (Resource ReSerVation Protocol)

Meer informatie hierover is terug te lezen in bijlage D. Omdat er geen algemene standaard voor het gebruiken van QoS is, is er gekozen om aan te houden wat Cisco voorschrijft (tabel 6). Deze keuze is gemaakt, omdat dit de enige leveranciers is die alle netwerkcomponenten aanbiedt en veel klanten gebruik maken van Cisco apparatuur.

Traffic Type	Layer 2 CoS	Layer 3 IP Precedence	Layer 3 DSCP
Voice RTP	5	5	EF
Voice control	3	3	AF31
Video conference	4	4	AF41
Streaming video (IP/TV)	1	1	AF13
Data	0-2	0-2	0-AF23

Tabel 6: Cisco QoS voorschrift (Bijlage D).

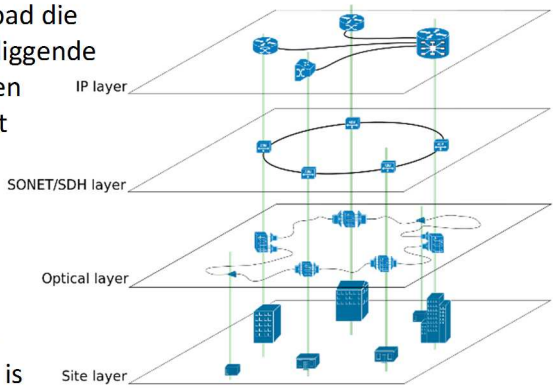
b) Welk netwerk architectuur kan het beste toegepast worden?
In deze sub vraag worden twee netwerk architecturen besproken [11]:

- Converged netwerk architectuur
- Overlay netwerk architectuur

Converged netwerk architectuur
Een converged IP netwerk verwijst naar het aanbieden van telefonie, video en data communicatie diensten binnen een enkel netwerk. Met andere woorden, het leveren van alle vormen van communicatie diensten door een “pijp”. Een doelstelling van deze integratie is het leveren van een betere dienstverlening en lagere prijzen voor de consument.

Alle gebruikers eisen een hoge quality of service, quality of experience, compatibiliteit, privacy etc. Met de evolutie van deze techniek ontstaan er ook steeds nieuwe uitdagingen voor de ontwikkelaars. De grote vraag naar bandbreedte is hierbij de belangrijkste, omdat applicaties steeds geavanceerder worden en gebruikers meer en meer “rich content” data uitwisselen.
Organisaties willen niet altijd telefonie en videoverkeer laten concurreren met kritieke data applicaties, zoals productiegegevens die over hetzelfde netwerk gaan. Waardoor een apparte QoS “overlay” netwerk ingezet kan worden voor spraak en video verkeer.

Overlay netwerk architectuur
Een overlay netwerk is een computernetwerk die boven op een ander netwerk is gebouwd (Figuur 9). Nodes in een overlay kunnen gezien worden als zijnde verbonden doormiddel van virtuele of logische verbindingen, die elk overeenkomt met een pad die mogelijk uit meerdere fysieke verbindingen bestaat in het onderliggende netwerk. Voorbeelden hiervan van zijn peer-to-peer netwerken en client-server applicaties, omdat deze nodes bovenop het internet werken. Het internet was oorspronkelijk gebouwd als overlay op het telefonie netwerk, maar tegenwoordig is dit omgekeerd en is telefonie een overlay op het internet.



Figuur 8: Overlay netwerk architectuur.

Overlay netwerken zijn zeer complex, omdat ze verschillende logische lagen combineren die gebruikt en beheert worden door verschillende entiteiten (bedrijven, universiteiten etc.). Hierdoor is VoIP en IPTV mogelijk geworden, want dit was niet te realiseren door een enkele provider.

c) Wat zijn de Multipoint bridging mogelijkheden?
Organisaties moeten overwegen of ze met meer dan twee partijen willen deelnemen in een videoconferentie. Als dit het geval is, is er een multipoint bridge nodig. Dit wordt ook wel een MCU (Multi Control Unit) genoemd. Er zijn drie mogelijkheden:

- De MCU kan aangeschaft en intern beheert worden.
- De bridging functionaliteiten kunnen worden uitbesteed aan een derde partij.
- Enkele eindpunten hebben een geïntegreerde multipoint bridge (gedecentraliseerd).

Indien de MCU gekocht wordt, zal de prijs voor een videoconfencing oplossing sterk toenemen en komen er ook extra kosten voor het beheer hiervan.

MCU
Alle deelnemers bellen naar de MCU of deze belt iedereen een voor een om aan de videoconferentie te kunnen deelnemen. Een MCU wordt gekenmerkt door het aantal gelijktijdige gesprekken dat het kan voeren en mogelijkheden zoals continuous presence, people plus content/dual streams, transcoding en transrating.
Continuous presence is de mogelijk dat alle deelnemers tegelijk op het scherm zichtbaar zijn. Hierdoor is het bijvoorbeeld mogelijk om 10 deelnemers tegelijk weer te geven. Hieronder volgen een paar keuzes die mogelijk zijn afhankelijk van het type conferentie:


Full Screen: Bij deze optie wordt de spreker die aan het woord is getoond op elk scherm. Dit wordt automatisch bepaalt op basis van wie er spreekt.


Split Screen: Bij deze optie worden alle deelnemers die meedoen gelijktijdig weergegeven.


Dominant Speaker plus Split: Dit is een combinatie van de boven genoemde opties, waarbij de spreker in een groot scherm wordt weergegeven en de rest van de deelnemers nog steeds zichtbaar zijn.

Het is ook mogelijk om je zelf te zien tijdens de conferentie, maar vaak wordt de vertraging tussen deze en de rest van de streams als afleidend gezien.

Transcoding is een optie die communicatie tussen videoconferenties met verschillende technieken mogelijk maakt. Hierdoor kunnen systemen die gebruikmaken van H.320 communiceren met andere systemen die van H.323 gebruikmaken. Transrating maakt het mogelijk dat deelnemers video kunnen ontvangen met verschillende bandbreedte.

Derde partijen
Het outsourcen van de bridging mogelijkheden is zeer populair voor kleinere bedrijven, die niet genoeg kapitaal en kennis hebben op dit gebiedt. Het grootste voordeel hiervan is dat deze partijen voldoende capaciteiten hebben om defecte apparatuur op te vangen, waardoor de eindgebruikers er niets van merken als er iets defect is. Het nadeel is dat je afhankelijk wordt/bent van dit bedrijf en dat bij storingen het buiten bedrijven hun macht ligt.

Alternatief - gedecentraliseerd
Cisco heeft als enige leverancier ook ingebouwde mogelijkheden binnen enkele eindpunten. Dit zijn de MX200 G2 en MX300 G2 voor een videoconferentie tot vier deelnemers inclusief zichzelf en de MX700 en MX800 voor een videoconferentie tot vijf deelnemer inclusief zichzelf. Het grootste voordeel ten opzichte van de MCU is dat er geen bottleneck ontstaat. Hierdoor is de kwaliteit vaak ook beter, omdat de video data niet langs een centraal punt hoeft. Het nadeel is ook gelijk dat deze systemen altijd mee moeten doen in de videoconferentie en het niet vanaf en met elk eindpunt kan.

Vidyo maakt geen gebruik van een MCU, want deze wordt overbodig gemaakt door het gebruik van de Vidyorouter. Er moet in plaats van een MCU een Vidyorouter of Vidyoportal aangeschaft worden om de communicatie te regelen.

d) Wat voor impact heeft video over IP op de netwerk performance?
Zoals uit voorgaande sub vragen al was gebleken is er een significante hoeveelheid bandbreedte nodig en een gecontroleerd hoeveelheid latency en packet loss voor het implementeren van video conferencing. Met een slechte videoconferentie kunnen leidinggevende het vertrouwen in de nieuwe technologie verliezen, daarom is het belangrijk dat de netwerk performance optimaal is. Het is

mogelijk dat klanten al een goede netwerk performance hebben waar VoIP al in gebruik is, maar dit moet niet onderschat worden want video stelt meer eisen aan het netwerk. Met de volgende punten kan de netwerk performance optimaal gemaakt en gehouden worden (extra informatie hierover is terug te vinden in bijlage D) [12]:

- Capaciteit plannen
- QoS
- CAC
- Multipoint brigde
- Monitoring

5.1.3 Deelvraag 3: Veiligheid

a) Hoe wordt de data beveiligd?

Encryptie is een omzettingsproces om informatie onleesbaar te maken voor iedereen behalve degenen die in het bezit zijn van de sleutel. Deze techniek wordt al vele jaren gebruikt binnen defensie en overheden om geheime communicatie te realiseren. Tegenwoordig wordt encryptie ook gebruikt voor de beveiliging van civiele systemen. Een toepassing is de beveiligen van de datatransport binnen bedrijfsnetwerken. Het versleutelen van de transportdata van bedrijven heeft als doel dit veilig te stellen, omdat het moeilijk is alle toegang tot netwerken fysiek te beveiligen.

Bij het toepassen van encryptie op video over IP moet er rekening worden gehouden dat dit niet ten kosten gaat van de kwaliteit [13]. Video bestaat, zelfs na compressie, uit een groot aantal bits en om deze te beveiligen moeten deze allemaal versleuteld worden. Om dit te realiseren is er veel rekenkracht nodig, waardoor de producten duurder worden. Naast het duurder worden van hardware kan dit tijd gevoelige verkeer, door het toepassen van encryptie, ook snel vertragingen oplopen, waardoor de kwaliteit van een videoconferentie sterk verminderd. Hierdoor zijn er nog veel bedrijven waar video over IP niet versleuteld wordt. Encryptie technieken die gebruikt worden in videoconferencing zijn:

- AES
- DES
- Triple-DES

Het AES algoritme wordt beschouwd als de meest geschikt vorm van encryptie voor video over IP, omdat deze de minste vertraging oploopt tijdens het versleutelen van de frames. Daarnaast is de extra overhead die het met zich meebrengt minimaal.

b) Zijn extra beveiligingstechnieken zoals firewall, natting en VPN mogelijk?

De meeste bedrijfsnetwerken maken gebruik van firewalls [14] [15] om te voorkomen dat hackers en onbevoegden toegang kunnen krijgen tot hun data. Spraak en video over IP gaan niet goed samen met beveiligingstechnieken zoals firewalls en natting. Bedrijven moeten dus nadenken over hoe ze veilig hiervan gebruik kunnen maken door veranderingen, herconfiguratie of upgrades door te voeren die dit mogelijk te maken.

Firewall

Doordat H.323 en SIP gebruik maken van veel dynamische poorten, is het niet mogelijk om deze voor te configureren in de firewalls zonder dat er veel poorten opgezet moeten worden om dit verkeer door te laten. Er zijn verschillende poorten gedefinieerd die open moeten staan om uitgaand video verkeer door te laten. Hieronder volgt een lijst met poorten die opengezet moeten worden om video over IP mogelijk te maken (tabel 7). Omdat er veel poorten zijn die opgezet moeten worden en per

leverancier verschillen is er in overleg met de opdrachtgever besloten dat deze nog niet compleet hoeft te zijn.

Poort	Type	Omschrijving	H.323 Client	H.323 Gatekeeper	H.323 MCU	SIP Client	SIP Registrar
80	Static TCP	HTTP Web Interface	x		x		
389	Static TCP	LDAP	x	x			x
443	Static TCP	HTTPS & Port Tunnelling	x				
1718	Static UDP	Gatekeeper Discovery	x	x			
1719	Static UDP	Gatekeeper RAS	x	x			
1720	Static TCP	H.323 Call Setup	x	x	x		
2326 - 2485	UDP	Cisco/Tandberg endpoints	x			x	
3230 - 3235	TCP	Polycom endpoints	x				
3230 - 3280	UDP	Polycom endpoints	x			x	
5001	TCP & UDP	Polycom PPCIP client	x				
5060	TCP & UDP	SIP endpoints				x	x
5061	TCP	SIP TLS				x	x
5555 - 5574	TCP	Cisco/Tandberg endpoints	x				
1024 - 65535	Dynamic TCP	H.245 (Call Parameters)	x		x		
1024 - 65535	Dynamic UDP	RTP (Video Stream Data)	x		x		
1024 - 65535	Dynamic UDP	RTP (Audio Stream Data)	x		x		
1024 - 65535	Dynamic UDP	RTCP (Control Information)	x		x		

Tabel 7: IP poorten en Protocollen die gebruikt worden bij H.323 en SIP (Bijlage D).

Door het open zetten van al deze poorten ontstaat een slechte firewall beleid, die niet door veel bedrijven geaccepteerd wordt. Daarnaast komen de inkomende gesprekken hierbij nog niet eens aan de orde.

Zowel SIP als H.323 maken gebruik van RTP voor het versturen van data. H.323 maakt daarnaast ook gebruik van de dynamic-port bases call signaleringsprotocol (H.245). Het probleem bij deze protocollen ontstaat, omdat ze allebei geen standaard laag 4 poortnummers gebruiken maar willekeurige poorten uit de 1024 tot 65534 reeks.

Het tweede probleem dat aan de orde komt is de interactieve spraak en video dat verstuurd wordt en zeer gevoelig is voor vertragingen. De oplossing voor de dynamische poorten is het gebruik maken van een proxy. Dit is een software onderdeel van de firewall die deelneemt aan het protocol. In H.323 betekend dit dat de proxy meedoet aan het H.323 gesprek, het gesprek beëindigd op de firewall en een tweede gesprek creëert naar de eindbestemming, en tot slot koppelt hij deze twee gesprekken aan elkaar. De firewall met proxy handelt al het opzet en afbreek werk van de

gesprekken af, evenals het verplaatsen van videoverkeer van alle eindpunten die voorbij de firewall proberen te praten. Ook dit brengt grote beveiliging en performance/scalability uitdagingen met zich mee voor zowel het protocol als de data die door de firewall heen gaat.

- Het ondersteunen van H.323 en SIP in de firewall maakt het ontwerp complex en kwetsbaar voor aanvallen.
- H.323 en SIP ondersteuning zorgt voor mogelijke vermindering van de performance en schaalbaarheid van de firewall.

NAT
Network Address Translation (NAT) is een methode waarbij ip adressen gemapped worden van het ene netwerk naar een ander, in een poging transparante routering aan eindpunten aan te bieden. NAT wordt gebruikt om privé adressen te koppelen aan publieke adressen. Het wordt voor twee doeleinden gebruikt.

1. Als mechanisme om de IPv4 uitputting tegen te gaan.
2. Voor beveilingsdoeleinden (zodat eindpunten verborgen blijven).

Bij NAT, vaak geïmplanteerd als onderdeel van de firewall, wordt het IP adres in header van de pakketten die daar doorheen gaan getransleerd naar een ander adres. Tegelijk wordt er een NAT tabel bijgehouden waarin de zogeheten mappings tussen IP adressen en poortnummers zijn terug te vinden.

Bij H.323 wordt het probleem veroorzaakt door H.225 en H.245, omdat die gebruik maken van embedded ip adressen. Als NAT wordt gebruikt, bevat de data private adressen in plaats van een publieke adres. Bijvoorbeeld een eindpunt (172.16.1.1), wordt vertaald door NAT naar 205.204.203.202. Als dit eindpunt probeert de verbinden met een ander eindpunt zal het verkeerde ip adres worden doorgegeven via H.225. De poging om met elkaar te verbinden met dit adres die niet gerouteerd kan worden zal dus mislukken.

Omdat SIP singalerings berichten ip adressen in het data segment van het IP pakket voegen, zal NAT ook SIP opbreken, behalve als ze “SIP aware” zijn gemaakt. Het probleem bij SIP is vaak dat de herkomst en eindbestemming van het bericht niet een directe relatie met de herkomst en eindbestemming van de video heeft.

5.1.4 Conclusie

Indien er gebruik wordt gemaakt van Office 365 is Microsoft Lync een goede oplossing voor onderlinge videoconferenties. Microsoft Lync zit standaard in Office 365 en steeds meer bedrijven maken hier gebruik van, omdat dit jaarlijks afgenomen kan worden en de licenties niet in een keer volledig betaald hoeven worden. Veel klanten van aan ADTS ICT gebruiken nog geen Office 365 in plaats daarvan maken ze gebruik van Cisco Jabber voor onderlinge videoconferenties.

Voor een zakelijk en professionele video oplossing biedt Cisco de meeste mogelijkheden. Naast het feit dat deze het beste integreert met telefonie, computers, mobiel, applicaties en browsers. Zijn de meesten klanten al in het bezit van een Cisco Unified Communications Manager (CUCM), waardoor deze niet apart aangeschaft hoeft te worden en aanzienlijk in prijs scheelt.

Het protocol die hierbij het beste gebruikt kan worden is SIP in plaats van H.323. SIP heeft als voordeel dat het flexibeler is dan H.323, waardoor het steeds populairder wordt. Ondanks dat deze flexibiliteit ook wat nadelen met zich mee brengt zal het meer mogelijkheden bieden in de toekomst.

De grootste kosten zitten in multipoint bridging. Doordat ADTS ICT B.V. deze optie niet door derde partijen wil laten beheren wordt de keuze aanzienlijk minder. Indien klanten hier niet in een keer veel geld in willen investeren is het een optie om deze dienst zelf volledig aan te schaffen en voor een maandelijkse bedrag aan te bieden aan klanten (net zoals office 365).

Tot slot zijn er veel afwegingen die gemaakt moeten worden om de kwaliteit te bepalen en te waarborgen. Hierbij kunnen we concluderen dat deze per situatie verschillend is, omdat er veel variabelen zijn waarmee rekening mee gehouden moet worden zoals: resolutie, framerate, bandbreedte, deelnemers etc.

5.2 Business case

Tijdens deze fase is ook een business case opgestelt na een gesprek met de opdrachtgever en de IT manager van Ampelmann Operations. Hieruit zijn de eisen voor de proof of concept van Ampelmann Operations te halen.

Ampelmann Operations is een klant van ADTS ICT B.V. en is gespecialiseerd in het overzetten van mensen op zee. Ze regelen de overstap met een innovatief systeem, die ze zelf ontwerpen en bouwen. Het is een soort loop brug die gestabiliseerd wordt, waardoor er niks meer van de golven gemerkt wordt. De bemanningsleden kunnen hierdoor veilig overlopen naar bijvoorbeeld een olieplatform of windmolen.

Situatie schets

Ampelmann Operations is gevestigd in Nederland. Het hoofdkantoor bevindt zich in Delft en de productie vindt plaats in Rotterdam. Daarnaast opereren ze wereldwijd (Figuur 9) en hebben ze medewerkers o.a. in Brunei, Singapore, Qatar etc. Doordat de werknemers van Ampelmann Operations over de hele wereld verspreid zitten en reizen veel geld en tijd kost, zijn ze opzoek naar een passende video over IP oplossing.

Figuur 9: Locatie medewerkers Ampelmann Operations.

Ampelmann Operations is om twee redenen opzoek naar een video oplossing. De eerste is voor het voeren van *sollicitatiegesprekking in het buitenland*. Op dit moment wordt dit gedaan met Skype, maar dit is geen zakelijke en professionele oplossing voor Ampelmann Operations. Dit komt mede door de slechte kwaliteit van zowel spraak als video.

De tweede reden is het verbeteren van de “*maandagochtend meeting*”, zodat er vanaf meerdere locaties aan deelgenomen kan worden. Momenteel is de beste oplossing om op locatie, in Delft, te zijn waar de meeting plaats vindt. Met Skype is het mogelijk om de meeting in Rotterdam te volgen,

maar veel informatie komt niet over omdat de kwaliteit dit niet toelaat. Deze meetings worden gehouden door Jan van der Tempel, CEO van Ampelmann Operations, en moeten zowel van hun hoofdkantoor in Delft als in Rotterdam gehouden kunnen worden.

In Delft en Rotterdam gaat het om een grote vergaderruimte waar ongeveer 75 personen tegelijkertijd aanwezig zijn. De externe locaties die aan de maandagochtend meeting mee moeten kunnen doen zijn: Singapore en Qatar. Bij deze externe locaties in het buitenland zullen niet meer dan 2 personen deelnemen.

Momenteel wordt er ook gebruik gemaakt van jabber om onderling te bellen en chatten. Integratie hiermee is daarom een belangrijk onderdeel van de video oplossing. Tot slot moet de totaal oplossing ook de communicatie binnen het bedrijf verbeteren, door de mogelijkheid om snel en moet goede kwaliteit te kunnen vergaderen met beeld.

Opsomming van de eisen:

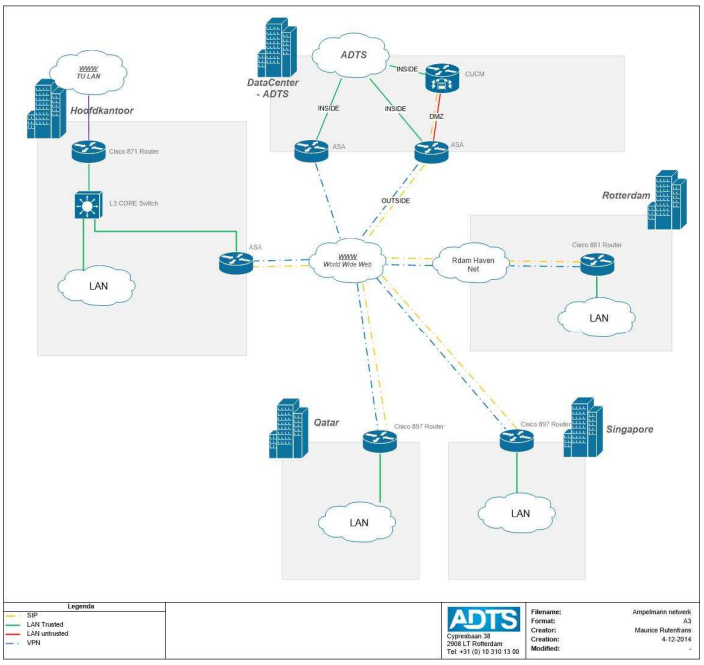
- HD kwaliteit
- Gebruiksvriendelijk
- Contentsharing mogelijk (zowel PowerPoint als detailtekeningen)
- Jabber integratie mogelijk
- Interne vergaderingen
- Multipoint met 4 locaties
- 2 locaties met 75 deelnemers
- 2 locaties met 2 deelnemers
- Mogelijk over een lokale internetverbinding
- Budget €25.000

6. Ontwerpfase

De ontwerpfase beschrijft het proces dat doorlopen is tijdens het ontwerpen en vastleggen van informatie met betrekking tot de proof of concept. In dit hoofdstuk wordt het fysieke en logische ontwerp, en keuzes die daarbij gemaakt zijn beschreven. Het resultaat van deze fase is het ontwerprapport (Bijlage F).

6.1 Fysiek ontwerp

Het huidige netwerk van Ampelmann Operations bestaat uit vier locaties die allemaal, doormiddel van een VPN, verbonden zijn met het datacenter van ADTS ICT B.V. (figuur 10). In het datacenter staan de servers (VMware), waarop o.a. de callmanager (CUCM) wordt gehost. Op de locaties wordt niets beheerd en kunnen gezien worden als “domme” locaties. Als een van de locaties technische problemen heeft of er een stroomuitval plaats vindt, ondervinden de rest van de locaties er geen problemen door.



Figuur 10: Huidige netwerk Ampelmann Operations

Tijdens het ontwerpen van de proof of concept is van binnen naar buiten ontworpen en zijn de volgende stappen doorlopen:

- Internet
- Locaties
- Lokale internet verbinding
- Eindpunten en platform
- Veiligheid en QoS

Internet

Voor de proof of concept wordt het Internet gesimuleerd met een layer 3 switch (figuur 11). Deze Layer 3 switch doet niets anders dan het verkeer doorsturen zonder er zelf wat mee te doen. In de huidige situatie kunnen alle locaties met elkaar praten doormiddel van VPN en routering. In deze proof of concept wordt dit gerealiseerd met het routeringsprotocol OSPF. Er is voor OSPF gekozen, omdat deze al gebruikt wordt in het huidige netwerk van Ampelmann Operations. Er wordt niet

gekozen voor het gebruik van VPN, omdat dit buiten de scope valt en geen invloed heeft op het eindresultaat.

Voor de verbindingen met de locaties worden verzonnen IP reeksen gebruikt. In een proof of concept is het mogelijk om de reeksen ruim te nemen, omdat er geen tekort kan ontstaan en niet naar de toekomst gekeken hoeft te worden. Om het realistisch te maken is er wel voor gekozen gebruik te maken van subnetten:

Vlan ID	Naam	IP range	IP
11	Delft	11.11.11.252/30	11.11.11.254
12	Rotterdam	11.11.12.252/30	11.11.12.254
13	Qatar	11.11.13.252/30	11.11.13.254
14	Singapore	11.11.14.252/30	11.11.14.254
15	Datacenter	11.11.15.252/30	11.11.15.254

Tabel 8: Internet IP ranges en IP adres

Locaties

Ook de locaties worden gesimuleerd met layer 3 switches. Deze locaties zijn verbonden met het internet (figuur 11) en routeren ook door middel van OSPF. De IP reeksen van de verbindingen met het internet zijn hiervoor al gedefinieerd. De locaties zelf krijgen een ruimere reeks toegekend, van 30 host, voor de belangrijkste vlans (tabel 9) in het Ampelmann netwerk. Vlans die niet zijn opgenomen zijn vlans zoals printer en guest die zeker niet in deze demonstatie voorkomen. Er zijn voor /27 subnets gekozen, omdat het aantal eindgebruikers die verbonden worden nog onbekend is en het beste flexibel gehouden kan worden.

Vlan id	**Naam**	**Delft**	**Rotterdam**	**Qatar**	**Singapore**	**Datacenter**
1	default	11.11.11.0/27	11.11.12.0/27	11.11.13.0/27	11.11.14.0/27	11.11.15.0/27
5	Monitoring	11.11.11.32/27	11.11.12.32/27	11.11.13.32/27	11.11.14.32/27	11.11.15.32/27
8	Management	11.11.11.64/27	11.11.12.64/27	11.11.13.64/27	11.11.14.64/27	11.11.15.64/27
11	Delft	11.11.11.252/30	x	x	x	x
12	Rotterdam	x	11.11.12.252/30	x	x	x
13	Qatar	x	x	11.11.13.252/30	x	x
14	Singapore	x	x	x	11.11.14.252/30	x
15	Datacenter	x	x	x	x	11.11.15.252/30
20	Office	11.11.11.96/27	11.11.12.96/27	11.11.13.96/27	11.11.14.96/27	11.11.15.96/27
100	Voice	11.11.11.128/27	11.11.12.128/27	11.11.13.128/27	11.11.14.128/27	11.11.15.128/27
104	Video	11.11.11.160/27	11.11.12.160/27	11.11.13.160/27	11.11.14.160/27	11.11.15.160/27
200	Server	11.11.11.192/27	11.11.12.192/27	11.11.13.192/27	11.11.14.192/27	11.11.15.192/27

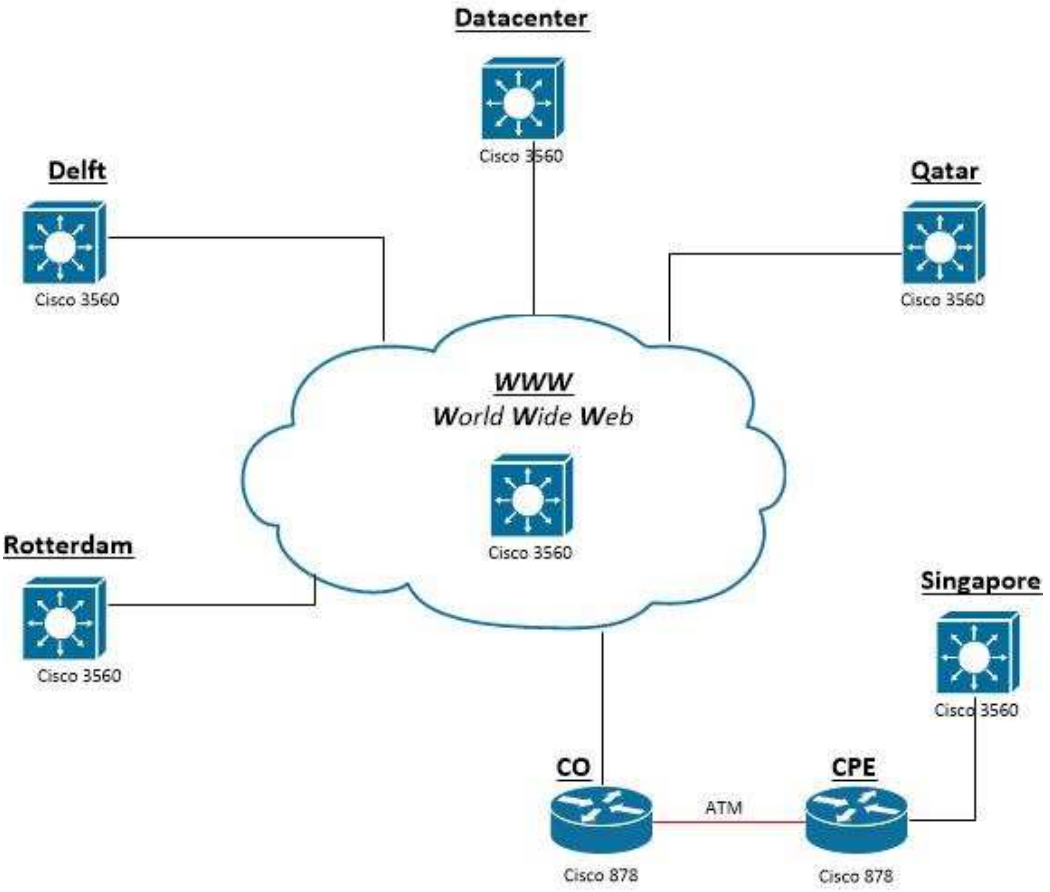
Tabel 9: IP plan locaties.

Lokale internet verbinding

Om een lokale internetverbinding te simuleren is de locatie Singapore uitgebreid met twee routers (CO en CPE), figuur 11. De twee toegevoegde routers zijn verbonden met een ATM verbinding. Hierdoor komt het overeen met de huidige situatie en daarnaast is het mogelijk om de bandbreedte in te stellen.

verbinding	IP range
Internet – CO	11.11.14.252/30
CO - CPE	11.11.14.248/30
CPE - Singapore	11.11.14.244/30

Tabel 10: Uitbreiding IP plan.



Figuur 11: Netwerk proof of concept

Eindpunten en platform

Het verschil in de ontwerpen zit in de eindpunten en het platform die gebruikt worden. Er zijn daarom twee verschillende ontwerpen gerealiseerd. In dit document wordt alleen het ontwerp die door Ampelmann Operations is gekozen behandeld. De andere is terug te vinden in bijlage F.

Allereerst is er gekeken naar de eindpunten die geschikt zijn voor Ampelmann Operations. Alle eindpunten van Cisco die ruim boven het budget zitten zijn in de eerste stap grijs gemaakt en zal niet naar gekeken worden (tabel 11). Categorieën die gehanteerd worden zijn groen (geschikt), oranje (mogelijk) en rood (niet geschikt).

Eindpunten	1-3 deelnemers	4-9 deelnemers	10+ deelnemers
Cisco IP Phone 8900 Series			
Cisco IP Phone 9900 Series			
Cisco DX650			
Cisco DX70 & 80			
Cisco TelePresence System 500			
Cisco TelePresence EX serie			
Cisco TelePresence MX200 en MX300			
Cisco TelePresence MX700 en MX 800			
Cisco TelePresence System Profile Serie			
Cisco TelePresence System 1100			
Cisco TelePresence TX9000 Serie			
Cisco TelePresence TX1310			

Tabel 11: Mogelijke eindpunten

Geschikt voor 1-3 deelnemers
Voor de externe locaties is in dit ontwerp gekozen voor de DX80. De DX80 levert dezelfde mogelijkheden als de EX60 en zal deze in de toekomst vervangen. Het grote verschil zit in de kosten en call control (tabel 12). Ampelmann Operations is al in het bezit van een Cisco Unified Communications Manager (CUCM) en hoeft deze niet extra aan te schaffen. Het grootste nadeel, op dit moment, is de lange levertijd van de DX80.

	DX80	**EX60**
Kosten	€3.000	€4.200
Call control	CUCM	Zowel CUCM als VCS
Extra	Lange levertijd	-

Tabel 12: Verschillen DX80 en EX60

De DX Serie bestaat uit drie varianten, waarvan de DX650 en DX70 afvallen omdat deze alleen voor een enkele deelnemer geschikt zijn:

- ~~DX650~~
- ~~DX70~~
- DX80

Geschikt voor 10+ deelnemers
Voor de vergaderruimte zijn geen van bovengenoemde eindpunten volledig geschikt, omdat de geïntegreerde schermen niet aan de eis kunnen voldoen om voor 75 deelnemers duidelijk beeld weer te geven. De MX300 G2 is mogelijk, maar de kans dat deze ook niet voldoet aan de eisen van Ampelmann Operations is zeer groot. Het voordeel van het gebruiken van de MX300 G2 is dat deze een geïntegreerde multipoint bridging capaciteit heeft, waardoor er geen TelePrecense server nodig is. Er is daarom gekeken naar een professionele camera die zelf geplaatst kan worden (Figuur 12).

Figuur 12: Voorbeeld hoe de SX20 gebruikt kan worden.

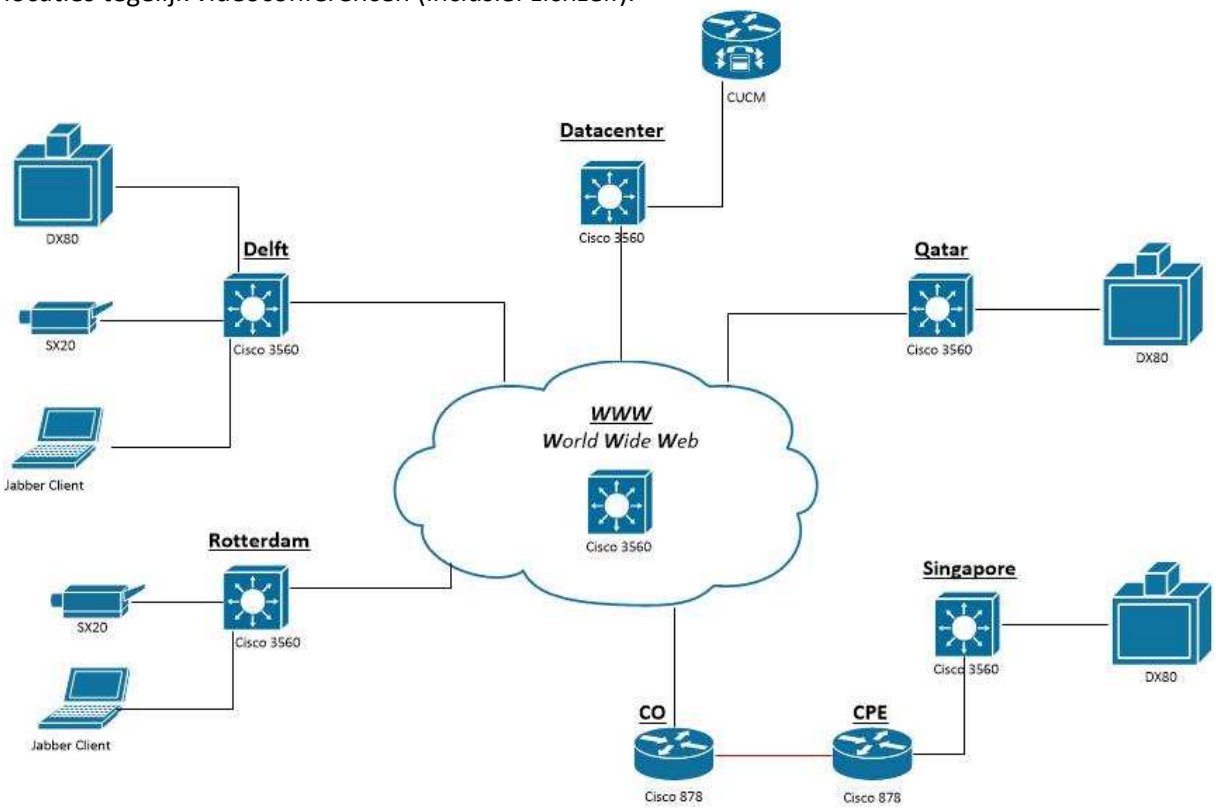
Hiervoor is gekozen voor de Cisco SX serie, die uit de volgende varianten bestaat:

- SX10
- SX20

De keuze is gevallen op de SX20, omdat de SX10 voor persoonlijk gebruik op een tv scherm dient en de SX20 gemaakt is voor videoconferentie zalen. Daarnaast heeft deze ook een geïntegreerde multipoint bridging capaciteit.

Platform

Ampelmann Operations is al in het bezit van een Cisco Communications Manager (CUCM), deze maakt point-to-point videoconferenties mogelijk. De sollicitatie gesprekken met de DX80 kunnen hiermee gerealiseerd worden. Voor videoconferenties waar meer dan twee locaties (multipoint) deelnemen moet een multipoint bridge gekozen worden. In dit ontwerp is gekozen voor de SX20, omdat deze een geïntegreerde multipoint bridging capaciteit bezit. De SX20 kan met maximaal vier locaties tegelijk videoconferencen (inclusief zichzelf).



Figuur 13: Gekozen netwerk ontwerp.

In tabel 13 is af te lezen wat de kosten zijn voor de hardware van deze oplossing. Dit is exclusief de aanschaf van presentatie apparatuur, extra beeldschermen en implementatie kosten.

Hardware	aantal	Prijs per stuk	Kosten
DX80	3	€3.000	€9.000
SX20	2	€4.800	€9.600
Multisite license SX20	1	€2.500	€2.500
Totaal:			€21.100

Tabel 13: Kostenplaatje.

Ampelmann Operations heeft gekozen voor het dit ontwerp, omdat de lagere kosten van de DX80 zwaarder wegen dan de langere levertijd. Voor de maandagmorgen meeting wordt er gebruik gemaakt van SX20 in combinatie met de multisite license. De keuze voor de SX20 is gemaakt om er zeker van te zijn dat hij gebruikt kan worden voor 75 man. De multisite license is gekozen vanwege de kosten, ondanks dat deze gelimiteerd is tot vier gelijktijdig deelnemers in een videoconference. De TelePresence server is een betere oplossing met het oog op de toekomst, omdat deze schaalbaar is. De investering ligt daarentegen aanzienlijk hoger, waardoor er gekozen is voor multisite license.

Veiligheid en QoS
Al het verkeer wordt verzonden via VPN tunnels naar elkaar. Hierdoor is het verkeer afgeschermd van de buitenwereld. Doordat er gebruik gemaakt wordt van VPN tunnels hoeft er geen rekening gehouden te worden met natting en firewalls. Het voordeel hiervan is dat een slecht firewall beleid vermeden wordt.
Voor intern wordt het voice en video verkeer standaard beschermt door de Cisco Unified Communications Manager (CUCM). Om het verkeer te beschermen wordt het TLS (Transport Layer Security) protocol gebruikt. Dit wordt voorgeschreven door Cisco en gebruikt AES 128 encryptie om het verkeer te versleutelen.

QoS is in de huidige situatie van Ampelmann Operations alleen intern in te regelen, omdat dit over het internet niet mogelijk is. Intern is er voldoende bandbreedte aanwezig, door het gebruik van gigabit verbindingen. Mede hierdoor en omdat het aantal eindpunten nog minimaal is, is het niet nodig om dit in te stellen.
Als er in de toekomst de vraag komt om dit in te regelen is het aan te raden om over te stappen op bijvoorbeeld MPLS (Multiprotocol Label Switching) om QoS/CoS in te regelen. De kosten hiervoor liggen daarentegen zeer hoog.

6.2 Logisch ontwerp

- Configuratie routers
- VMware
- Unified Communicatiosn manager

Configuratie routers
De configuraties van de routers zijn voor het grootste deel identiek aan elkaar, op hostname en IP reeksen na. Daarom wordt alleen de configuratie van de router “Delft” behandeld, de rest is terug te vinden in bijlage F.

```
hostname Delft
ip routing
ip domain name AMPELMANN.local          //Domain name is nodig om rsa sleutel te genereren

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa                 //Rsa sleutel gegenereerd voor het gebruik van ssh
2048                                    //Sleutelgrote is zeer veilig en standaard binnen ADTS

vlan 5                                  //Vlans aanmaken
name Monitoring
vlan 8
name Management
vlan 11
name Delft
vlan 20
name Office
vlan 100
```

```
name Voice
vlan 104
name Video
vlan 200
name Servers

interface Vlan1                          //IP adressen toekennen
 ip address 11.11.11.30 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan5
 description Monitoring
 ip address 11.11.11.62 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan8
 description Management
 ip address 11.11.11.94 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan11
 description Delft
 ip address 11.11.11.253 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan20
 description Office
 ip address 11.11.11.126 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan100
 description Voice
 ip address 11.11.11.158 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan104
 description Video
 ip address 11.11.11.190 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan200
 description Server
 ip address 11.11.11.222 255.255.255.224
```

```
 no ip proxy-arp
 no shutdown

interface FastEthernet0/1                    //Poort naar het internet
 description Internet
 switchport access vlan 11
 switchport mode access
 no shutdown

interface range FastEthernet0/2-23
 switchport mode access
 shutdown

interface FastEthernet0/24                   //Poort voor video eindpunt
 switchport access vlan 104
 switchport mode access
 no shutdown

interface range GigabitEthernet0/1-2
 switchport mode access
 shutdown

router ospf 1                                //Routering aangemaakt
 network 11.11.11.252 0.0.0.3 area 0
 network 11.11.11.0 0.0.0.31 area 11
 network 11.11.11.32 0.0.0.31 area 11
 network 11.11.11.64 0.0.0.31 area 11
 network 11.11.11.96 0.0.0.31 area 11
 network 11.11.11.128 0.0.0.31 area 11
 network 11.11.11.160 0.0.0.31 area 11
 network 11.11.11.192 0.0.0.31 area 11

ip dhcp excluded-address 11.11.11.126        //DHCP aangemaakt voor de nodige vlans
ip dhcp excluded-address 11.11.11.190
ip dhcp excluded-address 11.11.11.158

ip dhcp pool Office
network 11.11.11.96 255.255.255.224
default-router 11.11.11.126
dns-server 8.8.8.8

ip dhcp pool Voice
network 11.11.11.128 255.255.255.224
default-router 11.11.11.158
option 150 ip 11.11.15.200
dns-server 8.8.8.8

ip dhcp pool Video
network 11.11.11.160 255.255.255.224
default-router 11.11.11.190
```

dns-server 8.8.8.8

ip name-server 8.8.8.8

access-list 10 permit 11.11.11.64 0.0.0.31 //IP reeks waar vanaf ingelogd mag worden
access-list 10 deny any log

line vty 0 15
transport input ssh
access-class 10 in

VMware Server
De VMware server en Cisco Unified Communications Manager zijn volgens de ADTS standaard geïnstalleerd en ingesteld. Stappen zijn terug te lezen in Bijlage F.

Unified Communications Manager

- User aanmaken
- Regions aanmaken
- Eindpunten aanmaken

Als eerste zijn er een aantal users en device profiles aangemaakt met dezelfde nummerreeks die in het huidige Ampelmann netwerk gebruikt worden (tabel 14):

User	Nummer
Maurice Rutenfrans	9001
Bernhard van der Linde	9002
Rick Hoevenaar	9003
Emre Demir	9004
Jsco Hoornaar	9005
Marc Schuller	9006
Aloys Ruseler	9007
Hanneke Franken	9008
Amber Schot	9009
Robert van de Linde	9010

Tabel 14: Users en doorkiesnummers.

Vervolgens zijn er voor elke locatie een nieuwe region aangemaakt (tabel 15):

Region
AMP-NL-DFT-VIDEO
AMP-NL-RDM-VIDEO
AMP-QT-QTR-VIDEO
AMP-SG-SNG-VIDEO

Tabel 15: Regions.

De regions zijn nodig om de maximum bandbreedte voor video en de kwaliteit van spraak in- en extern te beheren:

- Spraak locaal G.711
- Spraak inter company G.729
- Maximum bandbreedte per gesprek 2048 kbps, voor alle locaties

Voor spraak worden de codecs die al in de huidige situatie aanwezig zijn gebruikt. De codec keuze wordt ook ondersteund met de resultaten uit het onderzoek. Voor video is gekozen om de bandbreedte van een gesprek te limiteren tot 2048 kbps. Hiervoor is gekozen, omdat hiermee een resolutie van 1920x1080/30 gehaald kan worden en meer dan voldoende is voor deze oplossing.

De video eindpunten worden aangemaakt als “logged out”, zodat er geen gebruikers profiel nodig is om hem te gebruiken. Daarom is er ook gekozen om een nieuwe nummerreeks hiervoor te beginnen (tabel 16):

Device	Nummer
DX80 - Delft	1001
DX80 - Qatar	1002
DX80 - Singapore	1003
SX20 - Delft	1004
SX20 - Rotterdam	1005

Tabel 16: Video eindpunten en nummers.

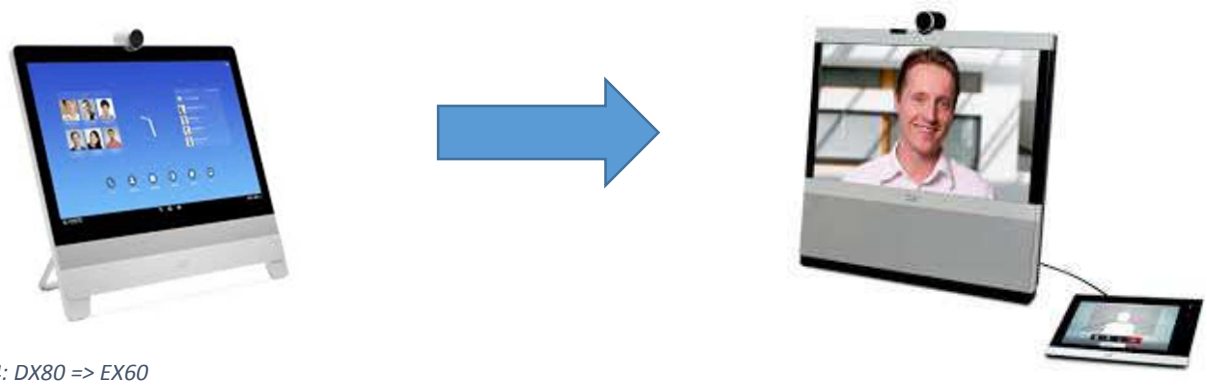
Om er voor te zorgen dat de users niet alle nummers van de conference systemen uit hun hoofd hoeven te kennen, worden ze toegevoegd aan de adressenlijst. Om dit te realiseren zijn de eindpunten ook als users aangemaakt (tabel 17):

User	Nummer
Delft Meetingroom 1	1001
Qatar Meetingroom 1	1002
Singapore Meetingroom 1	1003
Delft Meetingroom 2	1004
Rotterdam Meetingroom 1	1005

Tabel 17: Adressenlijst.

7. Implementatiefase

Tijdens de implementatiefase wordt het fysieke ontwerp gebruikt om de proof of concept op te bouwen en het logische ontwerp om de opstelling te configureren. Ampelmann Operations heeft gekozen voor het gebruik van de DX80, maar het was al bekend dat deze een lange levertijd hadden. Daarom is er in overleg met de opdrachtgever besloten om deze in de proof of concept te vervangen door EX60's (figuur 14).



Figuur 14: DX80 => EX60

Deze keuze heeft niet veel invloed op het ontwerp. Het enige verschil is dat er in plaats van DX80, EX60 eindpunten aangemaakt moeten worden in de Unified Communications Manager (groen aangegeven in de tabel 18).

Device	Nummer
~~DX80~~ EX60 - Delft	1001
~~DX80~~ EX60 - Qatar	1002
~~DX80~~ EX60 - Singapore	1003
SX20 - Delft	1004
SX20 - Rotterdam	1005

Tabel 18: Aanpassing

Tijdens deze fase bleek ook dat er voor de CUCM NTP nodig is, daarom is ervoor gekozen om het netwerk uit te breiden met een router die met het netwerk van ADTS ICT B.V. verbind. Via deze verbinding kan de publieke NTP server (141.138.138.136) bereikt worden. Voor de configuratie hiervoor is een extra hoofdstuk aan het ontwerprapport toegevoegd (bijlage F).

8. Testfase

Tijdens de testfase zijn de eisen uit de business case op de proef gesteld. Om dit te realiseren zijn er checklists gemaakt die 1 of meerdere eisen testen. Checklist 1 wordt hieronder als voorbeeld gegeven. Van de rest van de checklists worden alleen de eisen benoemd, de complete checklists zijn terug te vinden in Bijlage G.

Checklist 1: Point tot point

Met deze checklist worden de volgende eisen getest:

- Sollicitatie gesprek

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De EX60's zijn opgestart. • Hoofdschermen worden weergegeven.	**1. Van Delft naar Qatar bellen, om een sollicitatie gesprek te houden.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Qatar Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen.	#1. Er wordt een overzicht van contacten weergegeven. Na het maken van een keuze wordt het contact gebeld.	✓	
		#2. Op de EX60 in Qatar neemt de tester op door op "Accept" te klikken.	#2. Na het accepteren wordt de point to point videoconferentie gestart.	✓	
• Hoofdschermen worden weergegeven.	**2. Van Delft naar Singapore bellen, om een sollicitatie gesprek te houden.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Singapore Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen.	#1. Er wordt een overzicht van contacten weergegeven. Na het maken van een keuze wordt het contact gebeld.	✓	
		#2. Op de EX60 in Singapore neemt de tester op door op "Accept" te klikken.	#2. Na het accepteren wordt de point to point videoconferentie gestart.	✓	

Checklist 2: Point to multipoint (1)

Met deze checklist worden de volgende eisen getest:

- Maandag ochtend meeting
- 3 Locaties
- 4 Locaties
- >4 Locaties

Checklist 3: Point to multipoint (2)

Met deze checklist worden de volgende eisen getest:

- Maandag ochtend meeting
- 3 Locaties
- 4 Locaties
- >4 Locaties

Checklist 4: Deelnemers

Met deze checklist worden de volgende eisen getest:

- Qatar en Singapore, 2 deelnemers
- Delft en Rotterdam, 75 deelnemers

Checklist 5: Content sharing (1).
Met deze checklist worden de volgende eisen getest op de EX60:

- PowerPoint delen
- Detailtekeningen delen

Checklist 6: Content sharing (2).
Met deze checklist worden de volgende eisen getest op de SX20:

- PowerPoint delen
- Detailtekeningen delen

Checklist 7: Jabber
Met deze checklist worden de volgende eisen getest:

- Jabber integratie

Checklist 8: Lokale internetverbinding
Met deze checklist worden de volgende eisen getest:

- Mogelijk over een lokale internetverbinding.
- (tijdens de videoconferentie zal ook een file transfer plaats vinden om de impact te analyseren)

Checklist 9: gebruiksvriendelijkheid
Met deze checklist worden de volgende eisen getest:

- Gebruiksvriendelijkheid.

8.1 Conclusie

Uit het testrapport kunnen we concluderen dat de proof of concept aan alle eisen van Ampelmann Operations voldoet, op één enkele na. De eis die niet goed is gekeurd, is het voldoen aan 75 deelnemers. Helaas kon deze eis niet volledig getest worden, omdat er maar 19 deelnemers waren in plaats van 75. Hierdoor is het niet met zekerheid te zeggen of de SX20 ook daadwerkelijk aan deze eis voldoet.

Overige tests die zijn afgekeurd waren al voorspeld dat deze niet goed uitgevoerd konden worden. Zo is er getest of er meer dan vier sites gelijktijdig met elkaar konden video conferencen, maar uit het onderzoek was al gebleken dat dit er maximaal vier waren en niet kon. Bij het testen van de lokale internet verbinding is bewust gekozen om de bandbreedte te verminderen. Hierdoor is het inzichtelijk geworden wanneer deze onvoldoende is en slechte kwaliteit levert.

9. Evaluatie

Ter afsluiting van het afstudeerverslag wordt in dit hoofdstuk terug gekeken op de afstudeeropdracht. Zowel de kwaliteit van de geleverde producten als het proces worden geëvalueerd.

9.1 Productevaluatie

Plan van aanpak en Onderzoeksplan
In de voorbereidingsfase zijn het plan van aanpak en onderzoeksplan gerealiseerd. Tijdens het realiseren van deze producten ben ik niet tegen bijzondere dingen aangelopen. Mede door de vele ervaring die ik hiermee heb opgedaan tijdens mijn opleiding aan de Haagse Hogeschool.

Onderzoeksrapport
Over het onderzoekrapport ben ik tevreden alles staat erin wat ik had verwacht, met voldoende diepgang. Een enkele sub vraag vond ik niet juist gesteld of niet in de juiste volgorde. Een sub vraag heb ik aangepast, en een had sneller en beter beantwoord kunnen worden als die later in het onderzoek werd gesteld.

Ontwerprapport
Het ontwerprapport miste een klein onderdeel die tijdens de implementatiefase is toegevoegd. Tijdens het ontwerpen was er geen rekening mee gehouden dat er een NTP server nodig was voor de Cisco Unified Communications manager.

Proof of concept
Door het uitlopen van de onderzoeksfase en de lange levertijd van de door Ampelmann gekozen DX80, kon deze helaas niet gebruikt worden. Dit is ook opgenomen in de risico analyse. Er is daarom gekozen om deze in de proof of concept te vervangen met de EX60. Dit heeft niet veel veranderd aan het ontwerp of de implementatie, maar het is wel jammer dat het originele ontwerp niet aangehouden kon worden.

Testrapport
Het testrapport is volledig uitgevoerd en voldoet aan alle eisen op een na. Deze is helaas niet getest, omdat hier 75 personen voor aanwezig moesten zijn. De test wel uitgevoerd maar met minder mensen (19).

9.2 Procesevaluatie

Deadlines niet gehaald
De afstudeeropdracht is voornamelijk uitgelopen tijdens de onderzoeksfase. Dit komt door onbekendheid met de materie en sub vragen die in een andere volgorde sneller beantwoord hadden kunnen worden. Met de kennis van sub vraag 1c was het bijvoorbeeld eenvoudiger geweest om de datasheets door te nemen en te bepalen wat belangrijk was voor sub vraag 1b. Door het uitlopen van deze fase zijn alle deadlines opgeschoven, waardoor er tot op het eind nog hard aan gewerkt is. Doordat de planning voor deze afstudeeropdracht tot de kerst liep waren er nog drie weken om deze achterstand in te halen en zijn alle eindproduct alsnog opgeleverd.

Door de vertraging is de ontwerpfase ook later van start gegaan, waardoor er minder speling was voor het bestellen en leveren van producten. Hierdoor is er niet gebruik gemaakt van de door

Ampelmann gekozen DX80, want het was al van te voren bekend dat deze een lange levertijd hadden en niet op tijd geleverd kon worden.

Projectmethode
De projectmethode die hoorde bij de afstudeeropdracht was op maat gemaakt en naar mijn mening was het een goede methode met alle benodigde fases. Een goed leermoment vond ik de ontwerpfase. Als IT'er heb ik de neiging om direct een oplossing te gaan bouwen, terwijl een uitgedacht ontwerp ervoor kan zorgen dat een heel andere pad bewandeld wordt.

Achteraf had een iteratieve methode ook deels van toepassing kunnen zijn. Tijdens de implementatiefase kwam ik er bijvoorbeeld achter dat er een NTP server nodig was voor de Cisco Unified Communications manager. Door de keuze voor de watervalmethode is het hierdoor niet mogelijk om terug te gaan naar de ontwerpfase om dit aan te passen.

Doelstelling en probleemstelling
Het resultaat is een onderzoek naar video over IP en een proof of concept voor Ampelmann Operations. De doelstelling is daarmee voor een deel behaald, want van te voren was vast gesteld dat de proof of concept bedoelt was voor alle klanten van ADTS en niet alleen voor Ampelmann. Omdat elke klant andere behoeftes heeft is het niet mogelijk om een proof of concept te maken die daaraan voldoet.

Literatuurlijst

[1] Guide to Voice and Video over IP: Bookzz; bezocht op 1 september 2014 http://dlx.bookzz.org/genesis/966000/2eea03802de33520fef1f472797b5ff9/_as/[Lingfen_Sun,__Is-Haka_Mkwawa,__Emmanuel_Jammeh,__(BookZZ.org).pdf

[2] Video Over IP A Practical Guide to Technology and Applications; Bookzz; bezocht op 1 september 2014http://dlx.bookzz.org/genesis/402000/84ff86380fae1c3ba5db5f6a2209d4e1/_as/[Wes_Simpson]_Video_Over_IP_A_Practical_Guide_to_(BookZZ.org).pdf

[3] Visual Networking Index (VNI); Cisco; bezocht op 8 september 2014 http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~overview

[4] MKB Videoconferencing AV; ictloket; bezocht op 17 september 2014 http://www.ictloket.nl/kennisbank/mkb-videoconferencing-av/

[5] Video Conferencing Frequently Asked Questions; onevideoconferencing; bezocht op 18 september 2014 http://www.onevideoconferencing.com/video-conferencing-faq.html

[6] Voordelen van videoconferencing; conferencing4all; bezocht op 18 september 2014 http://www.conferencing4all.nl/videoconferencing_voordelen.html

[7] What you really need to know about Video Conferencing Systems; c21video; bezocht op 17 oktober 2014 http://www.c21video.com/video.html

[8] Quality of Service Design Overview; Ciscopress; bezocht op 20 oktober 2014 http://www.ciscopress.com/articles/article.asp?p=357102&seqNum=2

[9] Frequently Asked Questions About Voice and Video over IP Networks; Wainhouse; bezocht op 3 november 2014 http://www.wainhouse.com/files/papers/wr-faq-ip-conf.pdf

[10] Quality of Service (QoS) in High-Priority Applications; Transition; bezocht op 3 november 2014 http://www.transition.com/TransitionNetworks/Uploads/Literature/qos_wp.pdf

[11] Voice an Video conferencing Fundamentals; Bookzz; bezocht op 6 november 2014 http://dlx.bookzz.org/genesis/55000/fe05147ffe6a14b6ad5d83209c51a849/_as/[Scott_Firestone,_Thiya_Ramalingam,_Steve_Fry]_Voi(BookZZ.org).pdf

[12] WAN video conferencing network design requirements for QoS; Techtarget; bezocht op 10 november 2014 http://searchenterprisewan.techtarget.com/tip/WAN-video-conferencing-network-design-requirements-for-QoS

[13] The importance of encrypting video over IP; Cardinalpeak; bezocht op 13 november 2014 http://www.cardinalpeak.com/blog/the-importance-of-encrypting-video-over-ip/

[14] Why do firewalls cause problems with H.323 and SIP; Wainhouse; bezocht op 18 november 2014 http://www.wainhouse.com/files/papers/wr-faq-ip-conf.pdf

[15] Virtualization, Isolation and Encryption of IP Video Surveillance; Cisco; bezocht op 18 november 2014http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/IPVS/ip_video_surv/ipvs_virtual.html

Bijlagen

Bijlage A - Afstudeerplan

Afstudeerplan

Informatie afstudeerder en gastbedrijf

Afstudeerblok: 2014-2.1 (start uiterlijk 1 september 2014)
Startdatum uitvoering afstudeeropdracht:
Inleverdatum afstudeerdossier volgens jaarrooster: 9 januari 2015

Studentnummer: 10001468
Achternaam: dhr Rutenfrans
Voorletters: M.E.
Roepnaam: Maurice
Adres: Gildestraat 31
Postcode: 2624AW
Woonplaats: Delft
Telefoonnummer: -
Mobiel nummer: 0633611357
Privé emailadres: mauricerutenfrans@hotmail.com

Opleiding: Technische Informatica
Locatie: Den Haag
Variant: voltijd

Naam studieloopbaanbegeleider: R.A. van Neijhof
Naam begeleidend examinator: Jan Dirk Schagen
Naam tweede examinator: Madelon Nieuwland

Naam bedrijf: ADTS ICT B.V.
Afdeling bedrijf: Servicedesk en Engineering
Bezoekadres bedrijf: Cypresbaan 38
Postcode bezoekadres: 2908 LT
Postbusnummer: N.v.t
Postcode postbusnummer: N.v.t
Plaats: Capelle aan den IJssel
Telefoon bedrijf: +31 10 310 13 00
Telefax bedrijf: N.v.t
Internetsite bedrijf: www.adts.nl

Achternaam opdrachtgever: dhr. van der Linde
Voorletters opdrachtgever: B. D.
Titulatuur opdrachtgever: Ing.
Functie opdrachtgever: Directeur
Doorkiesnummer opdrachtgever: 30
Email opdrachtgever: bernhard.vanderlinde@adts.nl

Achternaam bedrijfsmentor: dhr. van der Linde
Voorletters bedrijfsmentor: B.D.
Titulatuur bedrijfsmentor: Ing.
Functie bedrijfsmentor: Directeur
Doorkiesnummer bedrijfsmentor: 30
Email bedrijfsmentor: bernhard.vanderlinde@adts.nl

Doorkiesnummer afstudeerder: 1340
Functie afstudeerder (deeltijd/duaal):

Titel afstudeeropdracht: Video-over-ip

Uitvoeren van een onderzoek naar en demonstratie van video-over-ip.

Opdrachtomschrijving

1. Bedrijf

ADTS ICT B.V is één van de drie business units van de ADTS Groep B.V. Vanaf september 2007 zijn er ict werkzaamheden aan de huidige activiteiten van de ADTS Groep toegevoegd. ADTS-ICT is een gespecialiseerde leverancier van hoogwaardige ict-infrastructuurproducten en diensten. Ze richt zich volledig op connectiviteit en is op een hoog niveau gecertificeerd partner van o.a. CISCO, Microsoft en JDM Software. De bedrijfsvisie is het leveren van "maatwerk" voor elke oplossing, omdat iedere aanvraag en opdracht andere eisen en wensen heeft. Data, Voice, Security en Wireless worden met elkaar geïntegreerd. Daarnaast wordt ook gekeken naar de mogelijkheden én de risico's deze van Tailor Made Connectivity.

2. Probleemstelling

De stijgende behoefte en noodzaak om werk en privé flexibel te kunnen combineren leidt tot een groeiende vraag bij klanten naar video-over-ip. Daarnaast willen steeds meer bedrijven een bijdrage leveren aan de duurzaamheid van hun leefomgeving en op lange termijn liggen de kosten lager dan reizen. Echter is er binnen ADTS weinig kennis over deze snel groeiende producten, die ervoor moeten zorgen dat klanten waar dan ook ter wereld op afstand kunnen samenwerken en communiceren.

3. Doelstelling van de afstudeeropdracht

Het doel van deze opdracht is het onderzoeken van de belangrijkste mogelijkheden van video-over-ip en de achterliggende architectuur, zodat de klanten van ADTS in de toekomst een op maat gemaakte oplossing kunnen krijgen. Dit onderzoek wordt ondersteund door een lab-opstelling waarin het onderzoek in de praktijk kan worden getest en gedemonstreerd.

4. Resultaat

Het resultaat van deze opdracht is een onderzoekrapport over video-over-ip waarin onder andere de benodigde apparatuur, netwerk designs, protocollen, netwerk impact etc. beschreven worden en wat de voor- en nadelen ervan zijn. Dit dient bewezen te worden aan de hand van een demonstratie. Daarnaast wordt deze demonstratie ondersteunt met een presentatie die gebruikt kan worden door ADTS voor de sales.

5. Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten

Voorbereidingsfase(10 dagen)

- Opstellen Plan van aanpak
- Opstellen Onderzoeksplan

Onderzoeksfase(40 dagen)

- Opstellen onderzoeksrapport

Ontwerpfase (15 dagen)

- Ontwerpen demonstratie
- Opbouwen demonstratie
- Configureren demonstratie
- Presentatie

Testfase (5 dagen)

- Testen demonstratie.

Afstudeerscriptie(15 dagen)

- Afronden afstudeerscriptie.

6. Op te leveren (tussen)producten

De producten die ik op zal opleveren tijdens mijn afstuderen zijn:

- Plan van aanpak
- Onderzoeksplan
- Onderzoeksrapport
- Ontwerprapport
- Testplan
- Testrapport

7. Te demonstreren competenties en wijze waarop

G1 Praktische aspecten hanteren in projecten
Deze beroepstaak voer ik uit op niveau 2 en toon ik aan door middel van de risicoanalyse uit het plan van aanpak.

A1 Analyseren van het probleemdomein
Deze beroepstaak voer ik uit op niveau 3 en toon ik aan door middel van een onderzoeksrapport waarin de werking van video-over-ip in kaart is gebracht.

C9 Ontwerpen van een infrastructuur
Deze beroepstaak voer ik uit op niveau 3 en toon ik aan door middel van een ontwerprapport.

D18 Testen van een infrastructuur
Deze beroepstaak voer ik uit op niveau 3 en toon ik aan door middel van een testplan en testrapport.

Uitleg niveaus
Er wordt gewerkt met 5 niveaus in het niveaumodel. Het niveau van een praktijkopdracht wordt in dit model bepaald door zowel de rol die ik zelf bij deze taak heb (taakrol) als door de omgevingsfactoren die invloed op de taak hebben (context). Welk niveau bij welke combinatie van taakrol en context hoort, is in de volgende matrix te lezen:

Ik moet minstens 1 beroepstaak op niveau 3 hebben. (Beroepstaken op niveau 3 of 4 zijn van invloed op het eindcijfer, want je wordt hierop beoordeelt)

Opdracht	Geleid	Zelfstandig	Sturend
Eenvoudig	1	2	3
Normaal	2	3	4
Moeilijk	3	4	5

Voorbeeld:
Niveau 3:

- Taakrol: zelfstandig – context: lastig
  Je bent medewerker in een projectgroep ofwel je bent als enige in de projectgroep deskundig op

dit vakgebied. De taken die je in het project hebt zijn nieuw en je moet zelf bepalen welke methoden en technieken je gebruikt om je taken tot een goed einde te brengen.
De resultaten van het project worden in het hele bedrijf ingevoerd, dus veel mensen zullen de gevolgen van je werk ondervinden. Omdat er dus ook veel afdelingen mee te maken krijgen, praten er ook veel mensen mee over dit project. Het is lastig om iedereen op één lijn te krijgen.

Bijlage B – Plan van aanpak

AFSTUDEERRAPPORT

ADTS ICT B.V. - NL - Capelle aan den IJsel

Video over IP

Auteur	:	Maurice Rutenfrans
Studentnummer	:	10001468
Document	:	Plan van aanpak
Releasedatum	:	05 sep. 14
Versie	:	1.0
Status	:	Definitief

Documenthistorie

Versie	Datum	Auteur	Commentaar
0.1	28 Aug. 14	Maurice Rutenfrans	Concept
0.1	03 Sep. 14	Maurice Rutenfrans	Controle Rick Hoevenaar
1.0	05 Sep. 14	Maurice Rutenfrans	Definitief

Distributielijst

Versie	Datum	Ontvanger	Email
0.1	28 Aug. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
1.0	05 Sep. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl

Relevante documenten

Versie	Datum	Auteur	Document

Voorwoord

In het kader van mijn opleiding Technische Informatica aan de Haagse Hogeschool ben ik werkzaam bij ADTS ICT B.V. Het plan van aanpak maakt onderdeel uit van mijn afstudeerstage en is bestemd voor de opdrachtgever en mijzelf.

Het plan van aanpak zal dienen als leidraad voor het definiëren en kaderen van de opdracht en het succesvol afronden daarvan. Daarnaast is dit plan van aanpak geschreven voor de opdrachtgever. Dit is Bernhard van der Linde, directeur van ADTS ICT. Hij zal middels dit plan van aanpak inzicht krijgen in wat ik tijdens deze opdracht aan activiteiten uit ga voeren. Tot slot is het beschikbaar voor een ieder die geïnteresseerd is en daartoe bevoegd is.

Rotterdam, september 2014
Maurice Rutenfrans

Inhoudsopgave

1. Inleiding

Het wordt steeds gebruikelijker om een conferentiezaal binnen te lopen en een tafel omringd met mensen met te zien, die live een spreker of presentatie op een andere locatie aan het volgen zijn. Dit wordt mogelijk gemaakt met video over IP, ook wel Networked Video en IP video genoemd. Deze snel groeiende technologie zorgt ervoor dat video getransporteerd kan worden over het standaard Internet Protocol (IP). Het helpt mensen om beter te communiceren, samen te werken, te leren en te beveiligen. Video over IP verandert het leven voor alles en iedereen, van grote ondernemingen en kleine bedrijven tot agentschappen in de publieke sector. Het wordt gebruikt voor verschillende doeleinden zoals video conferenties en e-learning om hiermee een organisatie te verbeteren en concurrentievoordeel te behalen.

Dit plan van aanpak zal dieper ingaan op de gewenste uitvoering van het project en is opgebouwd uit de volgende hoofdstukken:

2. Opdrachtomschrijving
3. Achtergrond
4. Project aanpak
5. Planning
6. Projectorganisatie
7. Risicoanalyse

2. Opdrachtsomschrijving

In dit hoofdstuk worden de probleemstelling, doelstelling, benodigdheden, scope en het resultaat van de opdracht beschreven.

2.1 Probleemstelling

De stijgende behoefte om o.a. werk en privé flexibel te kunnen combineren leidt tot een groeiende vraag bij klanten naar video over IP. Daarnaast willen steeds meer bedrijven een bijdrage leveren aan de duurzaamheid van hun leefomgeving en op lange termijn liggen de kosten lager dan reizen. Echter staat deze snel groeiende technologie, die ervoor moeten zorgen dat klanten waar dan ook ter wereld op afstand kunnen samenwerken en communiceren, nog in de kinderschoenen binnen ADTS ICT B.V.

2.2 Doelstelling

Het doel van deze opdracht is het onderzoeken van video over IP en de achterliggende architectuur, zodat de klanten van ADTS ICT B.V. in de toekomst een op maat gemaakte oplossing kunnen krijgen. Dit onderzoek wordt ondersteund door een lab-opstelling waarin het onderzoek in de praktijk zal worden getest en gedemonstreerd.

2.3 Benodigdheden

De volgende onderdelen zijn nodig om dit project tot een goed einde te brengen:

- Werkplek met Microsoft Office.
- Toegang internet en literatuur.
- Microsoft Visio voor het realiseren van netwerkontwerpen.
- Hardware/apparatuur voor de demonstratie.
- Labruimte voor demonstratie.

2.4 Scope

- Onderzoek naar video over IP.
- Onderzoek wordt gedaan met producten van Cisco, Microsoft, Polycom en Vidyo.
- Een van de mogelijkheden van video over IP wordt toegepast op een fictieve netwerk infrastructuur (Demonstatie van video over IP).
- Realiseren van een sales presentatie.

2.5 Resultaat

Het resultaat van deze opdracht is een onderzoekrapport over video over IP waarin onder andere de benodigde apparatuur, netwerk designs, protocollen, netwerk impact etc. beschreven worden en wat de voor- en nadelen hiervan zijn. Dit dient bewezen te worden aan de hand van een proof of concept. Daarnaast wordt deze demonstratie ondersteunt met een presentatie die gebruikt kan worden door ADTS ICT B.V. voor de sales.

3. Achtergrond opdrachtgever

In dit hoofdstuk wordt het bedrijf en de huidige situatie omschreven.

3.1 ADTS Groep B.V.

ADTS Groep B.V. is opgericht in 1994 en is gevestigd in Capelle aan den IJsel. Dit familiebedrijf met internationale expertise bestaat uit drie divisies:

4) ADTS Consultancy B.V.
5) ADTS Projects B.V.
6) ADTS ICT B.V.

Sinds 1994 is ADTS Consultancy B.V., als zelfstandig ingenieurs- en detacheringsbureau, werkzaam in de Civiele Techniek. De specialisten van ADTS Consultancy kunnen elk moment worden ingezet bij projecten op het gebied van risico- en projectmanagement, enginering, deskundigenrapportage, nulmetingen en kwaliteitszorg. Er wordt voornamelijk aan overheden en landelijke adviesbureaus deskundigheid en expertise geleverd.

De tweede business unit van ADTS Groep B.V. is ADTS Projects B.V. Deze business unit combineert techniek en marketing tot een geïntegreerd werkend geheel. Specialisten op het gebied van R&D (research and development) en trendwatchers werken nauw samen met technici en marketeers. Onlangs hebben ze de DEi (Diesel Engine Injection) op de markt gebracht. Dit is een computergestuurd gasinjectiesysteem, dat zowel het dieselbrandstofverbruik als uitstoot van schadelijke stoffen reduceert en de werking van de dieselmotor optimaliseert.

ADTS ICT B.V. is de derde business unit van ADTS Groep B.V. Vanaf september 2007 zijn er ICT werkzaamheden aan de huidige activiteiten van de ADTS Groep toegevoegd. ADTS ICT is een gespecialiseerde leverancier van hoogwaardige ict-infrastructuurproducten en diensten. Ze richt zich volledig op connectiviteit en is op een hoog niveau gecertificeerd partner van o.a. CISCO, Microsoft, VMware en NetApp. De bedrijfsvisie is het leveren van “maatwerk” voor elke oplossing, omdat iedere aanvraag en opdracht andere eisen en wensen heeft. Data, Voice, Security en Wireless worden met elkaar geïntegreerd.

De werkzaamheden van ADTS ICT B.V. zijn:

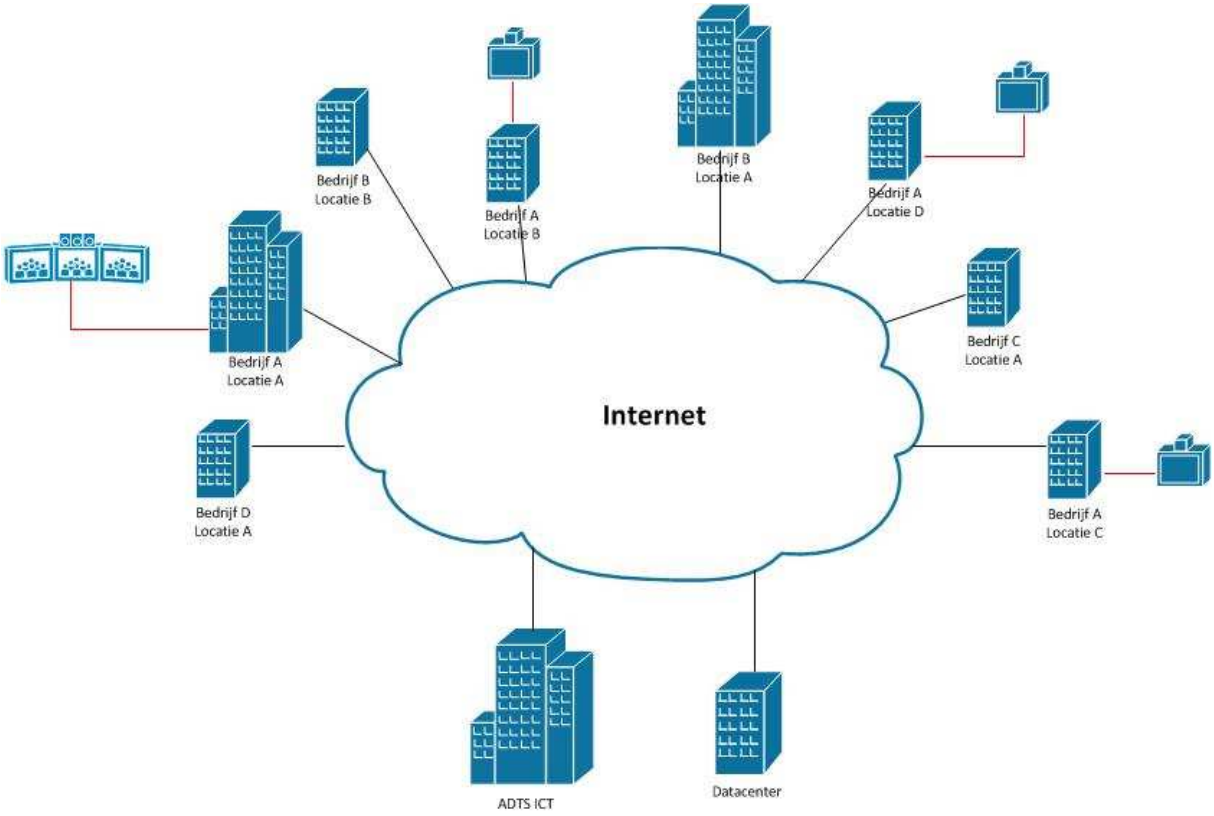
- Ontwerp van data- & voiceinfrastructuren
- Implementatie van data- & voiceinfrastructuren
- Routing & switching
- Security & Wireless
- Unified Communications
- (Remote) beheer van data- & voiceinfrastructuren
- Installatie en onderhoud servers & applicaties
- Datacenter oplossingen

3.2 Netwerk/huidige situatie

ADTS ICT B.V. richt zich op bedrijven die hun ict infrastructuur willen aanpassen op het gebied van Data, Voice, Security en Wireless. In de toekomst zal Video aan deze vier categorieën toevoegt worden. De aanpassingen kunnen in twee categorieën opgedeeld worden:

- Ontwerp en implementatie van een compleet netwerk.
- Het bestaande netwerk deels innoveren/verbeteren.

ADTS-ICT heeft verschillende klanten voor wie ze werk leveren en hebben geleverd. In de afbeelding hieronder (Figuur 1) staat een schematische weergave van het netwerk van ADTS en de samenhang met hun klanten. (De rode lijnen en achterliggende apparatuur is nog afwezig).



Figuur 15: Schematische weergave samenhang ADTS-ICT en hun klanten.

Zoals in de afbeelding te zien is heeft ADTS verschillende klanten die elk hun eigen wensen en eisen hebben. Er zijn klanten met een enkele vestiging die alleen maar een lokaal netwerk aangelegd willen krijgen, maar ook klanten met meerdere vestigingen die meer geïnteresseerd zijn in een Datacenter oplossing. Deze oplossing is niet alleen voor bedrijven die nationaal gevestigd zijn maar ook internationaal. Bedrijf A Locatie D kan zich bijvoorbeeld in China bevinden, terwijl de rest in Nederland gevestigd is. Bij deze bedrijven is er een groeiende vraag naar video over IP, voor uiteenlopende reden. Het kan hierbij gaan om een videoconferentie oplossing (zie Figuur 1), zodat de samenwerking en communicatie binnen het bedrijf bevorderd wordt, maar ook om video bewaking of e-learning.

4. Project aanpak

Tijdens dit project worden verschillende fases doorlopen om het tot een goed einde te brengen. De volgende fases worden doorlopen tijdens dit project:

- Voorbereidingsfase
- Onderzoeksfase
- Ontwerpfase
- Implementatiefase
- Testfase
- Afrondingsfase

Tijdens deze fases worden verschillende producten opgeleverd. Hieronder worden de fases nader toegelicht. Tijdens deze fases zal er ook gewerkt worden aan het afstudeerverslag.

4.1 Voorbereidingsfase

Tijdens deze fase wordt het voorbereidende werk verricht. Er wordt als eerste een plan van aanpak gerealiseerd. Hiermee kan er goed voorbereid begonnen worden aan het onderzoek. Naast het plan van aanpak zal er ook een oriënterend onderzoek plaats vinden naar video over IP.
Met de resultaten hiervan wordt een onderzoeksplan opgesteld. Deze zal dienen als leidraad voor de onderzoeksfase die daarop volgt. Naast het formuleren van de hoofd- en deelvragen, zal er ook geïnventariseerd worden wat voor hardware er aanwezig is binnen ADTS ICT B.V. voor het opstellen van een demonstratie.

4.2 Onderzoeksfase

Deze fase wordt doorlopen aan de hand van het onderzoeksplan die in de voorbereidingsfase is opgesteld. De hoofd- en deelvragen die hierin gedefinieerd zijn worden in deze fase beantwoord. Ook worden verschillende leveranciers met elkaar vergeleken. De resultaten worden verwerkt en vormen samen het onderzoeksrapport.

4.3 Ontwerpfase

Tijdens deze fase wordt er een ontwerprapport opgeleverd met daarin een fysiek en logisch ontwerp. Deze ontwerpen moeten de onderzochte informatie op de proef stellen. Zo zal er o.a. naar de netwerk impact van video over IP gekeken worden.

4.4 Implementatiefase

In deze fase wordt, er met behulp van het ontwerprapport, het netwerk voor de demonstratie opgezet. Voor het opbouwen van demonstratie wordt gebruikt gemaakt van het fysieke ontwerp. Vervolgens kan de opstelling geconfigureerd worden met behulp van het logisch ontwerp.

4.5 Testfase

Na het opbouwen en configureren van de demonstratie wordt er een testplan opgesteld, waarmee de omgeving getest kan worden. Met de resultaten van het testen wordt het testrapport opgesteld en vervolgens wordt de sales presentatie gerealiseerd.

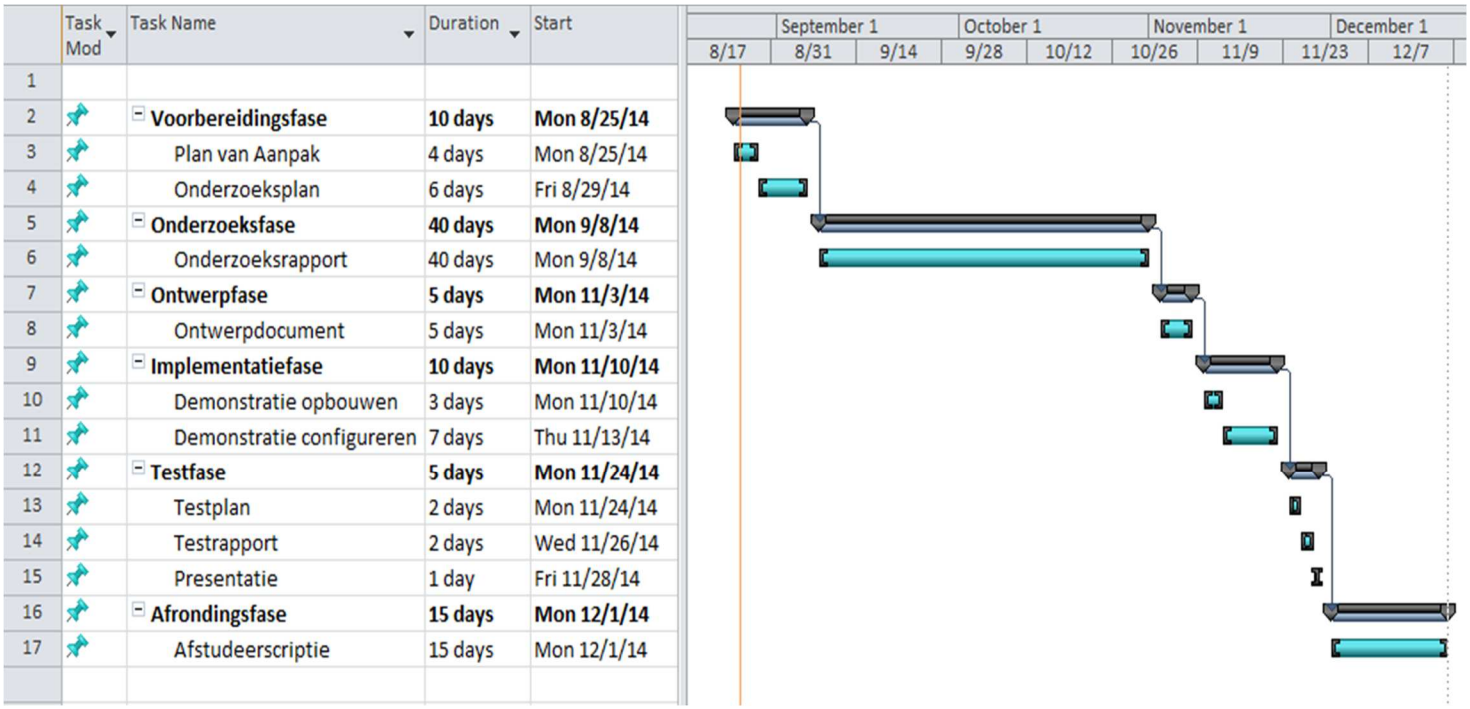
4.6 Afrondingsfase

Tot slot de afrondingsfase, waarin er gewerkt zal worden aan het afronden van het afstudeerverslag. De laatste informatie wordt hierin verwerk tot een geheel.

5. Planning

In dit hoofdstuk wordt de planning (Figuur 2) van dit project in kaart gebracht. De officiële startdatum is 25-08-2014 en de uiterlijke opleverdatum 09-01-2015. Naast deze planning zijn er ook wat extra data die niet in de planning zijn verwerkt, maar waar wel rekening mee gehouden zal worden. De exacte data zijn nog niet bekent en staan ook niet vermeld:

- 25% afspraak bedrijfsbezoek
- 45% voortgangsverslag
- 60% concept afstudeerdossier
- 80% tussentijds assessment (3 weken voor einde)



	Task Mod	Task Name	Duration	Start
1				
2		**Voorbereidingsfase**	**10 days**	**Mon 8/25/14**
3		Plan van Aanpak	4 days	Mon 8/25/14
4		Onderzoeksplan	6 days	Fri 8/29/14
5		**Onderzoeksfase**	**40 days**	**Mon 9/8/14**
6		Onderzoeksrapport	40 days	Mon 9/8/14
7		**Ontwerpfase**	**5 days**	**Mon 11/3/14**
8		Ontwerpdocument	5 days	Mon 11/3/14
9		**Implementatiefase**	**10 days**	**Mon 11/10/14**
10		Demonstratie opbouwen	3 days	Mon 11/10/14
11		Demonstratie configureren	7 days	Thu 11/13/14
12		**Testfase**	**5 days**	**Mon 11/24/14**
13		Testplan	2 days	Mon 11/24/14
14		Testrapport	2 days	Wed 11/26/14
15		Presentatie	1 day	Fri 11/28/14
16		**Afrondingsfase**	**15 days**	**Mon 12/1/14**
17		Afstudeerscriptie	15 days	Mon 12/1/14

Figuur 16: Planning.

6. Projectorganisatie

Het project wordt uitgevoerd door de stagiair, Maurice Rutenfrans. Hij zal binnen ADTS ICT B.V. door een en binnen de HHS door 2 stagebegeleiders begeleidt worden. In het onderstaande tabel (Tabel 1) zijn de contactgegevens terug te vinden.

Naam	E-mail	Telefoonnummer	Rolverdeling
Rick Hoevenaar	Rick.Hoevenaar@adts.nl	010-310-1313	Begeleider ADTS-ICT
Jan Dirk Schagen	J.D.Schagen@hhs.nl	070-445-8410	Begeleider HHS
Madelon Nieuwland	M.W.H.Nieuwland@hhs.nl	-	Examinator HHS

Tabel 2: Contactgegevens.

7. Risicoanalyse

In dit hoofdstuk worden de risico's die kunnen optreden tijdens dit project in kaart gebracht. Voor elke risico wordt er beschreven wat deze inhoud, wat de kans is, hoe deze verminderd kan worden, welke impact hij heeft, hoe deze verlaagd kan worden en tot slot een plan B.

Risico: Geen of onvoldoende hardware voor de demonstratie	
Beschrijving	Indien er geen of onvoldoende hardware aanwezig is kunnen sommige fases niet uitgevoerd worden. Dit heeft tot gevolg dat de implementatie- en testfase deels of niet doorlopen kunnen worden en de demonstratie niet uitgevoerd kan worden.
Kans	Groot, indien de benodigde apparatuur (deels) niet aanwezig is en te laat besteld/geleverd wordt.
Kans vermindering	Onderzoek snel starten, zodat het eerder duidelijk wordt of er extra hardware nodig is en op tijd besteld kan worden.
Impact	Groot.
Impact vermindering	Door een duidelijke scope te definiëren en een goede planning te maken waar het mogelijk is om bij deze fases uit te kunnen lopen.
Plan B	Als het mogelijk is gebruik maken van een remote lab van Cisco of de emulator GNS3.

Tabel 3: Risico 1: Geen of onvoldoende hardware.

Risico: Deadlines niet behalen	
Beschrijving	Er zijn verschillende redenen waardoor de deadlines niet gehaald kunnen worden. Dit kan bijvoorbeeld komen door ziekte of het verkeerd inschatten van de grootte van de opdracht.
Kans	Groot
Kans vermindering	De kans wordt verminderd door wekelijks een voortgang gesprekken te hebben met de stagebegeleider binnen ADTS ICT B.V.
Impact	Middelmatig
Impact vermindering	Achterstanden kunnen ingehaald worden buiten werkuren in de weekenden en op doordeweekse avonden.
Plan B	In overleg met de stagebegeleiders, van zowel ADTS ICT B.V. als van de HHS, de opdracht verkleinen.

Tabel 3: Risico 2: Deadlines niet behalen.

Bijlage C – Onderzoeksplan

AFSTUDEERRAPPORT

ADTS ICT B.V. - NL - Capelle aan den IJsel

Video over IP

Auteur	:	Maurice Rutenfrans
Studentnummer	:	10001468
Document	:	Onderzoeksplan
Releasedatum	:	16 sep. 14
Versie	:	1.0
Status	:	Definitief

Documenthistorie

Versie	Datum	Auteur	Commentaar
0.1	11 Sep. 14	Maurice Rutenfrans	Concept
0.1	14 Sep. 14	Maurice Rutenfrans	Controle Rick Hoevenaar
1.0	16 Sep. 14	Maurice Rutenfrans	Definitief

Distributielijst

Versie	Datum	Ontvanger	Email
0.1	11 Sep. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
1.0	16 Sep. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl

Relevante documenten

Versie	Datum	Auteur	Document
1.0	05 Sep. 14	Maurice Rutenfrans	Plan van aanpak

Voorwoord

In het kader van mijn opleiding Technische Informatica aan de Haagse Hogeschool ben ik werkzaam bij ADTS ICT B.V. Voor u ligt het onderzoeksplan dat onderdeel uitmaakt van mijn afstudeerstage, die plaats vindt van 25 augustus 2014 tot 9 januari 2015.

Dit onderzoeksplan zal opgeleverd worden aan Bernhard van der Linde, directeur van ADTS ICT B.V. Het zal ook beschikbaar zijn voor een ieder die geïnteresseerd is en daartoe bevoegd is.

Rotterdam, september 2014
Maurice Rutenfrans

Inhoudsopgave

1. Inleiding

Dit onderzoek is opgesteld voor ADTS ICT B.V. ADTS ICT B.V. is een gespecialiseerde leverancier van hoogwaardige ict-infrastructuurproducten en diensten, en willen zich ook onderscheiden op het gebied van video. Om dit onderzoek met succes af te ronden zijn er drie deelvragen met bijbehorende subvragen opgesteld. Door het beantwoorden van deze deelvragen kan uiteindelijk de hoofdvraag beantwoordt worden, die als volgt luidt:

“Hoe zet je een zo optimaal mogelijke videoconferencing over IP netwerk op voor Ampelmann Operations?”

In hoofdstuk twee wordt het theoretisch kader behandeld. Hierin wordt het onderwerp video over IP kort toegelicht. Vervolgens wordt in hoofdstuk drie en vier de reden voor dit onderzoek en de hoofd- en deelvragen beschreven. Daarna geeft hoofdstuk zes een globale planning weer en tot slot vindt in hoofdstuk zeven een inventarisatie van de hardware binnen ADTS ICT B.V. plaats.

Het onderzoek zal acht weken duren en dient op 31 oktober 2014 afgerond te zijn.

2. Theoretisch kader

Korte geschiedenis
Over de jaren heen werd eerst telefonie technologie ontwikkeld [1]. Al deze ontwikkelingen hebben het bestaan van video over IP mogelijk gemaakt. Samenvattend werd er een technologie voor telefoniebedrijven bedacht, dit was de ATM (Asynchronus Transfer Mode) [2]. Het werd gebruikt voor het verzenden van digitale spraak. Met het informatietijdperk is het belangrijk om een technologie te gebruiken die grote hoeveelheid data aan kan. ATM werkte goed, maar door de groei van computers en het internet nam IP over. Telefoniebedrijven realiserend zich dat ze veel geld konden besparen door het versturen van spraakverkeer over IP, net als al hun andere data. Hierdoor moesten televisieomroepen dezelfde keuze maken om over te stappen naar IP voor het verzenden van videoverkeer. Het gebruik nam toe ten gunste van IP waardoor ATM werd vervangen door IP.

Introductie
Video over IP [3], ook bekend als IP video en Networked Video, kan naar verschillende diensten verwijzen waarbij een videosignaal gedigitaliseerd en gecomprimeerd verzonden wordt naar zijn eindbestemming via een IP netwerk. Waar het vervolgens gedecomprimeerd, gedecodeerd en afgespeeld kan worden. Video over IP wordt voor verschillende soorten doeleinden zoals:

- Video Conference
- IP Video Surveillance
- E-Learning
- IPTV
- Video on Demand (VOD)

De mogelijkheid om video over IP netwerken te versturen brengt een enorme hoeveelheid nieuwe mogelijkheden voor zowel huishoudelijk als commerciële doeleinden met zich mee. De kwaliteit van de video is echter zeer gevoelig voor verschillende stoornissen die kunnen optreden tijdens/tussen het verzenden en ontvangen. Er zijn daarom verschillende uitdagingen voor dit tijd kritische verkeer, vergelijkbaar met die dan voice over IP zoals:

- Compressie
- Schaalbaarheid
- Foutbestendigheid
- Vertraging

Basisprincipes
Een video bestaat uit een serie beelden of frames die meestal met een snelheid tussen de 25 en 60 frames per seconden verstuurd worden, dit heet de frame rate. De resolutie wordt uitgedrukt in het aantal horizontale en verticale pixels die het scherm vormen. Hoe hoger de resolutie en frame rate, hoe groter de bitrate voor het verzenden van de video.
Sommige video systemen gebruiken “interlaced scanning” [4] om de benodigde bandbreedte te verminderen. Bij deze technologie wordt het videobeeld opgedeeld in twee “fields”. Het ene bestaat uit alle even horizontale lijnen (even scanlines), het andere uit alle oneven horizontale lijnen (odd scanlines). Om en om worden beide fields ververst, binnen een fractie van een seconde. Naast deze technologie bestaat er ook “progressive scanning”. Hierbij wordt er in tegenstelling tot interlaced scanning, het beeld in een keer getekenden waardoor de benodigde bandbreedte niet verminderd wordt.

Codec
Een codec [5] is soft- of hardware dat gebruikt wordt om het video verkeer te comprimeren en vervolgens te verzenden over het IP netwerk. Aan de ontvangende kant kan deze codec dit weer decomprimeren, zodat het afgespeeld kan worden.
Verschillende factoren kunnen de keuze van een codec beïnvloeden. Hieronder vallen onder andere kwaliteitseisen, beschikbare bandbreedte en of real-time compressie een vereiste is. Dit is belangrijk voor videoconferenties of live tv uitzending, bij van te voren opgenomen materiaal is het niet nodig dat dit real time gebeurt. Hieronder volgen een paar veel gebruikte video codec standaarden [6]:

H.261, is een ITU-T compressie standaard die ontwikkeld is voor real-time codering en versturen van video over ISDN. Deze standaard is in de meeste applicaties vervangen door H.263.

H.262, ook bekend als MPEG-2, is voornamelijk ontwikkeld voor de transport van digitale audio en video van televisie uitzendingen (kabel, satelliet en digitale televisie). Daarnaast wordt het ook gebruikt voor DVD's.

H.263, is ontworpen om dezelfde kwaliteit als H.261 te leveren, maar dan met de helft van de bitrate van H.261.

H.264, ook bekend als MPEG-4 AVC, is een groeiende standaard die ontworpen is om een hoge videokwaliteit met een lage bitrate te realiseren. H.264 gebruikt minder dan de helft van de bitrate die voor oudere standaards zoals MPEG-2 nodig is.

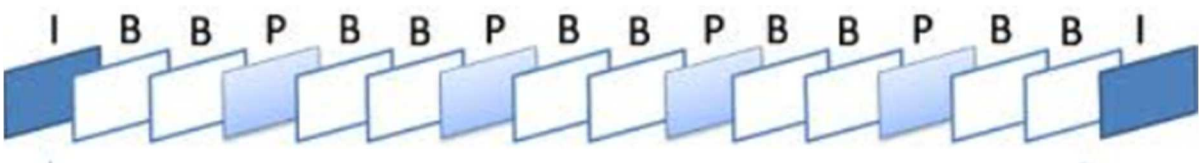
Frame types
Als een video wordt gecodeerd, worden de video frames geordend in series met een specifieke structuur en lengte (Group of Pictures of GOP) [7]. Een GOP bestaat uit een of meerdere van de volgende frame types (Figuur 1):

I-frame (intra gecodeerde frames), is een onafhankelijke gecodeerde frame. De eerste frame van een GOP is altijd een I-frame. Het zijn de grootste frames en kunnen gedecodeerd worden zonder dat hiervoor dat van een andere frame nodig is.

P-frame (voorspellend gecodeerde frames), zorgt voor meer compressie en is kleiner dan een I-frame. Om de frame te decoderen gebruikt hij data van de voorafgaande P- of I frame.

B frame (bidirectionele P-frames), zorgt voor de meeste compressie. Om te hem te decoderen gebruikt hij zowel de voorgaande als de volgende frame. B-frames worden nooit door andere frames gebruikt als referentieframe.

Naast deze gebruikt H.264 ook nog twee nieuwe frame types SI (Switching I) en SP (Switching P). Deze worden door de decoder gebruikt om tussen videostromen te schakelen doormiddel van verschillende bitrates. Elke video stroom bestaat uit achtereen volgende GOP's met een variabele structuur en lengte. De lengte van een GOP zit tussen de 15 en 250 frames.



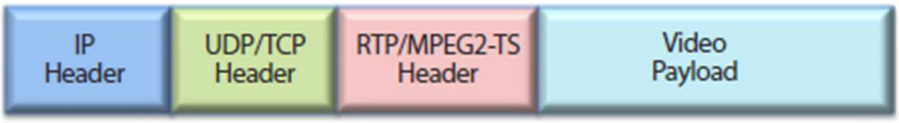
Figuur 17: Group of picture (GOP)

Video Compressie
Om de benodigde bandbreedte die nodig is voor het verzenden van videoverkeer te verminderen, worden videobeelden gecomprimeerd [8] waardoor de grote van de data kleiner wordt. Veel data binnen frames is overbodig en kan verwijderd worden zonder grote impact op de kwaliteit te hebben.
Video frames bevatten ruimtelijke redundantie, dit betekend dat aangrenzende pixels overeenkomsten met elkaar hebben binnen een frame. Ook is er tijdelijke redundantie tussen aangrenzende videoframes (gelijkenis met aangrenzende frames). Bovengenoemde codecs maken op twee manieren gebruik van deze vormen van redundantie om video te comprimeren. Dit zijn intraframecompressie om de ruimtelijke redundantie binnen frames te verminderen en interframecompressie om de tijdelijke redundantie tussen frames te verkleinen. I-frames worden gecodeerd met intraframecompressie en P- en B-frames met interframecompressie.

Intraframecompressie
Dit is dezelfde techniek die ook wordt toegepast bij het comprimeren van digitale foto's zoals JPEG. Tijdens dit proces wordt de frame opgedeeld in blokken van 8 bij 8 pixels, die allemaal door middel van een algoritmische functie gecomprimeerd worden, waardoor het aantal bits die nodig zijn verminderd wordt. De ontvangende codec voert dit proces omgekeerd uit, om de frame opnieuw op te bouwen. Bij deze techniek is de kwaliteit van de gereconstrueerde frame iets lager, maar in de meesten gevallen niet waarneembaar.
Het is mogelijk om alleen maar gebruik te maken van intraframecompressie, alleen is dit onpraktisch door de overhead en benodigde bandbreedte. Er wordt daarom vaak gebruik gemaakt van een combinatie voor minste overhead en de beste kwaliteit.

Interframecompressie
Dit is een methode om de grote van de data en bitrate nog meer te verkleinen. Vooral bij scenes waar weinig beweging is en er alleen maar kleine veranderingen van frame tot frame zijn is deze techniek effectief. In plaats van elk frame onafhankelijk te comprimeren, worden alleen de benodigde bewegingen berekend en gecomprimeerd (P-frame) van de vorige referentieframes.
Bij deze techniek kunnen fouten grote gevolgen hebben op de kwaliteit van de video, afhankelijk van het frame type die de fout bevat. Bij een I-frame is de fout in elke frame terug te vinden, terwijl een B-frame zich niet verspreid en niet opgemerkt wordt.

IP verkeer
Elk gecomprimeerde video frame wordt opgedeeld in een aantal transporteenheden [9], die elke geëncapsuleerd worden in een transportpakket (RTP of MPEG-2 Transport, of beide). Vervolgens in een UDP of TCP pakket en tot slot in een IP pakket, die verstuurd kan worden (figuur 2).



Figuur 18: IP pakket

Leveranciers
Dit onderzoek zal zich op vier leveranciers richten en die worden hieronder kort geïntroduceerd:

Cisco System, Inc.
Cisco is een bedrijf die opgericht in 1984 dat oorspronkelijk gespecialiseerd was in routers. Tegenwoordig produceert en verkoopt Cisco een grote variëteit aan netwerkapparatuur, waaronder video over IP apparatuur.

Microsoft
Microsoft is werelds grootste software bedrijf. Ze ontwikkelen, licenseren en ondersteunen een groot aantal producten die gerelateerd zijn aan computers. Microsoft heeft onder andere producten zoals Skype en Lync uitgebracht.

Polycom, Inc
Polycom is een bedrijf van Amerikaanse origine en is in 1990 opgericht. Ze zijn marktleider in op standaarden gebaseerde oplossingen voor Unified Communications & Collaboration-oplossingen (UC&C) voor spraak- en videosamenwerking.

Vidyo
Vidyo levert zowel op software gebaseerde technologie en product-gebaseerde oplossingen voor visuele communicatie. De conferencing oplossingen zijn de eerste in de videoconferencing-industrie die gebruik maken van de meeste recente verbetering van de H.264 standaard voor videocompressie, Scalable Video Coding (SVC).

Ampelmann Operations
Deze klant [10] van ADTS ICT B.V. is gespecialiseerd in het overzetten van mensen op zee. Ze regelen de overstap met een innovatief systeem, die ze zelf ontwerpen en bouwen. Het is een soort loop brug die gestabiliseerd wordt, waardoor er niks meer van de golven gemerkt wordt. De bemanningsleden kunnen hierdoor veilig overlopen naar een olieplatform of windmolen. Ampelmann opereert wereldwijd (Figuur 3) en heeft medewerkers o.a. in Brunei, Australië, Qatar etc. Doordat de werknemers van Ampelmann Operations over de hele wereld verspreid zitten en reizen veel geld en tijd kost, zijn ze geïnteresseerd in een passende video over IP oplossing.

Figuur 19: Locatie medewerkers Ampelmann Operations.

3. Reden onderzoek

Het wordt meer gebruikelijk om een collegezaal of vergaderruimte binnen te lopen, waarbij iedereen live een spreker of presentatie op een externe locatie volgt. Uit onderzoek [11] is gebleken dat video een steeds grotere rol in ons dagelijks leven gaat spelen, zowel op persoonlijk- als op zakelijk gebied. Daarnaast concludeert het onderzoek ook dat de markt voor HD video nog open ligt. Hoewel nu nog het grootste deel van video gebruikt wordt voor vermaak, nemen ook andere videodoeleinden zoals E-learning en videoconferencing toe. Het gebruik van video voor beveiliging wordt tot nu toe het minst toegepast.
Cisco voorspelt [12] dat het gebruik van video over IP over de komende jaren sterk blijft toenemen. Volgens dit onderzoek zal video 84% van al het internetverkeer voor zijn rekening nemen, dit is een toename van 6% in vier jaar tijd (2014-2018).

Deze snel groeiende techniek, die mensen beter laat communiceren, samenwerken, leren en beveiligen, staat binnen aan ADTS ICT B.V. nog in de kinderschoenen. Ook binnen deze technologie wil ADTS ICT B.V. zich onderscheiden, want beeld maakt nieuwe diensten op het gebied van samenwerking, training, simulatie en vermaak mogelijk. Daarnaast is er bij klanten een stijgende behoefte om o.a. werk en privé flexibel te kunnen combineren. Ook willen steeds meer bedrijven een bijdrage leveren aan de duurzaamheid van hun leefomgeving en op lange termijn liggen de kosten lager dan reizen.

4. Het onderzoek

4.1 Hoofdvraag

Hoe zet je een zo optimaal mogelijke videoconferencing over IP netwerk op voor Ampelmann Operations?

4.2 Deelvragen

Algemeen

4) Hoe werkt videoconferencing over IP?
    a. Wat is videoconferencing over IP en wat zijn de voor- en nadelen ervan?
    b. Welke apparatuur is er nodig voor videoconferencing over IP?
    c. Welke protocollen worden gebruikt voor videoconferencing over IP?
    d. Is er een minimale resolutie nodig?
    e. Wat is de invloed van de bandbreedte op de kwaliteit?

Implementatie

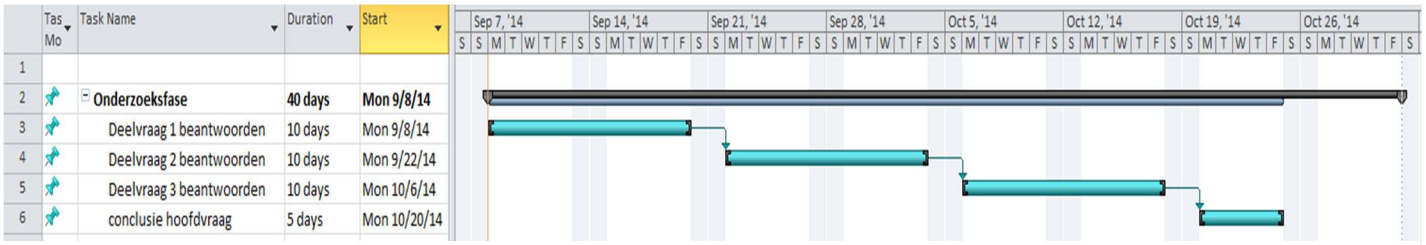
5) Wat zijn de grootste videoconferencing over IP implementatie problemen?
    a. Wat zijn de Quality of Service eisen voor video over IP?
    b. Welk netwerk architectuur kan het beste toegepast worden?
    c. Wat zijn de Multipoint bridging mogelijkheden?
    d. Wat voor impact heeft video over IP op de netwerk performance?

Veiligheid

6) Hoe veilig is video over IP?
    a. Hoe wordt de data beveiligd?
    b. Zijn extra beveiligingstechnieken zoals firewall, natting en VPN mogelijk?

5. Planning

De planning hieronder is gebaseerd op de eerder vermelde deelvragen, uit figuur 4 is te achterhalen dat de deadline van het onderzoek 31 oktober 2014 is. Tijdens het beantwoorden van de deelvragen zal er ook gewerkt worden aan het afstudeerverslag.



Figuur 20: Planning.

6. Inventarisatie hardware

Hieronder staat een lijst met hardware die aanwezig is binnen ADTS ICT B.V. en waarmee eventueel de demonstratie gerealiseerd kan worden.

Cisco 2960 Switches

De Cisco Catalyst 2960 serie [13] zijn gigabit ethernet switches (zie figuur 5), die layer 2 switching toepassen voor campus en branchapplicaties. Naast layer 2 switching ondersteunt het de volgende functies: Flexstack en Power over ethernet Plus.

Figuur 21: Cisco 2960 Switches.

Cisco 3560 Switches

De Cisco Catalyst 3560 serie [14] zijn layer 3 fast Ethernet switches (zie figuur 6). Het ondersteunt services zoals quality of service, rate limiting, access control list, Power over Ethernet en high performance IP routing.

Figuur 22: Cisco 3560 Switches.

Cisco 9971

De Cisco 9971 [15] is een IP telefoon die de gebruiker van zowel spraak als beeld, applicaties en accessoires voorziet (figuur 7).

Figuur 23: Cisco 9971 IP Phone.

Cisco EX60

De Cisco EX60 [16] transformeert de werkplek door het combineren van werk, communicatie en samenwerking (figuur 8). De EX60 is ontworpen voor medewerkers binnen een bedrijf en kan in de hele organisatie gebruikt worden, voor een snel video gesprek met een collega.

Figuur 24: Cisco EX60.

Cisco MX 300 G2

De Cisco MX 300 [17] maakt high-definition video samenwerking mogelijk voor iedereen binnen de organisatie (figuur 9). Nieuwe functies zoals dual display en een geintergreerd four-way MultiSite conferencing leveren meer kracht en flexibiteit.

Figuur 25: Cisco MX 300 G2.

Cisco 110L

Cisco 110L [18] is een LCD televisie die centraal beheerd kunnen worden via een speciaal hiervoor ontwikkeld platform (figuur 10).

Figuur 26: Cisco 110L LCD.

Cisco 4300E

De Cisco 4300E [19] is een high-definition IP camera die gebruikt maakt van H.264 compressie, 30fps en een resolutie van 1080p (figuur 11).

Figuur 27: Cisco 4300E IP Camera.

6.1 Software client

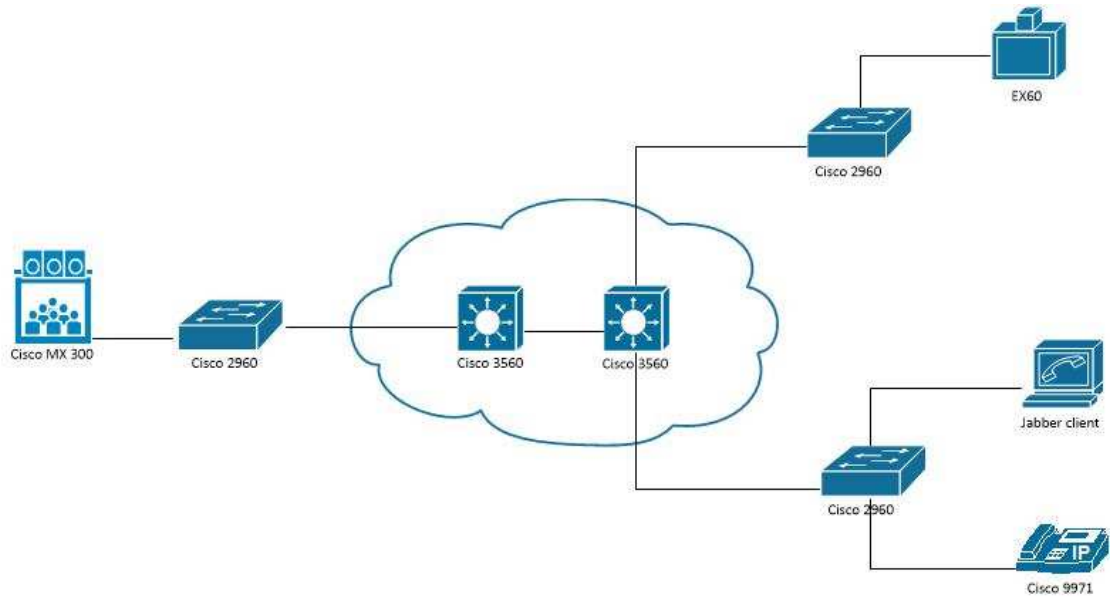
Jabber

Cisco jabber [20] is een unified communications platform met de volgende mogelijkheden: unifying presence, instant messaging, video, voice, voice messaging, screen sharing en conferencing capabilities via een client die compatibel is met verschillende hardware (figuur 12).

Figuur 28: Jabber.

6.2 Globaal ontwerp

Hier wordt uitgelegd hoe de aanwezig apparatuur eventueel voor de demonstratie gebruikt kan worden doormiddel van een globaal ontwerp (figuur 13). De Cisco 3560 layer 3 switches kunnen hierbij gebruikt worden om het internet te simuleren. Aan het “internet” zijn verschillende locaties gekoppeld, in dit voorbeeld drie. Deze worden gesimuleerd met de Cisco 2960 layer 2 switches. Op elke locatie wordt er van verschillende videoconferencing oplossingen gebruik gemaakt. In dit ontwerp zijn dit Cisco MX 300, EX60, Cisco 9971 en een PC met jabber client.



Figuur 29: Globaal ontwerp

7. Literatuurlijst

[1] A Brief History of Video Over IP; enzinearticles; bezocht op 1 september 2014
http://ezinearticles.com/?A-Brief-History-of-Video-Over-IP&id=599180

[2] Asynchronous Transfer Mode; Wikipedia; bezocht op 1 september 2014
http://nl.wikipedia.org/wiki/Asynchronous_Transfer_Mode

[3] Professional video over IP; Wikipedia; bezocht op 2 september 2014
http://en.wikipedia.org/wiki/Professional_video_over_IP

[4] Interlaced scanning; Wikipedia; bezocht op 2 september 2014
http://nl.wikipedia.org/wiki/Interlaced_scanning

[5] Codec; Wikipedia; bezocht op 3 september 2014 http://nl.wikipedia.org/wiki/Codec

[6] Video codec; Wikipedia; bezocht op 3 september 2014 http://en.wikipedia.org/wiki/Video_codec

[7] MPEG; Wikipedia; bezocht op 3 september 2014 http://nl.wikipedia.org/wiki/MPEG

[8] Intra-frame vs Inter-frame Compression; wolfcrow; bezocht op 4 september 2014
http://wolfcrow.com/blog/intra-frame-vs-inter-frame-compression/

[9] IP Video Encoding Explained; telchemy; bezocht op 4 september 2014
http://www.telchemy.com/appnotes/IP%20Video%20Encoding%20Explained.pdf

[10] Klant aan het woord, AMPELMANN; redwave; bezocht op 5 september 2014
http://www.redwave.nl/Nieuwsarchief/131400/2699248/Klant-aan-het-woord-Ampelmann.html

[11] Onderzoek Cisco: online video speelt bij 90 procent Nederlanders belangrijke rol in dagelijks leven; Cisco; bezocht op 8 september 2014
http://www.cisco.com/web/NL/news/berichten2009/news_persberichten_020909.html

[12] Visual Networking Index (VNI); Cisco; bezocht op 8 september 2014
http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~overview

[13] Cisco Catalyst 2960-S Series Switches Data Sheet; Cisco; bezocht op 9 september 2014
http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html

[14] Cisco Catalyst 3560 Series Switches Data Sheet; Cisco ; bezocht op 9 september 2014
http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-series-switches/product_data_sheet09186a00801f3d7d.html

[15] Cisco Unified IP Phone 9971 Data Sheet; Cisco ; bezocht op 9 september 2014
http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-9971/data_sheet_c78-565717.html

[16] Cisco TelePresence EX Series Data Sheet; Cisco; bezocht op 9 september 2014 http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/telepresence-system-ex-series/data_sheet_c78-627494.html

[17] Cisco TelePresence MX300 G2 and MX200 G2 Data Sheet; Cisco ; bezocht op 10 september 2014 http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/telepresence-mx-series/data-sheet-c78-729734.html

[18] Cisco Professional Series 47-inch LCD 110L; Cisco ; bezocht op 10 september 2014 http://www.cisco.com/c/en/us/products/collateral/video/professional-series-47-inch-lcd/data_sheet_c78-643770.html

[19] Cisco Video Surveillance 4500E High-Definition IP Cameras; Cisco ; bezocht op 10 september 2014 http://www.cisco.com/c/en/us/products/collateral/physical-security/video-surveillance-4000-series-ip-cameras/datasheet_c78-678041.pdf

[20] Cisco Jabber for Windows: Enterprise Collaboration Made Simple Data Sheet; Cisco ; bezocht op 10 september 2014 http://www.cisco.com/c/en/us/products/collateral/unified-communications/jabber-windows/data_sheet_c78-704195.html

Bijlage D – Onderzoeksrapport

AFSTUDEERRAPPORT

ADTS ICT B.V. - NL - Capelle aan den IJsel

Video over IP

Auteur	:	Maurice Rutenfrans
Studentnummer	:	10001468
Document	:	Onderzoekrapport
Releasedatum	:	01 dec. 14
Versie	:	1.0
Status	:	Definitief

Documenthistorie

Versie	Datum	Auteur	Commentaar
0.1	29 Okt. 14	Maurice Rutenfrans	Concept
0.2	24 Nov. 14	Maurice Rutenfrans	Concept
1.0	01 Dec. 14	Maurice Rutenfrans	Definitief

Distributielijst

Versie	Datum	Ontvanger	Email
0.1	29 Okt. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
0.2	24 Nov. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
1.0	01 Dec. 14	Rick Hoevenaar	Rick.Hoevenaar@adts.nl
		Bernhard van der Linde	Bernhard.vanderlinde@adts.nl

Relevante documenten

Versie	Datum	Auteur	Document
1.0		Maurice Rutenfrans	Plan van aanpak
1.0		Maurice Rutenfrans	Onderzoeksplan

Voorwoord

In het kader van mijn opleiding Technische Informatica aan de Haagse Hogeschool ben ik werkzaam bij ADTS ICT B.V. Voor u ligt het onderzoeksrapport dat onderdeel uitmaakt van mijn afstudeerstage, die plaats vindt van 25 augustus 2014 tot 9 januari 2015.

Dit onderzoeksrapport zal worden opgeleverd aan Bernhard van der Linde, directeur van ADTS ICT B.V. Het zal ook beschikbaar zijn voor een ieder die geïnteresseerd is en daartoe bevoegd is.

Rotterdam, oktober 2014
Maurice Rutenfrans

Inhoudsopgave

1. Inleiding

Dit onderzoek is opgezet voor ADTS ICT B.V. ADTS ICT is een gespecialiseerde leverancier van hoogwaardige ict-infrastructuurproducten en diensten. Ze willen zich onderscheiden op het gebied van Video over IP met andere ICT bedrijven. Deze techniek staat binnen ADTS ICT nog in de kinderschoenen. Dit onderzoek is primair opgezet om te achterhalen wat de beste videoconferencing oplossing is voor Ampelmann Operations. Secundair richt het zich op toekomstige klanten die ook gebruik willen maken van video over IP.

In hoofdstuk 2 is kort beschreven hoe het onderzoek is opgezet. De reden en hoofd- en deelvragen van dit onderzoek zijn hier terug te lezen.

In hoofdstuk 3 worden algemene vragen over video over IP besproken. Als eerste wordt er gekeken waarom er wel of niet voor een videoconferencing oplossing gekozen moet worden. Daarna welke hardware er nodig is en een samenvatting van wat de (van tevoren vastgelegde) leveranciers hebben. Aansluitend welke protocollen er gebruikt worden en wat deze inhouden. Vervolgens wordt de resolutie keuze en andere factoren die invloed hebben op de kwaliteit besproken. Tot slot wordt er gekeken naar de interoperabiliteit tussen leveranciers en integratie met telefonie, software, mobiel etc.

In hoofdstuk 4 worden implementatie problemen van video over IP behandeld. De QoS eisen van video over IP worden als eerst besproken. Daarna wordt er uitgelegd welke netwerk architecturen er zijn. Vervolgens wordt er dieper ingegaan op de multipoint bridging mogelijkheden. Tot slot komt de netwerkperformance aan bod.

In hoofdstuk 5 worden de veiligheidsaspecten van video over IP toegelicht. Als eerste wordt de encryptie van video over IP uitgelegd. Daarna worden de extra beveiligingstechnieken zoals firewall, natting en VPN besproken.

In hoofdstuk 6 geven we tot slot antwoord op de hoofdvraag: Hoe zet je een zo optimaal mogelijke videoconferencing over IP netwerk op voor Ampelmann Operations?

2. Het onderzoek

In dit hoofdstuk wordt kort beschreven hoe het onderzoek is opgezet. De volledige opdrachtsomschrijving is terug te lezen in het bijbehorende plan van aanpak en onderzoeksplan.

2.1 Reden onderzoek

Het wordt meer gebruikelijk om een collegezaal of vergaderruimte binnen te lopen, waarbij iedereen live een spreker of presentatie op een externe locatie volgt. Uit onderzoek [1] is gebleken dat video een steeds grotere rol in ons dagelijks leven gaat spelen, zowel op persoonlijk- als op zakelijk gebied. Daarnaast concludeert het onderzoek ook dat de markt voor HD video nog open ligt. Hoewel nu nog het grootste deel van video gebruikt wordt voor vermaak, nemen ook andere videodoeleinden zoals E-learning en videoconferencing toe. Het gebruik van video voor beveiliging wordt tot nu toe het minst toegepast.
Cisco voorspelt [2] dat het gebruik van video over IP over de komende jaren sterk blijft toenemen. Volgens dit onderzoek zal video 84% van al het internetverkeer voor zijn rekening nemen, dit is een toename van 6% in vier jaar tijd (2014-2018).

Deze snel groeiende techniek, die mensen beter laat communiceren, samenwerken, leren en beveiligen, staat binnen aan ADTS ICT B.V. nog in de kinderschoenen. Ook binnen deze technologie wil ADTS ICT B.V. zich onderscheiden, want beeld maakt nieuwe diensten op het gebied van samenwerking, training, simulatie en vermaak mogelijk. Daarnaast is er bij klanten een stijgende behoefte om o.a. werk en privé flexibel te kunnen combineren. Ook willen steeds meer bedrijven een bijdrage leveren aan de duurzaamheid van hun leefomgeving en op lange termijn liggen de kosten lager dan reizen. Zodoende is de volgende hoofdvraag geformuleerd.

2.2 Hoofd- en deelvragen

<u>Hoofdvraag</u>
Hoe zet je een zo optimaal mogelijke videoconferencing over IP netwerk op voor Ampelmann Operations?

Om een antwoord te verkrijgen op deze hoofdvraag zijn er verschillende deelvragen opgesteld. Hieronder staan de deelvragen die in chronologische volgorde beantwoordt worden.

<u>Deelvragen</u>

Algemeen

7) Hoe werkt videoconferencing over IP?
    a. Wat is videoconferencing over IP en wat zijn de voor- en nadelen ervan?
    b. Welke apparatuur is er nodig voor videoconferencing over IP?
    c. Welke protocollen worden gebruikt voor videoconferencing over IP?
    d. Hoe wordt de resolutie bepaald die nodig is?
    e. Wat is de invloed van de bandbreedte op de kwaliteit?
    f. Wat is het verschil tussen de leveranciers en zijn ze onderling compatibele?
    g. Is integratie met telefonie, computers, mobiel en software mogelijk?

Implementatie

8) Wat zijn de grootste videoconferencing over IP implementatie problemen?
    a. Wat zijn de Quality of Service eisen voor video over IP?
    b. Welk netwerk architectuur kan het beste toegepast worden?
    c. Wat zijn de Multipoint bridging mogelijkheden?
    d. Wat voor impact heeft video over IP op de netwerk performance?

Veiligheid

9) Hoe veilig is video over IP?
    a. Hoe wordt de data beveiligd?
    b. Zijn extra beveiligingstechnieken zoals firewall, natting en VPN mogelijk?

3. Algemeen

Er is niet altijd genoeg tijd en geld om elkaar persoonlijk te ontmoeten, waardoor er middelen gezocht worden om op afstand te kunnen communiceren. Dit kan onder andere doormiddel van telefoon, fax en internet alleen ontbreekt hierbij de non-verbale communicatie (expressie en emotie). Uit onderzoeken [3] is gebleken dat het non-verbale deel van de communicatie 60 tot 70% van de boodschap is en dus zeer essentieel. Videoconferencing over IP helpt naast tijd en geld winst ook bij het overbrengen van deze non-verbale communicatie.

3.1 Wat is videoconferencing over IP

Videoconferencing over IP maakt gebruik van audio- en videotelecommunicatie om personen op verschillende locaties bij elkaar te brengen voor een ontmoeting. Dit kan een ontmoeting zijn tussen twee personen die zich elk op een andere locatie bevinden (point-to-point), of een ontmoeting met meerdere personen in grote ruimten op meerdere locaties (point-to-multipoint). Naast het verzenden van audio en video kunnen er ook documenten en informatie op whiteboards gedeeld worden. Videoconferencing over IP is ook bekend als videocommunicatie, visual collaboration of net als bij spraak VoIP.
Om de data te verzenden moet deze eerst gedigitaliseerd en gecomprimeerd worden door middel van een codec. De resulterende digitale stroom van enen en nullen wordt onderverdeeld in gelabelde pakketten, die vervolgens worden verstuurd over een digitaal netwerk. Voor de overdracht van deze data kan er gebruik gemaakt worden van het IP protocol. Hierdoor is het mogelijk om te videoconference vanaf elke plek met internet.

De minimale benodigdheden voor videoconferencing over IP [4] zijn:

- Video input: Videocamera of webcam.
- Audio input: Microfoon.
- Video output: Beeldscherm, televisie of projector.
- Audio output: Luidsprekers of telefoon.
- Digitaal netwerk: LAN of internet.
- Computer: Data processing unit die alles met elkaar verbindt.

Nog niet lang geleden was videoconferencing in een redelijke resolutie met werkbaar geluid behoorlijk prijzig. Echter heeft videoconferencing over IP grote vooruitgang geboekt en is het een stuk voordeliger geworden. Er zijn verschillende voor- en nadelen die overwogen moeten worden voor het overstappen op videoconferencing over IP [3][5][6].

Voordelen:

- Tijdwinst, men hoeft minder te reizen.
- Kostenbesparing, de aanschaf van videoconferencing apparatuur is zeer prijzig, maar liggen op langer termijn lager dan de reis- en telefoonkosten.
- Snel face-to-face contact, er kan direct bijeengekomen worden indien dit nodig is, waardoor niet iedereen zich op een centrale plek hoeft te verzamelen.
- Samenwerking, het bevorderd de samenwerking binnen bedrijven.
- Gemak, in plaats van verre reizen of een vergadering in drukke schama's te plannen kan dit op elk moment van de dag gedaan worden.
- Schaalbaarheid, overal waar internet is kan het gebruikt worden en is dus eenvoudig uit te breiden.
- Milieuvriendelijk, vermindering van CO2 uitstoot door minder te reizen.

Nadelen:

- Persoonlijk contact, bij binnenkomst wordt er geen hand meer gegeven en tijdens de lunch of koffiepauze vindt er geen small talk meer plaats.
- Technische problemen, de techniek kan op kritische momenten falen door bv. Een stroomstoring bij de provider of een overbelast netwerk overbelast.
- Afhankelijkheid, de kwaliteit hangt ook af van de apparatuur (netwerk backbone) van de andere partij.
- Kosten, de kosten voor de aanschaf van goede apparatuur liggen hoog.
- Veiligheid, indien slecht geconfigureerd kan het door hackers gesaboteerd worden.

Voor de meeste bedrijven is het terugdringen van reiskosten de belangrijkste drijfveer [6]. Bij internationale bedrijven is het haalbaar gebleken om 75% van de reiskosten te besparen. Grote organisaties zien hun zakelijk reisverkeer zelden helemaal verdwijnen, omdat persoonlijk contact zeer belangrijk blijft en niet onderschat mag worden. Een directeur kan door deze techniek bijvoorbeeld zeer modern, maar ook zeer afstandelijk over komen.

3.2 Benodigde apparatuur

Zoals hierboven al aan bod is gekomen, zijn er minimaal twee locaties nodig die voorzien zijn van een camera, microfoon, internetverbinding en een computer die voor de datatransmissie zorgt. Voor het tot stand brengen van een video conference verbinding is ook software, een cloud dienst of video conferencing systeem nodig.

H.323 [7] is voorbeeld van een standaard die gebruikt wordt voor videoconferencing. Het definieert een aantal netwerkelementen die samenwerken voor het verzenden van rich multimedia communicatie. Niet alle van onderstaande elementen zijn nodig (minimaal 2 eindpunten):

Eindpunten [8][9][10]

- Personal video conferencing systems, onafhankelijk werkende apparatuur voor persoonlijk gebruik. Bijvoorbeeld een videotelefoon of een geïntegreerd systeem.
- Room-based videoconferencing systems, apparatuur geschikt voor een groep.
- Immersive videoconferencing systems, compleet systeem en omgeving. Hierbij zijn naast het systeem ook aanpassing aan de omgeving nodig voor de beste kwaliteit.

Multipoint control unit (MCU)/ Video bridge
Dit is nodig voor het tot stand brengen van een videoconference tussen meer dan twee eindpunten.

Gateway (optioneel)
Deze zorgt voor communicatie tussen H.323 netwerk en andere netwerken zoals ISDN en PSTN.

Gatekeeper
Een gatekeeper zorgt voor twee functies: adres vertaling van alias naar IP adres en bandbreedte beheer. Alle bovengenoemde componenten worden door een enkele gatekeeper beheerd en dit heet een H.323 Zone.

Omdat niet elk leverancier deze standaard hanteert wordt de benodigde apparatuur in dit hoofdstuk opgedeeld in 2 categorieën: eindpunten en platform. Hierbij zijn de eindpunten wat de gebruiker te zien krijgt (zie hierboven) en platform de achterliggende apparatuur. Om de inhoud van dit hoofdstuk te beperken zal er niet worden ingegaan op accessoires/randapparatuur.

3.2.1 Cisco

Eindelpunten [11] [12] [13] [14]

Personal

Personal - IP Phone	Kenmerken
	• 5 inch kleuren scherm. • 640 x 480/30 resolutie. • H.264/AVC compressie. • HD voice. • Ondersteund in CUCM met SCCP en SIP. • Drie varianten 8941 ($425), 8945 ($525) en 8961 $625.
Cisco IP Phone 9900 Series	• 5 of 5.6-inch kleuren scherm. • 640 x 480 resolutie. • HD voice. • SIP. • H.264/AVC compressie. • (uitgebreider dan 8900 serie) • Twee varianten: 9951 ($795) en 9971 ($995).
Cisco DX650	• 7 inch kleuren scherm. • 1920 x 1080/30 resolutie. • HD voice and video. • H.264/AVC compressie. • SIP. • Integratie met Cisco WebEx en Jabber. • $1,695

Personal - Desktop	Kenmerken
Cisco DX70 & 80	• 1920 x 1080/30 high-definition (HD) video • 14 of 23 inch scherm. • Zowel PC monitor als telepresence systeem. • H.264/AVC videocompressie. • IP-Phone die zich bij de CUCM registreert. • Responsetijd 25ms. • SIP. • Twee varianten: DX 70 ($2,750) en 80 ($3,990). • Integratie met Cisco WebEx en Jabber.
Cisco TelePresence System 500	• 32 inch schermen. • 1920 x 1080/30 high-definition (HD) video. • 12 inch besturingsinterface. • H.264 compressie. • SIP.Compatibel met CUCM, telepresence multipoint switch en telepresence Manager. • $33,900.
Cisco TelePresence EX serie	• 1920 x 1080/30 high-definition (HD) video • 21,5 of 24 inch scherm • Zowel PC monitor als telepresence systeem. • Integratie met CUCM. • 8 inch besturingsinterface. • Responsetijd 5ms. • H.323 of SIP • 2 varianten: EX60 (vanaf $8,970) en EX90 (vanaf $12,870)

Personal - Software	Kenmerken
Cisco jabber	• IM, voice, video en desktop sharing en conferencing. • Compatibel op Android, Blackberry, Iphone/Ipad, Mac en Windows platforms. • 720p • Vanaf $20 per licentie
WebEx	• Cloud-bases oplossing. • Compatibel met PCs, Macs, and iPads. • 1080p high-definition (HD) video and desktop sharing. • Tot 9 deelnemers te gelijk. • H.323 en SIP. • Vanaf $29 per licentie

Room

Room	Kenmerken
Cisco TelePresence MX200 en MX300	• 1920 x 1080/60 high-definition (HD) video. • 42 of 55 inch scherm. • 10 inch besturingsinterface. • Geen MCU nodig voor multipoint videoconferencing (tot 4 locaties). • Extra scherm voor content sharing mogelijk. • H.323 of SIP • Responsetijd 8ms. • Intergratie CUCM, VCS of Webex Telepresence. • H.264.SVC klaar. • $17,900 / $27,600.
Cisco TelePresence MX700 en MX 800	• 1920 x 1080/60 high-definition (HD) video. • 55 of 70 inch scherm. • (MX 700 heeft 2 schermen voor deelnemer + deelnemers of deelnemer + content) • 10 inch besturingsinterface. • 20x zoom • H.323/SIP • Mutipoint vereist CUCM, VCS en conductor (tot 5 locaties). • Responsetijd 8ms. • H.264 SVC and H.265 klaar • Vanaf $17,900
Cisco TelePresence System Profile Serie	• Twee varianten: 55 en 65 inch + de dualscreen optie. • 1920 x 1080/30 high-definition (HD) video. • H.323/SIP. • 5 video input/output. • CUCM support. • Multipoint met VCS en Telepresence MCU • Vanaf $35,620.
Cisco TelePresence System 1100	• 2 deelnemers (aan een kant). • 65-inch plasma scherm. • 1920 x 1080/30 high-definition (HD) video. • Multipoint met TelePresence Multipoint Switch • SIP in combinatie met CUCM. • H.264 compressie. • Meerdere variantenL 1300, 3010 en 3210 (geschikt voor

	meerdere deelnemers). • $79,000

Immersive

Immersive	Kenmerken
Cisco TelePresence TX9000 Serie	• 1920 x 1080/60 high-definition (HD) video (gelijktijdig). • 3x 65 inch schermen. • 12 inch besturingsinterface. • Integreert Cisco WebEx. • SIP. • H.264 compressie • Compatibel met CUCM, telepresence multipoint switch en telepresence Manager. • Twee varianten: TX9000 (1 rij 6 personen) en TX9200 (2 rijen 18 personen). • Vanaf $299,000
Cisco TelePresence TX1310	• 1920 x 1080/60 high-definition (HD) video (gelijktijdig) • 65-inch scherm. • 12 inch besturingsinterface. • SIP. • H.264 Compressie. • Compatibel met CUCM, telepresence multipoint switch en telepresence Manager. • 6 deelnemers (aan een kant). • $ 84,900

Platform

Platform	Kenmerken
Cisco Unified Communications Manager	• Call control platform • Video uitbreidt mogelijkheden. • Vanaf $ 13,795
Cisco TelePresence Server	• Schaalbare video conferencing bridge die samen werkt met CUCM. • Werkt ook samen met de conductor voor het bieden van een flexibele, kostenefficiënte conferentie. • Werkt samen met management suite voor conference reservering, planning en resource management. • Te verkrijgen als hardware of als applicatie om virtueel te draaien (compatibel met Cisco UCS servers). • Keuze van server hangt af van het aantal video die hij moet ondersteunen. • Vanaf $7,995.
Cisco TelePresence Conductor	• Beheer van video conferenties (toewijzen van resources aan deelnemers). • Ondersteund Telepresence server en Cisco MCU's. • Te verkrijgen als hardware of als applicatie om virtueel te draaien (compatibel met Cisco UCS servers). • Keuze hangt af van het aantal brigdes die ondersteund moeten worden. • $40,560

Cisco TelePresence Content Server	• Opnemen en delen van vergaderingen etc. • Van elke video eindpunt (H.323 en SIP). • Met de Cisco MXE 3500 erbij, kan het materiaal geedit worden. • 5 gelijktijdige opnames. • Intern en externe opslag mogelijkheden. • $43,920
Cisco TelePresence Video Communication Server (VCS)	• Schaalbaar. • any-to-any video communicatie. • SIP registrar and SIP proxy server. • H.323, H.264 SVC en SIP compatibiliteit. • Vanaf 2500 registraties en 100 gesprekken. • Vanaf $12,360
Cisco Prime Collaboration	• Management tool. • Biedt geautomatiseerde uitrol, vereenvoudigde monitoring en troubleshooting, en op lange termijn trends en analyses.
Cisco TelePresence Management Suite (TMS)	• Centraal beheer. • Volledig controle en management van multiparty conferencing, infrastructuur en eindpunten. • Ondersteund 5,000 apparaten en 100,000 gebruikers. • Integratie met Active Directory. • Vanaf $3,648

3.2.2 Vidyo

Eindpunten [15] [16]

Personal

Personal - Software	Kenmerken
VidyoDesktop	• Snelle installatie • Compatibel met bepaalde versies van Windows-, Macintosh- en Linux*-computers • Integratie met Microsoft Lync • 200 soft-client licenties • $900 voor 200 licenties
VidyoMobile	• Mogelijk op iOS of Android-gebaseerde smartphones en tablets • Eenvoudige installatie • Decoderen tot wel 720p en coderen tot en met VGA-kwaliteit • $900 voor 200 licenties

Room

Room	Kenmerken
VidyoRoom	• Levert tot 1080p/30 resolutie. • 16 deelnemers tegelijk. • Ondersteunen 1 scherm voor deelnemers en 1 een voor “shared content”. • HD-220 ($9,495, zonder schermen en speakerphone) • HD-100 ($5,894) • HD-50 ($2,250)

Immersive

Immersive	Kenmerken
VidyoPanorama	• Immersieve interactie tot wel 20 schermen tegelijk. • Resolutie van 1080p bij 60 fps. • $22,995 voor twee schermen (zonder scherm en geluid). • $5,700 extra per scherm kosten (zonder scherm).

Platform

Platform	Kenmerken
VidyoRouter	• Optimaliseert dynamisch de resolutie, bitrate en framerate. • H.264 SVC compressive. • Maakt MCU's overbodig . • Lage latency <20ms. • Elke ondersteunt 100 gelijktijdige HD connecties. • $6,000 • VidyoRouter XL ondersteunt 150 gelijktijdige HD connecties ($12,000).
VidyoRouter VE (Virtual Edition)	• Zelfde performance en mogelijkheden als VidyoRouter. • VE 25 ondersteunt 25 gelijktijdige HD connecties ($2,300). • VE 100 ondersteunt 25 gelijktijdige HD connecties ($4,625).
VidyoPortal	• Webgebaseerde videoconferentieomgeving • Gebruikers kunnen instellingen beheren. • Gecentraliseerd te beheren door IT. • Ondersteund 10,000 gebruikers (2,500 actief). • Integratie van LDAP/Active Directory. • Beheert VidyoRouter VidyoLine licenses. • Ingebouwde VidyoRouter tot 50 gebruikers • Beveiliging HTTPS, TLS, SRTP, AES 128 • $6,000
VidyoGateway	• Zorgt voor compatibiliteit met een groot aantal leveranciers waaronder Polycom en Cisco. • Ondersteund H.323- en SIP-signalering, H.264- en H.263-videocompressie, H.239-datasharing en H.235 versleutelde media • 1x HD 720p30 @ 1.5 Mbps of 4x 4CIF @ 768Kbps • $3,950
VidyoGateway MK-II (XL)	• Zelfde mogelijkheden als de VidyoGateway, met een betere performance en capaciteit. • 5x HD 720p30 @ 1.5Mbps of 15x 4CIF @ 768Kbps • $5,950
VidyoReplay	• Webcasting- en opnamesysteem dat door ieder Vidyo-eindpunt gebruikt kan worden. • Maximaal 5 HD opnames gelijktijdig. • 300 gelijktijdige streams. • 2500 uur HD video lokaal te bewaren (uitbreidt mogelijkheden met NAS) • $9,500

3.2.3 Polycom

Eindpunten [17] [18] [19]

Personal

Personal - IP Phone	Kenmerken
VVX serie	• Makkelijk te gebruiken touchscreen (7 inch) • HD voice • CIF 352x288/30 resolutie • H.323 and SIP omgeving • Twee varianten: VVX 1500 en 1500D • Tussen €600 - €900

Personal - Desktop	Kenmerken
HDX 4000 Series	• 1080p30 resolutie. • HD Content Sharing. • 5 mega pixel lens en conference phone • Twee varianten: 20 (4002) en 24 (4500) inch scherm • €6,133 en €9,199

Personal - Software	Kenmerken
RealPresence Desktop	• Compatibel met Windows en Mac. • SVC/AVC compressie • HD 720p • Ondersteund H.323 en SIP • Makkelijk uit te rollen en beheren met Active Directory • €74 per gebruiker, wordt goedkoper naarmate er meer worden afgenomen.
RealPresence Mobile	• Apple iOS en Android • SVC/AVC compressie • Singalerings protocol onafhankelijk • Makkelijk uit te rollen en beheren met Active Directory • Gratis te downloaden, maar voor de uitgebreide versie moet betaald worden.

Room

Room	Kenmerken
RealPresence Group Series	• H.264 High Profile compressie • 1080p60 resolutie. • 3 varianten: Group 300, 500 en 700 • Geïntegreerde multipoint, maximaal 8 deelnemers. • Compatibel met Microsoft Lync en Cisco TelePresence • €6,416 / €12,833 / €18,333, er zijn ook goedkopere varianten.
HDX Series	• H.264 High Profile compressie • 4 varianten: HDX 6000, 7000, 8000 en 9000 • Variant bepaalt o.a. de kwaliteit en het aantal in- en output's • €4,999 / €10,999 / €17,049 / €21,999 (zonder schermen), er zijn ook goedkopere varianten.

Immersive

Immersive	Kenmerken
RealPresence Immersive Studio	• H.264 High Profile compressie • 1080p60 resolutie. • 3x 84 inch schermen, geschikt tot 21 deelnemers. • Toegewijde beeldscherm voor “content sharing”. • Room-within-a-room ontwerp. • Startend vanaf €336,000.
Open Telepresence Experience (OTX)	• H.264 High Profile compressie • 1080p60 resolutie. • 1 of 3 65inch schermen met een maximum van 6 deelnemers. • Compatibel met Microsoft Lync en Cisco TelePresence • Omgeving uitbreiding voor maximale kwaliteit. • AES encryptie. • Startend vanaf €230,000 (voor 3 schermen).

Platform

Platform	Kenmerken
RealPresence Access Director (RPAD)	• Overal een veilige verbinding. • H.323/SIP Firewall traversal. • Ondersteunt Polycom SVC oplossingen. • Als hardware of als software (virtueel) te verkrijgen • Startend vanaf €9,999.
Video Border Proxy (VBP)	• Beveiliging van video verkeer. • H.323 Firewall traversal. • Verschillende groottes startend vanaf €1,780
RealPresence Distributed Media Application (DMA)	• Centrale managent • H.323 gatekeeper, SIP Registrar. • H.323/SIP Gateway. • MCU resource management tot 64 bridges. • Startend vanaf €7,700 voor 10 gelijktijdig gesprekken.
RealPresence Resource Manager	• Centraal punt voor beheer. • 100 tot 50,000 gebruikers. • H.323 en SIP voorziening en management. • Afhankelijk van externe gatekeeper/SIPRegistrar. • Hardware of software (virtueel) mogelijk. • Startend vanaf €11,500 met 100 licenties.
Collaboration Servers	• Software voor multiparty video, voice en content collaboration. • on-premises, hosted, hybrid of cloud. • Hardware of software (virtueel) mogelijk. • Startend vanaf €17,700
RealPresence Media Manager	• Opnemen, beheren en streamen van video's. • Van 250 tot 40,000 gebruikers. • Rechten aan te sturen via Active Directory. • Als software, virtueel of server te verkrijgen. • Startend vanaf €17,310.

3.2.4 Microsoft

Eindpunten [20]

Personal

Software	Kenmerken
Lync	• Lync wordt automatisch aangepast aan de netwerkkwaliteit. • H.264 SVC compressie. • Maximaal 5 deelnemers te gelijk. • Maakt gebruik van van SIP, TLS eb SRTP. • Te gebruiken op Windows en Mac pc's en Windows phone, iOS en android. • Lync is ook compatibel met Skype. • Om Lync te kunnen gebruiken is een Lync Server nodig, of Lync Online. • Logitech en Polycom werken samen met Microsoft Lync om een reeks van volledig geoptimaliseerd hardware aan te bieden. • Lync richt zich, in tegenstelling tot Skype, met een andere functie set op de bedrijfsomgeving.
Skype	• Te gebruiken op Windows, Mac en linux pc's en Windows, blackberry, iOS en android phone en tablet. • Gebruikt eigen protocol, waardoor het niet gehinderd wordt door firewalls. • Niet compatibel met andere leveranciers. • Gratis • Wordt vaak niet door bedrijven gebruikt: Onjuist gebruik van resources, Overmatig gebruik van bandbreedte, Beveiligingsreden.

Platfom

Platform	Kenmerken
Lync server	• On presmises • Real-time communications server software • Gebruikt SIP in combinatie met SIMPLE. • Server license ($3,646) en Client Access Licenses ($31)
Lync Online	• Microsoft-hosted • Aan te schaffen als afzonderlijke service bij Microsoft Office 365 ($6 per maand) of als onderdeel van een Office 365-pakket ($12,50 per maand)

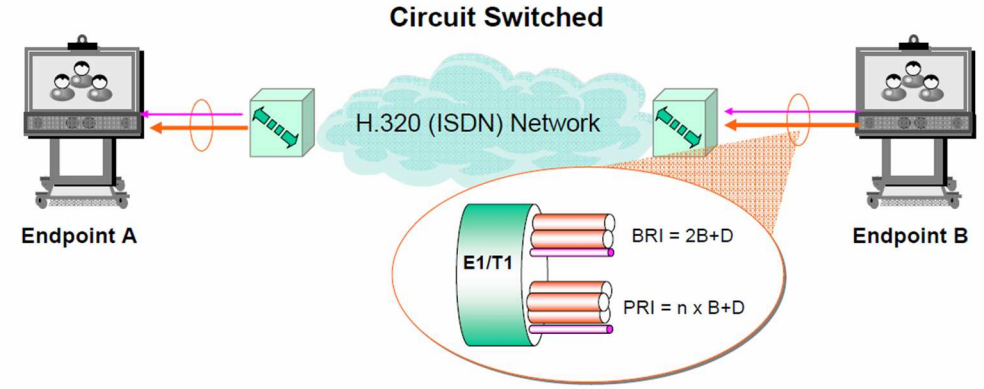
3.3 Protocollen

Er zijn verschillende standaarden waarvoor gekozen kan worden bij videoconferencing. Elke van deze standaarden schrijft een aantal protocollen voor die gebruikt worden. Hieronder volgende de drie populairste standaarden, onderverdeeld in circuit en packet switched [21]:

Circuit switched

1) H.320 definieert hoe circuit switched netwerken worden gebruikt in video communicatie (figuur 1). Het is ontwikkeld door de ITU en het meest voorkomende circuit switched netwerk

is ISDN (Integrated Switched Digital Networks). H.320 omvat signaleringsmechanismen over hoe spraak, video en andere data verstuurd wordt over een ISDN interface. Bij deze standaard wordt de bandbreedte niet gedeeld en is de hoeveelheid gegarandeerd. De data wordt op aanvraag verzonden in een bit stroom naar de ontvanger.



Figuur 30: Circuit switched netwerken.

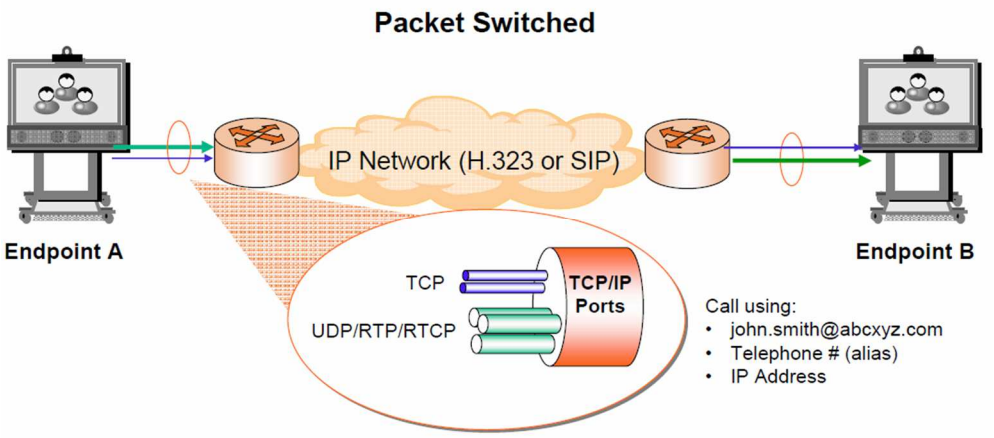
Er zijn twee mogelijkheden, Basic Rate Interface (BRI) en Primary Rate Interface (PRI). Deze bepalen het aantal kanalen die gebruikt worden, afhankelijk van de locatie. Protocollen die onder H.320 vallen zijn:

Audio: G.711, G.722, G.728, AAC-LC, AAC-LD
Video: H.264, H.263, H.261
Data: H.239
Control: H.221, H.231, H.242, H.243

Packet switched

2) H.323 [22] wordt gebruikt voor IP conferenties en maakt video over het internet mogelijk (figuur 2). Ook deze standaard is ontwikkeld door ITU. Net als bij H.320 omvat H.323 signaleringsmechanismen over hoe spraak, video verstuurd worden. Bij packet switched netwerken wordt de bandbreedte gedeeld en is de hoeveelheid niet gegarandeerd. De data wordt hierbij opgebroken in pakketten om verzonden te worden.

3) SIP (Session Initiation Protocol) [23] is een signalering protocol ontwikkeld door IETF Multiparty Multimedia Session Control working group. SIP definieert in tegenstelling tot bovengenoemde standaarden alleen de singalerings procedures, die gebruikt worden voor het opzetten, onderhouden en afbreken van een IP connectie die spraak, video en andere data bevat. SIP wordt steeds populairder, omdat het flexibeler is dan H.323. Door deze flexibiliteit zijn er geen strikte richtlijnen over welke functionaliteit een bepaald apparaat moet ondersteunen, wat compatibiliteit problemen kan veroorzaken tussen verschillende leveranciers [24].



Figuur 31: Packet switched netwerken.

Protocollen die onder H.323 en SIP vallen zijn:

Audio: G.711, G.722, G.723.1, G,726, G.728, G.729, AAC-LD
Video: H.264 High Profile, H.264, H.264 SVC, H.263, H.261
Data: H.239
Control: H.225, H.245, H.460
Transport: TCP, UDP, RTP

Audio [25]
G.711, is een ITU standaard voor het digitaliseren analoge signalen doormiddel van Puls Code Modulatie (PCM). Hierbij worden 3,1 kHz analoge spraaksignalen gedigitaliseerd in stroom van 64 Kbps. Het is een vereiste norm in vele technologieën.

G.722, digitaliseert analoge signalen door middel van een variant op PCM, genaamd Sub-Band Adaptive Differential Pulse Code Modulation (SB-ADPCM). Waarbij 7 kHz audio gecodeerd wordt in een 48, 56 of 64Kkbps stroom. Het biedt een hoge kwaliteit, maar gebruikt veel bandbreedte.

G.723.1, digitaliseert 3.4 kHz (Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s.) in een 5,3 en 6,4 Kbps stroom.

G.726, is een ITU ADPCM speech codec standaard voor de overdracht van spraak met een snelheid van 16, 24, 32, en 40 Kbps. De meest gebruikte variant is 32 Kbps, waarbij de bruikbare netwerkcapaciteit verdubbelt door het gebruiken van de helft van de bitrate van G.711.

G.728, Bij deze standaard wordt gebruik gemaakt van voorspellingen van de menselijke stem (CELP). Waarbij 3,4 kHz analoge audio wordt gecodeerd in een 16 kbps stroom. Deze standaard biedt een goede kwaliteit met een lage bitrate.

G.729, 3.4 kHz speech codec die goede kwaliteit audio codeert in een 8 Kbps stroom. Annex A is een minder complexe codec en Annex B ondersteunt stilteonderdrukking en comfort noise generation.

AAC-LD, Low Delay Advanced Audio Coding (AAC-LD) is een hoge kwaliteit met een lage vertraging audio codering standaard. Waarbij 20 kHz naloge spraaksignalen gedigitaliseerd in stroom van 128 Kbps.

Protocol	Bitrate	Vertraging	Kwaliteit
G.711	64	125 µs	Goed
G.722	48/56/64	125 µs	Goed
G.723.1	5	30 ms	Fair
G.726	16/24/32/40	125 µs	Fair
G.728	16	625 µs	Fair
G.729	8	10 ms	Fair
AAC-LD	128	20 ms	Uitstekend

Tabel 4: Vergelijkstabel, waarbij de kwaliteit is bepaalt met de Mean Option Score (MOS).

Video protocollen [22]

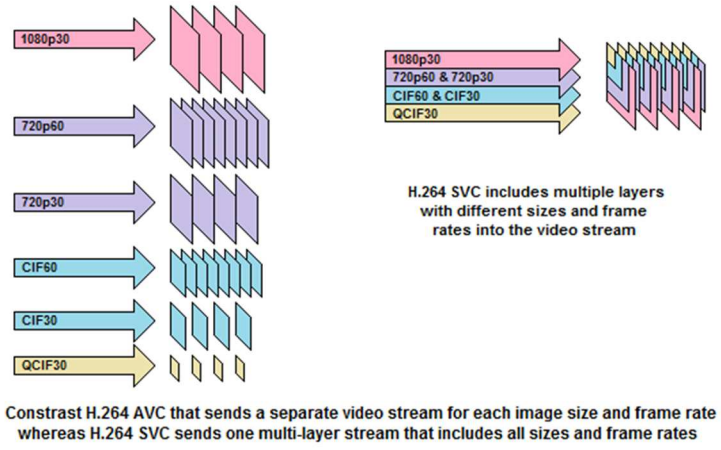
H.261, is een ITU-T compressie standaard die ontwikkeld is voor real-time codering en versturen van video (bitrate van 64Kbps). Deze standaard is in de meeste applicaties vervangen door H.263.

H.263, is ontworpen om dezelfde kwaliteit als H.261 te leveren, maar dan met de helft van de bitrate van H.261.

H.264, ook bekend als MPEG-4 AVC, is de recentste video compressie techniek die door videoconferentie systemen gebruikt wordt samen met zijn derivaten H.264 High-Profile en H.264 SVC. H.264 levert twee keer de kwaliteit ten opzichte van zijn voorganger H.263 met dezelfde hoeveelheid bandbreedte, of dezelfde kwaliteit met de helft van de bandbreedte.

H.264 High-Profile, is de krachtigste en efficiëntste compressie techniek en heeft een betere performance dan H.264.

H.264 SVC, is een opkomende compressie techniek die nog niet compatibel is tussen leveranciers. De techniek is schaalbaar en flexibeler door het netwerk, waardoor hij zeer nuttig als de hoeveelheid bandbreedte gelimiteerd is. Bij H.264 en H.264 High-Profile verstuurd elk eind punt een stroom voor elke resolutie en H.264 SVC, in tegenstelling tot de rest, een stroom met verschillende lagen die alle resoluties bevatten (figuur 3), waardoor elk eindpunt het gewenste formaat kiest zonder dat hiervoor extra codering of decodering nodig is of andere eindpunten beïnvloed worden.



Figuur 32: Verschil H.264 en H.264 SVC compressie.

Data protocollen [22]

H.239 (Dual Video) is de nieuwe standaard die ontworpen is voor de “data showing”, waar de voorkeur naar uit gaat. Deze vervangt de oude en achterhaalde T.120 “data sharing” standaard. H.239 definieert hoe extra media kanalen gebruikt en beheerd worden door videoconferencing

systemen. Het introduceert het principe van “data showing”, waarbij de PC desktop gedigitaliseerd en geconverteerd wordt en in een separate video stroom parallel wordt verzonden met het beeld van de deelnemers. Hier komt de naam Dual Video vandaan. Eindpunten die deze standaard ondersteunen geven deze twee stromen ook op aparte beeldschermen weer. Indien deze standaard niet ondersteund wordt door de eindepunten wordt het gedeelde beeldscherm weergegeven in plaats van de deelnemers.

Control protocollen [22]
H.225, is een belangrijk protocol in de VoIP architectuur gedefinieerd door ITU-T. Het beschrijft hoe audio, video, data en controle informatie beheert worden in packet based netwerken. H.225.0 bestaat uit twee grote delen: Call signaling en RAS (Registration, Admission and Status).

H.245, is een besturingsprotocol waarmee informatie die benodigd is voor multimedia communicatie kan worden getransporteerd. Het gaat hierbij om informatie over encryptie, flow control, jitter management, voorkeursinstellingen etc.

H.460, zorgt voor firewall en NAT traversal, waardoor het mogelijk is voor eindpunten om met elkaar te kunnen communiceren zonder dat daarvoor extra apparatuur voor nodig is.

Transport protocollen [22]
Het protocol die gebruikt wordt, word meestal bepaald door de behoefte aan een betrouwbare of onbetrouwbare verbinding. In het algemeen, stoppen de protocollen de gegevens in pakketten, met elke een header die de inhoud identificeert. Hieronder staan de verschillende transport protocollen die voor videoconferencing gebruikt worden:

TCP, is een betrouwbaar protocol voor het verzenden van alfanumeriek data en kan stoppen om zichzelf te corrigeren als er data verloren is gegaan. Dit protocol wordt gebruikt voor een garantie van een foutloze overdracht, wat kan leiden tot vertraging en een verlaagde verwerkingssnelheid. Dit kan vervelend zijn, vooral bij audio en video.

UDP, is een onbetrouwbaar protocol, omdat de voorkeur uitgaat naar het behouden van de stroom (flow). Hierdoor kan er data verloren gaan.

RTP, is ontwikkelt om met audio en video om te gaan en gebruikt IP multicast. Het is een afgeleide van UDP, waarbij een tijdstempel en volgnummer aan de header wordt toegevoegd. Met deze informatie kan de ontvanger de pakketten ordenen, eventuele kopieën verwijderen en het geluid synchroniseren. Real-Time Control Protocol (RTCP) wordt gebruikt om RTP te sturen.

3.4 Resolutie

De kwaliteit van een videoconferentie maakt of breekt de werkbaarheid van een video oplossing. Twee primaire factoren die de videoconferencing kwaliteit beïnvloeden zijn resolutie en framerate, en zijn direct verbonden met de hoeveelheid bandbreedte die nodig is. Het verhogen van de resolutie of framerate levert dus meer netwerkverkeer op. Hoewel compressie technieken de benodigde bandbreedte drastisch vermindert, kan dit ook maar tot een bepaalde hoogte (tabel 2) [26].

Schermgrootte	Resolutie	Framerate	Benodigde bandbreedte (H.264)	Benodigde bandbreedte (H.264 High Profile)
CIF	352 x 288	30 fps	128 kbps	64 kbps

4CIF	704x576	30 fps	256 kbps	128 kbps
HD720	1280x720	30 fps	1024 kbps	512 kbps
HD720	1280x720	60 fps	1512 kbps	832 kbps
HD1080	1920x1080	30 fps	2048 kbps	1024 kbps

Tabel 5: Resolutie en benodigde bandbreedte na compressie.

Het verschil voor en na compressie is zeer groot. Bijvoorbeeld voor High Definition HD720 met een framerate van 30fps is 664 Mbps nodig (1280 x 720 resolutie x 24 bits kleur en intensiteit x 30 framerate). Dit kan worden gecomprimeerd tot 512 kbps die verstuurd moet worden.

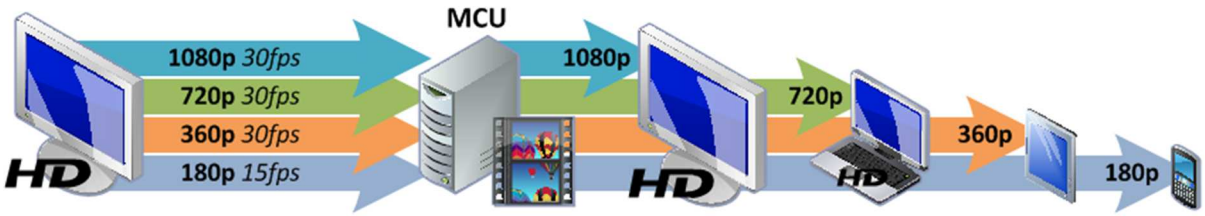
Om te bepalen welke resolutie nodig is wordt er o.a. gekeken naar het aantal pixels per gezicht [27] [28]. Een van de voordelen van videoconferencing is het zien van non verbale communicatie, waarbij gezichtsuitdrukkingen een grote rol spelen. Er moet dus genoeg resolutie zijn om gezichtsdetails te kunnen zien. De resolutie van een room-based omgeving met meerdere deelnemers is veel groter dan een persoonlijke omgeving met een persoon. Bij een persoonlijke omgeving zijn vaak alleen het hoofd en schouders in beeld, waarvan 20% of meer van het beeld door het gezicht bezet wordt. Hiermee is het aantal pixels per gezicht te berekenen. CIF heeft in dit geval 20.000 (352 x 288 x 0,20) pixels per gezicht.

In tegenstelling, bij room-based omgeving met meerdere deelnemers wordt er meer weergeven dan alleen een persoon en bezet een gezicht bv. maar 2% van het beeld. Om in deze situatie het zelfde resultaat te bereiken van 20.000 pixels per gezicht is de resolutie HD720 nodig (1280 x 720 x 0,02).

Naast de resolutie moet er ook rekening gehouden worden met de framerate [29]. Deze bepaalt hoe vaak een frame ververst wordt en hoe goed er dus wordt omgegaan met beweging. Het wordt aangeraden om minimaal 30fps aan te houden en de resolutie te verlagen indien de hoeveelheid bandbreedte gelimiteerd is. Daarnaast betekent een grotere resolutie en het gebruik van meer bandbreedte niet vanzelfsprekend een betere beeld kwaliteit (figuur 4).

Figuur 33: Grote resolutie betekend niet vanzelfsprekend een betere kwaliteit.

Ook moet er rekening worden gehouden met “content sharing”. Voor een PowerPoint met grote tekst is bijvoorbeeld een lagere resolutie nodig dan een gedetailleerde netwerk tekening. Tot slot ondersteunen apparatuur met een kleiner beeldscherm een lagere resolutie, en zien er nog steeds goed uit door hun kleine formaat (figuur 5). Daarnaast kan het menselijk oog HD1080 alleen onderscheiden als het beeld gelijk of groter is dan 70inch en op een afstand van 3 meter.



Figuur 34: Apparatuur met een kleiner scherm ondersteund een lagere resolutie.

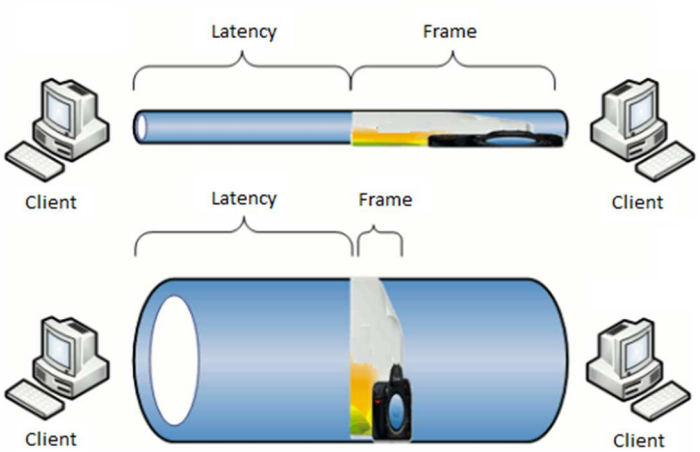
Samengevat hangt de resolutiekeuze af van de volgende aspecten:

- De omgeving en hoeveel personen tegelijk deelnemen.
- Framerate, indien de bandbreedte gelimiteerd is.
- Content sharing, waarvoor wordt het gebruikt.
- De grote van het scherm.

3.5 Kwaliteit

Zoals hierboven al aan bod is gekomen wordt de kwaliteit beïnvloed door o.a. resolutie en framerate, en deze zijn weer direct gekoppeld aan de benodigde bandbreedte. In indien er onvoldoende bandbreedte aanwezig is moeten er verschillende overwegingen gemaakt worden tussen resolutie en de framerate. De kwaliteit van de video wordt ook beïnvloed door andere factoren zoals latency en packet loss [30].

Latency [31] [32] beïnvloed de kwaliteit door eventuele netwerk vertraging, want de data moet van A naar B verzonden worden. De tijd die hiervoor nodig is wordt latency genoemd. Om bijvoorbeeld een afstand van 4000km te overbruggen met glasvezel duurt 20 milliseconden (4000km / 200000km/s). In de praktijk is deze tijd groter, omdat het door verschillende netwerk componenten verwerkt wordt en die zorgen op hun beurt voor nog meer vertraging. Er zal dus altijd een vertraging in het verzenden en ontvangen van data zitten. In dit geval maakt het verhogen van de bandbreedte niet uit, want een bit kan zich niet sneller verplaatsen. Het maakt het alleen mogelijk meer data parallel te verzenden (figuur 6).



Figuur 35: Meer bandbreedte verhelpt latency niet.

De latency kan verkleind en tot een minimum gehouden worden door een goede netwerk backbone, waardoor het verkeer geen onnodige vertraging oploopt door wachtrijen om verwerkt te worden. Dit wordt gerealiseerd door ervoor te zorgen dat een netwerk niet op zijn maximum capaciteit zit of door video verkeer een hogere prioriteit te geven.
In een live videoconference is een vertraging van minder dan 100 ms gedoogd, omdat dit kleine verschil door de meeste mensen niet wordt waargenomen. Boven de 200 ms begint de aandacht van

de deelnemers af te nemen en zullen ze na korte tijd vermoeidheid ervaren. Als de vertraging groter wordt dan 300 milliseconden, wordt het voor gebruikers vervelend om te videoconferencen en zal dit uiteindelijk resulteren in een onhandig gesprek waarbij iedereen door elkaar praat.

Naast latency hebben zelfs de best ontworpen IP netwerken een kleine hoeveelheid pakketten die verloren gaat, dit heet packet loss [33]. Het wordt veroorzaakt door botsingen van pakketten in het netwerk en het versterken van bit fouten in de onderliggende hardware. Dit wordt door veel professionele oplossing opgevangen door een foutcorrectie mechanisme, zodat de video alsnog gereconstrueerd kan worden ondanks dat er enkele pakketten verloren zijn gegaan. Het opnieuw verzenden van pakketten is bij video geen optie, door de sequentiële aard van een video signaal en zou dan veel te laat aankomen. Het effect van packet loss is een schok- en blokkerig beeld in combinatie met wegvallend geluid.

3.6 Interoperabiliteit tussen leveranciers

De beste videoconferentie systemen zijn zo goed als de mogelijkheid om met andere eindpunten te kunnen verbinden, ongeacht van welke leverancier ze afkomstig zijn. Interoperabiliteits problemen zijn dus ook niet minimaal in de ogen van een klant. Als dit niet kan of goed werkt zal het ook minder interessant worden voor bedrijven, waardoor de begroting voor een video investeringen ook minder zal worden. In het ergste geval kan dit leiden tot de overgang op consumenten producten zoals Skype.
Jaren lang was de interoperabiliteit tussen videoconferencing platformen een groot probleem, maar over de laatste jaren is dit aan het verbeteren. Interoperabiliteit tussen de leveranciers kan op twee manieren gerealiseerd worden. Door ingebouwde/standaard ondersteuning of door het gebruiken van software oplossingen, genaamd “gateways”. Dit zorgt vaak wel voor mindere kwaliteit en/of een onacceptabele latency [34][35][36][37].

Bedrijven zijn op zoek naar interoperabiliteit met een naadloze gebruikerservaring die:

- Hen instaat stelt te profiteren van nieuwe innovaties.
- Samenwerkt met (eventueel) bestaande en toekomstige investeringen.
- Extern werkt in verschillende omgevingen.

Alle leveranciers zorgen voor backward compatibiliteit, zodat hun klanten eerder aangeschafte product kunnen blijven gebruiken. Daarnaast is de interoperabiliteit tussen leveranciers verbeterd bij grote leveranciers. In het tabel hieronder is de interoperabiliteit tussen de leveranciers weergegeven (tabel 3), waarbij drie categorieën gehanteerd worden: groen (goed), oranje (matig) en rood (niet).

	Cisco	Vidyo	Polycom	Microsoft
Cisco				
Vidyo				
Polycom				
Microsoft				

Tabel 6: Interoperabiliteit tussen leveranciers.

Bij polycom zitten er voornamelijk knelpunten in verouderde systemen en codec’s die nog steeds ondersteund moeten worden en die voor problemen kunnen zorgen. Vidyo is door het gebruik H.264 SVC gelimiteerd, omdat dit nog geen standaard is en dus met derde partijen compatibiliteit problemen kan veroorzaken. Microsoft Lync wordt daarentegen door elke leveranciers ondersteunt en is bij sommige zelf geïntegreerd. Cisco doet het ook goed door het vrijgeven van hun TIP protocol die ook al door polycom gebruikt wordt en richt zich ook al op de toekomst met H.265.

3.7 Integratie met andere diensten

Naast onderlinge interoperabiliteit moet er ook gekeken worden naar de integratie met telefonie, computers, mobiel, applicaties en browsers. Om te voorkomen dat er veel en onoverzichtelijke tabellen gerealiseerd worden zal er naar de leveranciers in het algemeen gekeken worden en niet naar elk product (tabel 4). Ook hier worden drie categorieën gehanteerd: groen (goed), oranje (matig) en rood (niet) [38][39][40].

		Cisco	Vidyo	Polycom	Microsoft
Telefonie	Voice	x	-	x	x
	Voicemail	x	-	x	x
Computers (OS)	Linux	x	x	-	-
	Mac	x	x	x	x
	Windows	x	x	x	x
Mobiel (OS)	iOS	x	x	x	x
	Blackberry OS	x	-	-	-
	Microsoft Phone	x	-	-	x
	Android	x	x	x	x
Software	MS office	x	x	x	x
	Active directory	x	x	x	x
Browsers	Internet Explorer	x	x	x	x
	Chrome	x	x	x	-
	Firefox	x	x	x	x
	Safari	x	x	x	x

Tabel 7: Integratie vergelijking.

4. Implementatie problemen

Dit hoofdstuk zal zich richten op de implementatie problemen die zich voor doen bij video over IP.

4.1 QoS eisen

Real time netwerkverkeer zoals videoconferencing en VoIP zijn gevoeliger ten opzichte van ander verkeer zoals e-mail en file transfer. Quality of Service (QoS) is een netwerk term die verwijst naar de intelligentie in het netwerk om een netwerk performance te garanderen voor bepaald verkeer, zodat bv. spraak en video data voorrang krijgt en een minimale vertraging en verlies oploopt. Bij video over IP netwerken is het doel: het behouden van zowel essentiële data in het bijzijn van spraak en video, en het behouden van spraak en video kwaliteit in de aanwezigheid van onregelmatig data verkeer. Parameters die gebruikt worden voor het beschrijven van de QoS zijn de al eerder behandelde: Bandbreedte, Latency en packet loss.

Er zijn drie manieren om QoS in een netwerk in te regelen [41].

4. Provisioning, is het verzorgen van voldoende bandbreedte voor zowel spraak, video en data applicaties die van het netwerk gebruik maken. Bijvoorbeeld door gebruik te maken van een 100Mbps ethernet netwerk i.p.v. een 10Mbps. Er moet altijd rekening gehouden worden met een 20% verhoging van de bandbreedte door IP overhead.
5. Classifying (CoS), betekend het geven van een classificatie aan pakketten die gebaseerd is op hun prioriteit. Spraak pakketten krijgen de hoogste prioriteit, omdat deze het gevoeligst zijn voor vertraging. Video krijgt vaak een iets lager prioriteit en email pakketten krijgen bijvoorbeeld de laagste prioriteit.
6. Queuing, refereert naar een proces dat plaats vindt in routers en switches waarbij verschillende buffers (queues) worden vastgesteld voor de verschillende classificaties. Hiermee kan bijvoorbeeld een buffer gebruikt worden voor latency of packet loss gevoelig verkeer.

Om dit probleem voor video over IP op te lossen zijn twee fases nodig, zodat er geen bottlenecks meer aanwezig zijn. De kwaliteit is zo goed als het zwakste punt in het netwerk.

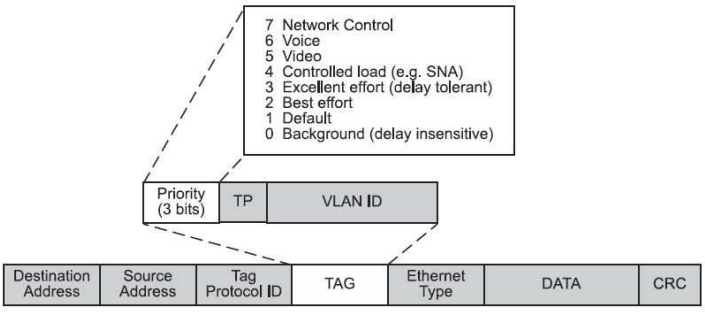
3. Garanderen van een QoS binnen een specifiek (gecontroleerd intranet) netwerk.
4. Garanderen van een QoS tussen verschillende locaties (WAN).

Er zijn vier grote QoS initiatieven [42]:

- 802.1p
- IP Precedence
- DiffServ (Differentiated Services)
- RSVP (Resource ReSerVation Protocol)

802.1p (CoS)

802.1p is een signalering techniek voor het prioriteren van netwerk verkeer op de data link laag (laag 2). De header bevat een 3 bit veld hiervoor, die ervoor zorgt dat pakketten gegroepeerd kunnen worden in verschillende klassen. Switches die dit protocol ondersteunen lezen de tag en verwerken het pakket in de bij behoorde prioriteitsbuffer. Bij deze techniek wordt er geen bandbreedte gereserveerd of opgevraagd.



Figuur 36: 802.1p TAG en prioriteitsniveaus.

Er zijn 8 prioriteitsniveaus (0-7) en dus ook 8 buffers die gemaakt kunnen worden, figuur 7. Hierbij is 7 de hoogste prioriteit en wordt toegekend aan kritische toepassingen. Niveau 6 en 5 worden gebruikt voor gevoelige applicaties zoals spraak en video. Niveau 4 en lager zijn geschikt voor dataoverdracht en videostreaming. Niveau nul wordt toegewezen aan verkeer dat alle nadelen van best-effort kan verdragen.

De switch analyseert het pakket op basis van de “P” tag en plaatst hem in de bijbehorende buffer (maximaal 8 prioriteitsbuffers). Met een aanpasbaar algoritme is te bepalen hoeveel pakketten er verzonden worden van elke buffer voordat een aantal pakketten van een lagere prioriteit verzonden worden. Een voorbeeld is 2 buffers (hoog en laag), waarvan er afwissend eerst 15 pakketten van hoog worden verstuurd en vervolgens 1 van laag.

IP Precedence

IP precedence is een laag 3 prioritering mechanisme binnen een LAN. Het IP protocol gebruikt ToS (Type of Service), een 8 bit veld bedoeld voor pakket prioritering. Drie van deze bits zijn geallokeerd om maximaal 8 prioriteitsniveaus te maken en drie om de latency en packet loss te beschrijven

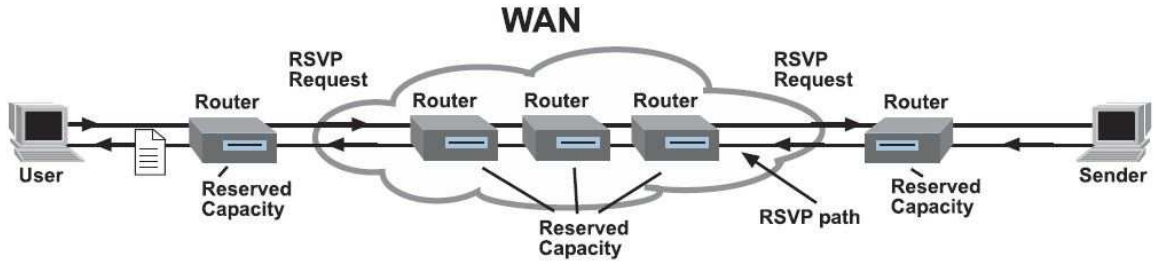
DiffServ

Ook DiffServ [43] is een laag 3 prioritering mechanisme binnen een LAN die zeer populair is. Deze schaalbare techniek wordt op de meeste nieuwe router producten en eindpunten ondersteund. Het prioriteert de verschillende verkeerstypen zoals spraak over andere type communicatie, daar het categoriseren van de IP pakketten in klassen. De zes bits van de ToS byte in de IP header van elk pakket, specificeert een bepaalt gedrag type die bepaalt de packet-forwarding regeling en de prioriteit. Differentiated services kan het volgende bieden:

- Expedited Forwarding (EF), definieert een minimum vertraging. EF houdt de hoge prioriteit buffer kort en is het meest geschikt voor spraak.
- Assured Forwarding (AF), AF 41 wordt vaak gebruikt voor video. Het wordt aangeraden om te voor zowel het beeld- als geluidpakketten van een videoconferentie in te stellen, want het biedt geen voordeel om geluid beter te behandelen.
- Best effort, gebruikt de overige bandbreedte die niet toegewezen is aan EF en AF.

Deze QoS mechanismes vormen geen onderdeel van een onderhandeling of signalering tussen apparatuur. De regels worden toegewezen door de netwerkbeheerders om de prioriteiten voor gebruiker, applicaties of diensten aan te passen. Ze zijn dus toegewezen en worden niet veranderd tijdens auto-negotiation of een andere signaleringsvorm. Dit zijn allemaal voorbeelden van Soft QoS technieken. Hard QoS beschrijft het proces waarmee netwerkapparatuur door middel van signalering kunnen onderhandelen, aanvragen en hun prioriteit kunnen aanpassen voor verschillend netwerk verkeer op basis van eerder overeengekomen waarden. Een voorbeeld van Hard QoS is RSVP.

RSVP



Figuur 37: RSVP.

RSVP (figuur 8) maakt het mogelijk voor routers en switches om de nodige/gegarandeerde bandbreedte van andere apparatuur voor specifiek verkeer op te vragen. Gewenste vertraging verschillen kunnen met dit protocol ook gedefinieerd worden. RSVP verstuurd een aanvraag om een specifieke hoeveelheid bandbreedte/ forwarding capaciteit te reserveren van andere apparatuur. Er zijn drie soorten aanvragen die verstuurd kunnen worden:

- Best-effort
- Rate-sensitive, VoIP vereist een gegarandeerde hoeveelheid bandbreedte voor video streaming applicaties.
- Delay-sensitive, VoIP vereist dat een maximale vertraging gedefinieerd wordt en dat deze niet overschreden mag worden.

Er is geen standaard voor het gebruiken van QoS, maar cisco schijft het volgende voor (tabel 5):

Traffic Type	Layer 2 CoS	Layer 3 IP Precedence	Layer 3 DSCP
Voice RTP	5	5	EF
Voice control	3	3	AF31
Video conference	4	4	AF41
Streaming video (IP/TV)	1	1	AF13
Data	0-2	0-2	0-AF23

Tabel 8: Cisco QoS voorschrift.

4.2 Netwerk architectuur

Er zijn twee netwerk architecturen, converged en de overlay, die in dit hoofdstuk nader besproken worden [44].

Converged netwerk architectuur

Een converged IP netwerk verwijst naar het aanbieden van telefonie, video en data communicatie diensten binnen een enkel netwerk. Met andere woorden, het leveren van alle vormen van communicatie diensten door een “pijp”. Deze architectuur wordt primaire gedreven door de ontwikkeling van technologie en de vraag ernaar. Een doelstelling van deze integratie is het leveren van een betere dienstverlening en lagere prijzen voor de consument. Het stelt de gebruikers in staat om uit een groter aanbod diensten en service providers te kiezen.

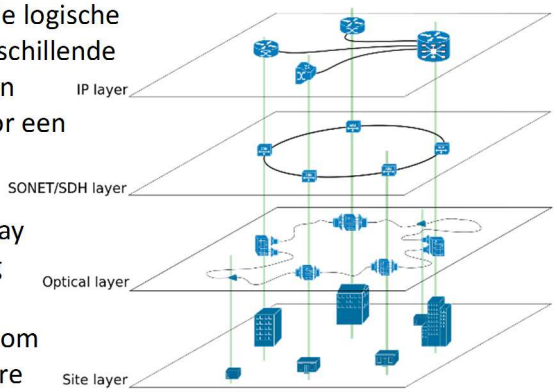
Alle gebruikers eisen een hoge quality of service, qualtiy of experience, compatibiliteit, privacy etc. Met de evolutie van deze techniek ontstaan er ook steeds nieuwe uitdagingen voor de ontwikkelaars. De grote vraag naar bandbreedte is hierbij de belangrijkste, omdat applicaties steeds geavanceerder worden en gebruikers meer en meer “rich content” data uitwisselen.
Organisaties willen niet altijd telefonie en videoverkeer laten concurreren met kritieke data applicaties, zoals productiegegevens die over het zelfde netwerk gaan. Waardoor een apparte QoS “overlay” netwerk ingezet kan worden voor spraak en video verkeer.

Overlay netwerk architectuur

Een overlay netwerk [45][46] is een computernetwerk die boven op een ander netwerk is gebouwd. Nodes in een overlay kunnen gezien worden als zijnde verbonden doormiddel van virtuele of logische verbindingen, die elk overeenkomt met een pad die mogelijk uit meerdere fysieke verbindingen bestaat in het onderliggende netwerk. Voorbeelden hiervan van zijn peer-to-peer netwerken en client-server applicaties, omdat deze nodes bovenop het internet werken. Het internet was

oorspronkelijk gebouwd als overlay op het telefonie netwerk, maar tegenwoordig is dit omgekeerd en is telefonie meer een overlay op het internet.

Overlay netwerken zijn zeer complex, omdat ze verschillende logische lagen combineren die gebruikt en beheert worden door verschillende entiteiten (bedrijven, universiteiten etc.). Hierdoor is VoIP en IPTV mogelijk geworden, want dit was niet te realiseren door een enkele provider.



Figuur 38: Overlay netwerk architectuur.

Internet is vandaag de dag de basis voor verschillende overlay Netwerken die geconstrueerd kunnen worden om routering berichten naar een eindbestemming te versturen die niet gespecificeerd is door een IP adres. Ook wordt het gebruikt om de routering te verbeteren, met QoS garanties om een betere streaming kwaliteit te realiseren. Andere QoS protocol zoals DifServ zijn nooit volledige geaccepteerd, omdat ze aanpassing op alle routers in het netwerk vereisen. Bij een overlay netwerk is er geen controle over hoe de pakketten gerouteerd worden in het onderliggende netwerk, maar het kan wel de volgorde van overlay nodes beïnvloeden die het bericht doorloopt.

4.3 Multipoint bridging mogelijkheden

Organisaties moeten overwegen of ze met meer dan twee partijen willen deelnemen in een videoconferentie. Als dit het geval is, is er een multipoint bridge nodig. Dit wordt ook wel een MCU (Multi Control Unit) genoemd. Er zijn twee mogelijkheden, de MCU kan aangeschaft en intern beheert worden of de bridging functionaliteiten kunnen worden uitbesteed aan een derde partij. Indien de MCU gekocht wordt, zal de prijs voor een videoconfencing oplossing sterk toenemen en komen er ook extra kosten voor het beheer hiervan.

MCU

Alle deelnemers bellen naar de MCU [47][48] of deze belt iedereen een voor een om aan de videoconferentie te kunnen deelnemen. Een MCU wordt gekenmerkt door het aantal gelijktijdige gesprekken dat het kan voeren en mogelijkheden zoals continuoos presence, people plus content/dual streams, transcoding en transrating.
Continuous presence is de mogelijk dat alle deelnemers tegelijk op het scherm zichtbaar zijn. Hierdoor is het bijvoorbeeld mogelijk om 10 deelnemers tegelijk weer te geven. Hieronder volgen een paar keuzes die mogelijk zijn afhankelijk van het type conferentie:


Full Screen: Bij deze optie wordt de spreker die aan het woord is getoond op elk scherm. Dit wordt automatisch bepaalt op basis van wie er spreekt.


Split Screen: Bij deze optie worden alle deelnemers die meedoen gelijktijdig weergegeven.


Dominant Speaker plus Split: Dit is een combinatie van de boven genoemde opties, waarbij de spreker in een groot scherm wordt weergegeven en de rest van de deelnemers nog steeds zichtbaar zijn.

Het is ook mogelijk om je zelf te zien tijdens de conferentie, maar vaak wordt de vertraging tussen deze en de rest van de streams als afleidend gezien.

Transcoding is een optie die communicatie tussen videoconferenties met verschillende technieken mogelijk maakt. Hierdoor kunnen systemen die gebruikmaken van H.320 communiceren met andere systemen die van H.323 gebruikmaken. Transrating maakt het mogelijk dat deelnemers video kunnen ontvangen met verschillende bandbreedte.

Derde partijen
Het outsourcen van de bridging mogelijkheden is zeer populair voor kleinere bedrijven, die niet genoeg kapitaal en kennis hebben op dit gebiedt. Het grootste voordeel hiervan is dat deze partijen voldoende capaciteiten hebben om defecte apparatuur op te vangen, waardoor de eindgebruikers er niets van merken als er iets defect is. Het nadeel is dat je afhankelijk wordt/bent van dit bedrijf en dat bij storingen het buiten bedrijven hun macht ligt.

Alternatief - gedecentraliseerd
Cisco heeft als enige leverancier ook ingebouwde mogelijkheden binnen enkele eindpunten. Dit zijn de MX200 G2 en MX300 G2 voor een videoconferentie tot vier deelnemers inclusief zichzelf en de MX700 en MX800 voor een videoconferentie tot vijf deelnemer inclusief zichzelf. Het grootste voordeel ten opzichte van de MCU is dat er geen bottleneck ontstaat. Hierdoor is de kwaliteit vaak ook beter, omdat de video data niet langs een centraal punt hoeft. Het nadeel is ook gelijk dat deze systemen altijd mee moeten doen in de videoconferentie en het niet vanaf en met elk eindpunt kan.

Vidyo maakt geen gebruik van een MCU, want deze wordt overbodig gemaakt door het gebruik van de Vidyorouter. Er moet in plaats van een MCU een Vidyorouter of Vidyoportal aangeschaft worden om de communicatie te regelen.

4.4 Netwerk performance

Zoals uit voorgaande hoofdstukken al was gebleken is er een significante hoeveelheid bandbreedte nodig en een gecontroleerd hoeveelheid latency en packet loss voor het implementeren van video conferencing. Met een slechte videoconferentie kunnen leidinggevende het vertrouwen in de nieuwe technologie verliezen, daarom is het belangrijk dat de netwerk performance optimaal is. Het is mogelijk dat klanten al een goede netwerk performance hebben waar VoIP al in gebruik is, maar dit moet niet onderschat worden want video stelt meer eisen aan het netwerk [49].

Capaciteit plannen
Video conferenties kunnen al gehouden worden vanaf 400Kbps netwerkverkeer, maar dit kan oplopen tot een hoogte van 4-6Mbps netwerkverkeer per deelnemer. Er moet dus bepaalt worden wat de optimale instellingen zijn [50][51]. Het berekenen van de benodigde bandbreedte start altijd met het inventariseren van de sites en eindpunten. Het bepalen van de resolutie en de benodigde bandbreedte (hiervoor levert elke leverancier een resolutie/bandbreedte tabel). De uiteindelijke hoeveelheid bandbreedte zal 20% hoger liggen dan dat door leverancier geleverde tabel waarden, want de IP overhead is hier nog niet bij opgeteld.

QoS
Spraak en video verkeer van video eindpunten moeten voorrang krijgen in het netwerk (overlay en converged), om de kwaliteit te behouden [50]. Een netwerkklasse moet toegewezen worden aan video en moet een hogere prioriteit hebben dat de rest van het verkeer behalve VoIP. De juiste markering voor deze klasse wordt vaak door de provider geleverd.

CAC
Als de benodigde bandbreedte voor het netwerk berekend en aanwezig is, moeten de videoconferencing applicaties ook binnen deze ontwerp beperkingen blijven. Zodra er extra systemen worden uitgerold is het mogelijk om het netwerk te overvloeden, waardoor packetloss gecreëerd wordt en dus ook een slechte kwaliteit. Daarom is er ook een call admission control (CAC) mechanisme nodig in het netwerk, zodat er geen extra conferenties kunnen plaats vinden als hiervoor geen bandbreedte beschikbaar voor is.

Multipoint bridge
Een videoconferencing bridge is een “hotspot” voor bandbreedte, omdat alle deelnemers die aan een multipoint conferentie meedoen hiermee verbinden, waardoor er veel bandbreedte nodig kan zijn. De beste plaats voor de bridge is een locatie direct gekoppeld met de WAN core. Deze locatie biedt een goedkope high-bandwith connectiviteit en maakt tegelijkertijd schaalbaarheid voor extra video conferentie systemen mogelijk.

Monitoring
Het blijft niet alleen bij het bepalen van de totale, beschikbare en gebruikte capaciteit van het netwerk, want dit laat het succes over aan toeval. Het is belangrijk om zichtbaarheid binnen het netwerk te verkrijgen. Hierdoor is te achterhalen waar eventuele problemen zich voordoen. Een Path-bases meetinstrument moet hiervoor gebruikt worden, want traditionele datanetwerk instrumenten zijn niet voldoende om het gedrag van spraak en video te monitoren. Het instrument moet 24/7 informatie kunnen verzamelen in een database. Niet elke leveranciers biedt deze mogelijkheid. Dit kan ook gedaan worden door derde partijen, een voorbeeld hiervan is Appneta’s pathview.

5. Veiligheid

Dit hoofdstuk zal zich richten op de veiligheid en veiligheidstechnieken van video over IP.

5.1 Data beveiliging

Encryptie is een omzettingsproces om informatie onleesbaar te maken voor iedereen behalve degenen die in het bezit zijn van de sleutel. Deze techniek wordt al vele jaren gebruikt binnen defensie en overheden om geheime communicatie te realiseren. Tegenwoordig wordt encryptie ook gebruikt voor de beveiliging van civiele systemen. Een toepassing is de beveiligen van de datatransport binnen bedrijfsnetwerken. Het versleutelen van de transportdata van bedrijven heeft als doel dit veilig te stellen, omdat het moeilijk is alle toegang tot netwerken fysiek te beveiligen.

Bij het toepassen van encryptie op video over IP moet er rekening worden gehouden dat dit niet ten kosten gaat van de kwaliteit [52]. Video bestaat, zelfs na compressie, uit een groot aantal bits en om deze te beveiligen moeten deze allemaal versleuteld worden. Om dit te realiseren is er veel rekenkracht nodig, waardoor de producten duurder worden. Naast het duurder worden van hardware kan dit tijd gevoelige verkeer, door het toepassen van encryptie, ook snel vertragingen oplopen, waardoor de kwaliteit van een videoconferentie sterk verminderd. Hierdoor zijn er nog veel bedrijven waar video over IP niet versleuteld wordt. Encryptie technieken die gebruikt worden in videoconferencing zijn AES, DES en Triple-DES [53][54][55].

AES

Advanced Encryption Standard (AES) is een standaard van de National Institute of Standards and Technology (NIST) sinds 2002. Deze standaard is sinds dien door verschillende regeringen waaronder die van VS in gebruik genomen om geheime gegevens veilig te versturen. Dit is de nieuwste standaard en is zeer veilig. AES bestaat uit drie sleutels die geïmplementeerd kunnen worden, de 128, 192 of 256 bits sleutel. Een eventueel nadeel is dat het niet standaard ondersteund word in VPN programma's.

DES

Data Encryption Standard (DES) is gebaseerd op een symmetrische sleutel algoritme, dat een 56-bits sleutel gebruikt. De sleutels is vervangen door de Advanced Encryption Standard (AES).

Triple-DES

Bij deze techniek wordt de Data Encryption Standard (DES) algoritme drie keer toegepast op elk gegevensblok. Triple-DES met drie onafhankelijke sleutels heeft een sleutellengte van 168 bits, maar biedt een effectieve beveiliging van een 112 bits sleutel.

Het AES algoritme wordt beschouwd als de meest geschikt vorm van encryptie voor video over IP, omdat deze de minste vertraging oploopt tijdens het versleutelen van de frames. Daarnaast is de extra overhead die het met zich meebrengt minimaal.

5.2 Extra beveiligingstechnieken

De meeste bedrijfsnetwerken maken gebruik van firewalls [56][57] en network address translation (NAT) [58][59] om te voorkomen dat hackers en onbevoegden toegang kunnen krijgen tot hun data. Spraak en video over IP gaan niet goed samen met beveiligingstechnieken zoals firewalls en natting. Bedrijven moeten dus nadenken over hoe ze veilig hiervan gebruik kunnen maken door veranderingen, herconfiguratie of geüpgrades door te voeren die dit mogelijk te maken.

Firewall

Doordat H.323 en SIP gebruik maken van veel dynamische poorten, is het niet mogelijk om deze voor te configureren in de firewalls zonder dat er veel poorten opgezet moeten worden om dit verkeer door te laten. Er zijn verschillende poorten gedefinieerd die open moeten staan om uitgaand video verkeer door te laten. Hieronder volgt een lijst met poorten die opengezet moeten worden om video over IP mogelijk te maken:

Poort	Type	Omschrijving	H.323 Client	H.323 Gatekeeper	H.323 MCU	SIP Client	SIP Registrar
80	Static TCP	HTTP Web Interface	x		x		
389	Static TCP	LDAP	x	x			x
443	Static TCP	HTTPS & Port Tunnelling	x				
1718	Static UDP	Gatekeeper Discovery	x	x			
1719	Static UDP	Gatekeeper RAS	x	x			
1720	Static TCP	H.323 Call Setup	x	x	x		
2326 - 2485	UDP	Cisco/Tandberg endpoints	x			x	
3230 - 3235	TCP	Polycom endpoints	x				
3230 - 3280	UDP	Polycom endpoints	x			x	
5001	TCP & UDP	Polycom PPCIP client	x				
5060	TCP & UDP	SIP endpoints				x	x
5061	TCP	SIP TLS				x	x
5555 - 5574	TCP	Cisco/Tandberg endpoints	x				
1024 - 65535	Dynamic TCP	H.245 (Call Parameters)	x		x		
1024 - 65535	Dynamic UDP	RTP (Video Stream Data)	x		x		
1024 - 65535	Dynamic UDP	RTP (Audio Stream Data)	x		x		
1024 - 65535	Dynamic UDP	RTCP (Control Information)	x		x		

Tabel 6: IP poorten en Protocollen die gebruikt worden bij H.323 en SIP

Door het open zetten van al deze poorten ontstaat een slechte firewall beleid, die niet door veel bedrijven geaccepteerd wordt. Daarnaast komen de inkomende gesprekken hierbij nog niet eens aan de orde.

Zowel SIP als H.323 maken gebruik van RTP voor het versturen van data. H.323 maakt daarnaast ook gebruik van de dynamic-port bases call signaleringsprotocol (H.245). Het probleem bij deze protocollen ontstaat, omdat ze allebei geen standaard laag 4 poortnummers gebruiken maar willekeurige poorten uit de 1024 tot 65534 reeks.

Het tweede probleem dat aan de orde komt is de interactieve spraak en video dat verstuurd wordt en zeer gevoelig is voor vertragingen. De oplossing voor de dynamische poorten is het gebruik maken

van een proxy. Dit is een software onderdeel van de firewall die deelneemt aan het protocol. In H.323 betekend dit dat de proxy meedoet aan het H.323 gesprek, het gesprek beëindigd op de firewall en een tweede gesprek creëert naar de eindbestemming, en tot slot koppelt hij deze twee gesprekken aan elkaar. De firewall met proxy handelt al het opzet en afbreek werk van de gesprekken af, evenals het verplaatsen van videoverkeer van alle eindpunten die voorbij de firewall proberen te praten. Ook dit brengt grote beveiliging en performance/scalability uitdagingen met zich mee voor zowel het protocol als de data die door de firewall heen gaat.

- Het ondersteunen van H.323 en SIP in de firewall maakt het ontwerp complex en kwetsbaar voor aanvallen.
- H.323 en SIP ondersteuning zorgt voor mogelijke vermindering van de performance en schaalbaarheid van de firewall.

NAT

Network Address Translation (NAT) is een methode waarbij ip adressen gemapped worden van het ene netwerk naar een ander, in een poging transparante routering aan eindpunten aan te bieden. NAT wordt gebruikt om privé adressen te koppelen aan publieke adressen. Het wordt voor twee doeleinden gebruikt.

3. Als mechanisme om de IPv4 uitputting tegen te gaan.
4. Voor beveilingsdoeleinden (zodat eindpunten verborgen blijven).

Bij NAT, vaak geïmplanteerd als onderdeel van de firewall, wordt het IP adres in header van de pakketten die daar doorheen gaan getransleerd naar een ander adres. Tegelijk wordt er een NAT tabel bijgehouden waarin de zogeheten mappings tussen IP adressen en poortnummers zijn terug te vinden.

Bij H.323 wordt het probleem veroorzaakt door H.225 en H.245, omdat die gebruik maken van embedded ip adressen. Als NAT wordt gebruikt, bevat de data private adressen in plaats van een publieke adres. Bijvoorbeeld een eindpunt (172.16.1.1), wordt vertaald door NAT naar 205.204.203.202. Als dit eindpunt probeert de verbinden met een ander eindpunt zal het verkeerde ip adres worden doorgegeven via H.225. De poging om met elkaar te verbinden met dit adres die niet gerouteerd kan worden zal dus mislukken.

Omdat SIP singalerings berichten ip adressen in het data segment van het IP pakket voegen, zal NAT ook SIP opbreken, behalve als ze “SIP aware” zijn gemaakt. Het probleem bij SIP is vaak dat de herkomst en eindbestemming van het bericht niet een directe relatie met de herkomst en eindbestemming van de video heeft.

6. Conclusie

Indien er gebruik wordt gemaakt van Office 365 is Microsoft Link een goede oplossing voor onderlinge videoconferenties. Microsoft Link zit standaard in Office 365 en steeds meer bedrijven maken hier gebruik van, omdat dit maandelijks afgenomen kan worden en de licenties niet in een keer volledig betaald hoeven worden. Veel klanten van aan ADTS ICT gebruiken nog geen Office 365 in plaats daarvan maken ze gebruik van Cisco jabber voor onderlinge videoconferenties.

Voor een zakelijk en professionele video oplossing biedt Cisco de meeste mogelijkheden. Naast het feit dat deze het beste integreert met telefonie, computers, mobiel, applicaties en browsers. Zijn de meesten klanten al in het bezit van een Cisco Unified Communications Manager (CUCM), waardoor deze niet apart aangeschaft hoeft te worden en aanzienlijk in prijs scheelt.

Het protocol die hierbij het beste gebruikt kan worden is SIP in plaats van H.323. SIP heeft als voordeel dat het flexibeler is dan H.323, waardoor het steeds populairder wordt. Ondanks dat deze flexibiliteit ook wat nadelen met zich mee brengt zal het meer mogelijkheden bieden in de toekomst.

De grootste kosten zitten in multipoint bridging. Doordat ADTS ICT deze optie niet door derde partijen wil laten beheren wordt de keuze aanzienlijk minder. Indien klanten hier niet in een keer veel geld in willen investeren is het een optie om deze dienst zelf volledig aan te schaffen en voor een maandelijkse bedrag aan te bieden aan klanten (net zoals office 365).

Tot slot zijn er veel afwegingen die gemaakt moeten worden om de kwaliteit te bepalen en te waarborgen. Hierbij kunnen we concluderen dat deze per situatie verschillend is, omdat er veel variabelen zijn waarmee rekening mee gehouden moet worden zoals: resolutie, framerate, bandbreedte, deelnemers etc.

7. Afkortingenlijst

Afkorting	Betekenis(sen)
IP	Internet Protocol
HD	High Definition
VoIP	Voice over Internet Protocol / Video over Internet Protocol
MCU	Multipoint control unit
ISDN	Integrated Switched Digital Networks
PSTN	Public switched telephone network
SIP	Session Initiation Protocol
ITU	International Telecommunication Union
IETF	Internet Engineering Task Force
Mbps	Megabit per seconde
Kbps	Kilobit per seconde
QoS	Quality of Service
CoS	Class over Service
RSVP	Resource ReSerVation Protocol
DiffServ	Differentiated Services
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
EF	Expedited Forwarding
AF	Assured Forwarding
CAC	Call Admission Control
WAN	Wide Area Network
NAT	Network Address Translation
VPN	Virtual Private Network
AES	Advanced Encryption Standard
DES	Data Encryption Standard
Triple-DES	Triple- Data Encryption Standard
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
RTP	Real-Time Transport Protocol
RTCP	Real-Time Control Protocol

8. Literatuurlijst

[1] Onderzoek Cisco: online video speelt bij 90 procent Nederlanders belangrijke rol in dagelijks leven; Cisco; bezocht op 8 september 2014
http://www.cisco.com/web/NL/news/berichten2009/news_persberichten_020909.html

[2] Visual Networking Index (VNI); Cisco; bezocht op 8 september 2014
http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~overview

[3] MKB Videoconferencing AV; ictloket; bezocht op 17 september 2014
http://www.ictloket.nl/kennisbank/mkb-videoconferencing-av/

[4] Videoconferencing; Wikipedia; bezocht op 17 september 2014
http://en.wikipedia.org/wiki/Videoconferencing

[5] Video Conferencing Frequently Asked Questions; onevideoconferencing; bezocht op 18 september 2014 http://www.onevideoconferencing.com/video-conferencing-faq.html

[6] Voordelen van videoconferencing; conferencing4all; bezocht op 18 september 2014
http://www.conferencing4all.nl/videoconferencing_voordelen.html

[7] Video Conferencing; uiowa; bezocht op 22 september 2014
http://its.uiowa.edu/support/article/100451

[8] Types of Video Conferencing Systems; voipsupply; bezocht op 22 september 2014
http://www.voipsupply.com/types-of-video-conferencing-systems

[9] Wat kost video conferencing?; clickon; bezocht op 22 september 2014
http://videoconference.clickon.nl/video-conferencing-solutions/video-conferencing-kenniscentrum/wat-kost-video-conferencing

[10] A closer look at video conferencing solutions, technology and vendors; techtarget; bezocht op 23 september 2014 http://searchunifiedcommunications.techtarget.com/feature/A-closer-look-at-video-conferencing-solutions-technology-and-vendors

[11] Collaboration Endpoints; Cisco; bezocht op 23 september 2014
http://www.cisco.com/c/en/us/products/collaboration-endpoints/index.html

[12] Conferencing; Cisco; bezocht op 24
http://www.cisco.com/c/en/us/products/conferencing/index.html

[13] Cisco TelePresence Product Catalog; zebrac; bezocht op 25 september 2014
http://www.zebrac.com/zebra/common/PreviewDocument.ashx?itemId=1053&refItemId=T470DOCUMENTS&refTableId=470&language=EN

[14] Video conferencing equipment price list; Cisco; bezocht op 26 september 2014 http://cisco-images.test.edgekey.net/web/strategy/government/mississippi/docs/video_conf_equip_price_list.pdf

[15] Producten; Vidyo; bezocht op 27 september 2014 http://nl.vidyo.com/

[16] Endpoint & peripherals; onevisionsolutions; bezocht op 29 september 2014 http://www.onevisionsolutions.com/dir/Vidyo_MSRP_Price_List.pdf

[17] ; Polycom; bezocht op 3 oktober 2014 http://www.polycom.nl/

[18] HD Video Conferencing & Telepresence Systems; Polycom; bezocht op 4 oktober 2014 http://www.polycom.co.uk/products-services/hd-telepresence-video-conferencing.html

[19] Polycom Video Price List; exertisgoconnect; bezocht op 6 oktober 2014 http://www.exertisgoconnect.nl/products/images/files/pricelist_polycom.pdf

[20] Microsoft Lync; Wikipedia; bezocht op 10 oktober 2014 http://en.wikipedia.org/wiki/Microsoft_Lync

[21] Video Conferencing Protocols; Wordpress; bezocht op 12 oktober 2014 http://thetechnicianpartition.files.wordpress.com/2010/04/6-video-conferencing-protocols.pdf

[22] What you really need to know about Video Conferencing Systems; c21video; bezocht op 13 oktober 2014 http://www.c21video.com/video.html

[23] SIP video conferencing systems: A standardized approach to integration; techtarget; bezocht op 13 oktober 2014 http://searchunifiedcommunications.techtarget.com/feature/SIP-video-conferencing-systems-A-standardized-approach-to-integration

[24] H.323 versus SIP: A Comparison; Packetizer; bezocht op 14 oktober 2014 http://www.packetizer.com/ipmc/h323_vs_sip/

[25] What is a codec; Askozia; bezocht op 14 oktober 2014 https://askozia.com/voip/what-is-a-codec/

[26] What you really need to know about Video Conferencing Systems; c21video; bezocht op 17 oktober 2014 http://www.c21video.com/video.html

[27] How Much Video Conferencing Resolution Do I Need?; nojitter; bezocht op 18 oktober 2014 http://www.nojitter.com/post/225401849/how-much-video-conferencing-resolution-do-i-need

[28] Video conferencing quality vs. bandwidth tradeoffs; techtarget; bezocht op 18 oktober 2014 http://searchunifiedcommunications.techtarget.com/tip/Video-conferencing-quality-vs-bandwidth-tradeoffs

[29] Telepresence vs HD Video Conferencing - Choosing Optimal Resolution and Frame Rate; Youtube; bezocht op 19 oktober 2014 http://www.youtube.com/watch?v=BeXT_1nuwis

[30] Quality of Service Design Overview; Ciscopress; bezocht op 20 oktober 2014 http://www.ciscopress.com/articles/article.asp?p=357102&seqNum=2

[31] Bandwidth, Latency, and the “Size of your Pipe”; Zoompf; bezocht op 21 oktober 2014 http://zoompf.com/blog/2011/12/i-dont-care-how-big-yours-is

[32] Is your network ready to handle videoconferencing; Techrepublic; bezocht op 24 oktober 2014 http://www.techrepublic.com/blog/data-center/is-your-network-ready-to-handle-videoconferencing/

[33] Professional video over IP; Wikipedia; bezocht op 24 oktober 2014 http://en.wikipedia.org/wiki/Professional_video_over_IP

[34] Stalking Videoconferencing Interoperability; Infocomm; bezocht op 25 oktober 2014 http://www.infocomm.org/cps/rde/xchg/infocomm/hs.xsl/36278.htm

[35] Video conferencing standaards and interoperability considerations; techtarget; bezocht op 25 oktober 2014 http://searchunifiedcommunications.techtarget.com/feature/Video-conferencing-standards-and-interoperability-considerations

[36] Video Interoperability in Lync 2013; Schertz; bezocht op 26 oktober 2014 http://blog.schertz.name/2012/07/video-interoperability-in-lync-2013/

[37] A Conference Gateway Supporting Interoperability
Between SIP and H.323; cmu; bezocht op 26 oktober 2014 https://www.cs.cmu.edu/afs/cs/project/cmcl/archive/Libra-papers/01mm.pdf

[38] Microsoft Lync; clickon; bezocht op 27 oktober 2014 http://videoconference.clickon.nl/video-conferencing-solutions/microsoft-lync-video-conferencing

[39] Comparison of web conferencing software; Wikipedia; bezocht op 28 oktober 2014 http://en.wikipedia.org/wiki/Comparison_of_web_conferencing_software

[40] Enterprise Voice in Lync Server 2013; miscosoft; bezocht op 28 oktober 2014 http://technet.microsoft.com/en-us/library/gg417163.aspx

[41] Frequently Asked Questions About Voice and Video over IP Networks; Wainhouse; bezocht op 3 november 2014 http://www.wainhouse.com/files/papers/wr-faq-ip-conf.pdf

[42] Quality of Service (QoS) in High-Priority Applications; Transition; bezocht op 3 november 2014 http://www.transition.com/TransitionNetworks/Uploads/Literature/qos_wp.pdf

[43] Quality of Service (QoS): A Good Traffic Engineering Component; Manageengine; bezocht op 4 november 2014 https://blogs.manageengine.com/network/netflowanalyzer/2013/12/04/quality-of-service-qos-a-good-traffic-engineering-component-2.html

[44] Frequently Asked Questions About Voice and Video over IP Networks; Wainhouse; bezocht op 5 november 2014 http://www.wainhouse.com/files/papers/wr-faq-ip-conf.pdf

[45] Overlay network; Wikipedia; bezocht op 5 november 2014 http://en.wikipedia.org/wiki/Overlay_network

[46] Voice an Video conferencing Fundamentals; Bookzz; bezocht op 6 november 2014 http://dlx.bookzz.org/genesis/55000/fe05147ffe6a14b6ad5d83209c51a849/_as/[Scott_Firestone,_Thiya_Ramalingam,_Steve_Fry]_Voi(BookZZ.org).pdf

[47] What is a video conferencing bridge?; uiowa; bezocht op 7 november 2014 http://its.uiowa.edu/support/article/100451

[48] Multipoint Video Conferencing (Bridge); udel; bezocht op 8 november 2014 http://ats.udel.edu/conferencing/multipoint.php

[49] WAN video conferencing network design requirements for QoS; Techtarget; bezocht op 10 november 2014 http://searchenterprisewan.techtarget.com/tip/WAN-video-conferencing-network-design-requirements-for-QoS

[50] Video conferencing bandwidth requirements for the WAN; Techtarget; bezocht op 11 november 2014 http://searchenterprisewan.techtarget.com/tip/Video-conferencing-bandwidth-requirements-for-the-WAN

[51] Preparing Your IP Network for Video Conferencing; Entouchcom; bezocht op 11 november 2014 http://www.entouchcom.com/files/46943425.pdf

[52] The importance of encrypting video over IP; Cardinalpeak; bezocht op 13 november 2014 http://www.cardinalpeak.com/blog/the-importance-of-encrypting-video-over-ip/

[53] Video Conferencing and Security; starnetdata; bezocht op 13 november 2014 http://www.starnetdata.com/wp-content/uploads/2010/01/LifeSizeSecurity_WhitePaper_en.pdf

[54] Encryption, IP security (IPsec) and VPNs; Ja; bezocht op 13 november 2014 https://community.ja.net/library/janet-services-documentation/encryption-ip-security-ipsec-and-vpns

[55] AES Key Exchange under H.235; Polycom; bezocht op 13 november 2014 http://support.polycom.com/global/documents/support/user/products/network/AES_Key_Exchange.pdf

[56] Firewall; c21video; bezocht op 17 november 2014 http://www.c21video.com/firewall.html

[57] What is a firewall? How does it affect H.323 video conferencing?; uiowa; bezocht op 17 november 2014 http://its.uiowa.edu/support/article/100451

[58] Why do firewalls cause problems with H.323 and SIP; Wainhouse; bezocht op 18 november 2014 http://www.wainhouse.com/files/papers/wr-faq-ip-conf.pdf

[59] Virtualization, Isolation and Encryption of IP Video Surveillance; Cisco; bezocht op 18 november 2014http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/IPVS/ip_video_surv/ipvs_virtual.html

Bijlage E – Business case

Businesscase – Ampelmann Operations

Ampelmann Operations is een klant van ADTS ICT B.V. en is gespecialiseerd in het overzetten van mensen op zee. Ze regelen de overstap met een innovatief systeem, die ze zelf ontwerpen en bouwen. Het is een soort loop brug die gestabiliseerd wordt, waardoor er niks meer van de golven gemerkt wordt. De bemanningsleden kunnen hierdoor veilig overlopen naar bijvoorbeeld een olieplatform of windmolen.

Situatie schets
Ampelmann Operations is gevestigd in Nederland. Het hoofdkantoor bevindt zich in Delft en de productie vindt plaats in Rotterdam. Daarnaast opereren ze wereldwijd (Figuur 1) en hebben ze medewerkers o.a. in Brunei, Singapore, Qatar etc. Doordat de werknemers van Ampelmann Operations over de hele wereld verspreid zitten en reizen veel geld en tijd kost, zijn ze opzoek naar een passende video over IP oplossing.

Figuur 39: Locatie medewerkers Ampelmann Operations.

Ampelmann Operations is om twee redenen opzoek naar een video oplossing. De eerste is voor het voeren van *sollicitatiegesprekking in het buitenland*. Op dit moment wordt dit gedaan met Skype, maar dit is geen zakelijke en professionele oplossing voor Ampelmann Operations. Dit komt mede door de slechte kwaliteit van zowel spraak als video.

De tweede reden is het verbeteren van de "*maandagochtend meeting*", zodat er vanaf meerdere locaties aan deelgenomen kan worden. Momenteel is de beste oplossing om op locatie, in Delft, te zijn waar de meeting plaats vindt. Met Skype is het mogelijk om de meeting in Rotterdam te volgen, maar veel informatie komt niet over omdat de kwaliteit dit niet toelaat. Deze meetings worden gehouden door Jan van der Tempel, CEO van Ampelmann Operations, en moeten zowel van hun hoofdkantoor in Delft als in Rotterdam gehouden kunnen worden.

In Delft en Rotterdam gaat het om een grote vergaderruimte waar ongeveer 75 personen tegelijkertijd aanwezig zijn. De externe locaties die aan de maandagochtend meeting mee moeten kunnen doen zijn: Singapore en Qatar. Bij deze externe locaties in het buitenland zullen niet meer dan 2 personen deelnemen.

Momenteel wordt er ook gebruik gemaakt van jabber om onderling te bellen en chatten. Integratie hiermee is daarom een belangrijk onderdeel van de video oplossing. Tot slot moet de totaal oplossing ook de communicatie binnen het bedrijf verbeteren, door de mogelijkheid om snel en moet goede kwaliteit te kunnen vergaderen met beeld.

Opsomming van de eisen:

- HD kwaliteit
- Gebruiksvriendelijk
- Contentsharing mogelijk (zowel PowerPoint als detailtekeningen)
- Jabber integratie mogelijk
- Interne vergaderingen
- Multipoint met 4 locaties.
- 2 locaties met 75 deelnemers
- 2 locaties met 2 deelnemers
- Mogelijk over een lokale internetverbinding
- Budget €25.000

Bijlage F – Ontwerprapport

AFSTUDEERRAPPORT

ADTS ICT B.V. - NL - Capelle aan den IJsel

Video over IP

Auteur	:	Maurice Rutenfrans
Studentnummer	:	10001468
Document	:	Ontwerprapport
Releasedatum	:	15 dec. 14
Versie	:	1.0
Status	:	Definitief

Documenthistorie

Versie	Datum	Auteur	Commentaar
0.1	05 dec. 14	Maurice Rutenfrans	Concept
0.2	09 dec. 14	Maurice Rutenfrans	Concept
1.0	15 dec. 14	Maurice Rutenfrans	Definitief

Distributielijst

Versie	Datum	Ontvanger	Email
0.1	05 dec. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
0.2	09 dec. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
1.0	15 dec. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl

Relevante documenten

Versie	Datum	Auteur	Document
1.0		Maurice Rutenfrans	Plan van aanpak
1.0		Maurice Rutenfrans	Onderzoeksplan
1.0		Maurice Rutenfrans	Onderzoeksrapport
1.0		Maurice Rutenfrans	Business case

Voorwoord

In het kader van mijn opleiding Technische Informatica aan de Haagse Hogeschool ben ik werkzaam bij ADTS ICT B.V. Voor u ligt het ontwerprapport dat onderdeel uitmaakt van mijn afstudeerstage, die plaats vindt van 25 augustus 2014 tot 9 januari 2015.

Dit ontwerprapport zal worden opgeleverd aan Bernhard van der Linde, directeur van ADTS ICT B.V. Het zal ook beschikbaar zijn voor een ieder die geïnteresseerd is en daartoe bevoegd is.

Rotterdam, december 2014
Maurice Rutenfrans

Inhoudsopgave

1. Inleiding

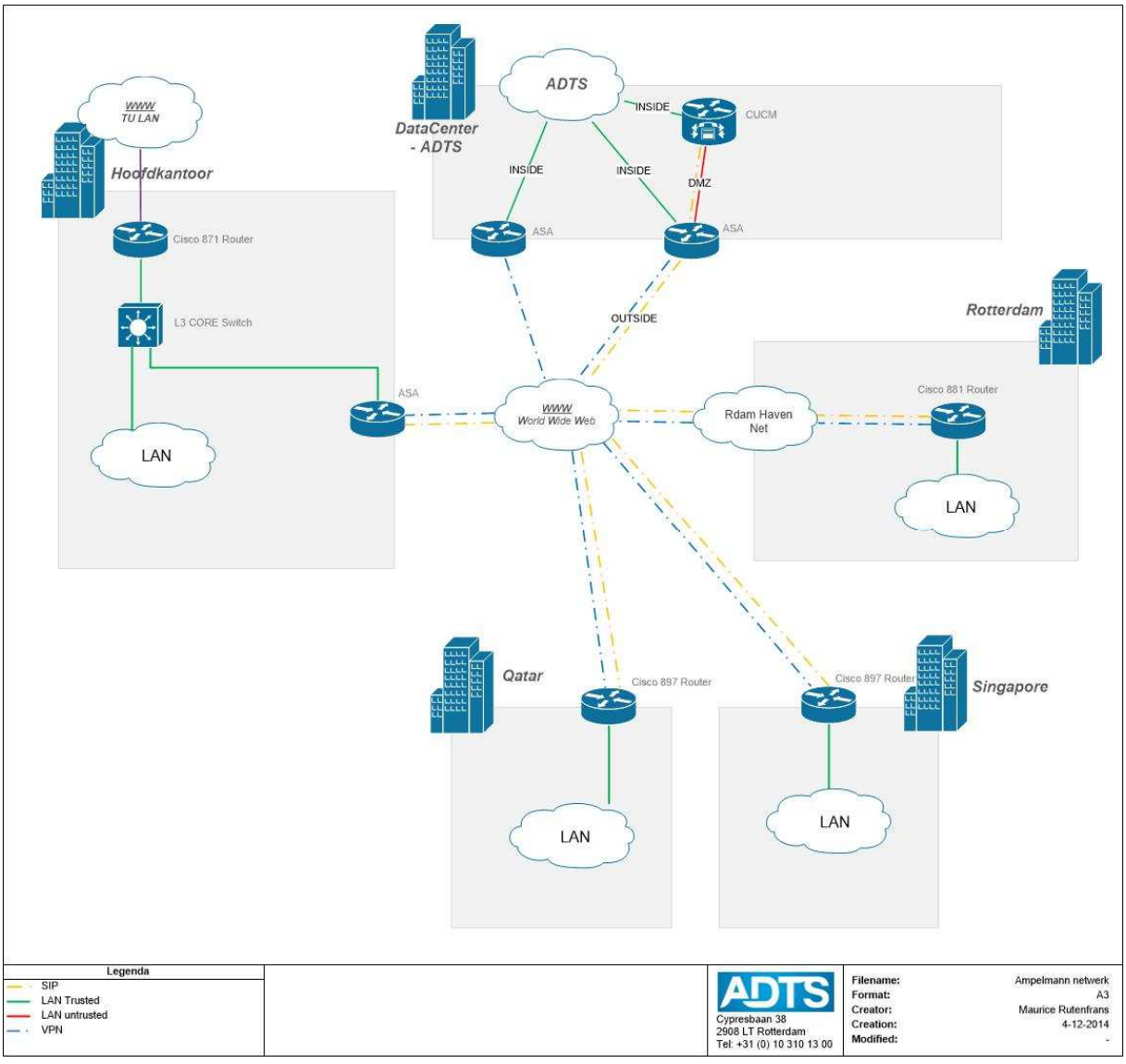
In dit document wordt de proof of concept uitgewerkt, bestaande uit twee hoofdstukken: fysiek ontwerp en logisch ontwerp. In het hoofdstuk fysiek ontwerp, wordt eerst de huidige situatie kort beschreven. Met deze informatie wordt eerst de basis en vervolgens de eindpunten en platform bepaalt. Tijdens het opstellen van de basis voor deze proof of concept wordt er ook al vast gelegd welke IP reeksen er gebruikt gaan worden.

Nadat er een netwerkontwerp is gekozen voor Ampelmann Operations, is deze uitgewerkt in het logisch ontwerp. In dit hoofdstuk wordt het ontwerp gedetailleerd uitgewerkt. Zo worden de configuraties van de apparatuur, de installatie van vmware, callmanager en de eindpunten beschreven. Hiermee is het voor een ieder met de juiste apparatuur mogelijk om deze proof of concept na te bouwen en configureren.

2. Fysiek ontwerp

2.1 Huidige netwerk

Het huidige netwerk van Ampelmann Operations bestaat uit vier locaties die allemaal, doormiddel van een VPN, verbonden zijn met het datacenter van ADTS ICT B.V. (figuur 1). In het datacenter worden de servers (VMware), waarop o.a. de callmanager (CUCM) wordt gehost. Op de locaties wordt niets beheerd en kunnen gezien worden als “domme” locaties. Als een van de locaties technische problemen heeft of er een stroomuitval plaats vindt, ondervinden de rest van de locaties er geen problemen door.



Figuur 40: Huidige netwerk Ampelmann Operations

2.2 Proof of concept

Hier wordt op basis van het huidige netwerk de fundering van de proof of concept bepaalt en vervolgens twee netwerk ontwerpen gerealiseerd.

Internet

Voor de proof of concept wordt het internet gesimuleerd met een layer 3 switch (figuur 2). Deze Layer 3 switch doet niets anders dan het verkeer doorsturen zonder er zelf wat mee te doen. In de huidige situatie kunnen alle locaties met elkaar praten doormiddel van VPN en routering. In deze proof of concept wordt dit gerealiseerd met het routeringsprotocol OSPF. Er is voor OSPF gekozen, omdat deze al gebruikt wordt in het huidige netwerk van Ampelmann Operations. Er wordt niet gekozen voor het gebruik van VPN, omdat dit buiten de scope valt en geen invloed heeft op het eindresultaat.

Voor de verbindingen met de locaties worden verzonnen IP reeksen gebruikt. In een proof of concept is het mogelijk om de reeksen ruim te nemen, omdat er geen tekort kan ontstaan en niet naar de toekomst gekeken hoeft te worden. Om het realistisch te maken is er wel voor gekozen gebruik te maken van subnetten:

Vlan ID	Naam	IP range	IP
11	Delft	11.11.11.252/30	11.11.11.254
12	Rotterdam	11.11.12.252/30	11.11.12.254
13	Qatar	11.11.13.252/30	11.11.13.254
14	Singapore	11.11.14.252/30	11.11.14.254
15	Datacenter	11.11.15.252/30	11.11.15.254

Tabel 9: Internet IP ranges en IP adres

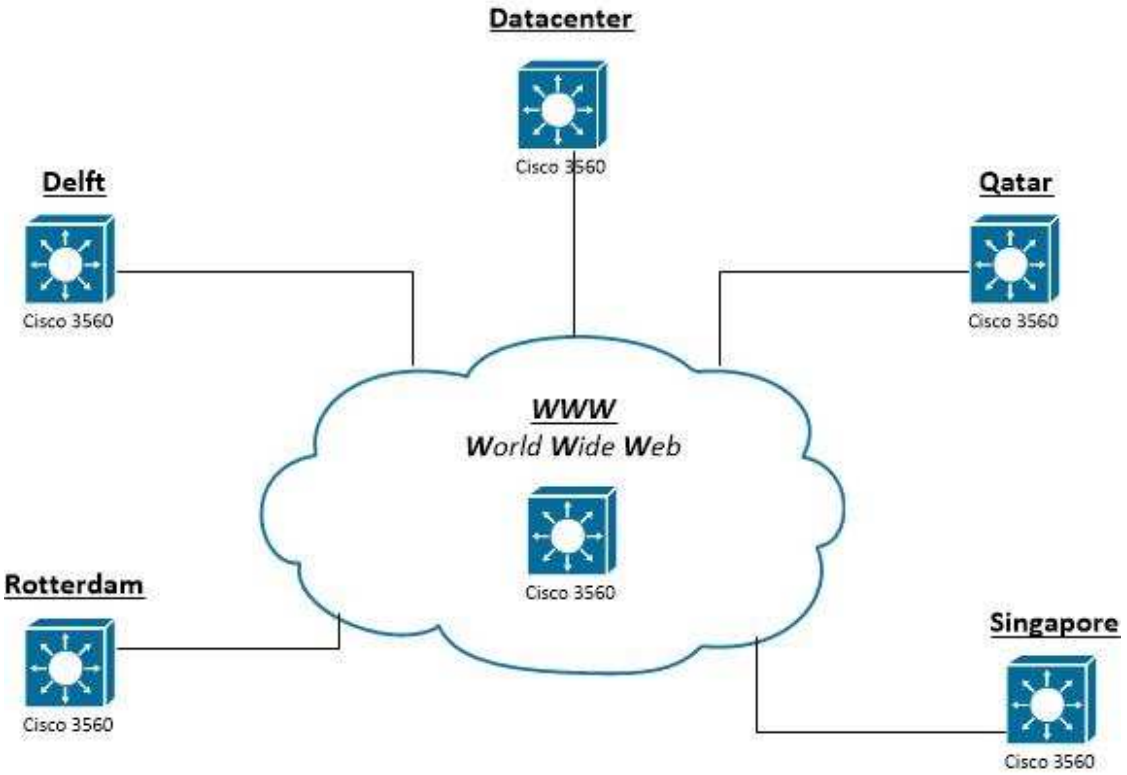
Figuur 41: Internet

Locaties

Ook de locaties worden gesimuleerd met layer 3 switches. Deze locaties zijn verbonden met het internet (figuur 3) en routeren ook doormiddel van OSPF. De IP reeksen van de verbindingen met het internet zijn hiervoor al gedefinieerd. De locaties zelf krijgen een ruimere reeks toegekend, van 30 host, voor de belangrijkste vlans (tabel 1) in het Ampelmann netwerk. Vlans die niet zijn opgenomen zijn vlans zoals printer en guest die zeker niet in deze demonstatie voorkomen. Er is voor /27 subnets gekozen, omdat het aantal eindgebruikers die verbonden worden nog onbekend is en het beste flexibel gehouden kan worden.

Vlan id	Naam	Delft	Rotterdam	Qatar	Singapore	Datacenter
1	default	11.11.11.0/27	11.11.12.0/27	11.11.13.0/27	11.11.14.0/27	11.11.15.0/27
5	Monitoring	11.11.11.32/27	11.11.12.32/27	11.11.13.32/27	11.11.14.32/27	11.11.15.32/27
8	Management	11.11.11.64/27	11.11.12.64/27	11.11.13.64/27	11.11.14.64/27	11.11.15.64/27
11	Delft	11.11.11.252/30	x	x	x	x
12	Rotterdam	x	11.11.12.252/30	x	x	x
13	Qatar	x	x	11.11.13.252/30	x	x
14	Singapore	x	x	x	11.11.14.252/30	x
15	Datacenter	x	x	x	x	11.11.15.252/30
20	Office	11.11.11.96/27	11.11.12.96/27	11.11.13.96/27	11.11.14.96/27	11.11.15.96/27
100	Voice	11.11.11.128/27	11.11.12.128/27	11.11.13.128/27	11.11.14.128/27	11.11.15.128/27
104	Video	11.11.11.160/27	11.11.12.160/27	11.11.13.160/27	11.11.14.160/27	11.11.15.160/27
200	Server	11.11.11.192/27	11.11.12.192/27	11.11.13.192/27	11.11.14.192/27	11.11.15.192/27

Tabel 10: IP plan Locaties.



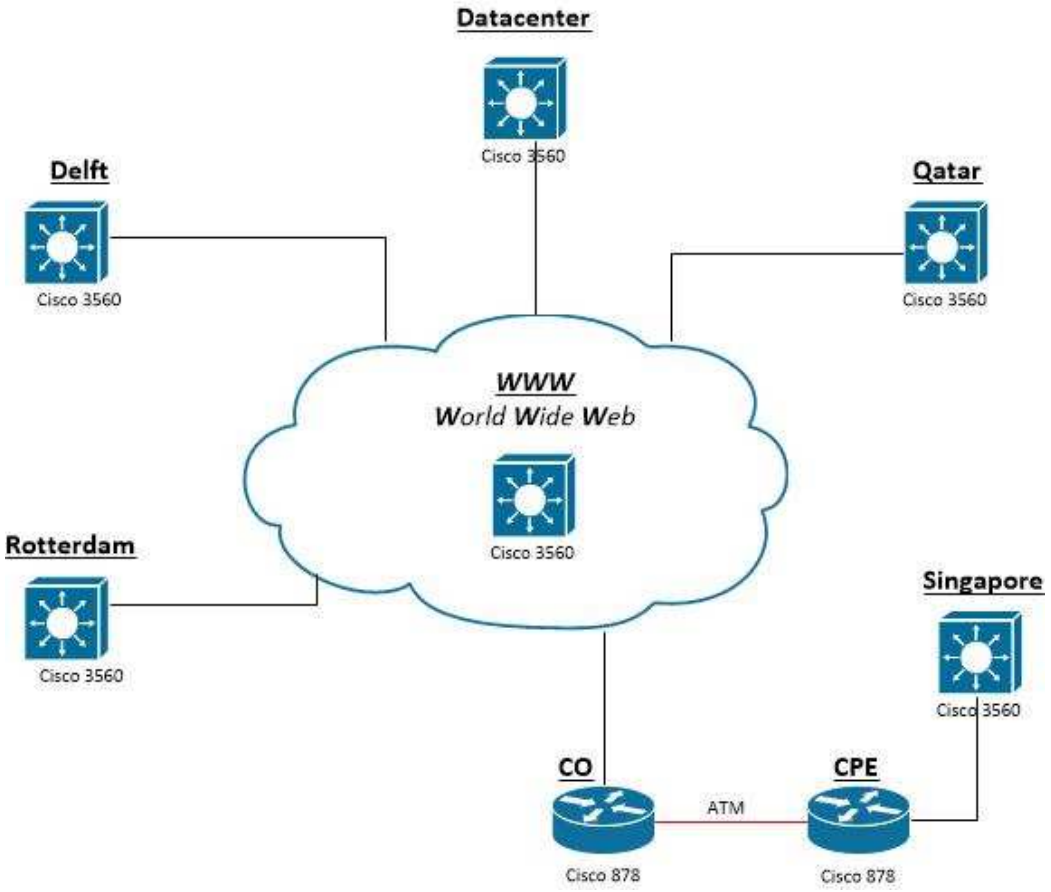
Figuur 42: Locaties.

Lokale internetverbinding

Om een lokale internetverbinding te simuleren is de locatie Singapore uitgebreid met twee routers (Figuur 4). De twee toegevoegde routers zijn verbonden met een ATM verbinding. Hierdoor komt het overeen met de huidige situatie en daarnaast is het mogelijk om de bandbreedte in te stellen.

verbinding	IP range
Internet – CO	11.11.14.252/30
CO - CPE	11.11.14.248/30
CPE - Singapore	11.11.14.244/30

Tabel 11: IP reeks uitgebreid.



Tabel 12: Lokale internetverbinding.

2.2.1 Proof of concept ontwerp 1

Het verschil in de ontwerpen zit in de eindpunten en het platform die gebruik worden. In dit onderdeel wordt één ontwerp uitgewerkt.

Eindpunten

Allereerst is er gekeken naar de eindpunten die geschikt zijn voor Ampelmann Operations. Alle eindpunten van Cisco die ruim boven het budget zitten zijn in de eerste stap grijs gemaakt en zal niet naar gekeken worden (tabel 2). Categorieën die gehanteerd worden zijn groen (geschikt), oranje (mogelijk) en rood (niet geschikt).

Eindpunten	1-3 deelnemers	4-9 deelnemers	10+ deelnemers
Cisco IP Phone 8900 Series			
Cisco IP Phone 9900 Series			
Cisco DX650			
Cisco DX70 & 80			
Cisco TelePresence System 500			
Cisco TelePresence EX serie			
Cisco TelePresence MX200 en MX300			
Cisco TelePresence MX700 en MX 800			
Cisco TelePresence System Profile Serie			
Cisco TelePresence System 1100			
Cisco TelePresence TX9000 Serie			
Cisco TelePresence TX1310			

Tabel 13: Mogelijke eindpunten

Geschikt voor 1-3 deelnemers

Voor de externe locaties is in dit ontwerp gekozen voor de EX serie. De IP Phone 8900 Series, IP Phone 9900 Series en DX650 vallen af, omdat ze niet geschikt zijn voor meerdere deelnemers vanwege het formaat. De MX200 en 300 zijn wel mogelijk, maar zijn bedoeld voor meerdere deelnemers en daarnaast is het budget niet toereikend om deze te gebruiken (> € 10.000). De DX serie is ook geschikt, maar heeft een lange levertijd.

De EX series bestaat uit twee varianten:

- EX60
- EX90

	EX60	**EX90**
Doelgroep	Medewerkers	Leidinggevenden of managers.
Scherm en beeld	21.5 inch scherm met 1920x1080 resolutie.	24 inch scherm met 1920x1200 resolutie.
Camera	PrecisionHD camera met 50 ° gezichtsveld.	PrecisionHD camera met optische zoom en 45-65 ° gezichtsveld.
Content sharing	DVI input	Meerdere digitale ingangen (DVI en HDMI).
Geluid	2 luidsprekers.	2 luidsprekers en 1 subwoofer.
Extra	Optioneel wandsteun, indien er beperkte ruimte is.	Dual display mogelijkheid.
Kosten	€4.000	€6.000

Tabel 14: Vergelijkstabel EX60 en EX90.

De keuze is gevallen op de EX60, omdat de EX90 een luxere variant is van de EX60 gemaakt voor leidinggevenden of managers (Tabel 6). De extra functies die geboden worden zijn niet van toepassing voor Ampelmann Operations.

Geschikt voor 10+ deelnemers

Voor de vergaderruimte zijn geen van bovengenoemde eindpunten volledig geschikt, omdat de geïntegreerde schermen niet aan de eis kunnen voldoen om voor 75 deelnemers duidelijk beeld weer te geven. De MX300 is mogelijk, maar de kans dat deze ook niet voldoet aan de eisen van Ampelmann Operations is zeer groot. Het voordeel van het gebruiken van de MX300 is dat deze een geïntegreerde multipoint bridging capaciteit heeft, waardoor er geen TelePrecense server nodig is. Er is daarom gekeken naar een professionele camera die zelf geplaatst kan worden (Figuur 4).

Figuur 43: voorbeeld hoe de SX20 gebruikt kan worden.

Hiervoor is gekozen voor de Cisco SX serie, die uit de volgende varianten bestaat:

- SX10
- SX20

De keuze is gevallen op de SX20, omdat de SX10 voor persoonlijk gebruik op een tv scherm dient en de SX20 gemaakt is voor videoconferentie zalen.

Platform

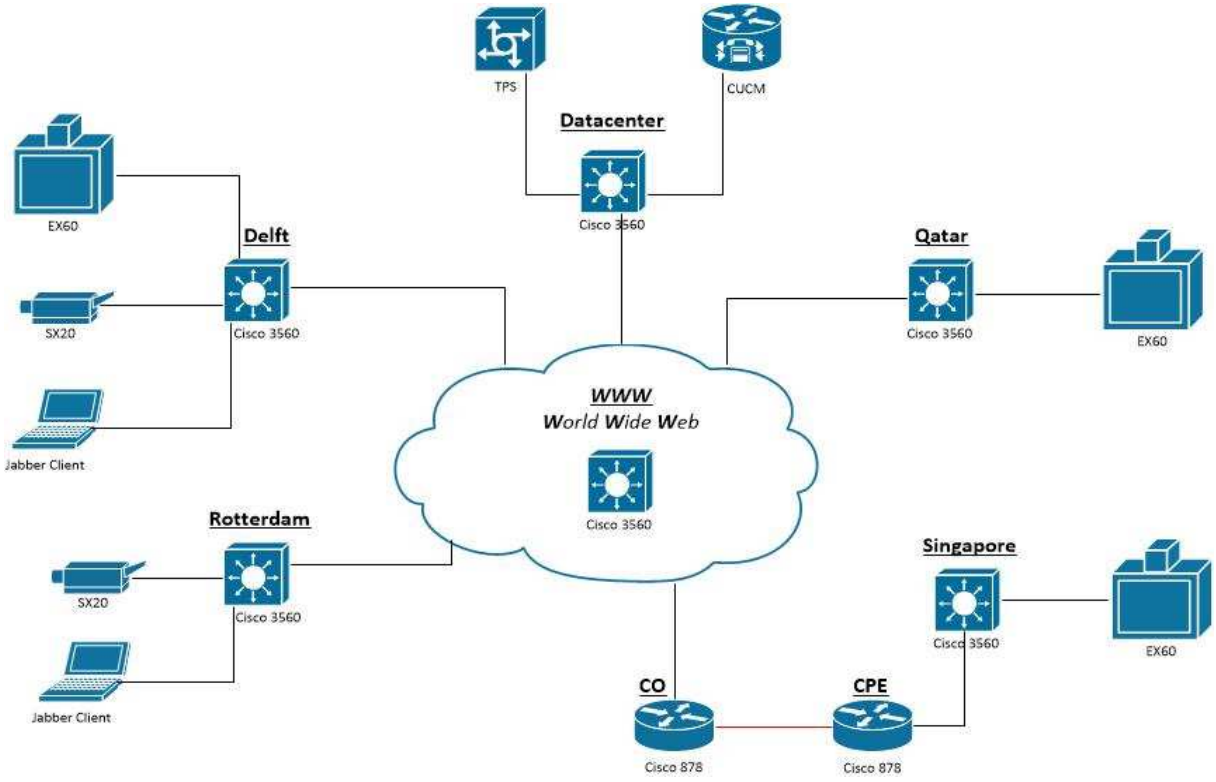
Ampelmann Operations is al in het bezit van een Cisco Unified Communications Manager (CUCM), deze maakt point-to-point videoconferenties mogelijk. De sollicitatie gesprekken met de EX60 kunnen hiermee gerealiseerd worden. Voor videoconferenties waar meer dan twee locaties (multipoint) deelnemen moet een multipoint bridge gekozen worden. In dit ontwerp is gekozen voor het kopen van een Cisco TelePresence Server, omdat zowel Ampelmann Operations als ADTS ICT B.V. ervoor kiezen om niet afhankelijk te zijn van derde partijen.

Platform	Kenmerken
Cisco Unified Communications Manager (CUCM)	Al in bezit
Cisco TelePresence Server	Nodig voor multipoint bridging
Cisco TelePresence Conductor	Optioneel
Cisco TelePresence Content Server	Optioneel
Cisco TelePresence Video Communication Server (VCS)	Niet nodig door CUCM
Cisco Prime Collaboration	Optioneel
Cisco TelePresence Management Suite (TMS)	Optioneel

Tabel 15: Platform componenten.

Netwerktekening

Het netwerk voor het eerste ontwerp van de proof of concept ziet er als volgt uit (figuur 5):



Figuur 44: Netwerk ontwerp 1.

Kosten
In tabel 8 is af te lezen wat de kosten zijn voor de hardware van deze oplossing. Dit is exclusief de aanschaf van presentatie apparatuur, beeldschermen en implementatie kosten.

Hardware	aantal	Prijs per stuk	Kosten
EX60	3	€4.200	€12.600
SX20	2	€4.800	€9.600
TelePresence Server licentie per poort	4	€5.500	€22.000
Totaal:			€44.200

Tabel 16: Kosten proof of concept 1.

2.2.2 Proof of concept ontwerp 2
In dit stuk wordt het tweede ontwerp voor de proof of concept uitgewerkt.

Eindpunten

Geschikt voor 1-3 deelnemers
Voor de externe locaties is in dit ontwerp gekozen voor de DX80. De DX80 levert dezelfde mogelijkheden als de EX60 en zal deze in de toekomst vervangen. Het grote verschil zit in de kosten en call control (tabel 9). Ampelmann Operations is al in het bezit van een Cisco Unified Communications Manager (CUCM) en hoeft deze niet extra aan te schaffen. Het grootste nadeel, op dit moment, is de lange levertijd van de DX80.

	DX80	EX60
Kosten	€3.000	€4.200
Call control	CUCM	Zowel CUCM als VCS
Extra	Lange levertijd	-

Tabel 17: Verschillen DX80 en EX60

De DX Serie bestaat uit drie varianten, waarvan de DX650 en DX70 afvallen omdat deze alleen voor een enkele deelnemer geschikt zijn:

- ~~DX650~~
- ~~DX70~~
- DX80

Geschikt voor 10+ deelnemers
Voor de werkomgeving in Delft is een MX300 mogelijk, maar het is niet met zekerheid te zeggen of dit scherm aan de eis van 75 deelnemers voldoet. Het voordeel van het gebruiken van de MX300 is dat deze een geïntegreerde multipoint bridging capaciteit heeft, waardoor er geen TelePresence server nodig is. Omdat de SX20 ook deze mogelijkheid heeft en deze zeker geschikt is voor een grote groep deelnemers is deze gekozen, voor zowel delft als rotterdam, in dit ontwerp.

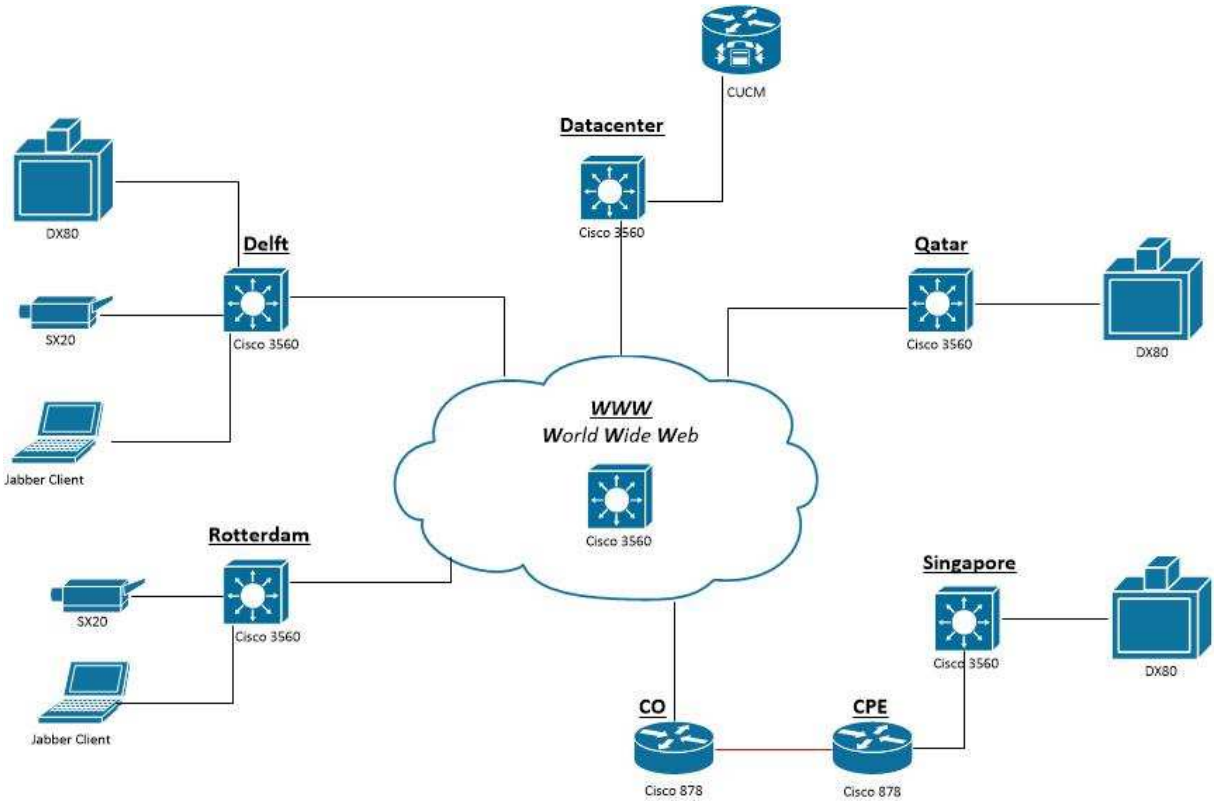
Platform
Ampelmann Operations is al in het bezit van een Cisco Communications Manager (CUCM), deze maakt point-to-point videoconferenties mogelijk. De sollicitatie gesprekken met de DX80 kunnen hiermee gerealiseerd worden. Voor videoconferenties waar meer dan twee locaties (multipoint) deelnemen moet een multipoint bridge gekozen worden. In dit ontwerp is gekozen voor de SX20, omdat deze een geïntegreerde multipoint bridging capaciteit bezit. De SX20 kan met maximaal vier locaties tegelijk videoconferencen (inclusief zichzelf).

Platform	Kenmerken
Cisco Unified Communications Manager (CUCM)	Al in bezit
Cisco TelePresence Server	Niet nodig door SX20
Cisco TelePresence Conductor	Niet nodig door SX20
Cisco TelePresence Content Server	Niet nodig door SX20
Cisco TelePresence Video Communication Server (VCS)	Niet nodig door CUCM
Cisco Prime Collaboration	Niet nodig door SX20
Cisco TelePresence Management Suite (TMS)	Niet nodig door SX20

Tabel 18: Platform

Netwerktekening

Het netwerk voor het tweede ontwerp van de proof of concept ziet er als volgt uit (figuur 6):



Figuur 45: Netwerk ontwerp 2.

Kosten

In tabel 11 is af te lezen wat de kosten zijn voor de hardware van deze oplossing. Dit is exclusief de aanschaf van presentatie apparatuur, extra beeldschermen en implementatie kosten.

Hardware	aantal	Prijs per stuk	Kosten
DX80	3	€3.000	€9.000
SX20	2	€4.800	€9.600
Multisite license SX20	1	€2.500	€2.500
Totaal:			€21.100

Tabel 19: Kosten proof of concept 1.

2.2.3 Definitieve proof of concept

Ampelmann Operations heeft gekozen voor het tweede ontwerp. Waarbij er voor de sollicitatie gesprekken gebruik gemaakt wordt van de DX80. De lagere kosten wegen zwaarder dan de langere levertijd. Voor de maandagmorgen meeting wordt er gebruik gemaakt van SX20 in combinatie met de multisite license. De keuze voor de SX20 is gemaakt om er zeker van te zijn dat hij gebruikt kan worden voor 75 man. De multisite license is gekozen vanwege de kosten, ondanks dat deze gelimiteerd is tot vier gelijktijdig deelnemers in een videoconference. De TelePresence server is een betere oplossing met het oog op de toekomst, omdat deze schaalbaar is. De investering ligt daarentegen aanzienlijk hoger, waardoor er gekozen is voor multisite license.

2.3 Veiligheid en QoS

Al het verkeer wordt verzonden via VPN tunnels naar elkaar. Hierdoor is het verkeer afgeschermd van de buitenwereld. Doordat er gebruik gemaakt wordt van VPN tunnels hoeft er geen rekening gehouden te worden met natting en firewalls. Het voordeel hiervan is dat een slecht firewall beleid vermeden wordt.
Voor intern wordt het voice en video verkeer standaard beschermt door de Cisco Unified Communications Manager (CUCM). Om het verkeer te beschermen wordt het TLS (Transport Layer Security) protocol gebruikt. Dit wordt voorgeschreven door Cisco en gebruikt AES 128 encryptie om het verkeer te versleutelen.

QoS is in de huidige situatie van Ampelmann Operations alleen intern in te regelen, omdat dit over het internet niet mogelijk is. Intern is er voldoende bandbreedte aanwezig, door het gebruik van gigabit verbindingen. Mede hierdoor en omdat het aantal eindpunten nog minimaal is, is het niet nodig om dit in te stellen.
Als er in de toekomst de vraag komt om dit in te regelen is het aan te raden om over te stappen op bijvoorbeeld MPLS (Multiprotocol Label Switching) om QoS/CoS in te regelen. De kosten hiervoor liggen daarentegen zeer hoog.

3. Logisch ontwerp

3.1 Configuratie internet – Layer 3 switch

```
hostname Internet
ip routing
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa
2048

vlan 11
name Delft
vlan 12
name Rotterdam
vlan 13
name Qatar
vlan 14
name Singapore
vlan 15
name Datacenter

interface Vlan11
 description Delft
 ip address 11.11.11.254 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan12
 description Rotterdam
 ip address 11.11.12.254 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan13
 description Qatar
 ip address 11.11.13.254 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan14
 description Singapore
 ip address 11.11.14.254 255.255.255.252
 no ip proxy-arp
 no shutdown
```

```
interface Vlan15
 description Datacenter
 ip address 11.11.15.254 255.255.255.252
 no ip proxy-arp
 no shutdown

interface FastEthernet0/1
 description Delft
 switchport access vlan 11
 switchport mode access
 no shutdown

interface FastEthernet0/2
 description Rotterdam
 switchport access vlan 12
 switchport mode access
 no shutdown

interface FastEthernet0/3
 description Qatar
 switchport access vlan 13
 switchport mode access
 no shutdown

interface FastEthernet0/4
 description Singapore
 switchport access vlan 14
 switchport mode access
 no shutdown

interface FastEthernet0/5
 description Datacenter
 switchport access vlan 15
 switchport mode access
 no shutdown

interface range FastEthernet0/6-24
 shutdown

interface range GigabitEthernet0/1-2
 shutdown

router ospf 1
 network 11.11.11.252 0.0.0.3 area 0
 network 11.11.12.252 0.0.0.3 area 0
 network 11.11.13.252 0.0.0.3 area 0
 network 11.11.14.252 0.0.0.3 area 0
 network 11.11.15.252 0.0.0.3 area 0
```

3.2 Configuratie locaties

3.2.1 Delft – Layer 3 switch

```
hostname Delft
ip routing
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa
2048

vlan 5
name Monitoring
vlan 8
name Management
vlan 11
name Delft
vlan 20
name Office
vlan 100
name Voice
vlan 104
name Video
vlan 200
name Servers

interface Vlan1
 ip address 11.11.11.30 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan5
 description Monitoring
 ip address 11.11.11.62 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan8
 description Management
 ip address 11.11.11.94 255.255.255.224
 no ip proxy-arp
 no shutdown
```

```
interface Vlan11
 description Delft
 ip address 11.11.11.253 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan20
 description Office
 ip address 11.11.11.126 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan100
 description Voice
 ip address 11.11.11.158 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan104
 description Video
 ip address 11.11.11.190 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan200
 description Server
 ip address 11.11.11.222 255.255.255.224
 no ip proxy-arp
 no shutdown

interface FastEthernet0/1
 description Internet
 switchport access vlan 11
 switchport mode access
 no shutdown

interface range FastEthernet0/2-23
 switchport mode access
 shutdown

interface FastEthernet0/24
 switchport access vlan 104
 switchport mode access
 no shutdown

interface range GigabitEthernet0/1-2
 switchport mode access
 shutdown
```

```
router ospf 1
 network 11.11.11.252 0.0.0.3 area 0
 network 11.11.11.0 0.0.0.31 area 11
 network 11.11.11.32 0.0.0.31 area 11
 network 11.11.11.64 0.0.0.31 area 11
 network 11.11.11.96 0.0.0.31 area 11
 network 11.11.11.128 0.0.0.31 area 11
 network 11.11.11.160 0.0.0.31 area 11
 network 11.11.11.192 0.0.0.31 area 11

ip dhcp excluded-address 11.11.11.126
ip dhcp excluded-address 11.11.11.190
ip dhcp excluded-address 11.11.11.158

ip dhcp pool Office
network 11.11.11.96 255.255.255.224
default-router 11.11.11.126
dns-server 8.8.8.8

ip dhcp pool Voice
network 11.11.11.128 255.255.255.224
default-router 11.11.11.158
option 150 ip 11.11.15.200
dns-server 8.8.8.8

ip dhcp pool Video
network 11.11.11.160 255.255.255.224
default-router 11.11.11.190
dns-server 8.8.8.8

ip name-server 8.8.8.8

access-list 10 permit 11.11.11.64 0.0.0.31
access-list 10 deny any log

line vty 0 15
transport input ssh
access-class 10 in
```

3.2.2 Rotterdam – Layer 3 switch

```
hostname Rotterdam
ip routing
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########
```

```
crypto key generate rsa
2048

vlan 5
name Monitoring
vlan 8
name Management
vlan 12
name Rotterdam
vlan 20
name Office
vlan 100
name Voice
vlan 104
name Video
vlan 200
name Servers

interface Vlan1
 ip address 11.11.12.30 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan5
 description Monitoring
 ip address 11.11.12.62 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan8
 description Management
 ip address 11.11.12.94 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan12
 description Rotterdam
 ip address 11.11.12.253 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan20
 description Office
 ip address 11.11.12.126 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan100
 description Voice
 ip address 11.11.12.158 255.255.255.224
```

```
 no ip proxy-arp
 no shutdown

interface Vlan104
 description Video
 ip address 11.11.12.190 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan200
 description Server
 ip address 11.11.12.222 255.255.255.224
 no ip proxy-arp
 no shutdown

interface FastEthernet0/1
 description Internet
 switchport access vlan 12
 switchport mode access
 no shutdown

interface range FastEthernet0/2-23
 switchport mode access
 shutdown

interface FastEthernet0/24
 switchport access vlan 104
 switchport mode access
 no shutdown

interface range GigabitEthernet0/1-2
 switchport mode access
 shutdown

router ospf 1
 network 11.11.12.252 0.0.0.3 area 0
 network 11.11.12.0 0.0.0.31 area 12
 network 11.11.12.32 0.0.0.31 area 12
 network 11.11.12.64 0.0.0.31 area 12
 network 11.11.12.96 0.0.0.31 area 12
 network 11.11.12.128 0.0.0.31 area 12
 network 11.11.12.160 0.0.0.31 area 12
 network 11.11.12.192 0.0.0.31 area 12

ip dhcp excluded-address 11.11.12.126
ip dhcp excluded-address 11.11.12.190
ip dhcp excluded-address 11.11.12.158

ip dhcp pool Office
network 11.11.12.96 255.255.255.224
```

```
default-router 11.11.12.126
dns-server 8.8.8.8

ip dhcp pool Voice
network 11.11.12.128 255.255.255.224
default-router 11.11.12.158
option 150 ip 11.11.15.200
dns-server 8.8.8.8

ip dhcp pool Video
network 11.11.12.160 255.255.255.224
default-router 11.11.12.190
dns-server 8.8.8.8

ip name-server 8.8.8.8

access-list 10 permit 11.11.11.64 0.0.0.31
access-list 10 deny any log

line vty 0 15
transport input ssh
access-class 10 in
```

3.2.3 Qatar – Layer 3 switch

```
hostname Qatar
ip routing
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa
2048

vlan 5
name Monitoring
vlan 8
name Management
vlan 13
name Qatar
vlan 20
name Office
vlan 100
name Voice
vlan 104
name Video
vlan 200
```

```
name Servers

interface Vlan1
 ip address 11.11.13.30 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan5
 description Monitoring
 ip address 11.11.13.62 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan8
 description Management
 ip address 11.11.13.94 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan13
 description Qatar
 ip address 11.11.13.253 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan20
 description Office
 ip address 11.11.13.126 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan100
 description Voice
 ip address 11.11.13.158 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan104
 description Video
 ip address 11.11.13.190 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan200
 description Server
 ip address 11.11.13.222 255.255.255.224
 no ip proxy-arp
 no shutdown
```

```
interface FastEthernet0/1
 description Internet
 switchport access vlan 13
 switchport mode access
 no shutdown

interface range FastEthernet0/2-23
 switchport mode access
 shutdown

interface FastEthernet0/24
 switchport access vlan 104
 switchport mode access
 no shutdown

interface range GigabitEthernet0/1-2
 switchport mode access
 shutdown

router ospf 1
 network 11.11.13.252 0.0.0.3 area 0
 network 11.11.13.0 0.0.0.31 area 13
 network 11.11.13.32 0.0.0.31 area 13
 network 11.11.13.64 0.0.0.31 area 13
 network 11.11.13.96 0.0.0.31 area 13
 network 11.11.13.128 0.0.0.31 area 13
 network 11.11.13.160 0.0.0.31 area 13
 network 11.11.13.192 0.0.0.31 area 13

ip dhcp excluded-address 11.11.13.126
ip dhcp excluded-address 11.11.13.190
ip dhcp excluded-address 11.11.13.158

ip dhcp pool Office
network 11.11.13.96 255.255.255.224
default-router 11.11.13.126
dns-server 8.8.8.8

ip dhcp pool Voice
network 11.11.13.128 255.255.255.224
default-router 11.11.13.158
option 150 ip 11.11.15.200
dns-server 8.8.8.8

ip dhcp pool Video
network 11.11.13.160 255.255.255.224
default-router 11.11.13.190
dns-server 8.8.8.8

ip name-server 8.8.8.8
```

```
access-list 10 permit 11.11.11.64 0.0.0.31
access-list 10 deny any log

line vty 0 15
transport input ssh
access-class 10 in
```

3.2.4 Singapore – Layer 3 switch

```
hostname Singapore
ip routing
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa
2048

vlan 5
name Monitoring
vlan 8
name Management
vlan 16
name LokaleInternetverbinding
vlan 20
name Office
vlan 100
name Voice
vlan 104
name Video
vlan 200
name Servers

interface Vlan1
 ip address 11.11.14.30 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan5
 description Monitoring
 ip address 11.11.14.62 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan8
 description Management
 ip address 11.11.14.94 255.255.255.224
```

```
 no ip proxy-arp
 no shutdown

interface Vlan16
 description Lokale internetverbinding
 ip address 11.11.14.245 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan20
 description Office
 ip address 11.11.14.126 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan100
 description Voice
 ip address 11.11.14.158 255.255.255.224
option 150 ip 11.11.15.200
 no ip proxy-arp
 no shutdown

interface Vlan104
 description Video
 ip address 11.11.14.190 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan200
 description Server
 ip address 11.11.14.222 255.255.255.224
 no ip proxy-arp
 no shutdown

interface FastEthernet0/1
 description Lokale internetverbinding
 switchport access vlan 16
 switchport mode access
 no shutdown

interface range FastEthernet0/2-23
 switchport mode access
 shutdown

interface FastEthernet0/24
 switchport access vlan 104
 switchport mode access
 no shutdown

interface range GigabitEthernet0/1-2
```

```
 switchport mode access
 shutdown

router ospf 1
 network 11.11.14.244 0.0.0.3 area 0
 network 11.11.14.0 0.0.0.31 area 14
 network 11.11.14.32 0.0.0.31 area 14
 network 11.11.14.64 0.0.0.31 area 14
 network 11.11.14.96 0.0.0.31 area 14
 network 11.11.14.128 0.0.0.31 area 14
 network 11.11.14.160 0.0.0.31 area 14
 network 11.11.14.192 0.0.0.31 area 14

ip dhcp excluded-address 11.11.14.126
ip dhcp excluded-address 11.11.14.190
ip dhcp excluded-address 11.11.14.158

ip dhcp pool Office
network 11.11.14.96 255.255.255.224
default-router 11.11.14.126
dns-server 8.8.8.8

ip dhcp pool Voice
network 11.11.14.128 255.255.255.224
default-router 11.11.14.158
dns-server 8.8.8.8

ip dhcp pool Video
network 11.11.14.160 255.255.255.224
default-router 11.11.14.190
dns-server 8.8.8.8

ip name-server 8.8.8.8

access-list 10 permit 11.11.11.64 0.0.0.31
access-list 10 deny any log

line vty 0 15
transport input ssh
access-class 10 in
```

3.2.5 Datacenter – Layer 3 switch

```
hostname Datacenter
ip routing
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
```

```
enable secret ##########

crypto key generate rsa
2048

vlan 5
name Monitoring
vlan 8
name Management
vlan 15
name Datacenter
vlan 20
name Office
vlan 100
name Voice
vlan 104
name Video
vlan 200
name Servers

interface Vlan1
 ip address 11.11.15.30 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan5
 description Monitoring
 ip address 11.11.15.62 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan8
 description Management
 ip address 11.11.15.94 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan15
 description Datacenter
 ip address 11.11.15.253 255.255.255.252
 no ip proxy-arp
 no shutdown

interface Vlan20
 description Office
 ip address 11.11.15.126 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan100
```

```
 description Voice
 ip address 11.11.15.158 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan104
 description Video
 ip address 11.11.15.190 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Vlan200
 description Server
 ip address 11.11.15.222 255.255.255.224
 no ip proxy-arp
 no shutdown

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 description Internet
 switchport access vlan 15
 switchport mode access
 no shutdown

interface range FastEthernet0/13-16
 description Server
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 200
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk

interface range FastEthernet0/23-24
 description Server
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 8
 switchport mode trunk
 spanning-tree portfast trunk

interface range FastEthernet0/2-12
 switchport mode access
 shutdown

interface range FastEthernet0/17-22
 switchport mode access
 shutdown
```

```
interface range GigabitEthernet0/1-2
 switchport mode access
 shutdown

router ospf 1
 network 11.11.15.252 0.0.0.3 area 0
 network 11.11.15.0 0.0.0.31 area 15
 network 11.11.15.32 0.0.0.31 area 15
 network 11.11.15.64 0.0.0.31 area 15
 network 11.11.15.96 0.0.0.31 area 15
 network 11.11.15.128 0.0.0.31 area 15
 network 11.11.15.160 0.0.0.31 area 15
 network 11.11.15.192 0.0.0.31 area 15

access-list 10 permit 11.11.11.64 0.0.0.31
access-list 10 deny any log

line vty 0 15
transport input ssh
access-class 10 in
```

3.2.6 CO - Router

```
Hostname CO
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa
2048

controller dsl 0
mode atm
line-term co
line-mode 4-wire
dsl-mode shdsl symmetric annex A
line-rate 4608

interface Dialer0
 ip address 11.11.14.250 255.255.255.252
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname adts-ict
 ppp chap password 0 ##########
```

```
interface ATM0
 pvc 2/32
  encapsulation aal5mux ppp dialer
  dialer pool-member 1

vlan 14
 name Singapore

int vlan 14
 description Singapore
 ip address 11.11.14.253 255.255.255.252
 no ip proxy-arp
 no shutdown

int FastEthernet0
 description Internet
 switchport access vlan 14
 switchport mode access
 no shutdown

router ospf 1
 network 11.11.14.252 0.0.0.3 area 0
 network 11.11.14.248 0.0.0.3 area 0

line vty 0 4
transport input ssh
```

3.2.7 CPE - Router

```
hostname CPE
ip domain name AMPELMANN.local

aaa new-model
aaa authentication login default local
username adts-ict secret ##########
enable secret ##########

crypto key generate rsa
2048

controller dsl 0
mode atm
line-term CPE
line-mode 4-wire
dsl-mode shdsl symmetric annex a
line-rate 4608

interface Dialer0
```

```
 ip address 11.11.14.249 255.255.255.252
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname adts-ict
 ppp chap password 0 ##########

interface ATM0
 pvc 2/32
  encapsulation aal5mux ppp dialer
  dialer pool-member 1

vlan 16
 name LokaleInternetverbinding

int vlan 16
 description Lokale internetverbinding
 ip address 11.11.14.246 255.255.255.252
 no ip proxy-arp
 no shutdown

int FastEthernet0
 description Lokale internetverbinding
 switchport access vlan 16
 switchport mode access
 no shutdown

router ospf 1
 network 11.11.14.248 0.0.0.3 area 0
 network 11.11.14.244 0.0.0.3 area 0

line vty 0 4
transport input ssh
```

3.2.8 NTP - Router

Voor de CUCM is NTP nodig, daarom is ervoor gekozen om het netwerk uit te breiden met een router die met het netwerk van ADTS ICT B.V. verbind. Via deze verbinding kan de publieke NTP server (141.138.138.136) bereikt worden.

NTP-router

```
interface FastEthernet0
 ip address dhcp
 duplex auto
 speed auto
 ip nat outside

interface FastEthernet2
 no sh
 description NTP
```

```
 switchport access vlan 17
 switchport mode access

vlan 17
 name NTP

Int vlan 17
 description NTP
 ip address 11.11.17.254 255.255.255.252
 no ip proxy-arp
 ip nat inside

router ospf 1
 network 11.11.17.252 0.0.0.3 area 15
 default-information originate

access-list 100 permit ip any any
ip nat inside source list 100 interface FastEthernet0 overload
```

deze ntp router is aan het datacenter gekoppeld:

Datacenter

```
vlan 17
 name NTP

interface FastEthernet0/2
 no sh
 description NTP
 switchport access vlan 17
 switchport mode access

Int vlan 17
 description NTP
 ip address 11.11.17.253 255.255.255.252
 no ip proxy-arp

router ospf 1
 network 11.11.17.252 0.0.0.3 area 15

ntp server 141.138.138.136
```

3.3 VMware server

3.3.1 VMware installeren

Server

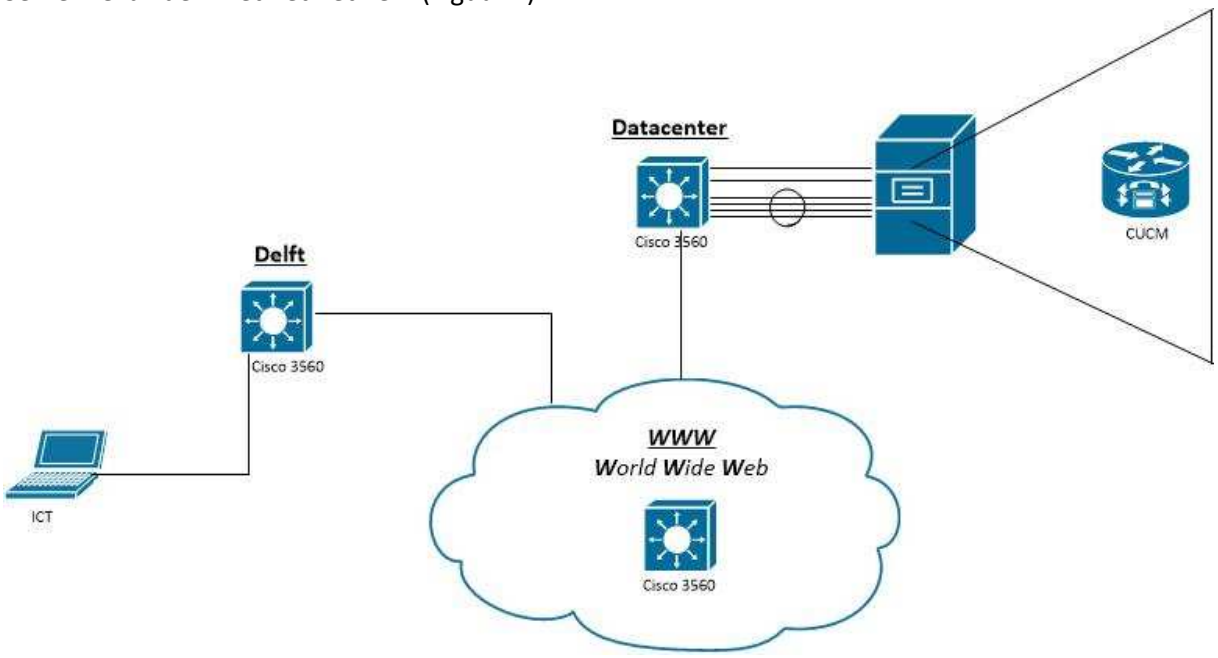
CIMC IP adress instellen, voor beheer fysieke server (F8)

- 11.11.15.65

Password instellen

- ##########

Server verbinden met het netwerk (Figuur 7):



Figuur 46: Deel opstelling inclusief VMware server, waarop de CUCM draait.

Computer - ICT

Controle

- Ping via cmd naar 11.11.15.65

Webinterface

- https:// 11.11.15.65

KVM console starten (java 1.5 of hoger vereist)

Vrituele drives aanmaken (via de webbios ctrl + H)

1) 5gb VMware
2) De rest

Disk koppelen

Boot device kiezen (F6)

VMware installeren

VMware management IP adres instellen

- 11.11.15.66

VMware management password instellen

- ##########

3.3.2 Cisco Unified Communications Manager

Via de VMware client met de volgende gegevens inloggen op de server:

- 11.11.15.66
- Root
- ##########

Datastore creëren

Netwerk kaart instellen

OFA deployen

ISO importeren

NTP instellen*

ISO installeren

- Username: administrator
- Password: ##########
- IP adres: 11.11.15.200

Via de webinterface is de callmanager te bereiken

- https://11.11.15.200/

3.4 Unified Communications Manager

Partities aanmaken:

Naam	Beschrijving
AMP-ALL	AMP-ALL
AMP-NL-DFT-ALL	Partition for Delft - ALL
AMP-NL-DFT-CSS07	Partition for Delft - CSS07
AMP-NL-DFT-LOGGED-OUT	Partition for Delft - Logged Out
AMP-NL-RDM-ALL	Partition for Rotterdam - ALL
AMP-NL-RDM-CSS07	Partition for Rotterdam - CSS07
AMP-NL-RDM-LOGGED-OUT	Partition for Rotterdam - Logged Out
AMP-QT-QTR-ALL	Partition for Qatar - ALL
AMP-QT-QTR-CSS07	Partition for Qatar- CSS07
AMP-QT-QTR-LOGGED-OUT	Partition for Qatar - Logged Out
AMP-SG-SNG-ALL	Partition for Singapore - ALL
AMP-SG-SNG-CSS07	Partition for Singapore - CSS07
AMP-SG-SNG-LOGGED-OUT	Partition for Singapore - Logged Out

Calling search space aanmaken en instellen:

Naam	Morgen bellen naar
AMP-NL-DFT-CSS07	AMP-ALL AMP-NL-DFT-CSS07
AMP-NL-DFT-LOGGED-OUT	AMP-ALL
AMP-NL-RDM-CSS07	AMP-ALL AMP-NL-RDM-CSS07
AMP-NL-RDM-LOGGED-OUT	AMP-ALL
AMP-QT-QTR-CSS07	AMP-ALL AMP-QT-QTR-CSS07
AMP-QT-QTR-LOGGED-OUT	AMP-ALL
AMP-SG-SNG-CSS07	AMP-ALL AMP-SG-SNG-CSS07
AMP-SG-SNG-LOGGED-OUT	AMP-ALL

Users en device profiles aanmaken:

User	Nummer
Maurice Rutenfrans	9001
Bernhard van der Linde	9002
Rick Hoevenaar	9003
Emre Demir	9004
Jsco Hoornaar	9005

Marc Schuller	9006
Aloys Ruseler	9007
Hanneke Franken	9008
Amber Schot	9009
Robert van de Linde	9010

Nieuwe regions aanmaken:

Region
AMP-NL-DFT-VIDEO
AMP-NL-RDM-VIDEO
AMP-QT-QTR-VIDEO
AMP-SG-SNG-VIDEO

De regions zijn nodig om de maximum bandbreedte voor video en de kwaliteit van spraak in- en extern te beheren:

- Spraak locaal G.711
- Spraak inter company G.729
- Maximum bandbreedte per gesprek 2048 kbps, voor alle locaties

Eindpunten aanmaken en instellen:

Device	**Nummer**
DX80 - Delft	1001
DX80 - Qatar	1002
DX80 - Singapore	1003
SX20 - Delft	1004
SX20 - Rotterdam	1005

Om er voor te zorgen dat de users niet alle nummers van de conference systemen uit hun hoofd hoeven te kennen, worden ze toegevoegd aan de adressen lijst. Om dit te realiseren zijn de eindpunten ook als users aangemaakt:

User	**Nummer**
Delft Meetingroom 1	1001
Qatar Meetingroom 1	1002
Singapore Meetingroom 1	1003
Delft Meetingroom 2	1004
Rotterdam Meetingroom 1	1005

3.5 Eindpunten

3.4.1 DX80

CUCM instellen

- 11.11.15.200
- Configuratie wordt gepushed door de CUCM

Password instellen via de webinterface (deze moet eerst enabeld worden in de CUCM)

- https://11.11.11.161
- https://11.11.13.161

- https://11.11.14.161

3.4.2 SX20

CUCM instellen (11.11.15.200)

- 11.11.15.200
- Configuratie wordt gepushed door de CUCM

Password instellen via de webinterface (deze moet eerst enabeld worden in de CUCM)

- https://11.11.11.162
- https://11.11.12.161

Multisite license importeren via de webinterface.

Bijlage G – Testrapport

AFSTUDEERRAPPORT

ADTS ICT B.V. - NL - Capelle aan den IJsel

Video over IP

Auteur	:	Maurice Rutenfrans
Studentnummer	:	10001468
Document	:	Testrapport
Releasedatum	:	24 dec. 14
Versie	:	1.0
Status	:	Definitief

Documenthistorie

Versie	Datum	Auteur	Commentaar
0.1	19 dec. 14	Maurice Rutenfrans	Concept
1.0	24 dec. 14	Maurice Rutenfrans	Definitief

Distributielijst

Versie	Datum	Ontvanger	Email
0.1	19 dec. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl
1.0	24 dec. 14	Bernhard van der Linde	Bernhard.vanderlinde@adts.nl
		Rick Hoevenaar	Rick.Hoevenaar@adts.nl

Relevante documenten

Versie	Datum	Auteur	Document
1.0		Maurice Rutenfrans	Plan van aanpak
1.0		Maurice Rutenfrans	Onderzoeksplan
1.0		Maurice Rutenfrans	Onderzoeksrapport
1.0		Maurice Rutenfrans	Business case
1.0		Maurice Rutenfrans	Ontwerprapport

Voorwoord

In het kader van mijn opleiding Technische Informatica aan de Haagse Hogeschool ben ik werkzaam bij ADTS ICT B.V. Voor u ligt het testrapport dat onderdeel uitmaakt van mijn afstudeerstage, die plaats vindt van 25 augustus 2014 tot 9 januari 2015.

Dit testrapport zal worden opgeleverd aan Bernhard van der Linde, directeur van ADTS ICT B.V. Het zal ook beschikbaar zijn voor een ieder die geïnteresseerd is en daartoe bevoegd is.

Rotterdam, december 2014
Maurice Rutenfrans

Inhoudsopgave

1. Inleiding

In dit document staat het testrapport dat is uitgevoerd voor deze afstudeerstage. Het testrapport is een ingevuld testplan. Alle checklists zijn uitgevoerd en getest volgens de methode die is beschreven in het testplan. Naast het afvinken van de scenario's zijn er bij de tests die een andere uitvoer hadden ook aantekeningen gemaakt met de opmerkingen van de tester.

2. Checklists

Checklist 1: Point tot point

Met deze checklist worden de volgende eisen getest:

- Sollicitatie gesprek

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De EX60's zijn opgestart. • Hoofdschermen worden weergegeven.	**1.** **Van Delft naar Qatar bellen, om een sollicitatie gesprek te houden.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Qatar Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen.	#1. Er wordt een overzicht van contacten weergegeven. Na het maken van een keuze wordt het contact gebeld.	✓	
		#2. Op de EX60 in Qatar neemt de tester op door op "Accept" te klikken.	#2. Na het accepteren wordt de point to point videoconferentie gestart.	✓	
• Hoofdschermen worden weergegeven.	**2.** **Van Delft naar Singapore bellen, om een sollicitatie gesprek te houden.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Singapore Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen.	#1. Er wordt een overzicht van contacten weergegeven. Na het maken van een keuze wordt het contact gebeld.	✓	
		#2. Op de EX60 in Singapore neemt de tester op door op "Accept" te klikken.	#2. Na het accepteren wordt de point to point videoconferentie gestart.	✓	

Checklist 2: Point to multipoint (1)

Met deze checklist worden de volgende eisen getest:

- Maandag ochtend meeting
- 3 Locaties
- 4 Locaties
- >4 Locaties

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven.	**1. Videoconferentie met drie locaties: Delft, Rotterdam en Qatar.**	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Rotterdam Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de SX20 in Rotterdam neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Rotterdam.	✓	
		#2. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Qatar Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de EX60 in Qatar neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to multipoint videoconferentie gestart, tussen Delft, Rotterdam en Qatar.	✓	

• Hoofdschermen worden weergegeven.	**2. Videoconferentie met vier locaties: Delft, Rotterdam, Qatar en Singapore.**	#1. De tester volgt de stappen uit het voorgaande test scenario van deze checklist.	Een point to multipoint videoconferentie wordt gestart, tussen Delft, Rotterdam en Qatar.	✓	
		#2. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Singapore Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de EX60 in Singapore neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt de point to multipoint videoconferentie uitgebreid naar Delft, Rotterdam, Qatar en Singapore.	✓	
• Hoofdschermen worden weergegeven.	**3. Videoconferentie met vijf locaties: Delft, Rotterdam, Qatar, Singapore en IP Phone.**	#1. De tester volgt de stappen uit het voorgaande test scenario’s van deze checklist.	Een point to multipoint videoconferentie wordt gestart, tussen Delft, Rotterdam, Qatar en Singapore.	✓	
		#2. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Maurice Rutenfrans” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de IP Phone neemt de tester op door op “Accept” te klikken.	De point to multipoint conferentie wordt in de wacht gezet en er wordt een nieuwe gestart tussen de SX20 en de IP Phone.	✗	Uit onderzoek was al gebleken dat dit niet mogelijk was.

Checklist 3: Point to multipoint (2)

Met deze checklist worden de volgende eisen getest:

- Maandag ochtend meeting
- 3 Locaties
- 4 Locaties
- >4 Locaties

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven.	**1. Videoconferentie met drie locaties: Delft, Rotterdam en Qatar.**	#1. Op de SX20 in Rotterdam klikt de tester op “Call” en zoekt in de Directory “Delft Meetingroom 2” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de SX20 in Delft neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Rotterdam.	✓	
		#2. Op de EX60 in Qatar klikt de tester op “Contacts” en zoekt “Delft Meetingroom 2” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de SX20 in Delft neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to multipoint videoconferentie gestart, tussen Delft, Rotterdam en Qatar.	✓	
• Hoofdschermen worden	**2. Videoconferentie met vier locaties: Delft,**	#1. De tester volgt de stappen uit het voorgaande test	Een point to multipoint videoconferentie wordt gestart, tussen Delft,	✓	

weergegeven.	**Rotterdam, Qatar en Singapore.**	scenario van deze checklist.	Rotterdam en Qatar.		
		#2. Op de EX60 in Singapore klikt de tester op “Contacts” en zoekt “Delft Meetingroom 2” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de SX20 in Delft neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt de point to multipoint videoconferentie uitgebreid naar Delft, Rotterdam, Qatar en Singapore.	✓	
• Hoofdschermen worden weergegeven.	**3. Videoconferentie met vijf locaties: Delft, Rotterdam, Qatar en Singapore.**	#1. De tester volgt de stappen uit het voorgaande test scenario’s van deze checklist.	Een point to multipoint videoconferentie wordt gestart, tussen Delft, Rotterdam, Qatar en Singapore.	✓	
		#2. Op de IP Phone van Maurice Rutenfrans belt de tester naar het nummer 1004 om mee te doen aan de videoconferentie. Op de SX20 in Delft neemt de tester op door op “Accept” te klikken	De point to multipoint conferentie wordt in de wacht gezet en er wordt een nieuwe gestart tussen de SX20 en de IP Phone.	✗	Uit onderzoek was al gebleken dat dit niet mogelijk was.

Checklist 4: Deelnemers

Met deze checklist worden de volgende eisen getest:

- Qatar en Singapore, 2 deelnemers
- Delft en Rotterdam, 75 deelnemers

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven.	**1. Videoconferentie met twee EX60's, met elk twee deelnemers.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Qatar Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen. Op de EX60 in Qatar neemt de tester op door op "Accept" te klikken. Vervolgens wordt er 10min vergaderd om een goed beeld te geven.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Qatar. Tijdens de 10min durende vergadering zal er voor alle deelnemers duidelijk beeld en geluid geleverd worden.	✓	
• Hoofdschermen worden weergegeven.	**2. Videoconferentie met twee SX20's, met elk 75 deelnemers.**	#1. Op de SX20 in Delft klikt de tester op "Call" en zoekt in de Directory "Rotterdam Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen. Op de SX20 in Rotterdam neemt de tester op door op "Accept" te klikken. Vervolgens wordt er 10min vergaderd om een goed beeld te geven.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Rotterdam. Tijdens de 10min durende vergadering zal er voor alle deelnemers duidelijk beeld en geluid geleverd worden.	✗	Er waren maar 19 personen voor de test aanwezig, maar het resultaat voor deze 19 was positief.

Checklist 5: Content sharing (1).

Met deze checklist worden de volgende eisen getest op de EX60:

- PowerPoint delen
- Detailtekeningen delen

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven. • Laptop/desktop aangesloten met PowerPoint klaar om te gebruiken.	**1. Videoconferentie met twee EX60's, waarbij een PowerPoint presentatie gedeeld wordt.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Qatar Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen. Op de EX60 in Qatar neemt de tester op door op "Accept" te klikken. Vervolgens klikt de tester op "View PC" en "Start Presenting".	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Qatar. Vervolgens wordt de PowerPoint gedeeld in combinatie met beeld.	✓	
• Hoofdschermen worden weergegeven. • Laptop/desktop aangesloten met detailtekening klaar om te gebruiken.	**2. Videoconferentie met twee EX60's, waarbij een detailtekening gedeeld wordt.**	#1. Op de EX60 in Delft klikt de tester op "Contacts" en zoekt "Qatar Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen. Op de EX60 in Qatar neemt de tester op door op "Accept" te klikken. Vervolgens klikt de	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Qatar. Vervolgens wordt de detailtekening gedeeld in combinatie met beeld.	✓	

		tester op “View PC” en “Start Presenting”.			

Checklist 6: Content sharing (2).

Met deze checklist worden de volgende eisen getest op de SX20:

- PowerPoint delen
- Detailtekeningen delen

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven. • Laptop/desktop aangesloten met PowerPoint klaar om te gebruiken	**1. Videoconferentie met twee EX60’s, waarbij een PowerPoint presentatie gedeeld wordt.**	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Rotterdam Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de SX20 in Rotterdam neemt de tester op door op “Accept” te klikken. Vervolgens klikt de tester op “Share” om het bureaublad te delen.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Rotterdam. Vervolgens wordt de PowerPoint gedeeld in combinatie met beeld.	✓	
• Hoofdschermen worden weergegeven. • Laptop/desktop aangesloten met detailtekening klaar om te gebruiken.	**2. Videoconferentie met twee EX60’s, waarbij een detailtekening gedeeld wordt.**	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Rotterdam Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Rotterdam. Vervolgens wordt de detailtekening gedeeld in combinatie met beeld	✓	

		Op de SX20 in Rotterdam neemt de tester op door op “Accept” te klikken. Vervolgens klikt de tester op “Share” om het bureaublad te delen.			

Checklist 7: Jabber

Met deze checklist worden de volgende eisen getest:

- Jabber integratie

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven. • Jabber opgestart.	**1. Videoconferentie tussen EX60 en een jabber client**	#1. De tester belt via de jabber client naar “Delft Meetingroom 1”. Op de EX60 in Delft neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen de jabber client en de EX60 in delft.	✓	
• Hoofdschermen worden weergegeven. • Jabber opgestart.	**2. Videoconferentie tussen SX20 en twee jabber clients**	#1. De tester belt via de jabber client naar “Delft Meetingroom 2”. Op de SX20 in Delft neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen de jabber client en de SX20in delft.	✓	

Checklist 8: Lokale internetverbinding

Met deze checklist worden de volgende eisen getest:

- Mogelijk over een lokale internetverbinding.
- (tijdens de videoconferentie zal ook een file transfer plaats vinden om de impact te analyseren)

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven. • Bandbreedte ingesteld	**1.** Videoconferentie tussen Delft en Singapore met een bandbreedte van 4608 kbps.	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Singapore Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de EX60 in Singapore neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Singapore. De kwaliteit van de conferentie zal goed zijn.	✓	
• Hoofdschermen worden weergegeven. • Bandbreedte ingesteld	**2.** Videoconferentie tussen Delft en Singapore met een bandbreedte van 2048 kbps	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Singapore Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen. Op de EX60 in Singapore neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Singapore. De kwaliteit van de conferentie zal voldoende zijn.	✓	
• Hoofdschermen worden weergegeven. • Bandbreedte	**3.** Videoconferentie tussen Delft en Singapore met een	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Singapore	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Singapore.	✗	Kwaliteit onacceptabel als er gelijktijdig een file transfer plaatsvindt.

ingesteld	bandbreedte van 1024 kbps	Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen. Op de EX60 in Singapore neemt de tester op door op "Accept" te klikken.	De kwaliteit van de conferentie zal matig zijn.		
• Hoofdschermen worden weergegeven. • Bandbreedte ingesteld	**4.** Videoconferentie tussen Delft en Singapore met een bandbreedte van 512 kbps	#1. Op de SX20 in Delft klikt de tester op "Call" en zoekt in de Directory "Singapore Meetingroom 1" op. Vervolgens selecteert hij deze en klikt op "Call" om hem te bellen. Op de EX60 in Singapore neemt de tester op door op "Accept" te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Singapore. De kwaliteit van de conferentie zal onvoldoende zijn	✗	Kwaliteit onacceptabel.

Checklist 9: gebruiksvriendelijkheid

Met deze checklist worden de volgende eisen getest:

- Gebruiksvriendelijkheid.

Pre condities	Test scenario	Beschrijving	Uitvoervoorspelling	Werkelijke uitvoer	Opmerkingen
• De systemen zijn opgestart. • Hoofdschermen worden weergegeven.	**1.** 10 willekeurige personen laten video conferencen met de EX60.	#1. Op de EX60 in Delft klikken de willekeurige personen "Contacts" en zoeken "Qatar Meetingroom 1" op. Vervolgens selecteert zij deze en klikken op "Call" om hem te bellen.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Qatar.	✓	

		Op de EX60 in Qatar neemt de tester op door op “Accept” te klikken.			
• Hoofdschermen worden weergegeven.	**2.** 10 willekeurige personen laten video conferencen met de SX20.	#1. Op de SX20 in Delft klikt de tester op “Call” en zoekt in de Directory “Rotterdam Meetingroom 1” op. Vervolgens selecteert hij deze en klikt op “Call” om hem te bellen Op de SX20 in Rotterdam neemt de tester op door op “Accept” te klikken.	Na het accepteren wordt een point to point videoconferentie gestart, tussen Delft en Rotterdam		
• Video conferentie is bezig • Systemen zijn gekoppeld met laptop/desktop.	**3.** 10 willekeurige personen content laten sharen.	#1. (EX60) De willekeurige personen klikken op “View PC” en “Start Presenting”. #2. (SX20) De willekeurige personen klikken op “Share” om het bureaublad te delen.	Het bureaublad wordt gedeeld door de willekeurige gebruikers.	✓	
• Video conferentie is bezig	**4.** 10 willekeurige personen de video call laten afsluiten.	#1. Zowel op de EX60 als de SX20 wordt er door de willekeurige personen op “End” gedrukt.	De videoconferentie eindigt door de willekeurige gebruikers.	✓	
• Hoofdschermen worden weergegeven.	**5.** 10 willekeurige personen de video call laten opnemen.	#1. Zowel op de EX60 als de SX20 wordt er door de willekeurige personen op “Accept” gedrukt.	De videoconferentie start door de willekeurige gebruikers.	✓	

3. Conclusie

Uit het testrapport kunnen we concluderen dat de proof of concept aan alle eisen van Ampelmann Operations voldoet, op één enkele na. De eis die niet goed is gekeurd, is het voldoen aan 75 deelnemers. Helaas kon deze eis niet volledig getest worden, omdat er maar 19 deelnemers waren in plaats van 75. Hierdoor is het niet met zekerheid te zeggen of de SX20 ook daadwerkelijk aan deze eis voldoet.

Overige tests die zijn afgekeurd waren al voorspeld dat deze niet goed uitgevoerd konden worden. Zo is er getest of er meer dan vier sites gelijktijdig met elkaar konden video conferencen, maar uit het onderzoek was al gebleken dat dit er maximaal vier waren en niet kon. Bij het testen van de lokale internet verbinding is bewust gekozen om de bandbreedte te verminderen. Hierdoor is het inzichtelijk geworden wanneer deze onvoldoende is en slechte kwaliteit levert.