Oberman
Telecom
Management
Consultants bv

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

VoIP, consequenties voor de "alles in één" infrastructuur

Auteurs: ing V.M. Kroon, ing A. Molenaar, ir M.R. Oberman

De ontwikkeling van datanetwerken is al heel wat jaren gaande en nog steeds volop in beweging. Zoals met veel nieuwe technologieën kenmerkt de ontwikkelingsperiode zich door bewegingen rond de hoofdas, die in de loop van de tijd, uiteindelijk convergeren naar meer uniforme, gestandaardiseerde oplossingen.

Hoewel VoIP de opmaat is naar de "alles in één" infrastructuur ("IP maat"), is het niet nog lang niet zo ver. In algemene zin zijn het de volgende punten die de ontwikkeling van de VoIP infrastructuur hinderen:

1. De datacommunicatie-infrastructuur is vaak niet op orde in het licht van de eisen die VoIP daaraan stelt.
2. Er zijn veel aansluitingen die verder weg zijn dan 100 meter van een SER.
3. Er zijn veel telefoonaansluitingen op plaatsen waar geen (data) IP aansluiting noodzakelijk is; dit vergt dus een ethernetpoort, en mogelijk nieuwe bekabeling, voor alleen een telefoontoestel.
4. Er zijn nog veel analoge aansluitingen t.b.v. faxen en modems.
5. De uitval van spraak en data in conjunctie leidt tot grotere bedrijfsschade dan uitval van spraak en data afzonderlijk.
6. Er zijn veel draadloze toestellen nodig.

Niettemin zal VoIP de basis zijn voor elk modern spraak communicatie netwerk zijn, of het nu om de draadgebonden communicatie gaat of om de draadloze communicatie. Zelfs de huidige GSM providers bereiden een overgang naar IP voor.
VoIP stelt een aantal andere of soms aanvullende eisen aan de datacommunicatie-infrastructuur. Dat zijn onder andere:

1. Lokale netwerken moeten switched zijn.
2. Voldoende basis toegangsnelheid en dan ook nog full duplex.
3. Passend opstartprotocol om de VoIP toestellen te initialiseren over het (hele) netwerk heen en met voldoende capaciteit voor een restart.
4. Scheiding van verschillende verkeerstromen bv op basis van VLAN en IP-VPN.
5. CoS/QoS configuratie (end to end) om te zorgen dat de realtime eisen van de verbinding voldoende zijn.
6. Een korte tijdvertraging in het transportpad en een minimale variatie daarop.
7. Er mogen geen (spraak-)pakketten verloren gaan.
8. VoIP moet in het bestaande IP adresschema ingepast worden.

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

De integratie van spraak en data stelt in feite eisen aan de kwaliteit en performance van de datacommunicatie-infrastructuur. Dit komt niet alleen door de stringentere tijdeisen, die VoIP aan een datacommunicatie-infrastructuur stelt, maar ook de behoefte aan een hoge uptime. Storingen (ongepland down) hebben een zwaardere impact op het functioneren van een organisatie, wanneer door de toename van netwerkgebonden applicaties bedrijfsprocessen bij storingen niet meer functioneren. Gepland down betekent een (gecontroleerde limitering aan de communicatiemogelijkheden tijdens bijvoorbeeld aanpassingen, upgrading en andere netwerkactiviteiten die de gebruikelijke communicatie belemmeren.

In het bijzonder geldt voor upgrading van de communicatie-infrastructuur dat er een aantal eisen gesteld moet worden, met als strekking om de gepland down periode te minimaliseren. Het gaat dan enerzijds om continuïteit van de service en anderzijds het laden en activeren van de nieuwe software. Er is bijvoorbeeld een aantal systemen, waarbij de hardware redundancy tijdelijk opgeheven kan worden, waardoor het systeem in twee enkelvoudige systemen te splitsen is. Op die wijze is het ene deel aan te passen, om te schakelen en te testen, daarna kan afhankelijk van de resultaten het andere deel aangepast worden en weer samengevoegd worden tot een redundant systeem. De praktijk heeft inmiddels uitgewezen dat met VoIP systemen er betere redundancy concepten en oplossingen mogelijk zijn dan met de klassieke PABX systemen. Daarnaast dragen die concepten niet direct bij in een kostenverhoging(!), maar wel in een kostenreductie voor de leverancier. Een storing in een redundant systeemcomponent kan namelijk beschouwd worden als een minor storing indien de dienstverlening niet verminderd wordt. Het is dan in feite iets als “intelligent opgeslagen” spares on site van de klant.
De ervaring heeft geleerd dat dit soort constructies erg nuttig zijn voor een verhoging van de uptime en daarmee de continuïteit voor de geïntegreerde dienstverlening.

Ter overdenking is de praktisch-technische keuze:

- kiezen voor een technisch geïntegreerd redundant systeem
- twee enkelvoudige systemen, die elkaar bewaken ten behoeve van de redundancy.

In het laatste geval is er ook een zekere bescherming mogelijk tegen lokale fysieke calamiteiten. De systemen hoeven dan namelijk niet naast elkaar geplaatst te worden, maar kunnen ook op enige afstand van elkaar functioneren.

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

Los van de mogelijkheden van een IP netwerk, zal er een keuze gemaakt moeten worden voor de andere IP diensten die een netwerk kan of soms moet leveren aan een VoIP service op een netwerk. Dat kan zijn tijdinformatie (synchronisatie tbv call detail record, of gespreksregistratie over het netwerk heen), maar ook de DHCP (Dynamic Host Configuration Protocol) werking. Geen DHCP betekent geen kiestoon, geen email etc., kortom, een cruciale service in een IP netwerk. Hetzelfde geldt voor DNS (Domain Name System). Daarnaast komen er direct ook andere vragen op dit punt naar voren. Wordt gebruik gemaakt van de DHCP server uit het datanetwerk, of die van de VoIP dienst. Hoe zit het met het vernieuwen van het IP adres door het IP toestel. Is er dan nog communicatie mogelijk tussen de PC en het IP netwerk, terwijl de toestel IP switch er nog tussen geschakeld is. Dit en andere vragen dienen voor de implementatie beantwoord te zijn, om te komen tot een ongestoorde werking van de VoIP dienstverlening over het datanetwerk.

VoIP en VLAN's

Met VLAN technologie kunnen netwerken op een (layer 2) switch logisch van elkaar gescheiden worden. Dit betekent dat men op een enkele switch, of een samenstelling daarvan, verschillende netwerken kan definiëren zonder dat er sprake is van onderling verkeer. Groot voordeel van een VLAN is dus dat men de fysieke apparatuur kan inzetten voor diverse netwerken; anders gezegd, een switch wordt virtueel in stukken opgedeeld en elk deel bedient een apart netwerk. Net als bij gescheiden netwerken is het mogelijk om tussen deze delen te routeren. Bij gebruik van een layer 3 switch (met inherente routering) is dit op een eenvoudige wijze te bewerkstelligen.
Het koppelen van een host aan een VLAN kan op 2 manieren gerealiseerd worden. De ene manier is om in het netwerk, de switches, de VLAN's te definiëren en toe te kennen aan switchpoorten. De aangesloten host sluit daarmee met zijn fysieke connectie aan op het VLAN dat op de poort gedefinieerd is. De andere manier is om de host te laten bepalen met welk VLAN connectie nodig is d.m.v. 802.1q tagging. Hiermee wordt de keuze aan de randapparatuur over gelaten.

Er zijn verscheidene redenen om VLAN's in een netwerk te implementeren. Zoals gezegd is het kostenaspect er één van. Met virtuele netwerken is het mogelijk om op switches en verbindingen te besparen. Naast de hardwarekosten bespaart dit natuurlijk ook op onderhoudscontracten, rack-ruimte, energie en airco.
Maar waarom zou men een netwerk in verschillende delen willen opsplitsen? Twee belangrijke redenen zijn het segmenteren van het netwerkverkeer (op grond waarvan dan ook) en beveiliging.

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

Om met de tweede reden te beginnen; de ketting is zo sterk als de zwakste schakel. Zowel met de techniek als met het beheer, het configureren, kunnen zich problemen voordoen waarmee de beoogde scheiding en daarmee beveiliging geminimaliseerd wordt. Zo kan een fout in het besturingssysteem van de switch er voor zorgen dat kwaadwillenden de configuratie veranderen en daarmee de zorgvuldig opgezette en geïmplementeerde beveiliging om zeep helpt. Maar ook niet bedoelde en dus niet opzettelijk gemaakte configuratiefouten kunnen voor problemen zorgen. Goede opleiding van beheerders in combinatie met configuratiebeleid en onderhoud op de switches, door implementatie van nieuwe releases, zijn essentieel om deze risico's te reduceren. Indien de omgeving dit vereist kan het aantal maatregelen om de scheiding tussen netwerken op te voeren nog uitgebreid worden. Hierbij kan gedacht worden aan het gebruik van routers, firewall's, virusscanners en intrusion detection systems. Deze systemen werken op de hogere lagen van het communicatiemodel en hiermee wordt op andere gronden dan alleen adresinformatie besloten of verkeer doorgestuurd of geblokkeerd moet worden.

Netwerkverkeer kan ook gesegmenteerd worden om redenen van beschikbaarheid en performance. Indien zich problemen voordoen in een 'plat' netwerk dan kan het gehele netwerk plat gaan. Indien zich problemen voordoen in een, b.v. door VLAN's, gesegmenteerd netwerk dan zal meestal een gedeelte van het (V)LAN niet of minder beschikbaar zijn. Dit is dan het gedeelte van het netwerk waarin zich het probleem manifesteert. Problematisch verkeer is namelijk in de meeste gevallen van een type dat niet gerouteerd wordt naar andere delen van het netwerk. Uiteraard kan verkeer alleen op een ander VLAN komen als er routering tussen de VLAN's is geïmplementeerd. Naast segmentering zijn er ook meer directe functies gericht op beveiliging en toegangscontrole. Eén ervan is de standaard IEEE *802.1x* Die gaat over de authenticatie van het aangesloten apparaat. Dit aangevuld met multi-supplicant maakt 802.1x dat het individuele aangesloten apparaat op een switchpoort herkend wordt door het beheersysteem. Is het de PC of is het het VoIP apparaat? Op basis van deze herkenning kunnen (toegangs)rechten gegeven worden aan het aangesloten individuele apparaat.

Het indelen van een netwerk in VLAN's is technisch gezien simpel. Toch is het raadzaam om pas aan deze exercitie te beginnen nadat er goed over nagedacht is. Als eerste moeten een aantal vragen beantwoord worden, met als meest essentiële vraag: "waarom segmentatie moet plaatsvinden". Is het alleen te doen om foutisolatie bij problemen of gaat het om beveiligingsmaatregelen of nog andere invalshoeken.

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

De verschillende vormen hebben ieder hun eigen benadering. Hierbij is het van belang om een goed inzicht te hebben in alle verkeersstromen. Tevens moet bij de opzet ook bedacht worden dat het gebruik van VLAN's prima is maar dat het aantal niet meer dan strikt noodzakelijk moet zijn. Dit komt omdat de VLAN's beheer vergen, al is maar de administratie. Deze administratie welke belangrijk is, krijgt vaak onvoldoende aandacht, wat techneuten geheel eigen is. Ook een goed doordacht en toekomstvast IP adresplan is onlosmakelijk onderdeel van de opzet van het segmentatieplan.

De eisen die VoIP stelt aan het datanetwerk onderdeel maken deel uit van de opzet en de indeling van de datacommunicatie-infrastructuur. Immers IP transport van voice, maar ook video, moet isochroon van karakter zijn. Voor de meeste andere datacom toepassingen is dit niet nodig en daarom moeten er voorzorgsmaatregelen getroffen worden. Deze kunnen geïmplementeerd worden via QoS (Quality of Service) met 802.1p en q, en 802.11e aanvullingen voor wireless LAN's.

IP?
De datacommunicatie-infrastructuur is geordend door het gebruik van IP adressen. Elk aangesloten systeem maakt gebruik van een IP-adres. Deze kunnen statisch of dynamisch zijn. Ze zijn statisch als ze eenmalig toegewezen worden, of dynamisch wanneer er sprake is van beperkte houdbaarheid. Wanneer de houdbaarheidsdatum verlopen is, of in de aanloop daar naar toe, dan zal er om een nieuw IP adres gevraagd worden.
Er zijn voor deze twee adresseringsmogelijkheden verschillen, die hun invloed hebben op de VoIP dienstverlening. Om hier meer duidelijkheid in te krijgen zal eerst ingegaan worden op de globale werking van het adrestoewijzings-mechanisme. Hierbij wordt er vanuit gegaan dat de VoIP toestellen in een eigen VLAN geplaatst zijn,bijvoorbeeld vanwege beveiligingsaspecten.

DHCP werking
De volgende stappen zijn te onderscheiden:

1. Een VoIP toestel vraagt een adres aan op een switchpoort waarop eventueel ook een PC aangesloten is. Deze PC bevindt zich in een VLAN die niet dezelfde is als waar het VoIP toestel in geplaatst moet worden.
2. De DHCP server moet aangeven waar het toestel zijn echte IP adres op moet halen, dus het VoIP VLAN met de bijbehorende DHCP server voor dat VLAN. Sommige netwerksystemen geven op basis van een MAC adres het juiste IP- De DHCP server moet aangeven in welk VLAN het toestel zijn echte IP adres op moet halen.

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

3. Daar haalt het toestel zijn IP adres op. Vervolgens moet het eerste IP adres (in het PC VLAN) vrijgegeven. Bij initiële aanmelding zal het toestel als eerste de meest recente firmware ophalen en laden.

Voor kleinschalige omgevingen is de IP adrestoewijzing over het algemeen geen issue. Voor de grootschalige omgevingen moet hier echter wel goed over nagedacht worden.

Quality of Service (QoS)
QoS biedt de mogelijkheid om binnen de datacom-infrastructuur bepaalde vertragingstijden te garanderen. Spraak is een communicatietoepassing met vrij stringente eisen aan de tijd performance parameters van de datacom infrastructuur. De belangrijkste zaken die de kwaliteit van spraakcommunicatie aantasten zijn:

- Packet loss. De maximale packet loss moet onder 1% blijven. Als pakketten verloren gaan, dan heeft het vanwege het real-time karakter van spraak geen zin om retransmissies te doen. Voor datatoepassingen is retransmissie essentieel.
- Vertraging (delay). Op zich heeft dit geen invloed op de kwaliteit van het geluid, maar wordt wel storend bij het voeren van een conversatie, als deze groter wordt dan 150 msec.
- Variatie in de vertraging. Deze gaat wel ten koste van de geluidskwaliteit en moet daarom kleiner zijn dan 20 msec.

QoS moet deze invloeden minimaliseren, de oorzaken en remedies zijn:
Oorzaken:

- Te zware (tijdelijke) belasting van het netwerk leidt tot verlies van pakketten.
- Pakketten die te lang onderweg zijn, gaan verloren.
- De transporttijd van pakketten varieert door de variërende belasting van het netwerk. Deze variatie zit in belastingsverschillen op verbindingen en in switches en routers.

Remedie:

- Admission control mechanismen. Deze voorkomen dat nieuw verkeer aan het netwerk wordt aangeboden als de grens van de transportcapaciteit bereikt is. Binnen een LAN wordt vaak gewerkt met CoS (Class of Service). Deze methode geeft geen garantie dat spraak met een max. vertraging wordt afgeleverd bij de bestemming, maar wel dat de een Class voorrang krijgt boven de andere.
- Beperking van het gebruik van codecs die meer bandbreedte gebruiken.
- Prioriteit geven aan pakketten met real-time informatie.

De Wingerd 4
3951 XK Maarn
tel: 0343 - 444301
e-mail oberman@otmc.nl

Conclusie

VoIP biedt nieuwe kansen in het kader van functionaliteiten en uptime. Wel zal het samenspel met de gemeenschappelijke drager, het datanetwerk, goed uitgeregeld moeten zijn. Dat kan soms tot aanpassingen leiden van de inrichting van het datanetwerk.