

Beschrijving toolset Netwerk/Protocol/Applicatie test

Datum 11 januari 2012
Auteur Louis de Wolff
Versie 1.0

Netwerk evaluatie tools

Inleiding

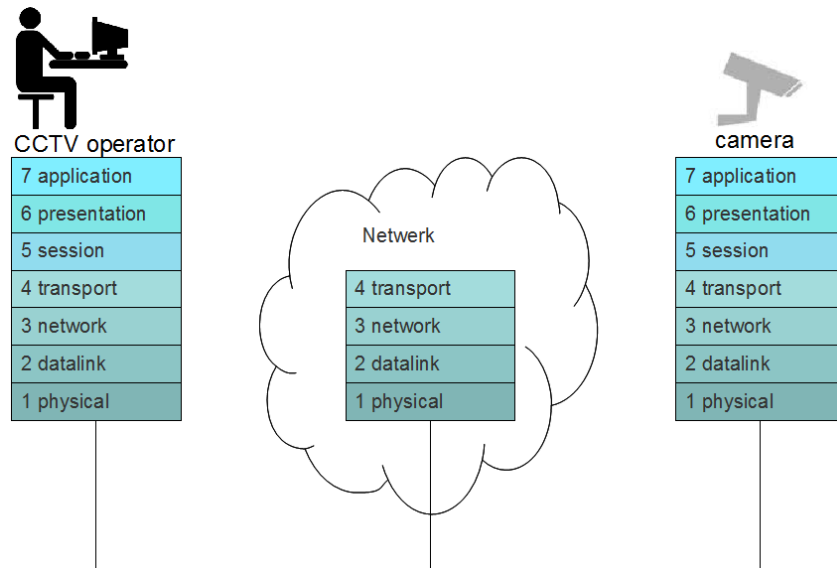
In een pakket geschakelde netwerk gebeurt de communicatie d.m.v. communicatieprotocollen. Deze communicatieprotocollen zijn meestal toegespitst op een bepaalde toepassing en de implementatie ervan kan per fabrikant variëren.

Deze communicatieprotocollen hebben bepaalde grenzen waarbinnen ze functioneren of waarbinnen de bovenliggende applicatie kan functioneren. Deze grenzen kunnen liggen in bandbreedte, netwerk vertraging, volgordelijkheid van de pakketten in aankomst, verlies van pakketten, enz. Wanneer het netwerk binnen deze grenzen blijft zal de applicatie functioneren. Wanneer het netwerk echter buiten deze grenzen komt, kan de applicatie problemen gaan geven. Dit kan zich uiten door verminderde performance; onvoorspelbaar gedrag van de applicatie, of de meest vervelende complicatie 'vastlopen'.

Als in de praktijk een probleem met een applicatie optreedt blijkt dit vaak lastig op te lossen. Dit komt doordat netwerk problemen over het algemeen niet continue zijn. Ze treden soms op als gevolg van bijvoorbeeld congestie in het netwerk. Dit maakt dat dit soort problemen wel worden waargenomen, maar slecht reproduceerbaar zijn. Bij het oplossing van dergelijke 'vage' of sporadische problemen wordt daarom vaak naar paardenmiddelen gegrepen zoals het substantieel verhogen van de bandbreedte (in het geval van een verbinding bij een provider) of het uitwisselen of toevoegen van apparatuur. De hoop is dat dit dan het probleem verhelpt, maar feitelijk zijn dergelijke oplossingen meer 'trial and error' dan wijsheid.

Probleem analyse

Wanneer de communicatie van een applicatie over een netwerk gestructureerd wordt geanalyseerd is het goed om te beseffen dat de communicatie over het algemeen volgende de diverse lagen van het OSI model verloopt. Iedere laag kent zijn eigen communicatieprotocollen en daarmee specifieke kenmerken.



In de bovenstaande figuur is de bediening en het uitkijken van een CCTV camera als voorbeeld applicatie getoond. Het netwerk heeft invloed op de eerste vier lagen van het OSI model. Daarmee lijkt het alsof voor de bovenliggende lagen het netwerk transparant is. Dit is echter niet waar indien het netwerk niet binnen de eisen blijft die voor de bovenliggende lagen nodig zijn. Vreemd genoeg zijn deze eisen niet altijd bekend of indien wel bekend zijn zij meestal niet opgenomen in de technische documentatie.

Wat ook meespeelt is dat bij veel applicaties geldt dat apparatuur of software van verschillende leveranciers wordt gebruikt. Hoewel protocollen over het algemeen gestandaardiseerd zijn, zijn er toch verschillen in de implementatie hiervan.

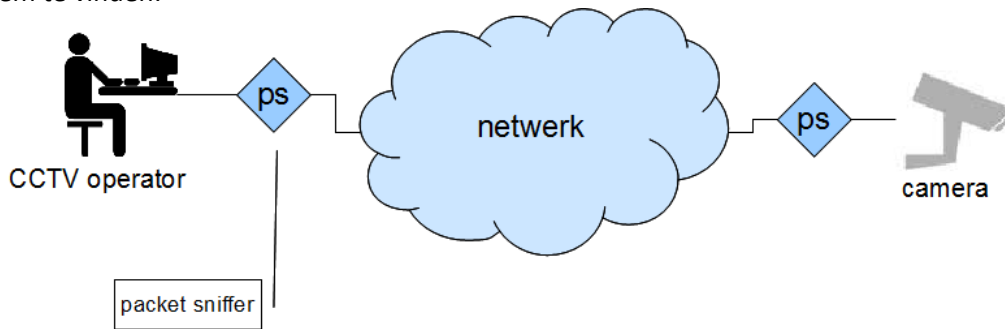
Benodigde gereedschappen voor systematische analyse

Voor een systematische analyse van netwerkproblemen zijn de volgende universele gereedschappen nodig:

- | | |
|--------------------|--|
| Protocol analyser | Dit is een tool waarmee pakketten en protocollen geanalyseerd kunnen worden. Voor iedere laag van het OSI model worden de specifieke details weergegeven zodat duidelijk wordt wat de bedoeling van het protocol is. |
| Packet sniffer | Dit is opname software waarmee dataverkeer kan worden opgenomen voor latere analyse. Op een packet sniffer kunnen filters worden ingesteld die ervoor zorgen dat alleen bepaalde pakketten of reeksen van pakketten worden opgenomen. Hierdoor is het mogelijk om in een grote hoeveelheid verkeer toch over langere tijd relevante metingen te verrichten. |
| Packet generator | Dit is software waarmee willekeurige pakketten gegenereerd kunnen worden. Hierdoor is het mogelijk om specifieke pakketten of reeksen van pakketten over een netwerk te sturen en op die manier netwerk gedrag voor een bepaald type verkeer inzichtelijk te maken. |
| Packet manipulator | Dit is software die de pakketten in een netwerk ongemerkt kan manipuleren. Dit is vooral handig om vast te stellen of een protocol voldoende beveiligd is tegen manipulatie. |
| Network simulator | Dit is een router waarbij ongewenst netwerk gedrag ingesteld kan worden. In de praktijk is ongewenst netwerk gedrag lastig te simuleren omdat netwerk elementen dit soort gedrag pas bij congestie gaan vertonen. Simulatie van dit gedrag maakt dat applicaties in een geconditioneerde omgeving met het meest uiteenlopende netwerk gedrag kunnen worden geconfronteerd. |

Het overnemen en vermenigvuldigen van (delen van) dit document is slechts geoorloofd na schriftelijke toestemming van GoudsConcept

Deze tools worden als volgt ingezet om een systematische analyse van een netwerk-applicatie probleem te vinden:

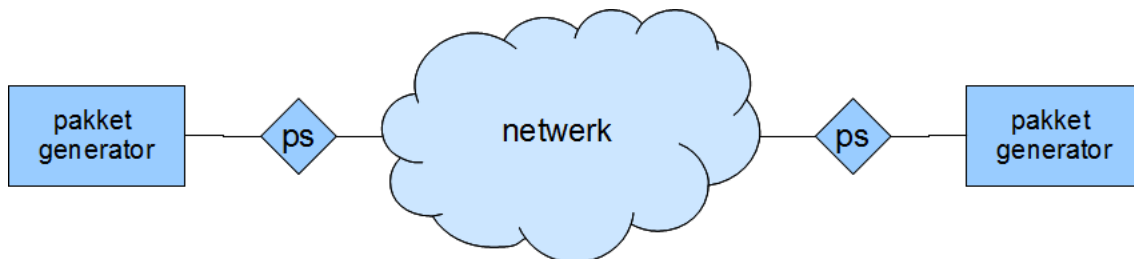


Stap 1 luisteren/opnemen

De eerste stap in analyse is het opnemen van het verkeer om te weten welke protocollen precies gebruikt worden en welk karakter het verkeer heeft. (Denk hierbij aan burstvormig, pakketgrootte en de variatie daarin en dergelijke kenmerken).

Stap 2 simuleren

Nadat bekend is welke communicatie er plaats vindt, volgt stap 2 waarin dit verkeer gesimuleerd wordt. Met behulp van een pakketgenerator wordt het applicatie typische verkeer gesimuleerd. Het grote voordeel van simulatie is dat de diverse kenmerken van het verkeer voorspelbaar kunnen worden gegenereerd waardoor het gedrag van het netwerk zelf (hier weergegeven door een wolk) kan worden gemeten.



Door aan beide zijden van het netwerk een pakketgenerator en een packet sniffer te plaatsen kan het gedrag van het netwerk nauwkeurig op performance parameters (packet loss, latency, packet jitter, bandwidth) worden gemeten. Doordat het typische verkeerspatroon van de applicatie wordt gesimuleerd kan ook het netwerkgedrag bij dit type verkeer worden gemeten. Zaken als pakketgrootte, gebruikte protocol en burstvormigheid van het verkeer kunnen van grote invloed zijn op de netwerkperformance.

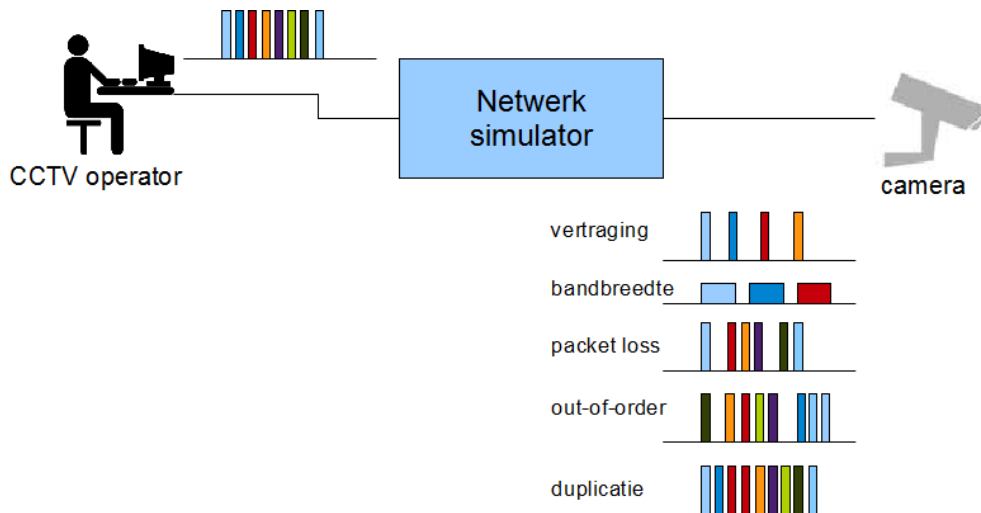
Door de opstelling over langere tijd te laten functioneren kan ook een beeld worden gekregen over de performance van een netwerk over de gemeten periode. Metingen van 24 uur of zelfs enkele dagen/weken zijn niet ongebruikelijk en kunnen soms heel verrassende inzichten geven.

Bij een meting die voor een VoIP verbinding werd gedaan was heel duidelijk wanneer het netwerk gebruikt werd door andere applicaties. De netwerk vertraging bereikte gedurende werktijden waardes tot 200msec terwijl dit onder 'normale' omstandigheden slechts enkele milliseconden was.

Stap 3 manipuleren

Naast dat het netwerk een bepaalde performance kan geven, zal de applicatie bepaalde eisen stellen aan de netwerkperformance. Vaak zijn deze eisen niet direct verwoord in de beschikbare documentatie en het komt ook regelmatig voor dat een leverancier zijn software hier eenvoudigweg niet op getest heeft. Dit geeft niet direct problemen zolang het netwerk maar binnen de tolerantie van de applicatie blijft. Om echter vast te stellen wat de netwerk tolerantie van de applicatie is, wordt de applicatie op een netwerk simulator aangesloten.

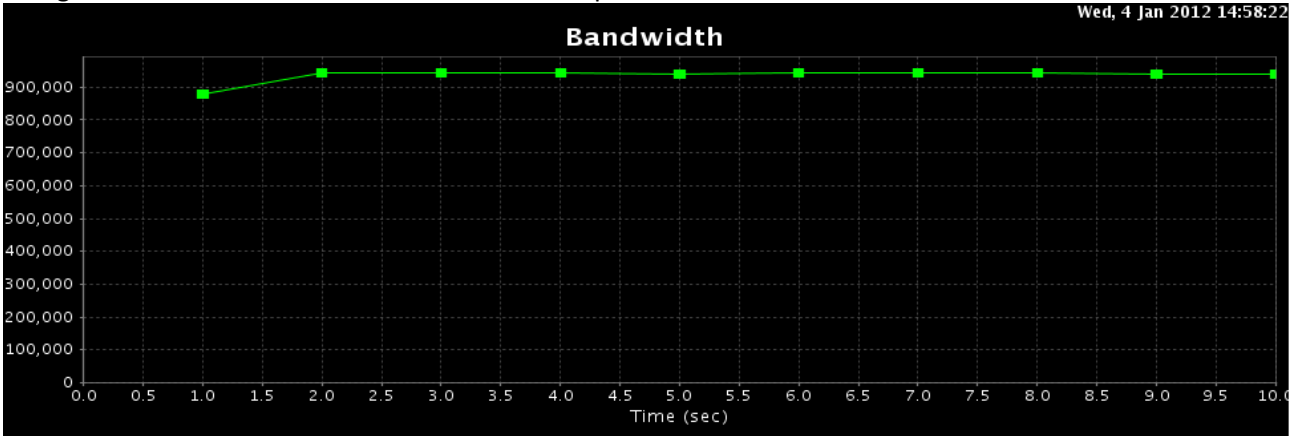
De netwerk simulator is vergelijkbaar met een router. Deze router is er echter op gemaakt om juist ongewenst netwerk gedrag te introduceren. Zo kan naar wens vertraging, jitter (variatie in pakket vertraging), out-of-order delivery, duplicatie, bandbreedtebeperking etc. worden ingesteld. Hierdoor is vast te stellen welke effect dit op de applicatie heeft en waar de grenzen van de applicatie precies liggen.



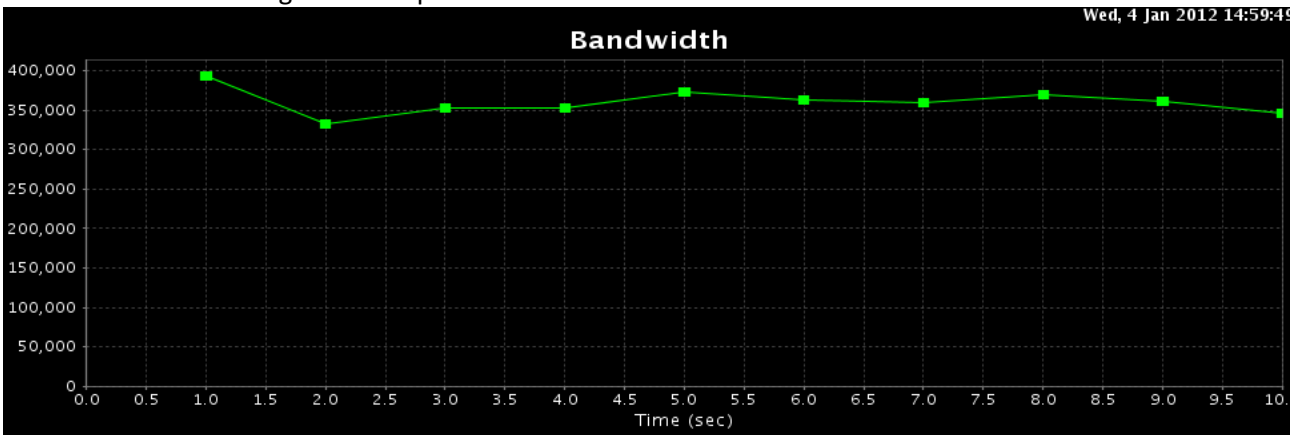
Enkele praktische voorbeelden

Enkele praktische voorbeelden van waargenomen netwerkgedrag:

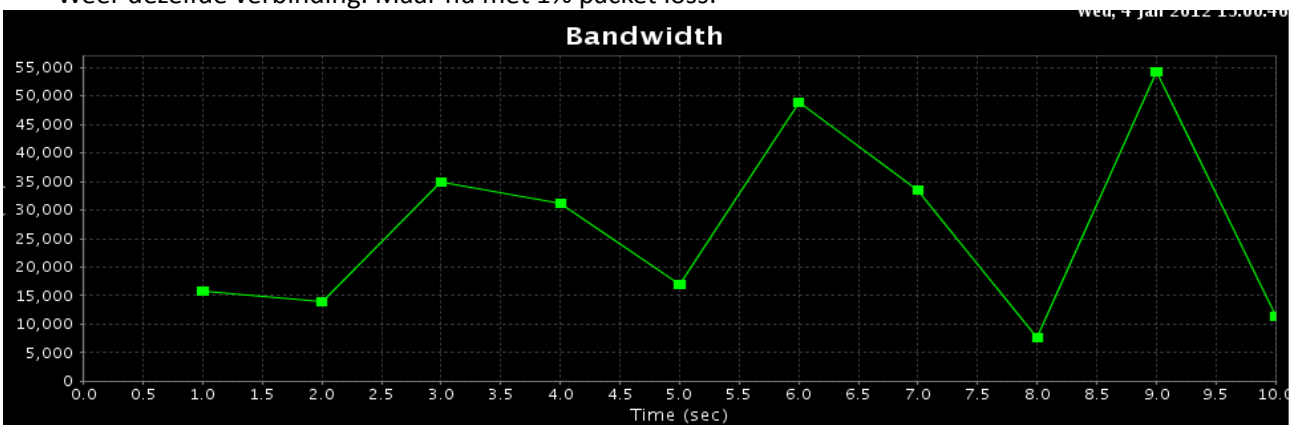
Een bandbreedtemeting van een 1Gbit/s verbinding zonder vertraging of packet loss en gebruikmakend van het TCP-IP communicatieprotocol:



Dezelfde verbinding met 1%% packet loss:



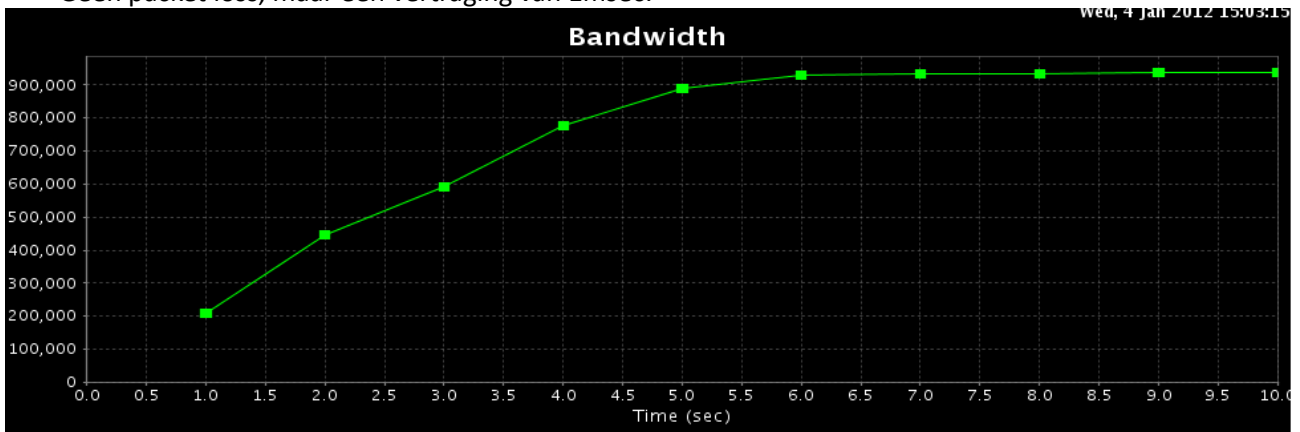
Weer dezelfde verbinding. Maar nu met 1% packet loss:



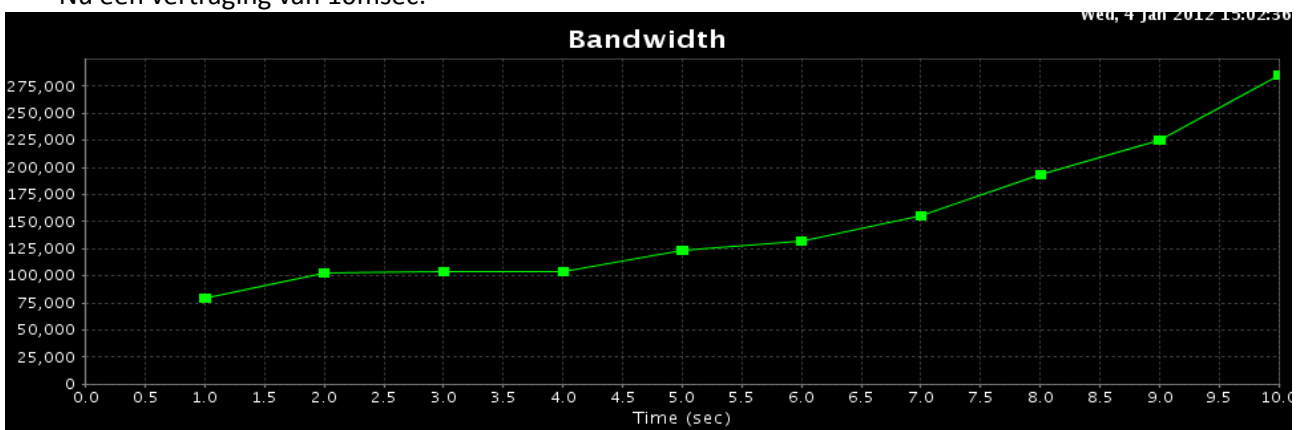
Het overnemen en vermenigvuldigen van (delen van) dit document is slechts geoorloofd na schriftelijke toestemming van GoudsConcept

www.goudsconcept.nl – Hoge Gouwe 7, 2801 LA, Gouda – 0182-585878

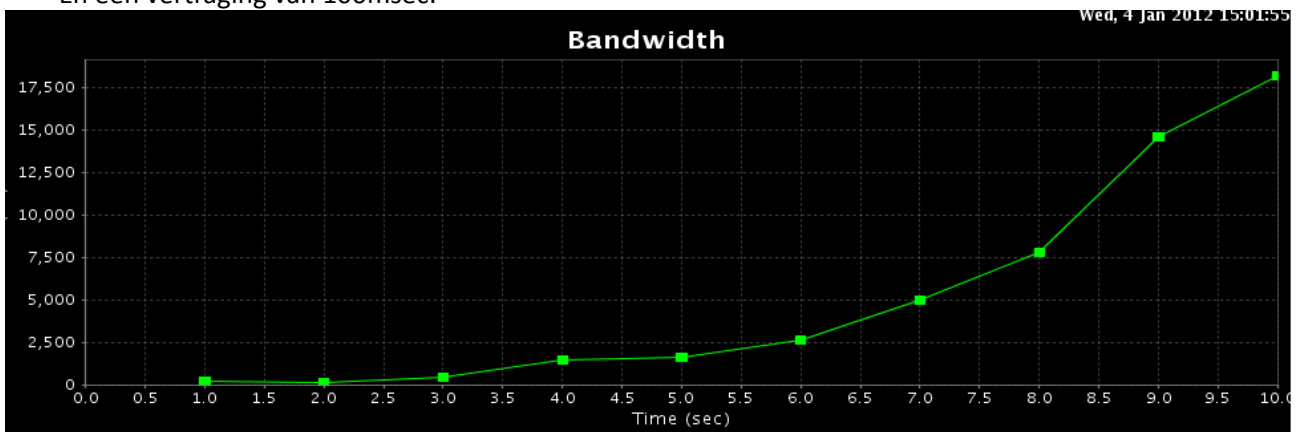
Geen packet loss, maar een vertraging van 1msec:



Nu een vertraging van 10msec:



En een vertraging van 100msec:



Het overnemen en vermenigvuldigen van (delen van) dit document is slechts geoorloofd na schriftelijke toestemming van GoudsConcept

www.goudsconcept.nl – Hoge Gouwe 7, 2801 LA, Gouda – 0182-585878

Wat duidelijk blijkt uit deze voorbeelden is dat het TCP-IP protocol erg veel last heeft van ongewenst netwerk gedrag. Duidelijk wordt dat de beschikbare bandbreedte al zeer sterk afneemt bij maar het geringste pakket verlies. 1%% pakket verlies (1 op de 1000 pakketten) geeft al een halvering van de beschikbare bandbreedte.

Verder blijkt dat netwerkvertraging een langzamere opbouw van de maximale bandbreedte geeft. Tel hierbij dat netwerkvertraging van 40msec niet ongewoon zijn en dat een packet loss van 1% als acceptabel wordt beschouwd en het is duidelijk dat veel netwerken niet echt de maximale performance geven bij gebruik van TCP-IP.

Conclusies

De combinatie van netwerk en gebruikte applicatie bepaalt of iets een bruikbare oplossing is of niet. Van beide componenten zal dan ook vastgesteld moeten worden wat de performance danwel tolerantie is.

De ervaring leert dat een ogenschijnlijk kleine afwijking in het netwerk, grote gevolgen voor een protocol of een applicatie kan hebben indien deze voor die afwijking gevoelig is.

Bijlage Details over tools en meetinstrumenten

De gebruikte tools en meetinstrumenten draaien allen op een Linux platform. De gebruikte hardware is geoptimaliseerd voor het doel waarvoor het gebruikt wordt.

De netwerk simulator draait op een high performance Linux platform met een groot aantal netwerk interfaces. Als operating system wordt FreeBSD gebruikt omdat dit een grote overlap heeft met Unix en daarmee veel netwerk faciliteiten biedt.

De packet generator en packet sniffer draaien op een portable Linux platform met daarop Backtrack 5 als operating system. Backtrack 5 biedt een groot aantal netwerk- en applicatie gerelateerde toepassingen en is daarmee zeer geschikt voor het uitvoeren van de meest uiteenlopende tests.

De software die gebruikt wordt bestaat voor een deel uit vrij toegankelijke OpenSource pakketten aangevuld met eigen ontwikkelde software. Ontwikkeling gebeurt in C++ omdat hiervoor een groot aantal bibliotheken beschikbaar zijn voor het uitvoeren van netwerk gerelateerde handelingen.

Hoewel Microsoft Windows op geen enkel onderdeel deel uitmaakt van het instrumentarium is het geen enkel probleem om een op Microsoft gebaseerde applicatie of een ander operating system te testen met de beschreven tools. De onderliggende communicatieprotocollen zijn gestandaardiseerd en de leveranciers specifieke implementatie onderdelen kunnen gemeten of geanalyseerd worden.