Netwerk storingsonderzoek makkelijker dan je denkt

“Waar ben ik en wat meet ik?” (geleerd van André de Rozario, mijn eerste groepschef)
“Apparatuur is stuk, of apparatuur is verkeerd in gebruik.” (zelf veel geleerde les)

Een storing laat zich vrij eenvoudig definiëren: De geleverde dienst wijkt – zonder dat we daarvan de reden te kennen – sterk af van de verwachting. Als die afwijkend geleverde dienst ons Internet verkeer betreft dan hebben we grofweg drie mogelijkheden: doet het niet, doet het soms, of is te langzaam. Zolang we onkundig zijn van de oorzaak van de afwijking beleven we de teleurstellende dienst als storing.

Bij zo’n storing is er op zijn minst één ongerijmdheid in onze keten van middelen die wij benutten. Met ieder van die middelen kan iets aan de hand zijn. Dat geldt niet alleen voor netwerk apparatuur, ook de grootste techbedrijven hebben af en toe te maken met storingen. Ook kan het zijn dat een eindgebruiker hogere verwachtingen heeft dan de eigen middelen waar kunnen maken.

Een storing kunnen we opheffen als we de oorzaak van de ongerijmdheid kennen. Bij de meeste storingen is er slechts één grondoorzaak, maar er zijn ook situaties waarin combinaties van op zichzelf correcte instellingen toch tot storingen kunnen leiden. Voorbeelden: verschillende instellingen van Interfaces, het aanbieden van verschillende VLANs, of een combinatie van verschillende optische transceivers. Dit soort problemen doet zich dan voor op een enkel punt in het netwerk. De kans dat er ten tijde van de storing op twee heel verschillende plaatsen storingsoorzaken bestaan, is niet nul, maar doorgaans wel verwaarloosbaar. En ook als dat aan de hand is zal dat ons niet beletten goed storingsonderzoek te doen en de problemen de wereld uit te helpen.

Alleen met een precieze analyse van het probleem ontdekken we waar dat de oorzaak van onze ongerijmdheid schuil gaat. Pas dan kunnen we begrijpen waarom de prestatie zich niet verhoudt met onze verwachting. We kunnen dan het probleem oplossen door de oorzaak weg te nemen. Of we moeten concluderen dat onze verwachtingen niet passen bij de ingezette middelen. Alleen met verkregen inzicht kunnen we werken aan oplossing of aan de acceptatie van wat eerder een onbegrepen probleem was.

Veruit de meeste mensen klagen nooit zomaar over een teleurstellend netwerk. Het is wel zo dat de meeste mensen niet in staat zijn het onderscheid te maken tussen een trage computer, een slechte Wifi verbinding, een trage (eigen) router, een traag Internet of een trage service provider/server aan de andere kant van het internet.
Een grondhouding bij storingsonderzoek is die van openheid. Trek lering uit wat je eerder hebt ervaren maar laat je nooit leiden door je herinnering van een soortgelijke storing die je eerder hebt opgelost.

Als je diagnostische software gebruikt van apparatuur die deel uitmaakt van het netwerk waarin een storing zit, bedenk dan dat er een verhoogde kans is dat deze diagnostische software zelf ook een verkeerde voorstelling van zaken kan geven!

Tactiek bij onderzoek (goed voor meer dan 99% van de gevallen)

Segmenteer. Welk netwerk gedeelte functioneert normaal, in welk deel zit het probleem? Hebben de buren soortgelijke problemen? Het hele project? Licht dan tweedelijns in.
Is de link wel up maar geen geldig IPv4 adres? Licht dan tweedelijns in.
Verhuist de fout mee als ik de router/tablet/PC/laptop/whatever ergens anders gebruik? Sluit een goed functionerende laptop aan op de netwerkaansluiting van de woning en doe een speedtest. Als de speedtest goed is, dan is er een probleem met de apparatuur van de eindgebruiker. Laatste firmware versie in router van eindgebruiker aanwezig? Strategische positie WIFI router in de woning? Goed Wifi signaal in huis? Is het gewoon een kapotte of slecht functionerende router?
Is de speedtest niet goed, onderzoek dan of er oplopende CRC-fouten zijn op de betrokken netwerk poort van de CWNetwerk switch. Controleer alle betrokken kabels/stekkers tussen de CWNetwerk switch en de router van de eindgebruiker. Vervang de patchkabel tussen de huisaansluiting en de router. Als dat niet werkt, neem een andere poort in gebruik op de CWNetwerk switch. Als dat niet helpt, raadpleeg iemand (zo nodig tweedelijns) om het bekabelingsprobleem op te lossen.

Uit te vragen bij de gebruiker, te benutten middelen

Verkrijg overzicht van de plaats van apparatuur. Maak een netwerktekening met hierin:

- Fysiek overzicht van de gebruikte apparatuur. Ook Client en server
- Eventueel gebruik van virtualisatie lagen.
- Functionele gelaagdheid apparatuur (converter, switch, router, proxy, gateway)
- Eventuele in gebruik zijnde netwerk hiërarchieën: VLAN's, VPN tunnels, MPLS, etc
- IP netwerk adressen, gateway adres, routering, stabiliteit van routering
- Routing protocollen, spanning tree protocollen
- Apparatuur en toegekende rollen: (bijv. DHCP-server, caching DNS)
- Transmissie media en hun instellingen (bijv. glasvezel, koper kabel type, Wifi)
- Interface snelheden
- Eventuele plaats van bandbreedte beperkingen, CoS, Policing, Traffic Shaping
- Failover, redundancy middelen, maatregelen en daarvoor gebruikte protocollen
- firmware, software in de gebruikte netwerk elementen

Klachtomschrijving

- Wat werkt er niet? Wat werkt wel?
- Is het probleem doorlopend aanwezig?
- Is het probleem reproduceerbaar? Onder welke omstandigheden?

Probleem afhankelijkheid van bepaalde

- tijden?
- netwerk belasting (bursts), congestie, latency/round-trip tijden?
- afmetingen packets, frames, datagrammen?
- status bestemmingen, routes, VPNs, logische netwerk topologie?
- applicaties?
- firewall instellingen, NAT?
- Policing, traffic shaping?

Te achterhalen indien van toepassing

- DNS instellingen, /etc/hosts, %windir%\system32\drivers\etc\hosts
- poort statistieken, foutstatistieken, logs
- uptime van netwerkelementen
- processor belasting netwerkelementen
- firmware netwerkelementen
- media eigenschappen link partners, interface snelheden
- poort instellingen link partners
- bezetting wifi kanalen
- plaats van DHCP server
- instellingen m.b.t. spanning tree, routing
- mate van aanwezige broadcasts, multicasts
- Voorkomen van MAC-IP en vice versa duplicaten

Metingen

- Interface statistieken, CRC fouten, packet loss, drops, etc.
- Vergelijking vanaf verschillende plaatsen in netwerk ping tijden, traceroute
- Tools ter achterhaling spoofing (DHCP, ARP, Flooding, poisoning, routing, etc)
- Sniffing (WireShark) via remote span ports, splitters
- Verkeersemulatie met iperf, xcap,

Middelen voor monitoring, visualisatie van poort statistieken zijn nuttig maar alleen echt waardevol bij een juiste interpretatie. Getallen over (totaal) opgetreden fouten of - packet loss zijn aanwijzingen van een storingsoorzaak, maar zonder tijdsinformatie is er geen enkele relatie te leggen met het moment waarop de klacht zich voordeed. Ook gerealiseerde down- of upload snelheden geven geen gedetailleerde aanwijzingen over de technische staat van het netwerk. Een vergelijking: Iemand kan zich met 50 km/h verplaatsen. Als ik niet weet met wat voor vervoersmiddel dat is en of dat in de lucht, op de weg, op – of onder water is, is 50km/h dan langzaam of snel? En ik kan al helemaal niet bepalen of er een probleem is met het vervoersmiddel.