RAPPORT INZAKE INCIDENT NETWERK 17-04-2022

Samenvatting

Op 17-4-2022 vond tussen 14.37 en 16.54 uur een storing op het BIT-netwerk plaats, die tot gevolg had dat het netwerk grotendeels onbereikbaar werd. De oorzaak lag in een verbinding met een derde partij waarover een grote hoeveelheid multicast verkeer ontvangen werd. Dit had tot gevolg dat de CPU's van linecards van core routers overbelast raakten, waardoor verkeer niet goed afgehandeld werd. Na uitschakeling van deze verbinding herstelde het netwerk zich.

Details

14:37	Netwerkapparatuur logt meldingen dat er problemen zijn in het netwerk.
14:40	Het monitoringsysteem meldt de dienstdoende engineer over onbereikbaarheid van veel diensten.
14:46	Klanten melden telefonisch onbereikbaarheid van hun diensten.
14:50	Het probleem wordt intern geëscaleerd, meerdere collega's worden bijgeschakeld om de oorzaak van het probleem te vinden.
14:55	Een storingsmelding wordt op www.bit.nl geplaatst. Deze website was op dit moment nog bereikbaar.
15:04	Engineers zetten diverse poorten in het access netwerk uit om loops in het netwerk uit te sluiten.
15:05	www.bit.nl is niet meer bereikbaar, er wordt een melding geplaatst op www.bit.org.
15:24	Engineers rebooten de core router in BIT-1.
15:30	Omdat deze reboot niet geholpen heeft worden meer externe verbindingen naar het BIT-netwerk uitgeschakeld om invloed van externe factoren te beperken.
16:00	Het netwerk lijkt kortstondig beter bereikbaar zonder duidelijk aanwijsbare oorzaak. Na enkele minuten wordt de bereikbaarheid van het netwerk weer slecht
16:16	Er worden nog meer delen van het netwerk uitgeschakeld om het probleem te isoleren.
16:42	Verdachte verkeerspatronen worden gezien op poorten in het core netwerk.
16:54	Poorten tussen routers en core switches worden uitgeschakeld. Onmiddellijk herstelt het netwerk zich. Dit wordt bevestigd door monitoringsystemen en klanten.
16:59	Verder onderzoek toont aan dat er verdacht verkeer ontvangen wordt op een poort in Amsterdam, wat getransporteerd wordt naar de core routers in Ede. Deze verbinding wordt uitgeschakeld.
17:00	Alle uitgeschakelde delen van het netwerk worden stapsgewijs weer ingeschakeld, behalve de poort waarop verdacht verkeer gezien wordt.
17:09	Er wordt een update geplaatst op www.bit.org dat er herstel gezien wordt.
17:32	Het terugdraaien van wijzigingen is afgerond.
17:41	De storing wordt afgemeld op www.bit.org.

Voorlopige conclusie

De twee core routers van BIT zorgen voor routering van internetverkeer. Deze zijn ontworpen om uitval van één van de twee routers op te kunnen vangen. Deze routers verbinden het access netwerk in Ede, waarop BIT diensten levert, externe netwerken (zoals transits en internet exchanges) en het core netwerk wat tussen Ede en twee locaties in Amsterdam loopt. In Amsterdam worden via het core netwerk klanten aangesloten en wordt er gekoppeld met dienstenleveranciers.

Tijdens deze verstoring werd een zeer grote hoeveelheid multicastverkeer (in de orde van grootte van honderdduizenden packets per seconde) op een poort in het core netwerk in Amsterdam ontvangen. Dit verkeer werd getransporteerd naar beide core routers in Ede, omdat deze samen een virtuele gateway vormen in dit netwerk.

De CPU van de linecard (een module in een router waarop een aantal netwerkpoorten beschikbaar is) van beide routers waarop dit verkeer binnenkwam werd overbelast. Het gevolg daarvan was dat alle netwerkpoorten op deze linecards niet goed meer functioneerden: de link bleef actief maar verkeer werd niet meer gerouteerd. Dit betrof onder andere verbindingen tussen het core netwerk en het access netwerk, waardoor het access netwerk volledig onbereikbaar werd. Deze routers zijn normaliter in staat om veel grotere hoeveelheden packets

per seconde af te handelen (bijvoorbeeld bij DDoS-aanvallen). Er wordt met de leverancier verder onderzocht waarom dit bij deze storing niet het geval was en waarom aanwezige beschermingsmechanismes tegen overbelasting van de CPU's onvoldoende gewerkt hebben.

Uit monitoring was af te leiden dat de CPU's van deze linecards overbelast waren. De oorzaak van deze overbelasting was echter niet direct duidelijk. Op basis van meldingen in monitoring werd vermoed dat een loop in het access netwerk een mogelijke oorzaak kon zijn. Daarom zijn stap voor stap delen van het BIT-netwerk uitgeschakeld. Dit betrof interne redundant uitgevoerde verbindingen. De meldingen werden echter veroorzaakt door het niet goed functioneren van de linecards; ze waren het gevolg van de storing en niet de oorzaak.

Omdat dit uitschakelen van interne verbindingen geen effect had zijn daarna stap voor stap andere delen van het netwerk (verbindingen met internet exchanges en het core netwerk) uitgeschakeld. Bij het uitschakelen van verbindingen tussen de routers en het core netwerk trad herstel op. Hierna kon gericht gezocht worden op afwijkingen binnen het core netwerk en werd de oorzaak gevonden.

Het is nog onbekend waarom wij opeens deze grote hoeveelheid multicast verkeer van een klant ontvingen en waarom dit tot overbelasting van CPU's van de linecards van de core routers leidde. Gesprekken met de klant en leverancier van de routers zijn hierover nog gaande. De RFO zal geüpdatet worden als er meer duidelijkheid is over beide punten.

Verbeterpunten
De eventueel te maken verbeteringen hangen deels af van informatie die nog verkregen moet worden van de routerleverancier en de klant. De volgende verbeterpunten zijn nu al geïdentificeerd:

- Er wordt onderzocht of aanvullende alarmering ingericht kan worden op afwijkende verkeerstypen.
- Er wordt onderzoek gedaan naar betere bescherming tegen pieken in multicastverkeer.
- Er wordt overwogen om verbindingen tussen core routers en access anders te verdelen over de aanwezige linecards. Bij overbelasting van de CPU van één linecard zou dit mogelijk de impact van de verstoring kunnen verkleinen.

Update 27-05-2022
Na overleg met zowel routerleverancier als klant zijn de onderstaande verbeterpunten uitgerold of zullen binnenkort uitgerold worden:

- De klant vanuit wiens netwerk de multicast flood ontvangen werd heeft zijn configuratie nagelopen. De misconfiguratie die de oorzaak was van dit verkeer is gevonden en hersteld.
- De koppeling met deze klant is naar een andere plaats in ons netwerk verhuisd. Mocht een soortgelijke flood zich opnieuw voordoen zal de impact ervan op de rest van ons netwerk tot een minimum beperkt blijven.
- De monitoringsystemen zijn uitgebreid met alarmeringen op meer afwijkende verkeerspatronen. Mocht een dergelijk incident zich herhalen kan er mogelijk ingegrepen worden voordat er overlast voor de rest van het netwerk ontstaat. In ieder geval zal de oorzaak veel sneller duidelijk zijn zodat er sneller ingegrepen kan worden.
- De routerleverancier heeft BIT voorzien van advies hoe de impact van multicast floods beperkt kan worden. De voorgestelde wijzigingen worden in het lab getest en zullen indien geschikt uitgerold worden naar het productienetwerk.

Contact
Mocht u naar aanleiding van dit rapport vragen hebben, dan kunt u contact opnemen met onze afdeling Customer Care via 0318 648 688 of support@bit.nl.