NETWORK INCIDENT REPORT 17-04-2022

Summary
On 17 April 2022 between 14.37 and 16.54 a disruption occurred on the BIT network. As a result, the network became largely unavailable. The source of the problem was a connection to a third party through which a large amount of multicast traffic was received. As a result, the CPUs of the core routers' line cards became overloaded, and traffic was not handled properly. The network recovered after this connection was switched off.

Timeline

14:37	Network equipment logs reports that there are problems in the network.
14:40	The monitoring system reports to the engineer on call that many services are unreachable.
14:46	Customers report the unavailability of their services by telephone.
14:50	The problem is escalated internally. Multiple colleagues are called in to find the cause of the problem.
14:55	A disruption of service message is placed on www.bit.nl. At this time this website is still reachable.
15:04	Engineers turn off various ports in the access network to rule out loops in the network.
15:05	www.bit.nl is no longer reachable, a notification is placed on www.bit.org.
15:24	Engineers reboot the core router in BIT-1.
15:30	This reboot did not help, so more external connections to the BIT network are switched off to limit the influence of external factors.
16:00	The network seems to be more accessible for a short while, without any apparent reason. After a few minutes, network accessibility becomes bad again.
16:16	Further parts of the network are shut down to isolate the problem.
16:42	Suspicious traffic patterns are seen on the ports in the core network.
16:54	Ports between routers and core switches are disabled. The network recovers immediately. This is confirmed by both monitoring systems and customer reports.
16:59	Further investigation shows that suspicious traffic is received on a port in Amsterdam, which transported to the core routers in Ede. This connection is switched off.
17:00	All switched-off parts of the network are gradually switched on again, except the port on which suspicious traffic is seen.
17:09	An update that recovery is seen, is posted on www.bit.org.
17:32	Reversal of changes is completed.
17:41	The disruption of service message is closed on www.bit.org.

Preliminary conclusion
BIT's two core routers ensure the routing of internet traffic. They are designed to handle the failure of one of the two routers. These routers connect the access network in Ede (on which BIT provides services), external networks (like transits and internet exchanges) and the core network which runs between the Amsterdam location and the two locations in Ede. In Amsterdam, customers are connected via the core network and are linked to service providers.

During this disruption, a very large amount of multicast traffic (in the order of hundreds of thousands of packets per second) was received on a port in the core network in Amsterdam. This traffic was transported to both core routers in Ede, as these together form a virtual gateway in this network.

The CPU of the line card (a module in a router on which a number of network ports are available) of both routers on which this traffic came in was overloaded. As a result, all network ports on these line cards stopped functioning properly: the link remained active, but traffic was no longer routed. This also applied to the core network and the access network, rendering the access network completely inaccessible. These routers can normally handle much larger volumes of packets per second (e.g. DDoS attacks). Together with the supplier, we will

investigate further why this was not the case with this disruption and why existing protection mechanisms against CPU overload did not work sufficiently.

Monitoring showed that the CPUs of these line cards were overloaded. However, the cause of this overload was not immediately clear. Based on reports from monitoring it was suspected that a loop in the access network could be a potential cause. Therefore, parts of the BIT network were switched off step by step. This involved internal redundantly implemented connections. However, the reports were caused by the malfunctioning of the line cards; they were a consequence of the disruption, not the cause.

The switching off of the internal connections had no effect, so other parts of the network (connections to internet exchanges and the core network) were switched off step by step. Recovery occurred when the connections between the routers and the core network were switched off. It was then possible to search specifically for deviations within the core network, and the cause was found.

It is still unknown why we suddenly received such a large amount of multicast traffic from a customer and why this led to an overload of the CPUs of the line cards of the core routers. Further discussions with the customer and the supplier of the routers are ongoing. The RFO will be updated when there is more clarity on both points.

Points for improvement
The improvements that can be made depend partly on information still to be obtained from the router supplier and the customer. The following points for improvement have already been identified:

- The possibility of setting additional alarms for abnormal traffic types is being investigated.
- Better protection against peaks in multicast traffic is being investigated.
- Consideration is being given to redistributing connections between core routers and access over the existing line cards. In the event of an overload of the CPU of one line card, this could potentially reduce the impact of a disruption.

Update 27 May 2022
Following consultation with both our router supplier and the customer, the following improvements have been or will soon be implemented:

- The customer from whose network the multicast flood was received has checked their configuration. The misconfiguration that caused the traffic has been identified and corrected.
- The uplink to this customer was moved to different location in our network. If a similar flood occurs in the future, the impact on the rest of our network will be minimised.
- Alerts on additional anomalous traffic patterns were added to the monitoring systems. If an incident like this one occurs again, we may be able to intervene before it causes disruption to the rest of the network. In any case, the cause will be come clear much faster, allowing for faster action.
- The router supplier advised BIT on how to mitigate the effects of multicast floods. The proposed changes are being tested in the lab and, if successful, will be rolled out to the production network.

Contact
If you have any questions regarding this report, please contact our Customer Care Department on 0318 648 688 or support@bit.nl.