From: **Fan-Chiang, Patrick, Vodafone UK** Patrick.Fan-Chiang@vodafone.com 📎
Subject: RE: Routing Loop Detected
Date: October 15, 2020 at 12:15
To: Page, Jamie, Vodafone UK Jamie.Page@vodafone.com, Wright, Martin, Vodafone UK Martin.Wright01@vodafone.com, TransportUKIPCore, Vodafone UK TransportUKIPCore@vodafone.co.uk, >NCIPSupport, Vodafone ncipsupport@vodafone.com, >CWA NOC Team CWANOCTeam@vodafone.com, DL-IP Mobile Core IPMobileCore@vodafone.com, Tipton, Richard, Vodafone UK richard.tipton@vodafone.com
Cc: >Access Repair Team AccessRepairTeam@vodafone.com, >IPAdmin IPAdmin@vodafone.com, DL - IP Services Team DL-IPServicesTeam@vodafone.co.uk, Johnson, Howard, Vodafone UK howard.johnson@vodafone.com

Thanks to Jamie and Martin's investigation and analysis.
I have taken a look on the IWF policy configuration level. Stackoverflow.com is still defined in the Test URL category along with example.com, **but this category is not used by any active policy**. The reason to have this customer category is for testing purpose before this IWF solution went live last year, and for court order blocking testing if we receive the request to activate it.
Since both stackoverflow.com (151.101.129.69) and example.com (93.184.216.34) are defined in the custom category even not in use, it still triggers the IWF to advertise both IPs to the IGWs. This will result the traffic routed to the IWF filters, but the IWF filters will allow the traffic go through and route it back to the IGW. It seems the routing loop is happened between the IGWs and IWF filters.
@Richard – I recall there was a tag deployed to prevent this type of looping. Do you remember how it was implemented and could this be related please?
Kind regards,
Patrick

C2 General

From: Page, Jamie, Vodafone UK <Jamie.Page@vodafone.com>
Sent: 15 October 2020 11:20
To: Wright, Martin, Vodafone UK <Martin.Wright01@vodafone.com>; TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>; >NCIPSupport, Vodafone <ncipsupport@vodafone.com>; >CWA NOC Team <CWANOCTeam@vodafone.com>; DL-IP Mobile Core <IPMobileCore@vodafone.com>
Cc: >Access Repair Team <AccessRepairTeam@vodafone.com>; >IPAdmin <IPAdmin@vodafone.com>; DL - IP Services Team <DL-IPServicesTeam@vodafone.co.uk>; Johnson, Howard, Vodafone UK <howard.johnson@vodafone.com>; Fan-Chiang, Patrick, Vodafone UK <Patrick.Fan-Chiang@vodafone.com>
Subject: RE: Routing Loop Detected
I have done a double check on WAHP06-IGW to confirm we really are getting that route from the IWF rather the router 'keeping a stale entry'
Everything at the moment indicates we are receiving that route from the IWF
Paths: (4 available, best #1)
Advertised to CE peers (in unique update groups):
90.255.254.97
Path #1: Received by speaker 0
Advertised to CE peers (in unique update groups):
90.255.254.97
65511
10.200.18.34 from 10.200.18.34 (10.200.18.34)
Origin EGP, metric 100, localpref 100, valid, external, best, group-best, import-candidate
Received Path ID 0, Local Path ID 1, version 155208893
Community: 5378:2550
Extended community: RT:5378:40 RT:25135:1111
Path #2: Received by speaker 0
Not advertised to any peer
65511, (received-only)
10.200.18.34 from 10.200.18.34 (10.200.18.34)
Origin EGP, localpref 100, valid, external
Received Path ID 0, Local Path ID 0, version 0
Path #3: Received by speaker 0
Not advertised to any peer
65513
63.130.108.240 (metric 205004) from 63.130.108.247 (63.130.108.240)
Received Label 24000
Origin EGP, metric 100, localpref 100, valid, internal, group-best, imported
Received Path ID 0, Local Path ID 0, version 0
Community: 5378:2550
Extended community: RT:5378:40 RT:25135:1111

Extended community: RT:5378:40 RT:25135:1111
Originator: 63.130.108.240, Cluster list: 0.3.0.0
Source AFI: VPNv4 Unicast, Source VRF: default, Source Route Distinguisher: 62.130.108.240:40
Path #4: Received by speaker 0
Not advertised to any peer
65512
63.130.108.235 (metric 201613) from 63.130.108.247 (63.130.108.235)
Received Label 24001
Origin EGP, metric 100, localpref 100, valid, internal, group-best, backup, add-path, imported
Received Path ID 0, Local Path ID 2, version 155208893
Community: 5378:2550
Extended community: RT:5378:40 RT:25135:1111
Originator: 63.130.108.235, Cluster list: 0.3.0.0
Source AFI: VPNv4 Unicast, Source VRF: default, Source Route Distinguisher: 63.130.108.235:40
Regards

Jamie Page
Technology Operations IP Networks(UK)
Mobile: +44 7990698551

From: Wright, Martin, Vodafone UK <Martin.Wright01@vodafone.com>
Sent: 15 October 2020 11:07
To: Page, Jamie, Vodafone UK <Jamie.Page@vodafone.com>; TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>; >NCIPSupport, Vodafone <ncipsupport@vodafone.com>; >CWA NOC Team <CWANOCTeam@vodafone.com>; DL-IP Mobile Core <IPMobileCore@vodafone.com>
Cc: >Access Repair Team <AccessRepairTeam@vodafone.com>; >IPAdmin <IPAdmin@vodafone.com>; DL - IP Services Team <DL-IPServicesTeam@vodafone.co.uk>; Johnson, Howard, Vodafone UK <howard.johnson@vodafone.com>; Fan-Chiang, Patrick, Vodafone UK <Patrick.Fan-Chiang@vodafone.com>
Subject: RE: Routing Loop Detected

Hi all,

Just an update on what I've learned so far (bear in mind I'm a DSL engineer not an IP engineer so apologies if anything is slightly wrong)

The 'IWF Filter Server' mentioned below is part of a new IWF solution that was installed about 18 months ago to eventually replace the existing DNS based solution that only works for HBB. By intercepting traffic at the IP level on an IGW it can work on all broadband and mobile services, as well as the fact it can't be bypassed by using 3rd party DNS.

From what I can tell the solution works by installing a new route to itself for /32 IP addresses that it wants to check. It has added routes to the IGW for both IP addresses mentioned below;
stackoverflow.com 151.101.129.69
imgur.com 151.101.60.193

I have spoken to Howard who confirms that neither domain name is currently on the IWF watchlist. We had previously whitelisted the imgur.com domain on the DNS solution but do not believe it's whitelisted on this new solution – though this shouldn't be related to the current problem as neither domain is on the list at the moment.

As such the problem seems to be that the routes exist in the first place. The routing loop is caused by the server sending the traffic back to the IGW as Jamie mentions, but I don't think it should be going there in the first place.

I've had a word with Patrick Fan-Chiang who's currently having a look. Apparently stackoverflow.com was the domain they used for testing in a lab environment before deployment, but we don't know if that's just a coincidence.

The issue is NOT present on all IGWs, just MCRN12-IGW-A1, SQYN02-IGW-A1, WAHP06-IGW-A1 & BKLN05-IGW-A1;
RP/0/RP0/CPU0:LDSCD2-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 09:55:56.551 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 63.130.127.205{ldscd2-pabr-a1} [MPLS: Labels 30491/24000 Exp 0] 6 msec 3 msec 2 msec
2 194.159.105.62{mcrn12-pabr-a1} [MPLS: Labels 30799/24000 Exp 0] 4 msec 2 msec 2 msec
3 195.89.96.113 2 msec 2 msec 2 msec
4 195.2.9.97 8 msec 8 msec 8 msec
5 * * *
6 * * *
RP/0/RP0/CPU0:SDNN13-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 09:56:42.184 UTC
Type escape sequence to abort

Tracing the route to 151.101.129.69
1 63.130.127.209{sdnn06-pabr-a1} [MPLS: Labels 29254/24001 Exp 0] 4 msec 2 msec 3 msec
2 10.200.18.45 3 msec 3 msec 3 msec
3 195.2.2.217 3 msec 3 msec 3 msec
4 195.2.24.34 4 msec 5 msec 4 msec
5 * * *
6 * * *
RP/0/RP0/CPU0:EDBTN1-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 09:58:34.307 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 63.130.127.201{edbtn1-pabr-a1} [MPLS: Labels 28046/24000 Exp 0] 9 msec 8 msec 8 msec
2 194.159.105.93{glwn07-pabr-a1} [MPLS: Labels 26455/24000 Exp 0] 10 msec 8 msec 8 msec
3 194.159.105.90{mcrn12-pabr-a1} [MPLS: Labels 25770/24000 Exp 0] 8 msec 8 msec 8 msec
4 195.2.9.97 13 msec 13 msec 13 msec
5 * * *
6 *
RP/0/RSP0/CPU0:MCRN12-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 09:59:41.187 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 * * *
2 10.200.18.53 !A * !A
RP/0/RSP0/CPU0:SQYN02-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 09:26:44.092 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 63.130.105.129 [MPLS: Labels 26904/24001 Exp 0] 2 msec 1 msec 1 msec
2 194.159.105.2 [MPLS: Labels 25241/24001 Exp 0] 1 msec 1 msec 0 msec
3 63.130.105.130 1 msec 1 msec 1 msec
4 63.130.104.194 2 msec 2 msec 2 msec
5 10.200.18.37 2 msec 2 msec 2 msec
6 63.130.105.130 1 msec 1 msec 1 msec
RP/0/RSP0/CPU0:WAHP06-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 09:25:17.841 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 * * *
2 * * *
3 63.130.104.194{wahp06-igw-a1} 1 msec 0 msec 0 msec
4 * * *
5 * * *
6 63.130.104.194{wahp06-igw-a1} 2 msec 1 msec 1 msec
RP/0/RSP0/CPU0:BSHN07-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 10:02:03.112 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 63.130.140.125{bhmn07-pabr-a1} [MPLS: Labels 25789/24000 Exp 0] 4 msec 3 msec 3 msec
2 194.159.105.46{mcrn12-pabr-a1} [MPLS: Labels 26090/24000 Exp 0] 3 msec 3 msec 3 msec
3 195.89.96.113 4 msec 7 msec 3 msec
4 195.2.9.97 8 msec 6 msec 6 msec
5 * * *
6 * * *
RP/0/RSP0/CPU0:BKLN05-IGW-A1#traceroute vrf Internet 151.101.129.69
Thu Oct 15 10:03:00.036 UTC
Type escape sequence to abort.
Tracing the route to 151.101.129.69
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *

Martin Wright
Engineering Authority
Technology Operations
07920 814 006
martin.wright01@vodafone.com

Vodafone, Atlas Park, Simonsway, Wythenshawe,
M22 5RR

vodafone.co.uk

The future is exciting.
Ready?

From: Wright, Martin, Vodafone UK <Martin.Wright01@vodafone.com>
Sent: 14 October 2020 16:39
To: Page, Jamie, Vodafone UK <Jamie.Page@vodafone.com>; TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>; >NCIPSupport, Vodafone <ncipsupport@vodafone.com>; >CWA NOC Team <CWANOCTeam@vodafone.com>; DL-IP Mobile Core <IPMobileCore@vodafone.com>
Cc: >Access Repair Team <AccessRepairTeam@vodafone.com>; >IPAdmin <IPAdmin@vodafone.com>; DL - IP Services Team <DL-IPServicesTeam@vodafone.co.uk>
Subject: RE: Routing Loop Detected

Hi Jamie, thanks for taking a look.

I know that imgur.com, being an image hosting website, quite often got flagged on the IWF list. I think after a lot complaints (customers not being to get to it at all over https) we eventually whitelisted it. Maybe it's a bad example. I can't imagine stackoverflow.com would ever get IWF flagged though.

Martin

From: Page, Jamie, Vodafone UK <Jamie.Page@vodafone.com>
Sent: 14 October 2020 16:33
To: TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>; Wright, Martin, Vodafone UK <Martin.Wright01@vodafone.com>; >NCIPSupport, Vodafone <ncipsupport@vodafone.com>; >CWA NOC Team <CWANOCTeam@vodafone.com>; DL-IP Mobile Core <IPMobileCore@vodafone.com>
Cc: >Access Repair Team <AccessRepairTeam@vodafone.com>; >IPAdmin <IPAdmin@vodafone.com>; DL - IP Services Team <DL-IPServicesTeam@vodafone.co.uk>
Subject: RE: Routing Loop Detected

If you follow that path then 151.101.60.193 is being injected by the IWF function(so this is a very dodgy site !!!)

```
RP/0/RSP0/CPU0:WAHP06-IGW-A1#show route vrf Internet 151.101.60.193
Wed Oct 14 15:30:33.721 UTC
Routing entry for 151.101.60.193/32
Known via "bgp 5378", distance 20, metric 100
Tag 65511
Number of pic paths 1 , type internal and external
Installed Oct 14 01:21:13.398 for 14:09:20
Routing Descriptor Blocks
10.200.18.34, from 10.200.18.34, BGP external
Route metric is 100
63.130.108.235, from 63.130.108.247, BGP backup path
Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
Route metric is 100
No advertising protos.
RP/0/RSP0/CPU0:WAHP06-IGW-A1#show route vrf Internet 10.200.18.34
Wed Oct 14 15:30:48.924 UTC
Routing entry for 10.200.18.32/30
Known via "connected", distance 0, metric 0 (connected)
Installed Mar 11 05:07:56.230 for 31w0d
Routing Descriptor Blocks
directly connected, via TenGigE0/6/0/18
Route metric is 0
No advertising protos.
RP/0/RSP0/CPU0:WAHP06-IGW-A1#show interfaces tenGigE 0/6/0/18
Wed Oct 14 15:30:59.501 UTC
TenGigE0/6/0/18 is up, line protocol is up
Interface state transitions: 1
Hardware is TenGigE, address is d46d.5036.c892 (bia d46d.5036.c892)
Layer 1 Transport Mode is LAN
Description: WAHP06-IGW-A1 Te0/6/0/18 to WAHP03-IWF-F1 Eth0 for IWF Filter Server
Internet address is 10.200.18.33/30
MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, LR, link type is force-up
```

output flow control is off, input flow control is off
Carrier delay (up) is 10 msec
loopback not set,
Last link flapped 31w0d
ARP type ARPA, ARP timeout 04:00:00
Last input 00:00:10, output 00:00:00
Last clearing of "show interface" counters 14w5d
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 18765000 bits/sec, 22711 packets/sec
511080 packets input, 37972515 bytes, 249 total input drops
0 drops for unrecognized upper-level protocol
Received 208314 broadcast packets, 0 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
125012378499 packets output, 13333411984203 bytes, 0 total output drops
Output 0 broadcast packets, 0 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
RP/0/RSP0/CPU0:WAHP06-IGW-A1#
I have copied the IP services team in to see if they can clarify why they are routing the packet back to the IGW.
Regards
Jamie Page
Technology Operations IP Networks(UK)
Mobile: +44 7990698551

From: TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>
Sent: 14 October 2020 16:25
To: Wright, Martin, Vodafone UK <Martin.Wright01@vodafone.com>; TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>; >NCIPSupport, Vodafone <ncipsupport@vodafone.com>; >CWA NOC Team <CWANOCTeam@vodafone.com>; DL-IP Mobile Core <IPMobileCore@vodafone.com>
Cc: >Access Repair Team <AccessRepairTeam@vodafone.com>; >IPAdmin <IPAdmin@vodafone.com>
Subject: RE: Routing Loop Detected
Hi CPN Team,
Could you be able to assist Martin with regards to customers observing this routing loop.

Tajinder Grewal
Specialist Engineer
UKNOC SHIFT B IP

Vodafone HQ, The Connection, Newbury,
Berkshire, RG14 2FN,
+ 44 7342 073 762
+ 3333042555 option 1

Tajinder.Grewal@vodafone.com
vodafone.co.uk

The future is exciting.
Ready?
From: Wright, Martin, Vodafone UK <Martin.Wright01@vodafone.com>
Sent: 14 October 2020 16:22
To: TransportUKIPCore, Vodafone UK <TransportUKIPCore@vodafone.co.uk>; >NCIPSupport, Vodafone <ncipsupport@vodafone.com>; >CWA NOC Team <CWANOCTeam@vodafone.com>
Cc: >Access Repair Team <AccessRepairTeam@vodafone.com>; >IPAdmin <IPAdmin@vodafone.com>
Subject: Routing Loop Detected
Hi all,
We've had reports of a routing loop from customers trying to get to certain sites:

We've had reports of a routing loop from customers trying to get to certain sites,
stackoverflow.com 151.101.129.69
imgur.com 151.101.60.193
I can replicate this from the IGW, sorry not sure which team would normally deal with this. Could
someone have a look please?
Cheers,
Martin

RP/0/RSP0/CPU0:SQYN02-IGW-A1#show route vrf Internet 151.101.60.193
Wed Oct 14 15:16:29.277 UTC
Routing entry for 151.101.60.193/32
Known via "bgp 5378", distance 200, metric 100
Tag 65511
Number of pic paths 1 , type internal
Installed Oct 14 01:21:13.616 for 13:55:15
Routing Descriptor Blocks
63.130.108.235, from 63.130.108.247, BGP backup path
Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
Route metric is 100
63.130.108.239, from 63.130.108.247
Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
Route metric is 100
No advertising protos.
RP/0/RSP0/CPU0:SQYN02-IGW-A1#traceroute vrf Internet 151.101.60.193
Wed Oct 14 15:17:02.052 UTC
Type escape sequence to abort.
Tracing the route to 151.101.60.193
1 63.130.105.129 [MPLS: Labels 26904/24001 Exp 0] 2 msec 1 msec 0 msec
2 194.159.105.2 [MPLS: Labels 25241/24001 Exp 0] 1 msec 0 msec 0 msec
3 63.130.105.130 1 msec 1 msec 1 msec
4 63.130.104.194 2 msec 2 msec 2 msec
5 10.200.18.37 2 msec 2 msec 3 msec
6 63.130.105.130 1 msec 1 msec 2 msec
7 63.130.104.194 3 msec 3 msec 3 msec
8 10.200.18.37 3 msec 4 msec 3 msec
9 63.130.105.130 2 msec 3 msec 3 msec
10 63.130.104.194 4 msec 4 msec 4 msec
11 10.200.18.37 4 msec 4 msec 4 msec
12 63.130.105.130 3 msec 3 msec 3 msec
13 63.130.104.194 5 msec 4 msec 5 msec
14 10.200.18.37 5 msec 5 msec 5 msec
15 63.130.105.130 4 msec 4 msec 5 msec
16 63.130.104.194 6 msec 6 msec 6 msec
17 10.200.18.37 6 msec 6 msec 6 msec
18 63.130.105.130 5 msec 6 msec 6 msec
19 63.130.104.194 7 msec 7 msec 7 msec
20 10.200.18.37 7 msec 7 msec 7 msec
21 63.130.105.130 6 msec 6 msec 6 msec
22 63.130.104.194 8 msec 8 msec 8 msec
23 10.200.18.37 8 msec 8 msec 9 msec
24 63.130.105.130 7 msec 7 msec 7 msec
25 63.130.104.194 9 msec 9 msec 9 msec
26 10.200.18.37 9 msec 9 msec 9 msec
27 63.130.105.130 8 msec 8 msec 9 msec
28 63.130.104.194 10 msec 10 msec 11 msec
29 10.200.18.37 10 msec 11 msec 10 msec
30 63.130.105.130 10 msec 10 msec 10 msec
RP/0/RSP0/CPU0:SQYN02-IGW-A1#

Martin Wright
Engineering Authority
Technology Operations
07920 814 006
martin.wright01@vodafone.com

Vodafone, Atlas Park, Simonsway, Wythenshawe,
M22 5RR

vodafone.co.uk

The future is exciting.
Ready?