## Tails - Bug #9268

**obfs4 bridges often don’t work (maybe MTU?)**

04/21/2015 05:00 AM - emmapeel

<table>
<thead>
<tr>
<th>Status:</th>
<th>Duplicate</th>
<th>Start date:</th>
<th>04/21/2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>emmapeel</td>
<td>% Done:</td>
<td>20%</td>
</tr>
<tr>
<td>Category:</td>
<td>Tor configuration</td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
<td>Spent time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Feature Branch:</td>
<td>bugfix/9268-deal-with-smaller-MTU</td>
<td>Starter:</td>
<td></td>
</tr>
<tr>
<td>Type of work:</td>
<td>Research</td>
<td>Affected tool:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

There have been some reports of obfs4 bridges not working.

A user has found out on the router being used some error messages like:

```
ICMP 185.xx.xx.xx unreachable - need to frag (mtu 1456), length 556
```

This is not happening with other bridges or pluggable transports.

I did some searches online and found out some information regarding MTU and encapsulating that I cannot really follow, like [http://opsmonkey.blogspot.com/2007/02/path-mtu-discovery-and-mtu.html](http://opsmonkey.blogspot.com/2007/02/path-mtu-discovery-and-mtu.html)

And in [https://ubuntuforums.org/archive/index.php/t-979821.html](https://ubuntuforums.org/archive/index.php/t-979821.html) I found a workaround but the user reports no change after applying it (ifconfig wlan0 mtu 1462)

Do we need to do something about this problem? I think obfs4 bridges need to use bigger packages. Maybe it is a documentation issue, or maybe the configuration should be changed when using obfs4 bridges.

**Related issues:**

- Related to Tails - Bug #12197: Confusing UI/log when trying to use obfs4 brid... Duplicate 01/31/2017
- Related to Tails - Bug #15168: Improve UX when hardware clock is set to local... Resolved 01/15/2018
- Duplicates Tails - Bug #15548: Tails can't establish a connection with obfs4 ... Confirmed 05/09/2018

**Associated revisions**

**Revision 1d1c83de - 05/07/2015 03:37 PM - intrigeri**

Enable Packetization Layer Path MTU Discovery for IPv4.

If any system on the path to the remote host has a MTU smaller than the standard Ethernet one, then Tails will receive an ICMP packet asking it to send smaller packets ([https://en.wikipedia.org/wiki/Path_MTU_Discovery](https://en.wikipedia.org/wiki/Path_MTU_Discovery)). Our firewall will drop such ICMP packets to the floor, and then the TCP connection won't work properly. This can happen to any TCP connection, but so far it's been reported as breaking obfs4 for actual users.

The other options would be:

- arbitrarily set a smaller MTU; but it will lower performance for everybody (even the 99% of use cases that could actually very well handle the default, larger MTU); worse, the chosen number will be arbitrary, given Yawning says that the "only MTUs that are guaranteed to be correct (ignoring horrifically misconfigured hosts) are 576 bytes/1280 bytes (IPv4/IPv6)", and we would probably not want to set this small a MTU.

- accept the ICMP messages that are needed to make Path MTU Discovery work; the security implications are unclear.

05/15/2020
So, instead we enable Packetization Layer PMTUD (RFC 4821). The value “1”, that we set, will selectively enable probing if the kernel thinks it's stuck in an ICMP black hole. This should have a lower performance impact than the value “2”, that makes the kernel always probe.

Thanks to Yawning for the help! ;)

Will-Fix: #9268

---

**History**

#1 - 04/25/2015 06:25 AM - intrigeri

A user has found out on the router being used some error messages like:

```
ICMP 185.xx.xx.xx unreachable - need to frag (mtu 1456), length 556
```

Do we need to do something about this problem? I think obfs4 bridges need to use bigger packages. Maybe it is a documentation issue, or maybe the configuration should be changed when using obsf4 bridges.

My current understanding is that this problem with obfs4 is exposing a much broader one: if any system on the path to the remote host has a MTU smaller than the standard Ethernet one, then Tails will receive an ICMP packet asking it to send smaller packets (https://en.wikipedia.org/wiki/Path_MTU_Discovery). Our firewall will drop such ICMP packets to the floor, and then the TCP connection won't work properly. This can happen to any TCP connection, not only to obfs4 ones.

I'm not sure how to correctly fix this problem. We could:

1. arbitrarily set a smaller MTU; but it will lower performance for everybody (even the 99% of use cases that could actually very well handle the default, larger MTU);
2. accept the ICMP messages that are needed to make Path MTU Discovery work; perhaps we can even accept such packets only from the default gateway;
3. anything else?
Updated the description, as the user reported the workaround didn't helped.

intrigeri wrote:

My current understanding is that this problem with obfs4 is exposing a much broader one: if any system on the path to the remote host has a MTU smaller than the standard Ethernet one, then Tails will receive an ICMP packet asking it to send smaller packets (https://en.wikipedia.org/wiki/Path_MTU_Discovery). Our firewall will drop such ICMP packets to the floor, and then the TCP connection won't work properly. This can happen to any TCP connection, not only to obfs4 ones.

This is correct.

I'm not sure how to correctly fix this problem. We could:

1. arbitrarily set a smaller MTU; but it will lower performance for everybody (even the 99% of use cases that could actually very well handle the default, larger MTU);

This is a fairly poor choice at least currently. The only MTUs that are guaranteed to be correct (ignoring horrifically misconfigured hosts) are 576 bytes/1280 bytes (IPv4/IPv6). Naturally most links can support higher, though 1456 is a relatively common lower one (certain PPPoE configurations).

1. accept the ICMP messages that are needed to make Path MTU Discovery work; perhaps we can even accept such packets only from the default gateway;

This is one way to fix it, but I'm not sure as to if it introduces any risks. I'd like to say "not really" because anyone that can inject ICMP messages can likely also mess with the user's traffic...

1. anything else?

Linux implements Packetization Layer PMTUD (RFC 4821), which has the TCP/IP stack probe for the PMTU. This is disabled by default, since it has a performance impact for links where this is not necessary.

The feature is gated by "/proc/sys/net/ipv4/tcp_mtu_probing". Setting the value to "1" will selectively enable probing if the kernel thinks it's stuck in an ICMP black hole, setting it to "2" will always probe.

I suspect that either setting will address this case, with "1" being preferable for the bulk of users.
#4 - 05/07/2015 03:50 PM - Dr_Whax
- Status changed from Confirmed to In Progress
- Assignee set to intrigeri
- Target version set to Tails_1.4.1
- % Done changed from 0 to 10
- Feature Branch set to bugfix/9268-deal-with-smaller-MTU

#5 - 05/07/2015 03:51 PM - intrigeri
Applied in changeset 1d1c83de90d4d949a80005ff687742d3b173b1.

#6 - 05/07/2015 04:22 PM - _adamb

2. accept the ICMP messages that are needed to make Path MTU Discovery work; perhaps we can even accept such packets only from the default gateway;

I'm not sure what you mean by 'accept such packets only from the default gateway' but if you mean the IP source header, that's not going to work. PMTU ICMP packets can validly come from any gateway between 2 hosts attempting to establish a connection.

#7 - 05/07/2015 04:31 PM - _adamb

"only MTUs that are guaranteed to be correct (ignoring horrifically misconfigured hosts) are 576 bytes/1280 bytes (IPv4/IPv6)"

And with greatest respect to Yawning, this is not correct. MTUs are often set for efficiency to match underlying layer 2 frame sizes (ethernet, frame relay, ATM whatever). There are no guaranteed correct values.

#8 - 05/08/2015 01:18 AM - yawning

_adamb wrote:

"only MTUs that are guaranteed to be correct (ignoring horrifically misconfigured hosts) are 576 bytes/1280 bytes (IPv4/IPv6)"

And with greatest respect to Yawning, this is not correct. MTUs are often set for efficiency to match underlying layer 2 frame sizes (ethernet, frame relay, ATM whatever). There are no guaranteed correct values.
There are no guaranteed correct values, because people are free to ignore standards. I'd be highly surprised (and would mercilessly make fun of) an ISP that exposed the 53 byte ATM cell size to IP for example.

RFC 791 "INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION":

All hosts must be prepared to accept datagrams of up to 576 octets (whether they arrive whole or in fragments). It is recommended that hosts only send datagrams larger than 576 octets if they have assurance that the destination is prepared to accept the larger datagrams.

RFC 2460 "Internet Protocol, Version 6 (IPv6) Specification":

IPv6 requires that every link in the internet have an MTU of 1280 octets or greater. On any link that cannot convey a 1280-octet packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.

Anyway PLPMTUD is designed for this sort of situation, so it should address the problem. Since the conservative setting was chosen the probing will kick in once the TCP retransmission timer fires. The good news is that this information is cached so under normal circumstances will only happen once.

#9 - 05/08/2015 11:00 AM - intrigeri
PLPMTUD is enabled in the topic branch referenced by this ticket. I've merged it into our experimental branch, so there are "nightly" built ISO images with the proposed change: [http://nightly.tails.boum.org/build_Tails_ISO_experimental/](http://nightly.tails.boum.org/build_Tails_ISO_experimental/)

Next steps:

1. I'll make it go through a test suite run to make sure it doesn't break anything obvious;
2. then I'll ask emmapeel to ask the original bug reporter to confirm that PLPMTUD fixes the problem they were experiencing.

#10 - 05/16/2015 04:38 PM - intrigeri
- Assignee changed from intrigeri to emmapeel
- % Done changed from 10 to 20
- QA Check changed from Dev Needed to Info Needed

Full test suite passes for me with an ISO built from experimental (that has the feature branch merged in).
emmapeel, may you please ask the affected bug reporter(s) if they can reproduce the bug with the latest experimental ISO from http://nightly.tails.boum.org/build_Tails_ISO_experimental/?

#11 - 05/18/2015 07:21 AM - emmapeel
- Assignee changed from emmapeel to intrigeri
- QA Check deleted (Info Needed)

I am afraid the user claims this is not solving the problem with http://nightly.tails.boum.org/build_Tails_ISO_experimental/latest.iso of May 16th.
Tor logs and TCP dumps forwarded.

#12 - 05/18/2015 03:17 PM - intrigeri
- Assignee changed from intrigeri to emmapeel
- QA Check set to Info Needed

I am afraid the user claims this is not solving the problem with http://nightly.tails.boum.org/build_Tails_ISO_experimental/latest.iso of May 16th.

Thanks! I'm no expert in this field, but the network dumps I've seen seem to indicate that Tails learns about the MTU it should use, and the need for fragmenting packets. The same log lines that were reported previously (that contain "unreachable - need to frag (mtu") are basically the same.

emmapeel: does that obfs4 bridge at all work outside of Tails? (the user provided their exact obfs4 config so you can easily try and reproduce that yourself)

yawning: do these "ICMP 185.xx.xx.xx unreachable - need to frag (mtu 1456), length 556" message indicate that PLPMTUD doesn't work?

#13 - 05/19/2015 08:58 AM - emmapeel
I can connect to the Tor network with the obfs4 bridge provided by the user.

#14 - 05/19/2015 09:04 AM - emmapeel
- Assignee changed from emmapeel to intrigeri
- QA Check deleted (Info Needed)

#15 - 05/19/2015 09:06 AM - intrigeri
- Assignee changed from intrigeri to yawning
- QA Check set to Info Needed

#16 - 05/19/2015 01:35 PM - yawning
I'd need to see a copy of the logs and tcpdump output. I've tested obfs4proxy with lower MTUs so I know the code can handle it, though that was with explicitly lowering my interface MTU and not with any sort of probing (home network setup doesn't make doing that easy, unfortunately).
I'd need to see a copy of the logs and tcpdump output.

Sent to you privately. Thanks a lot for looking into this :)

---

- Target version changed from Tails_1.4.1 to Tails_1.5

Postponing to 1.5. yawning, any news on this front?

- Target version changed from Tails_1.5 to Tails_1.6

Postponing again.

- Target version changed from Tails_1.6 to Tails_1.7

Dumb questions: Is it saying that the "Next-Hop MTU" field shows 1456 while the total packet length derived from the IP header of the original datagram is 556? Why would that need fragmentation? Should the Don't Fragment flag be set to true?

Are the first 8 bytes of the original datagram's data being sent in the clear via ICMP?

http://www.networksorcery.com/enp/rfc/rfc792.txt
http://www.networksorcery.com/enp/rfc/rfc1191.txt

---

- Target version changed from Tails_1.7 to Tails_2.0

Postponing to a release that's in the future. yawning: do you think you'll have time to look at it any time soon? Otherwise, it's fine, I think we should not spend more time than needed on this corner case, and I'll reject this ticket if there's not been progress in a month or two.
#23 - 02/08/2016 06:29 PM - sajolida
- Status changed from In Progress to Rejected
- Assignee deleted (yawning)
- Target version deleted (Tails_2.0)
- QA Check deleted (Info Needed)

"a month or two" have passed so I'm rejecting this.

#24 - 01/14/2017 06:13 PM - goupille
- Status changed from Rejected to New
- Assignee set to intrigeri

I reopened this ticket and redirecting a user experiencing the issue here

#25 - 01/15/2017 07:45 AM - intrigeri
- Assignee changed from intrigeri to goupille

I reopened this ticket and redirecting a user experiencing the issue here

Cool. Please reassign to me once there's something I can do about it.

#26 - 01/24/2017 02:11 PM - goupille
- Assignee changed from goupille to intrigeri

#27 - 06/05/2017 03:52 PM - intrigeri
- Assignee deleted (intrigeri)

I've not seen "a user experiencing the issue here" and can't find any corresponding WhisperBack bug report (if there was one), sorry! In general, please mention the ID of the WhisperBack bug report when referring to one, so it's realistic that we find it next time we need it.

So I dunno what should be the state of this ticket, and don't dare rejecting it again.

#28 - 06/27/2017 02:11 PM - Anonymous
- Assignee set to goupille

intrigeri wrote:

I've not seen "a user experiencing the issue here" and can't find any corresponding WhisperBack bug report (if there was one), sorry! In general, please mention the ID of the WhisperBack bug report when referring to one, so it's realistic that we find it next time we need it.

So I dunno what should be the state of this ticket, and don't dare rejecting it again.
@goupille can you please try to find the ID of the whisperback report? If you don't, can we reject this ticket?

#29 - 06/27/2017 03:22 PM - Anonymous
- Related to Bug #12197: Confusing UI/log when trying to use obfs4 bridges / impossible to use obfs4 added

#30 - 07/28/2017 05:14 PM - goupille
- Assignee changed from goupille to intrigeri

other users experienced issues with obfs4 bridges and send us some info
so I reassign this ticket to intrigeri and forward the logs

#31 - 09/21/2017 01:10 PM - intrigeri
- Assignee deleted (intrigeri)

The logs goupille list of 21 (!) obfs4 bridges, a bunch of Proxy Client: unable to connect to IP:PORT ("general SOCKS server failure") lines, and the fact goupille could not reproduce (presumably using the same list of bridges, I guess). I'm afraid I can't do anything about it with this little info :/

#32 - 09/21/2017 01:13 PM - intrigeri
Another report I've received shows clock issues => dear help desk, whenever you get such reports please ask the user to ensure their hardware clock is correct and in UTC timezone.

#33 - 09/21/2017 09:04 PM - yawning
intrigeri wrote:

Another report I've received shows clock issues => dear help desk, whenever you get such reports please ask the user to ensure their hardware clock is correct and in UTC timezone.

UTC does not matter at all.

https://golang.org/pkg/time/#Time.Unix
But the system time does need to be somewhat close to the bridge:

#34 - 11/25/2017 06:35 PM - mercedes508
- Status changed from New to Confirmed
intrigeri wrote:

Another report I've received shows clock issues => dear help desk, whenever you get such reports please ask the user to ensure their hardware clock is correct and in UTC timezone.

UTC does not matter at all.

https://golang.org/pkg/time/#Time.Unix

But the system time does need to be somewhat close to the bridge:

Technically you're (of course!) correct but in practice Tails starts with a system clock set to whatever the RTC says and assumes it's in UTC so if the RT is set to localtime != UTC, the system time will be wrong and then all kinds of issues happen (e.g. #15548, that's a bug in our time syncing crappy pile of hacks rather than in obfs4proxy).

Anonymous wrote:

The clock issue is tracked on #15548.
The MTU issue was merged.

I'm unsure about more users reporting issues with obfs4 bridges.
@helpdesk: were there any?
If not: please close this ticket and reopen if necessary.
If yes: unassign yourself and send logs to intrigeri.

#40 - 08/19/2018 12:13 PM - intrigeri
No need to send me logs, just follow #9268#note-32.

#41 - 08/20/2018 09:33 AM - intrigeri
- Related to deleted (Bug #15743: Too much log when using obfs4 in Tails)

#42 - 08/24/2018 01:33 PM - goupille
- Assignee changed from goupille to mercedes508

u wrote:

I'm unsure about more users reporting issues with obfs4 bridges.
@helpdesk: were there any?

we've got at least one user complaining about not being able to connect with obfs4 bridges these days, I reassign this ticket to the helpdesk member on duty

#43 - 09/05/2018 08:21 AM - mercedes508
- Status changed from Confirmed to Rejected
- Assignee changed from mercedes508 to emmapeel

goupille wrote:

u wrote:

I'm unsure about more users reporting issues with obfs4 bridges.
@helpdesk: were there any?

we've got at least one user complaining about not being able to connect with obfs4 bridges these days, I reassign this ticket to the helpdesk member on duty

Closing it for now, as I didn't received bug report about this issue recently.
What do you think emma?
This problem is still very much alive: it made it to the hot topics from help desk twice in the last 6 months, so let's not close this ticket.

Instead, please follow #9268#note-32.

Two years after I've posted #9268#note-32, I've no indication that there is another problem here than #15548: I've seen no report about obfs4 not working with a hardware clock (RTC) set to the correct UTC time. So I'll consider that we've identified the root cause of the problem: #15548. See you there!

Related to deleted (Bug #15548: Tails can't establish a connection with obfs4 bridges and a hardware clock too far away from UTC)

Duplicates Bug #15548: Tails can't establish a connection with obfs4 bridges and a hardware clock too far away from UTC added