Check path MTU when SSH works but large transfers stall

A working SSH login does not prove that larger network packets can cross the same route. If small requests succeed but a TLS exchange or file transfer stalls, a path MTU problem is one possibility. Packet loss, storage delays and application timeouts can produce similar symptoms, so treat these checks as evidence gathering.

1. Define a repeatable symptom

Write down the source and destination, IPv4 or IPv6, protocol, time and approximate point where the transfer stops. Use a harmless file and an endpoint you control. Note whether a VPN, tunnel or container network is involved; additional encapsulation can reduce the space available for the inner packet.

Keep an existing management session open. The commands below do not change the interface MTU, routes or firewall. Replace the documentation-only destination address with the affected address that you are authorised to test.

2. Record the route and local interface

```
ip route get 192.0.2.10
ip -br link
tracepath -4 -n 192.0.2.10
```

The route shows which interface Linux intends to use. `tracepath` sends probes and can report a discovered path MTU. It may be supplied by a separate package rather than installed by default. An incomplete path or “no reply” can result from filtered probes; it does not by itself establish an

outage or a bad hop. Avoid repeated long runs.

3. Compare two bounded IPv4 probes

```
ping -4 -c 3 -W 2 -M do -s 1200 192.0.2.10
ping -4 -c 3 -W 2 -M do -s 1472 192.0.2.10
```

These sizes describe the ICMP payload. With ordinary IPv4 headers, 1472 bytes plus 28 bytes of headers totals 1500 bytes. The `-M do` option asks for path-MTU discovery without fragmentation. A local “message too long” response can mean Linux already knows a smaller usable size. A larger probe that disappears while the smaller one succeeds is worth investigating, but different ICMP filtering can also explain it.

Do not apply the IPv4 header calculation to IPv6. Test the address family used by the failing application and keep the two sets of results separate.

4. Compare the actual application path

Repeat one normal transfer from the same machine and record whether its failure aligns with the probe results. If access is available, ask the other endpoint's administrator for an equivalent check in the reverse direction. Routes and filtering can be asymmetric. A successful ping to a different public site is not a comparison of the affected route.

Inspect tunnel configuration and firewall counters read-only with the responsible administrator. Path-MTU discovery depends on appropriate network error messages reaching the sender. Do not disable all ICMP protections, enable arbitrary forwarding, or set a permanent MTU from one ping result.

Escalate with evidence

Send support the route/interface output, discovered MTU if any, both short probe results, address family and transfer timestamps. Redact unrelated private routes. If a network change is needed, arrange console access, a rollback and a controlled verification window rather than experimenting

on the active management interface.

Related: IPv6 diagnostics and safe SFTP transfers.

Official references

- Debian tracepath manual
- Debian ping manual
- Debian ip route manual

Revision #1
Created 2026-11-10 10:51:41 UTC by CloudExa Hosting Admin
Updated 2026-11-10 10:51:41 UTC by CloudExa Hosting Admin