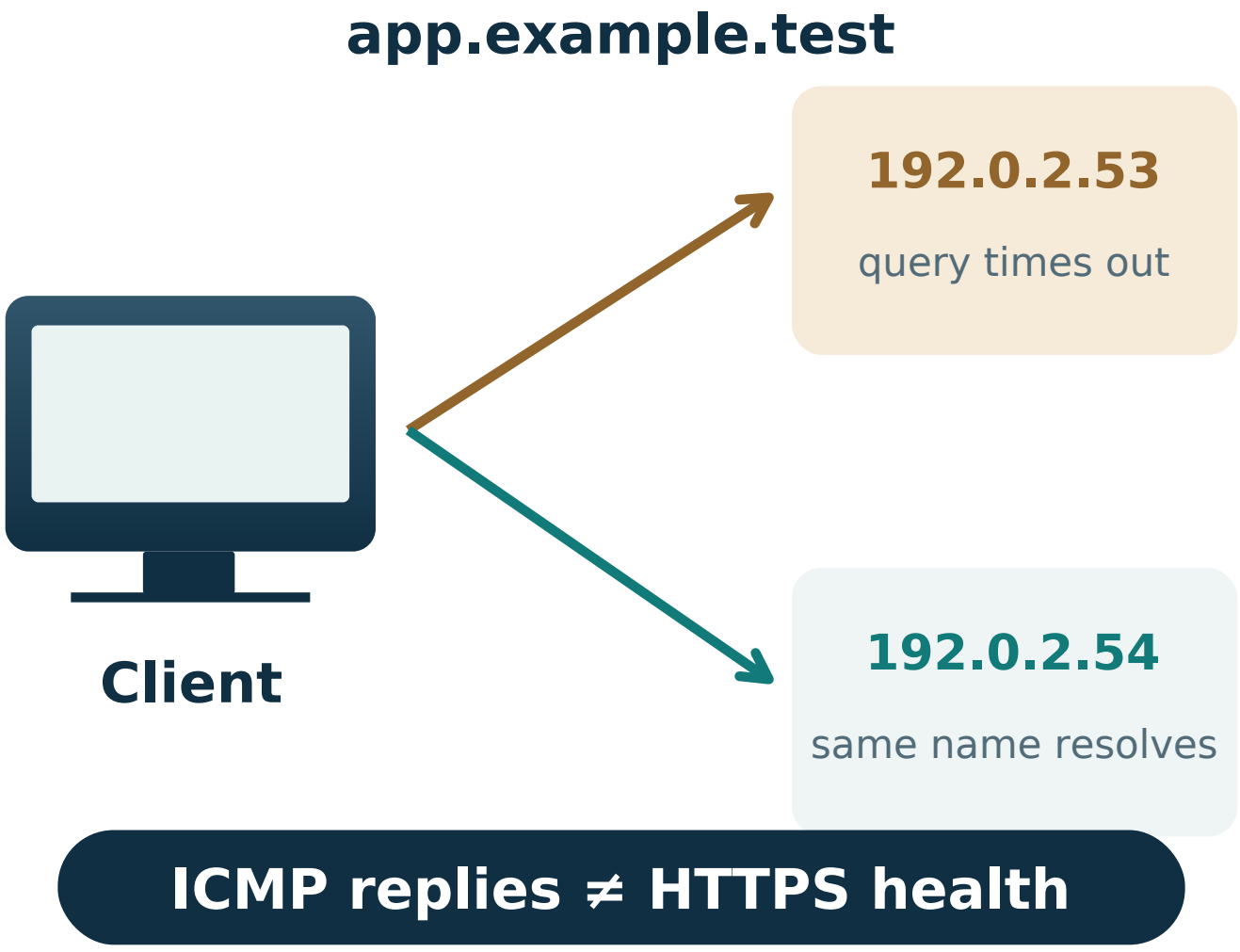
APLUS-U02 / SEE THE CONCEPT

The IP works. The name still fails.

Read the visual model, then test the reasoning.



A timeout narrows the question; it does not finish the diagnosis.

A website fails by name. Fictional documentation-address observations show gateway and remote ICMP replies. The same DNS name times out through one approved resolver and succeeds through another.

APLUS-U02 / WORK THE CASE

The IP works. The name still fails.

Follow the stated conditions. Check the answer against the original case.

CLIENT 192.0.2.34/24 GATEWAY 192.0.2.1

ICMP	Gateway + 198.51.100.20	Replies
DNS 192.0.2.53	app.example.test	Timeout
DNS 192.0.2.54	app.example.test	198.51.100.20

Same queried name + changed approved resolver = a narrower hypothesis.

1. **SEPARATE THE TESTS**

   Gateway and remote ping replies show the stated ICMP reachability. They do not prove HTTPS works or that every route is healthy.

2. **NARROW THE HYPOTHESIS**

   The alternate resolver returns the same name. Investigate the first resolver or the client’s path/policy to it; the exact fault is still unresolved.

3. **VERIFY A TARGETED FIX**

   Compare from a second authorized client and inspect DNS/path logs. After an authorized correction, retest the same query and the actual HTTPS application.

TEST YOUR REASONING

Does a DNS timeout prove that the name does not exist?

No. It records no timely answer to that query. An unavailable resolver and a blocked DNS path still need to be distinguished.

Record time, name, resolver and result. Avoid broad firewall shutdowns and simultaneous unrelated changes; restore the prior setting if the targeted change fails.