

End-to-End principle

End-to-end Principle

- **Broad networking principle**
 - First implementation in French CYCLADES network (after ARPA) (1970)
 - Articulated in its most recognizable form by Saltzer, Reed, Clark (1981) [[paper](#)]
- Guidance on placing functionality such as reliability, security, etc.—in network or at endpoints (hosts)?
 - Argues for endpoint placement

IDEAS

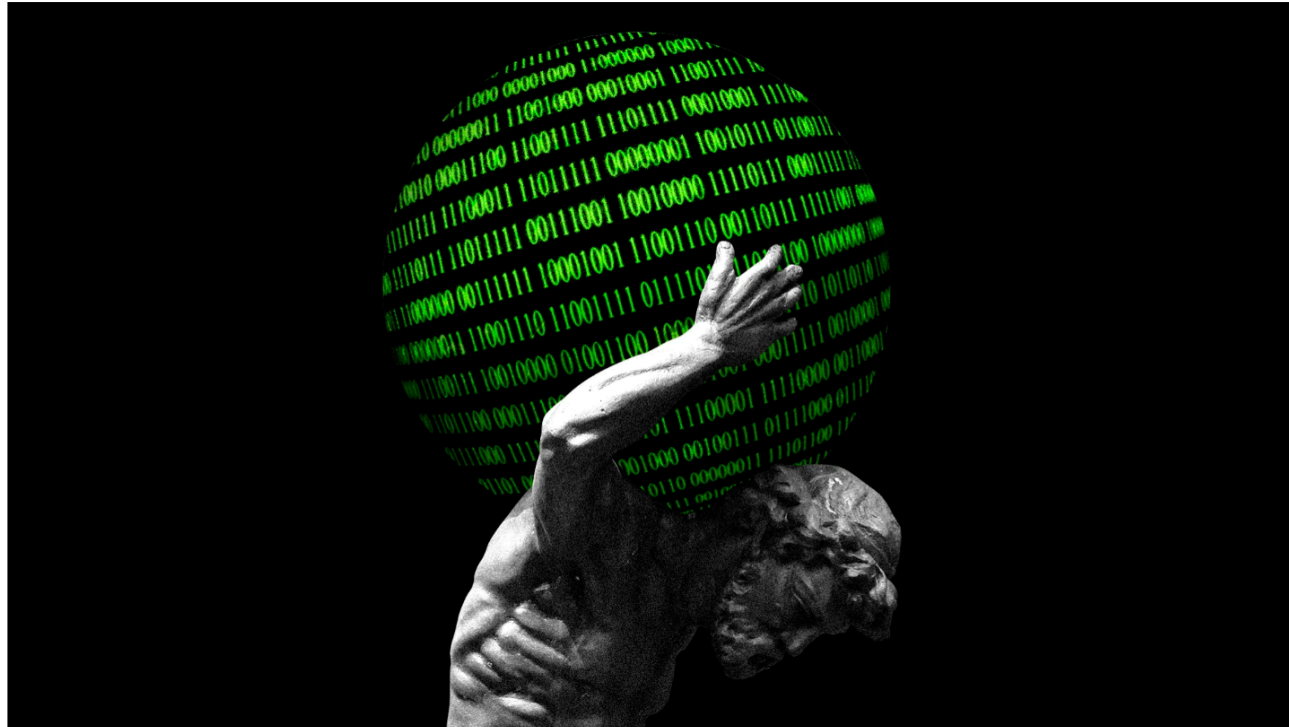
The System That Actually Worked

How the internet kept running even as society closed down around it

MAY 6, 2020

Charles Fishman

Journalist and author of *One Giant Leap*

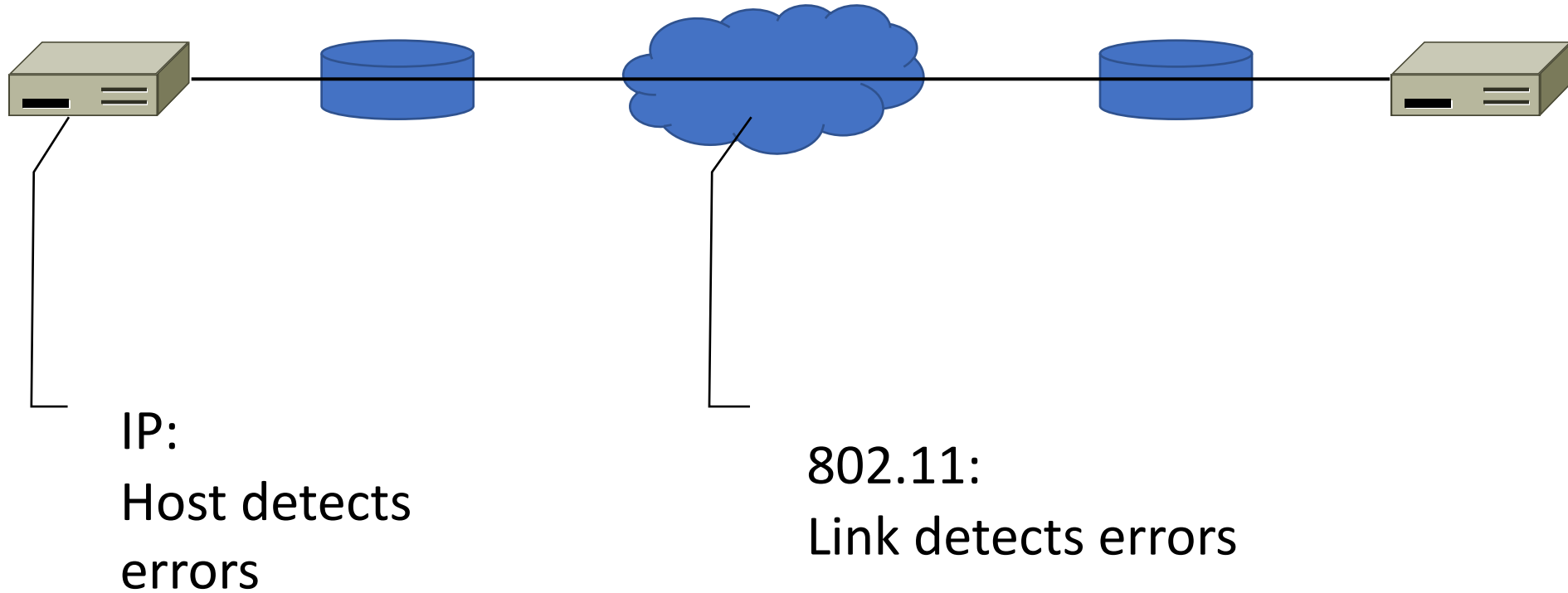


PAUL SPELLA / THE ATLANTIC

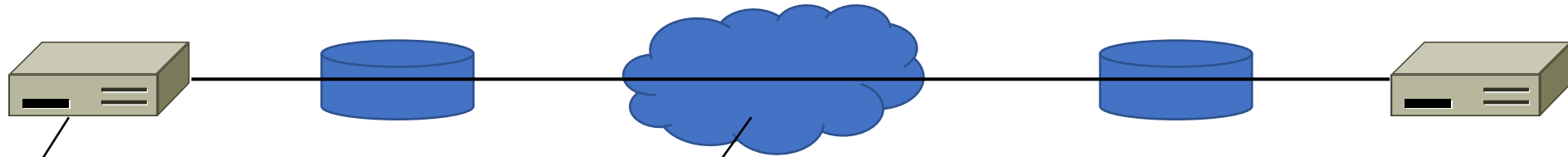
Multiple interpretations of the principle

- The network cannot be trusted. Do it yourself.
 - The network can suffer heavy damage
 - Nuclear attacks (but not DDoS attacks!)
 - Need end-to-end correctness anyway
- Diminishing returns from in-network functionality
 - Not everyone needs it
- Place functionality in the network only when necessary (e.g., for performance)

E2E Example: Error-correcting codes



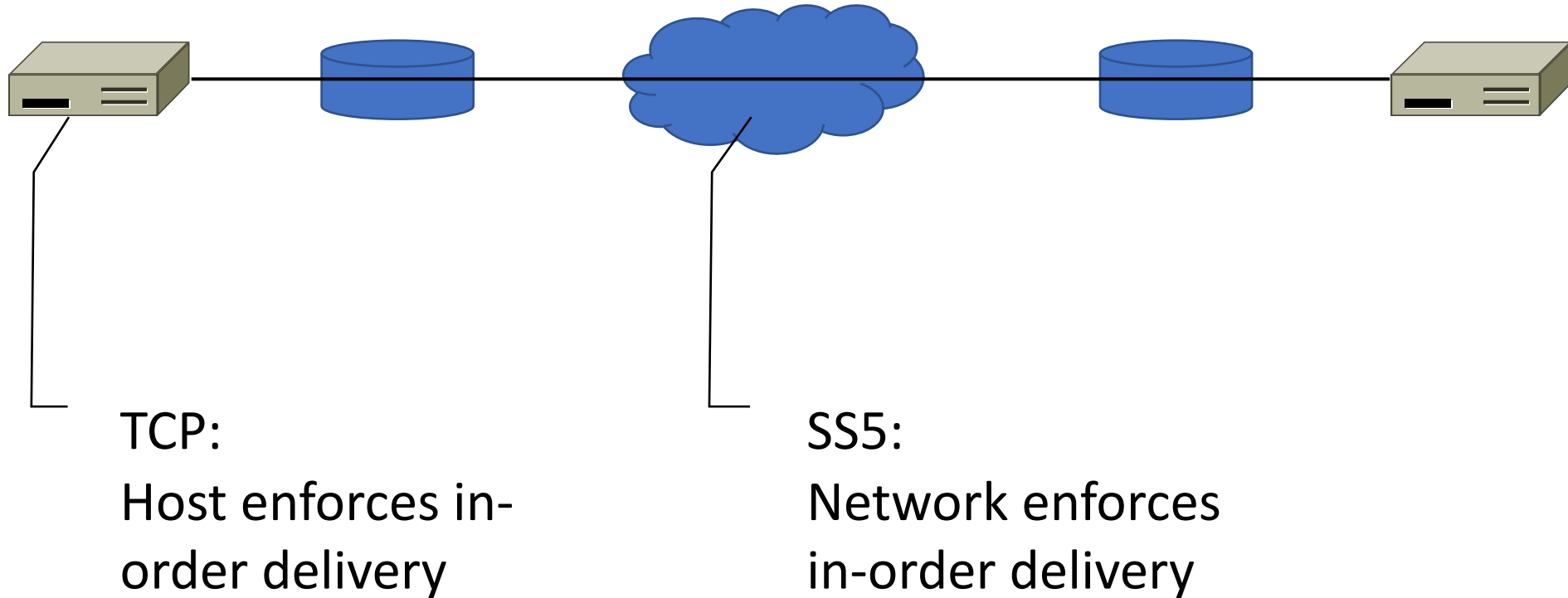
E2E Example: ARQ



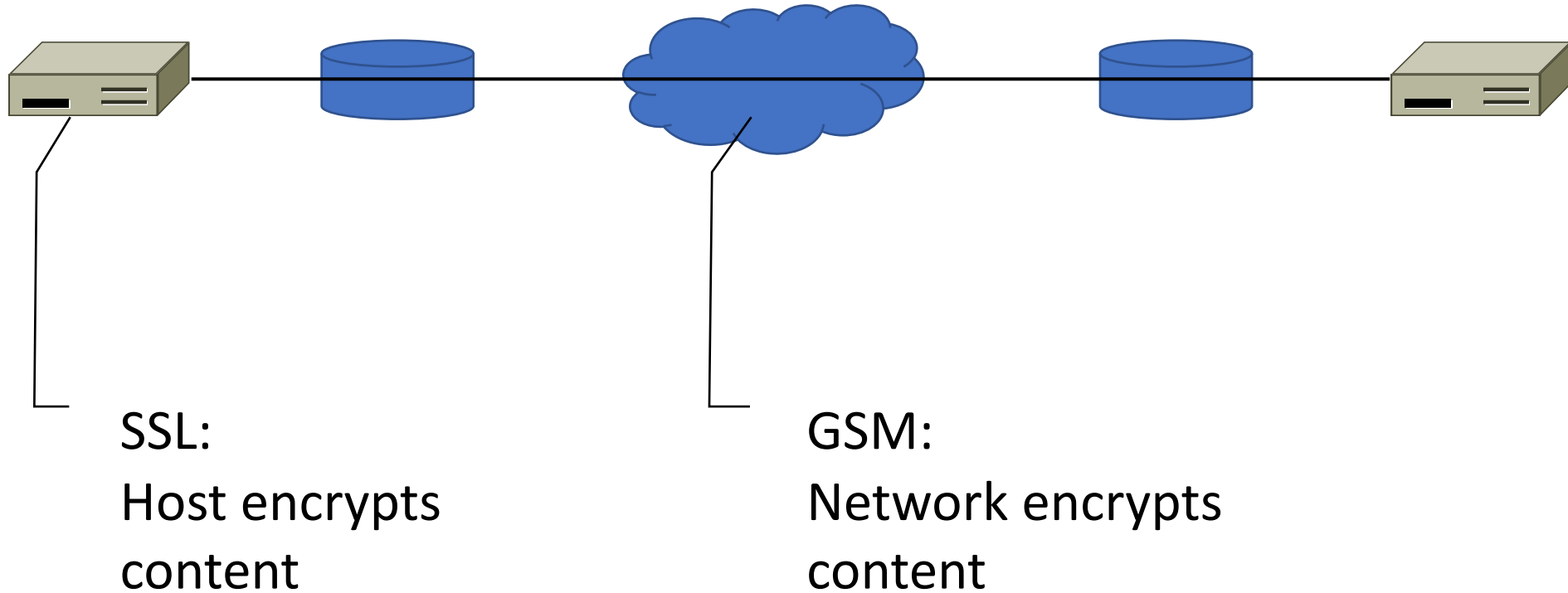
TCP:
Host retransmits
on failure

802.11:
Link detects drops
and retransmits

E2E Example: In-order delivery



E2E Example: Security



End-to-End limitations

- Some functionality cannot be implemented at endpoints
 - NATs, DoS protection, ... the principle is silent on these
- Assumes a clear dividing line between network and endpoints
 - Reality of distributed applications (e.g., CDNs) is more complex
- No guidance on how much functionality can go in the network for performance