COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Networking and Mix networking

Information Privacy with Applications

David Sidi (dsidi@email.arizona.edu)

Administrative Items

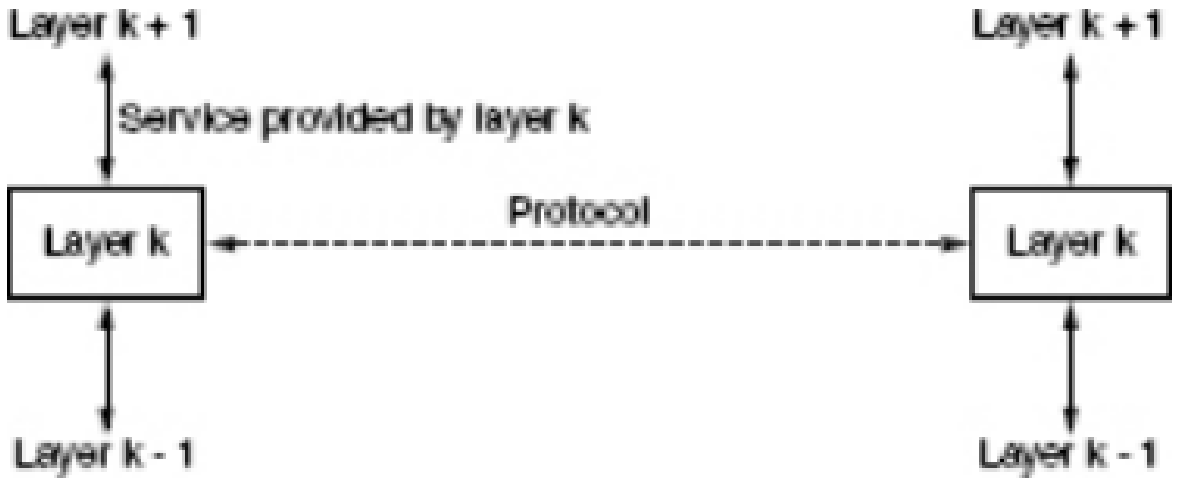
- Final project proposals

Student project example

As conversations were increasingly being had over the phone and internet and computational analysis became more efficient and powerful, someone had the idea that they could listen to what a user was typing on the other end of a conversation and recreate what their keystrokes, just by hearing the clicks of the keyboard. It's not perfect in all cases, but if there is a sufficient sample size an accuracy of more than 90% can be reached. The goal of this project is to prevent any useful data from being gathered through just listening.

Student project example 2

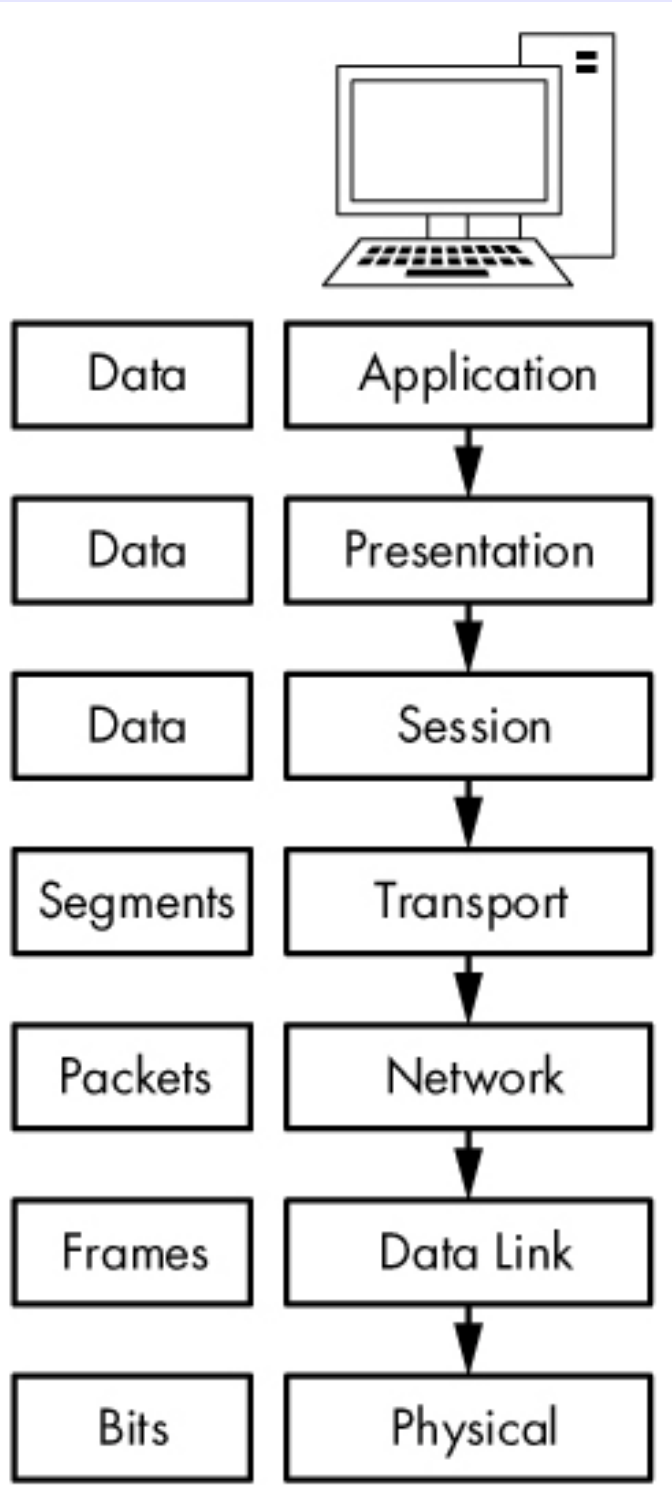
- Obfuscate ourselves on the web for protection
- Obfuscate traffic (headers and JavaScript values)
- Eventually add fake traffic too (fake requests)
- We are trying to address traffic surveillance, browser fingerprinting. We want to browse the web anonymously.
- Fingerprinting and tracking on the web is becoming rampant. We have to fake things because turning JavaScript off and other forms of disabling tracking is itself, a way of fingerprint.

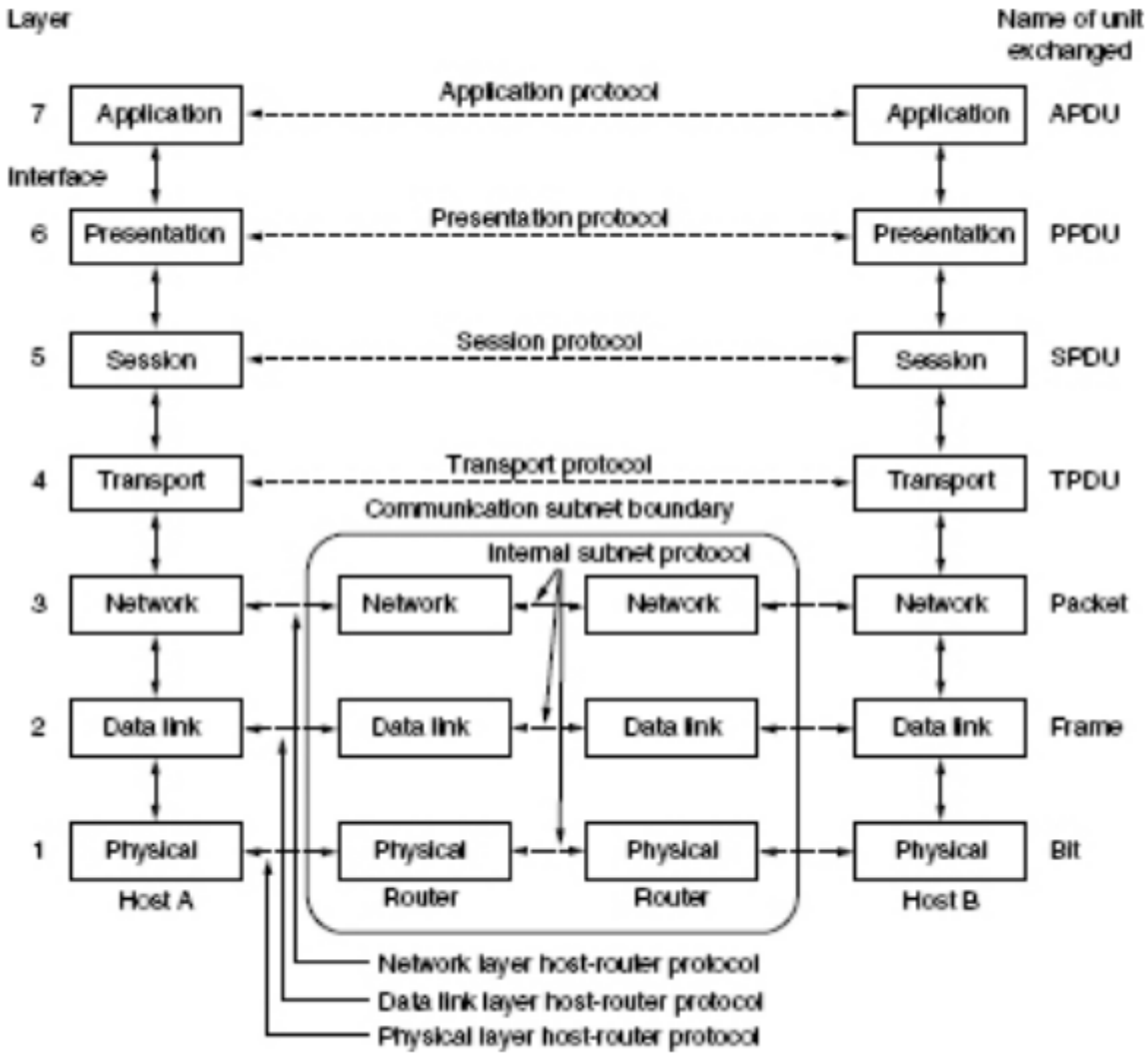


Tanenbaum, A. *Computer Networks*, Figure 1-19.

The Seven-Layer OSI Reference Model

“the way up is the way down.” -Heraclitus

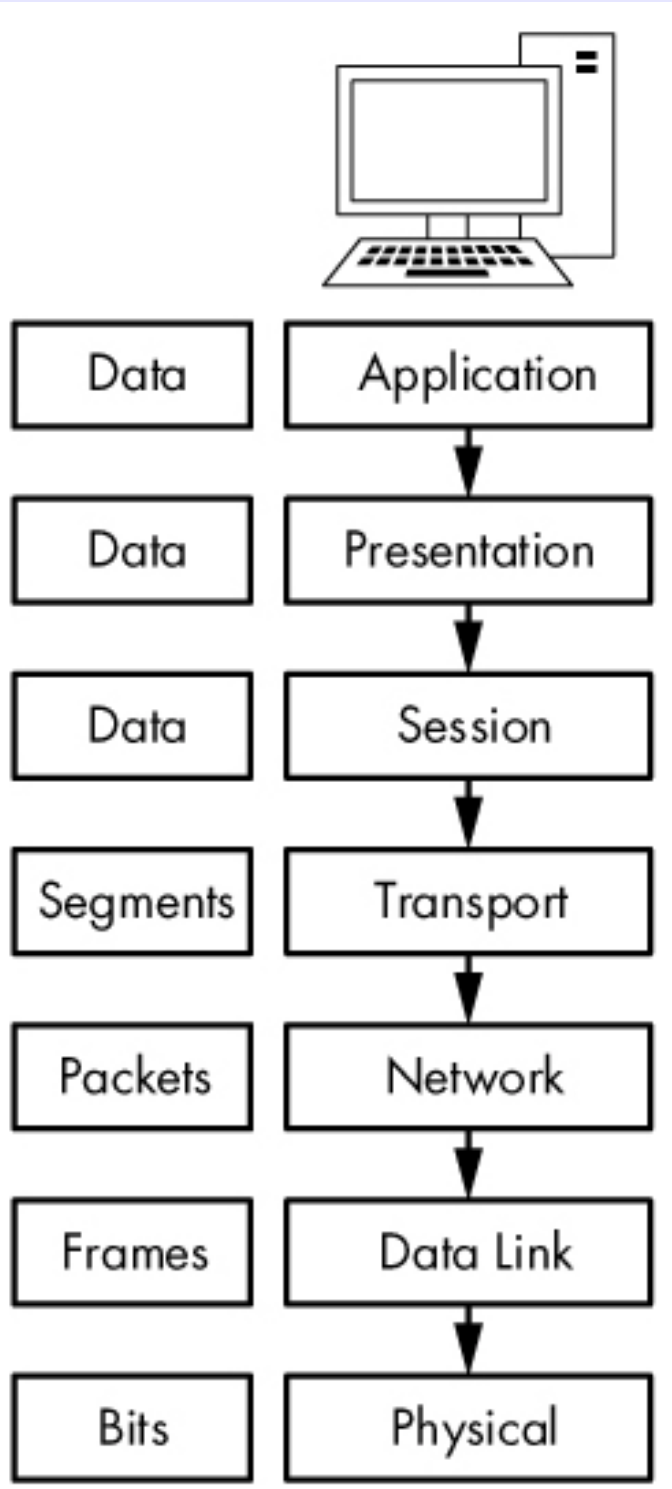




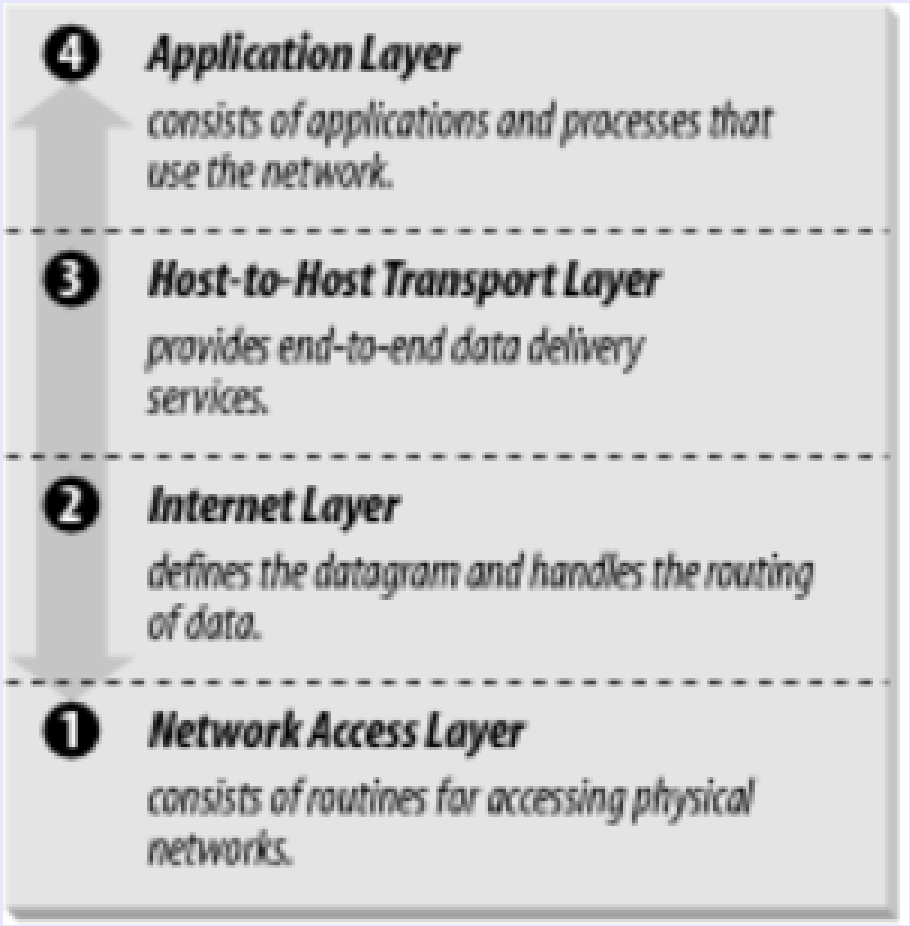
Tanenbaum, A. *Computer Networks*, Figure 1-19.

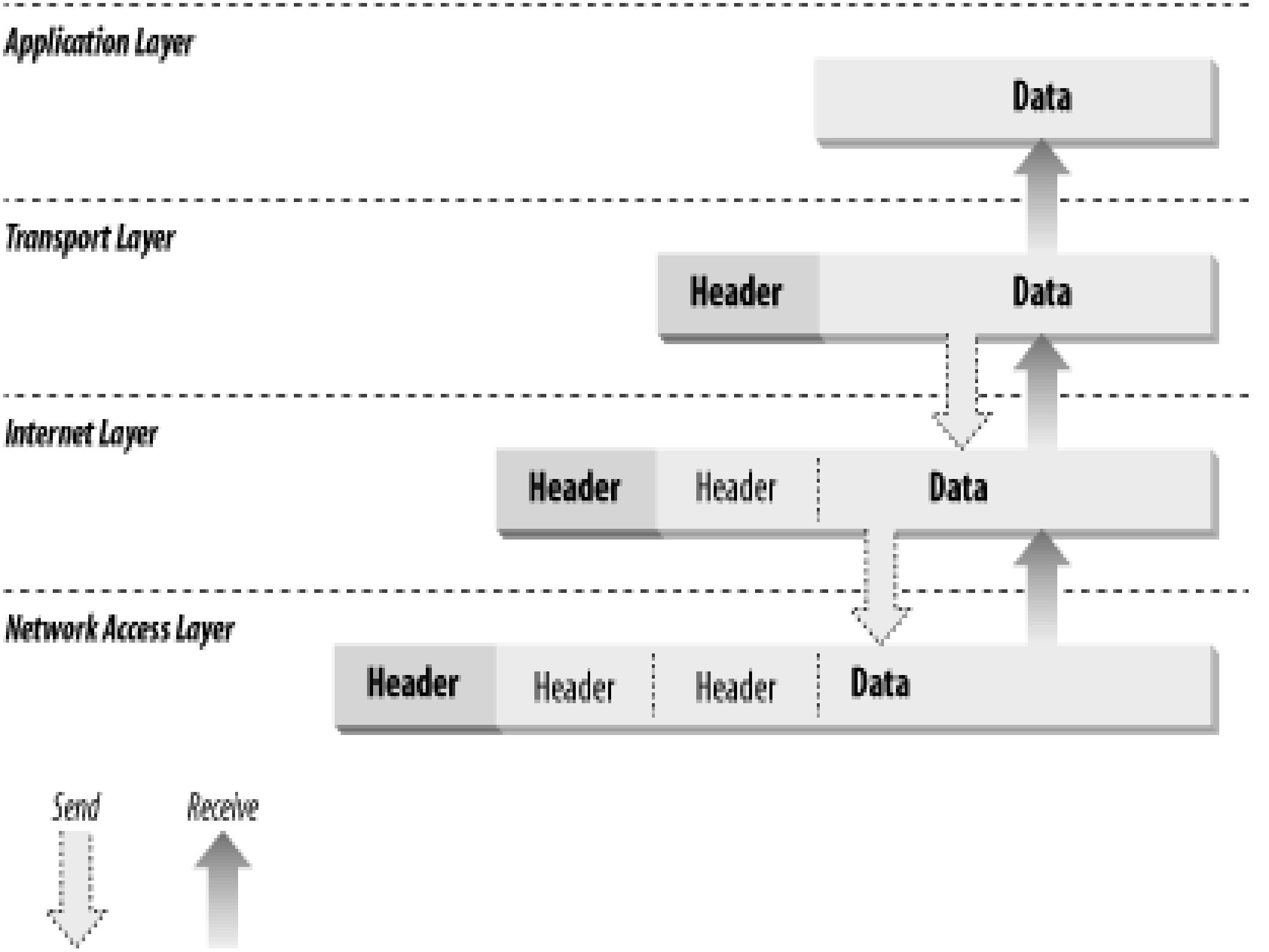
The Seven-Layer OSI Reference Model

“the way up is the way down.” -Heraclitus



TCP/IP Protocol Stack



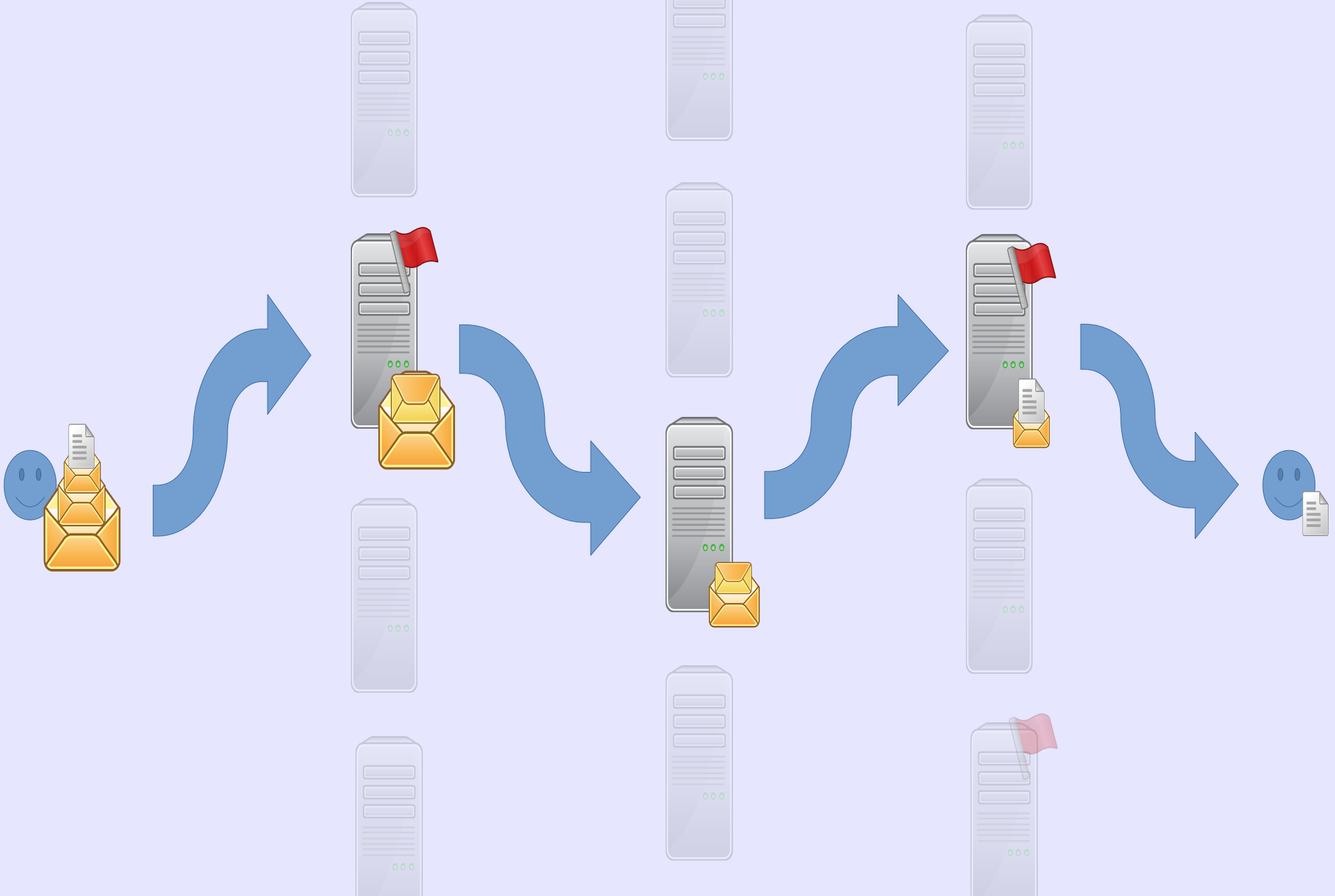

Application Layer
Data
Transport Layer
Header
Data
Internet Layer
Header
Header
Data
Network Access Layer
Header
Header
Header
Data
Send
Receive

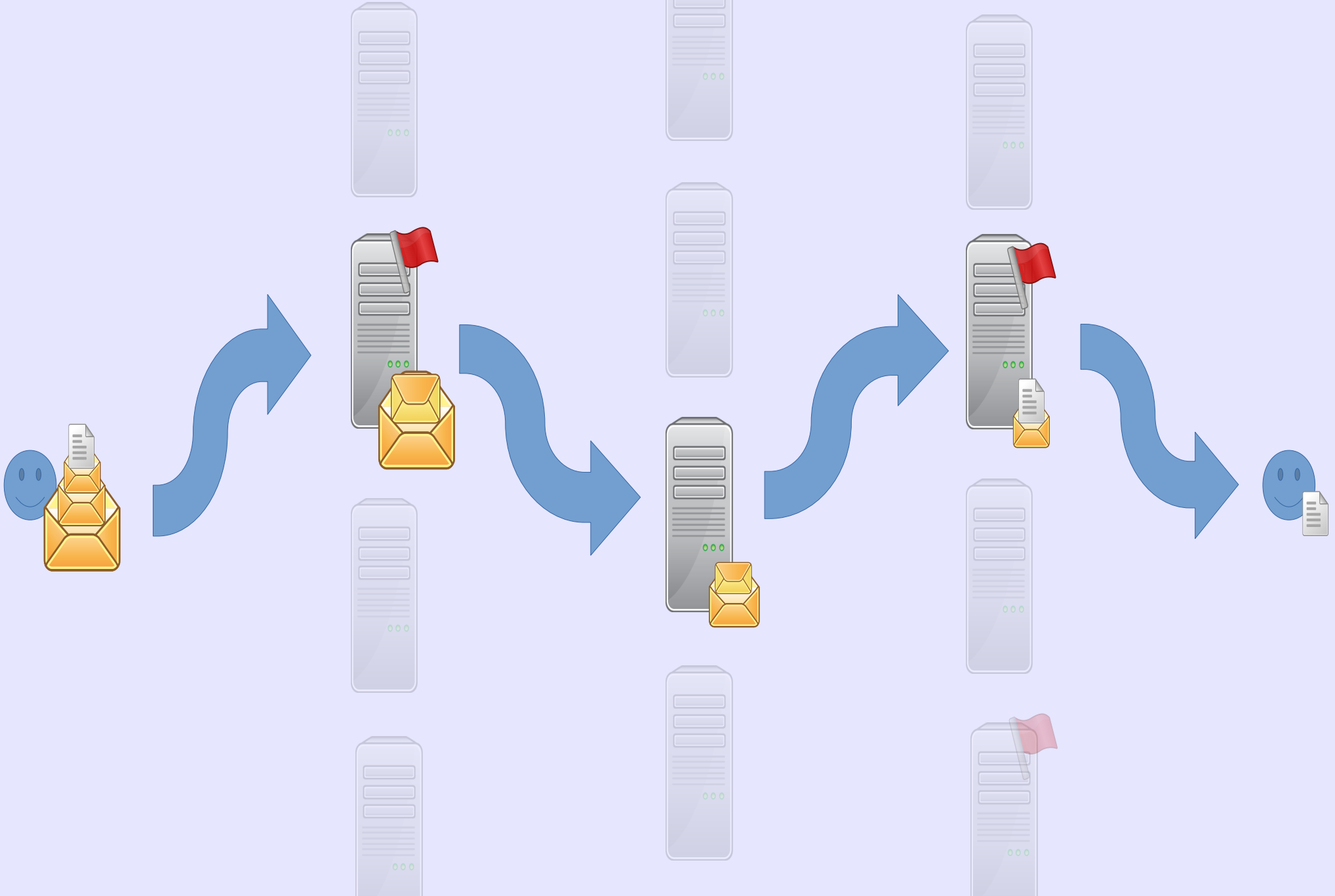
Chaum 1981:

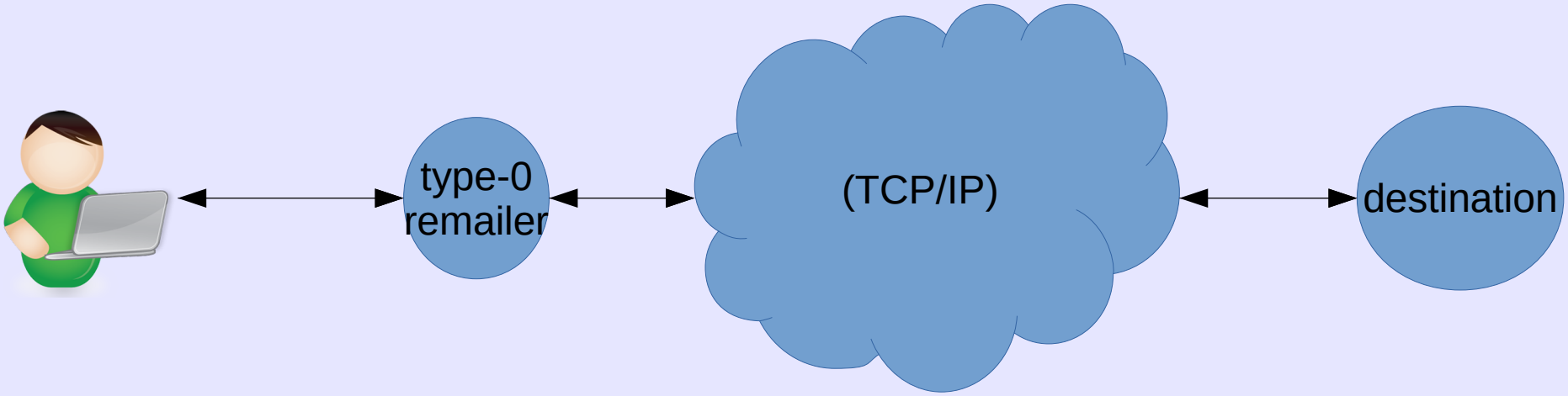
process each item of mail before it is delivered. A participant prepares a message M for delivery to a participant at address A by sealing it with the addressee's public key K_a, appending the address A, and then sealing the result with the mix's public key K_1. The left-hand side of the following expression denotes this item which is input to the mix:

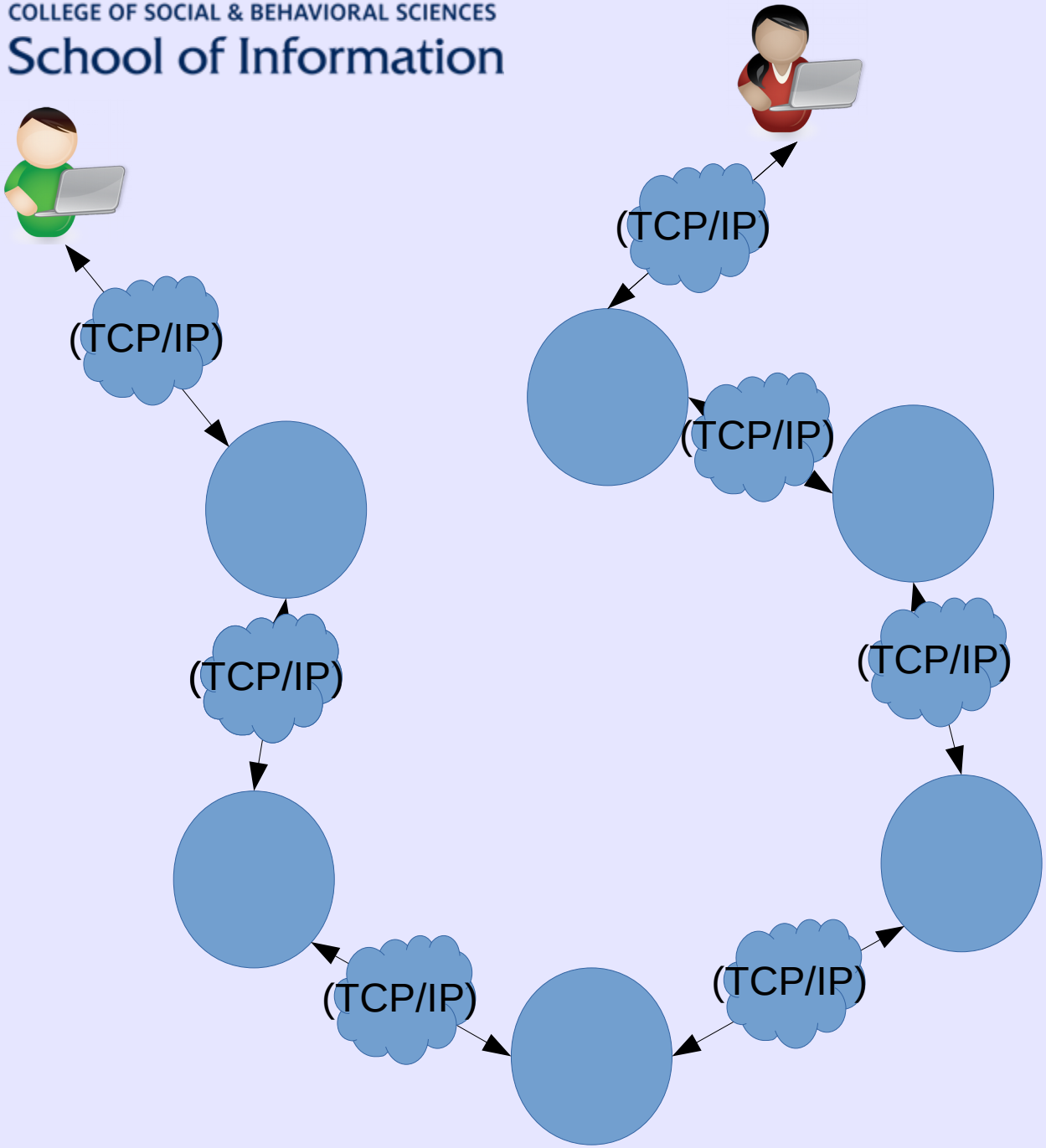
$$K_1(R_1, K_a(R_0, M), A) \rightarrow K_a(R_0, M), A.$$

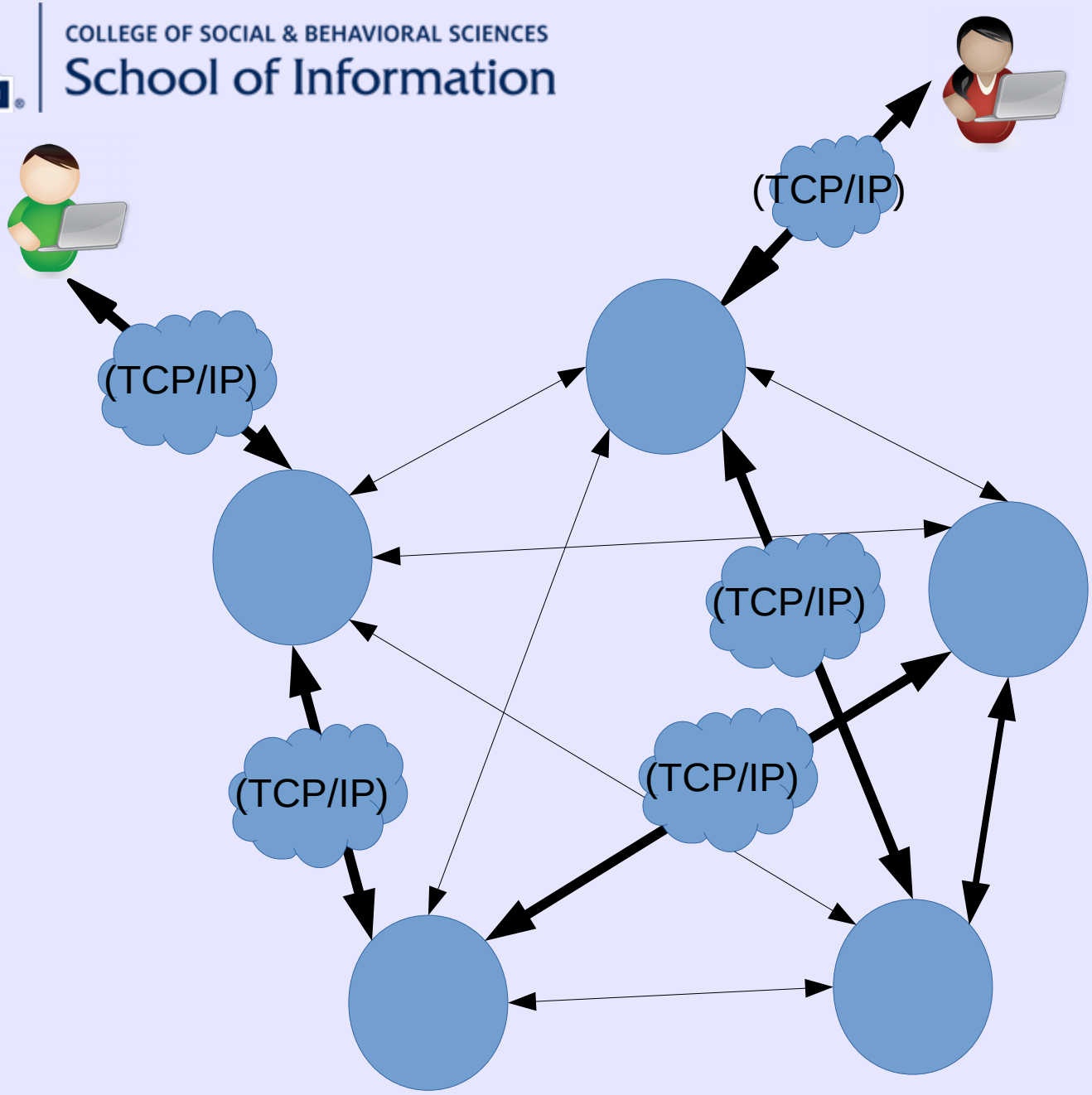
How does the message get to A?
One answer: overlay network

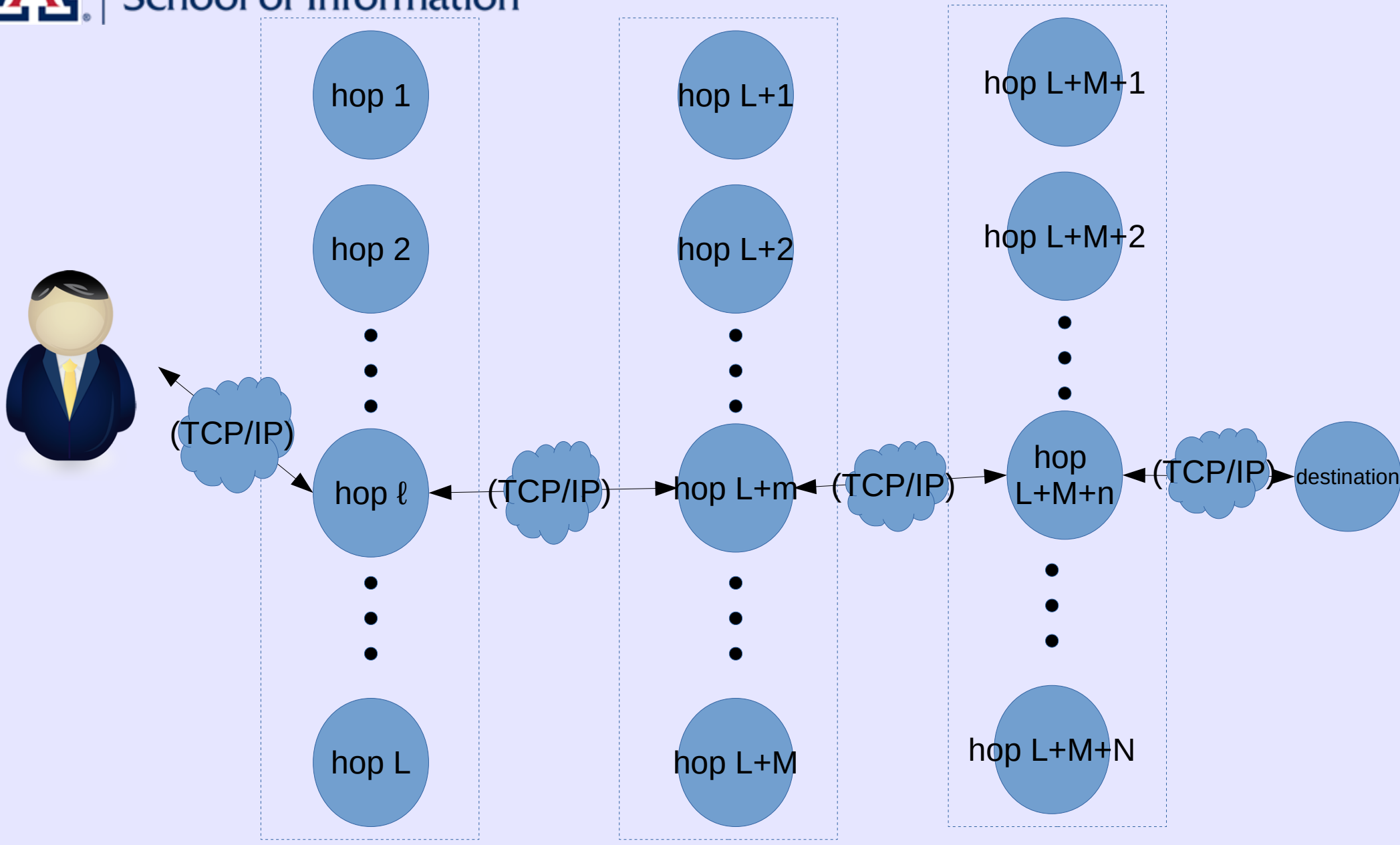


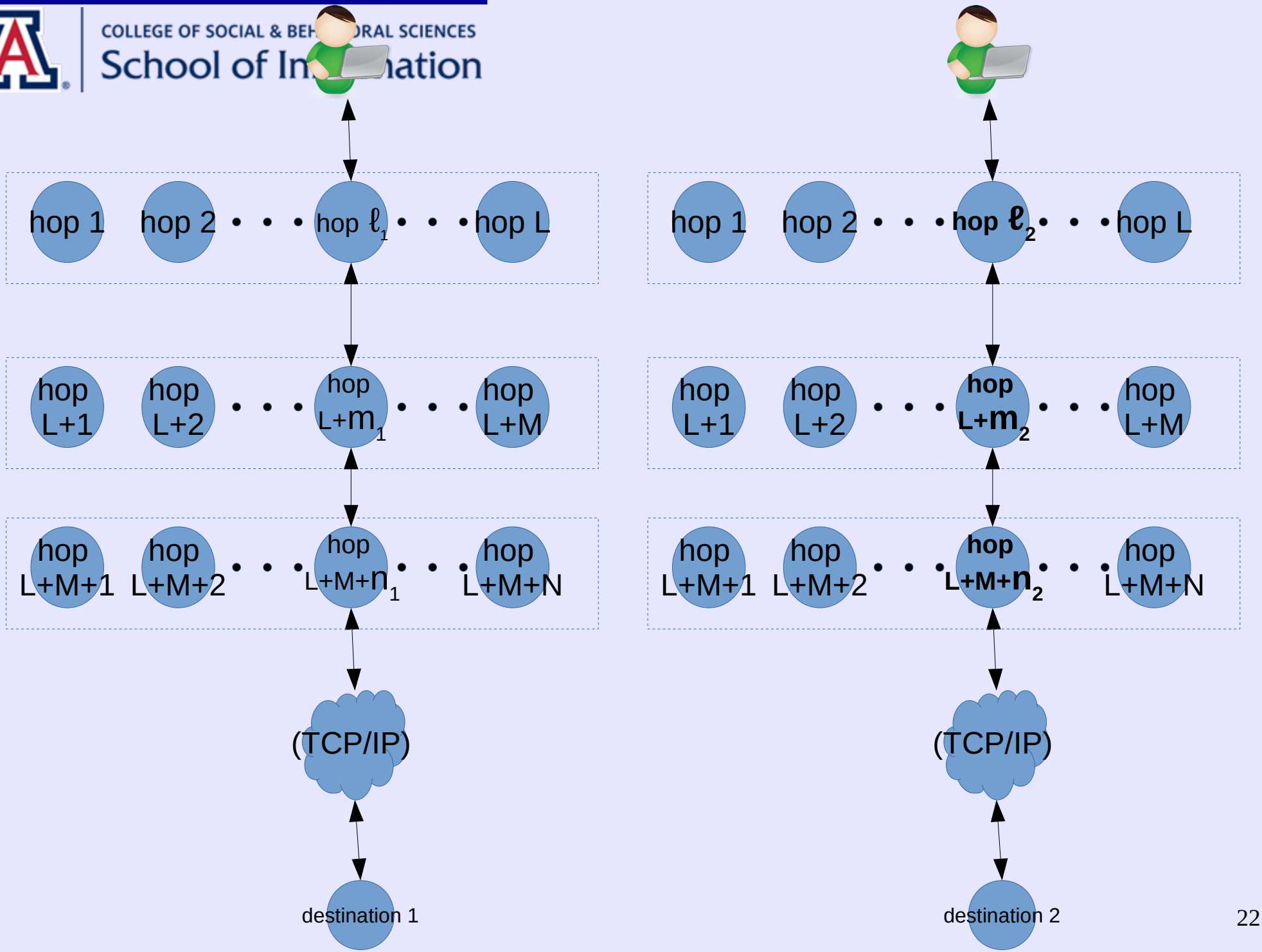



type-0
remailer
(TCP/IP)
destination


(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)


(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)


hop 1
hop 2
hop ℓ
hop L
hop L+1
hop L+2
hop L+m
hop L+M
hop L+M+1
hop L+M+2
hop L+M+n
hop L+M+N
(TCP/IP)
(TCP/IP)
(TCP/IP)
(TCP/IP)
destination


hop 1
hop 2
hop ℓ_1
hop L
hop L+1
hop L+2
hop L+m_1
hop L+M
hop L+M+1
hop L+M+2
hop L+M+n_1
hop L+M+N
(TCP/IP)
destination 1
hop 1
hop 2
hop ℓ_2
hop L
hop L+1
hop L+2
hop L+m_2
hop L+M
hop L+M+1
hop L+M+2
hop L+M+n_2
hop L+M+N
(TCP/IP)
destination 2

Topologies for Mixnets

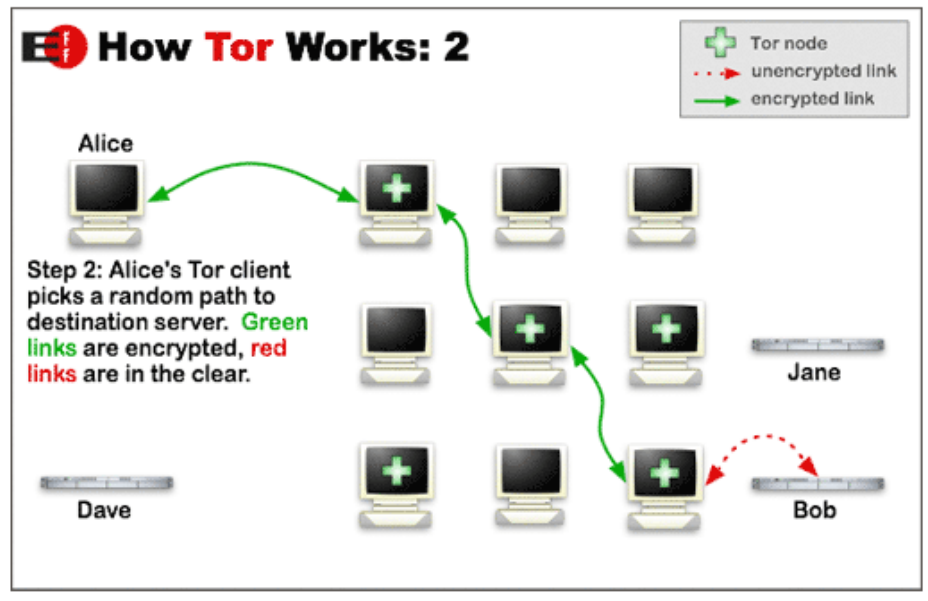
- Cascading: All nodes are always used, in the same order
- Scalability is a problem, requires setting up a fixed route with all nodes
- Only requires one honest node to preserve anonymity

Topologies for Mixnets

- User specified: user arbitrarily picks its route through the network
- Scalable, does not require initial configuration of a route
- Not anonymous if only one node is honest (nodes can figure out their positions)

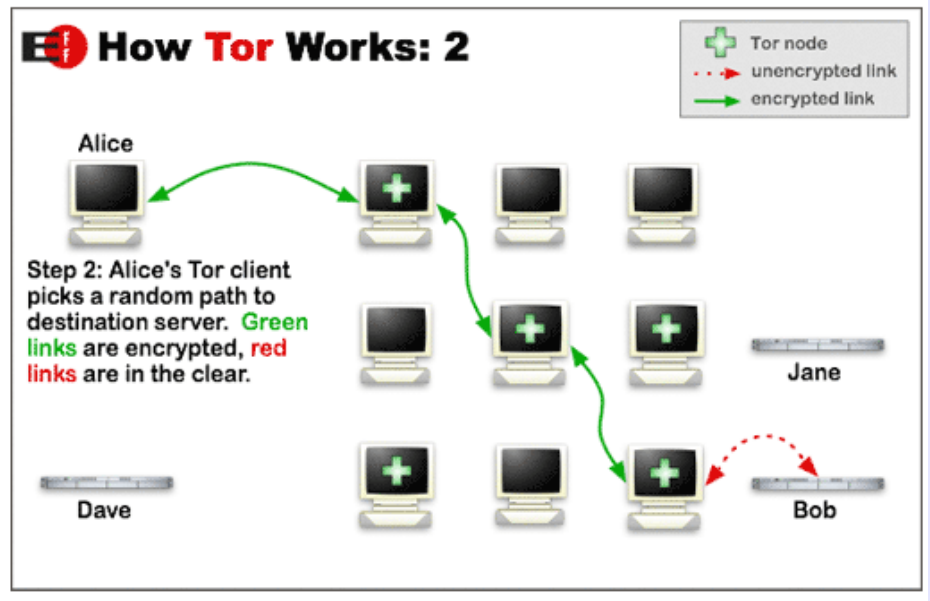
Onion Routing

- First was from the US Naval Laboratory, 1996
  - pure peering at this stage, loafers!
- Freedom Network was an independent onion routing network from Zero Knowledge Systems
- Tor is a third-gen. onion routing network



Tor is an onion routing system

- Example: simplified, slightly out-of-date Tor (*link*)
- Distributed TCP overlay network
- Sets up a “virtual circuit” as a cascade of three onion relays (OR) from the initial client onion proxy (OP)
- guard (from “helper nodes”), relay, and exit nodes
  - each node only knows its immediate predecessor and successor



Tor is an onion routing system

- originally, onion routing systems sent an initial onion message that was “just layers” to set up the circuit; Tor does it in stages (“telescoping”)
- Next hop in the circuit is determined by unwrapping an “extend” relay cell with a symmetric key, which causes the OR to send its own “create” control cell

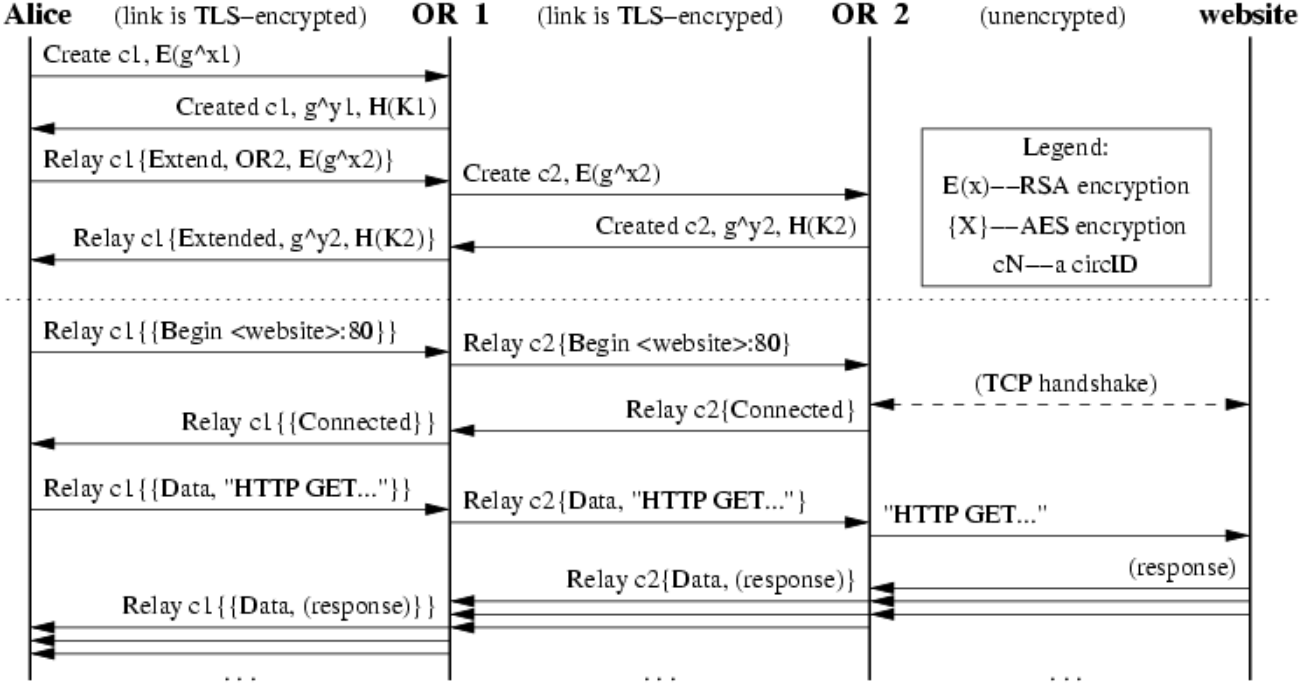


Figure 1: Alice builds a two-hop circuit and begins fetching a web page.

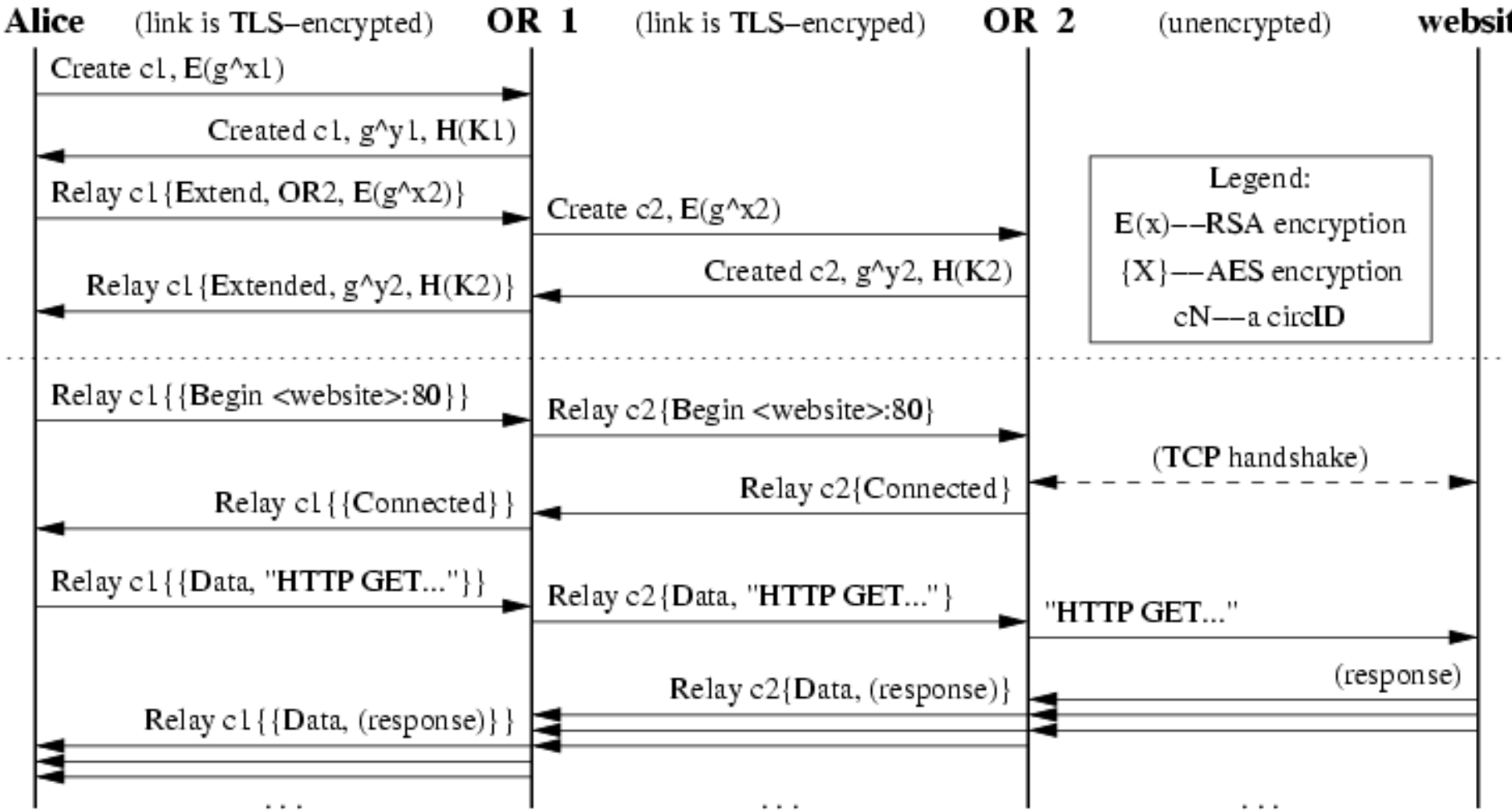


Figure 1: Alice builds a two-hop circuit and begins fetching a web page.