CS 6014 — Networking and Security

Instructor: Matthew Flatt
mflatt@cs.utah.edu

About This Course

Networking:

- Top-down dive into how networks work
- Lots of terminology
- Some programming APIs

Cryptography:

- Principles of secure communication
- *Why* and *how* of the math
- Some specific algorithms

Computer/Network Security:

- Putting the pieces together
- Consequences of failure

Goals

For future situations where you build software that communicates, this course should help you

- know what components you need to build on,
- diagnose networking problems, and
- build systems that are secure.

About the Instructor

My research is in *programming languages*

I develop a language called **Racket**

About the Instructor

Racket provides networking libraries

I develop and manage several online services:

- Racket nightly builds
- Racket package system
- CS 3520 handin server
- Department graduate admissions server
- Department course-tracking server

So, not a networking or security expert in the academic sense, but a long-time practitioner

Homework, Midterm, and Grading

- 3 written assignments
- 3 programming assignments — 70% of grade
- 1 team presentation

Midterm exam: February 28 — 15% of grade

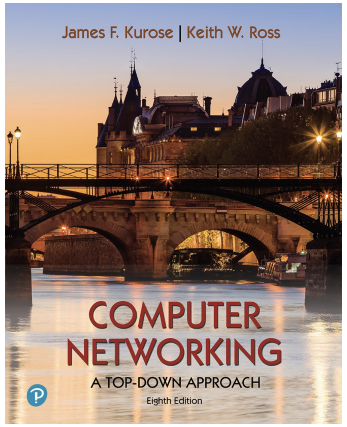
Class participation — 15% of grade

Videos and Lecture

A set of videos accompanies each day's lecture

These videos are a kind of "textbook" for the course that you can watch before/after class

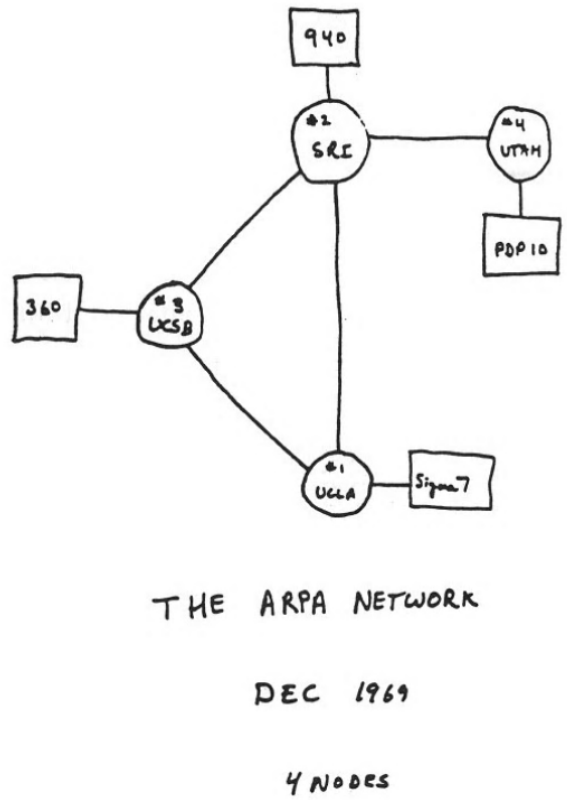
Real textbook:



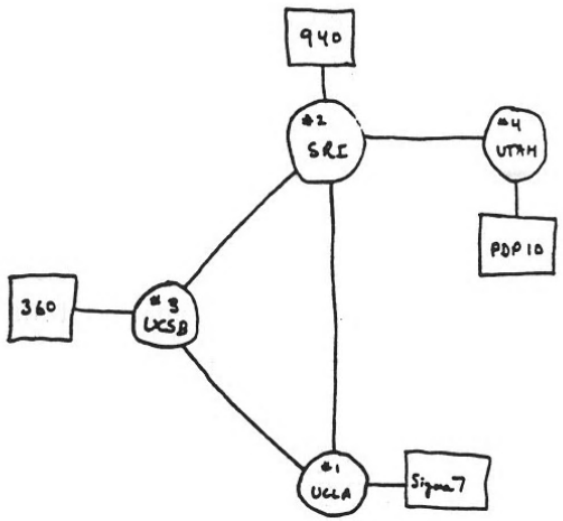
Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
2020

Some slide diagrams are based on this book

The Internet



The Internet



THE ARPA NETWORK

DEC 1969

4 NODES

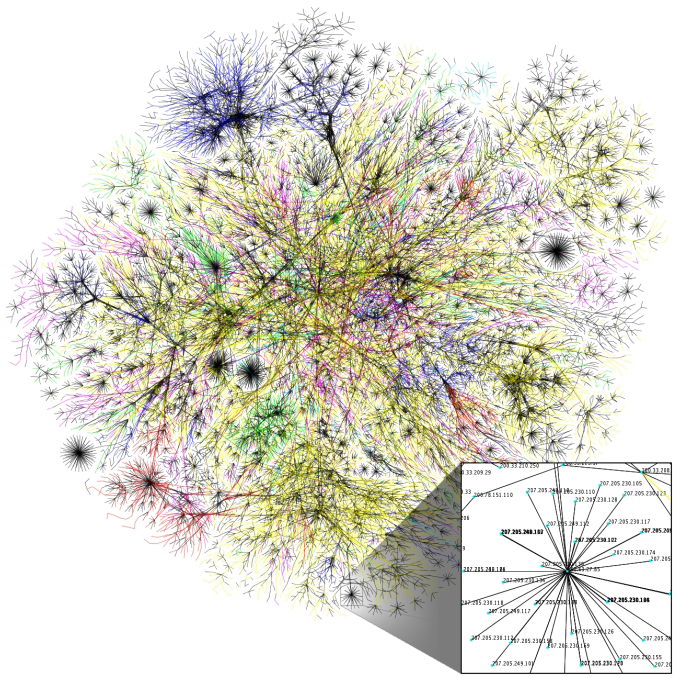
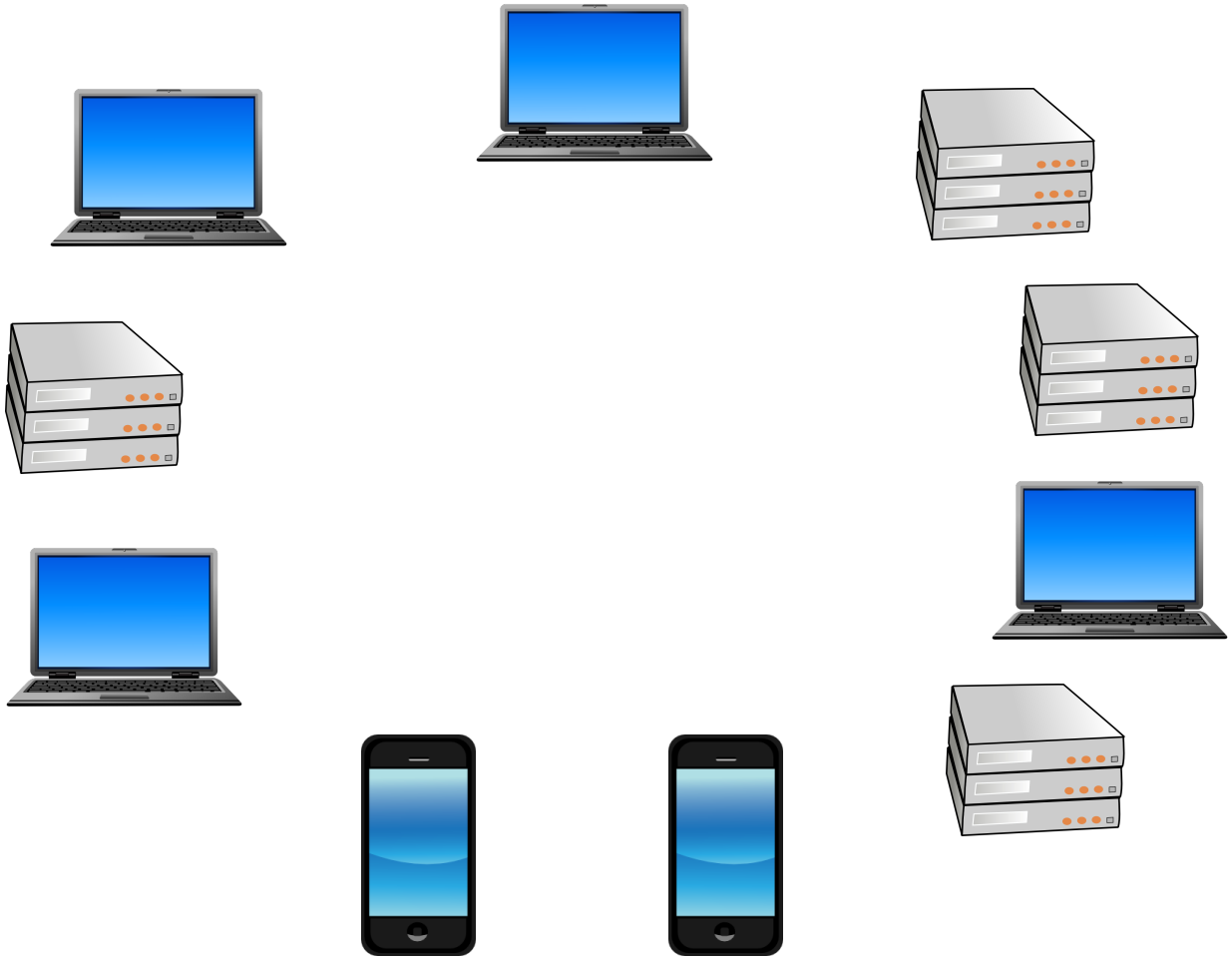


image from
wikipedia.org

Today

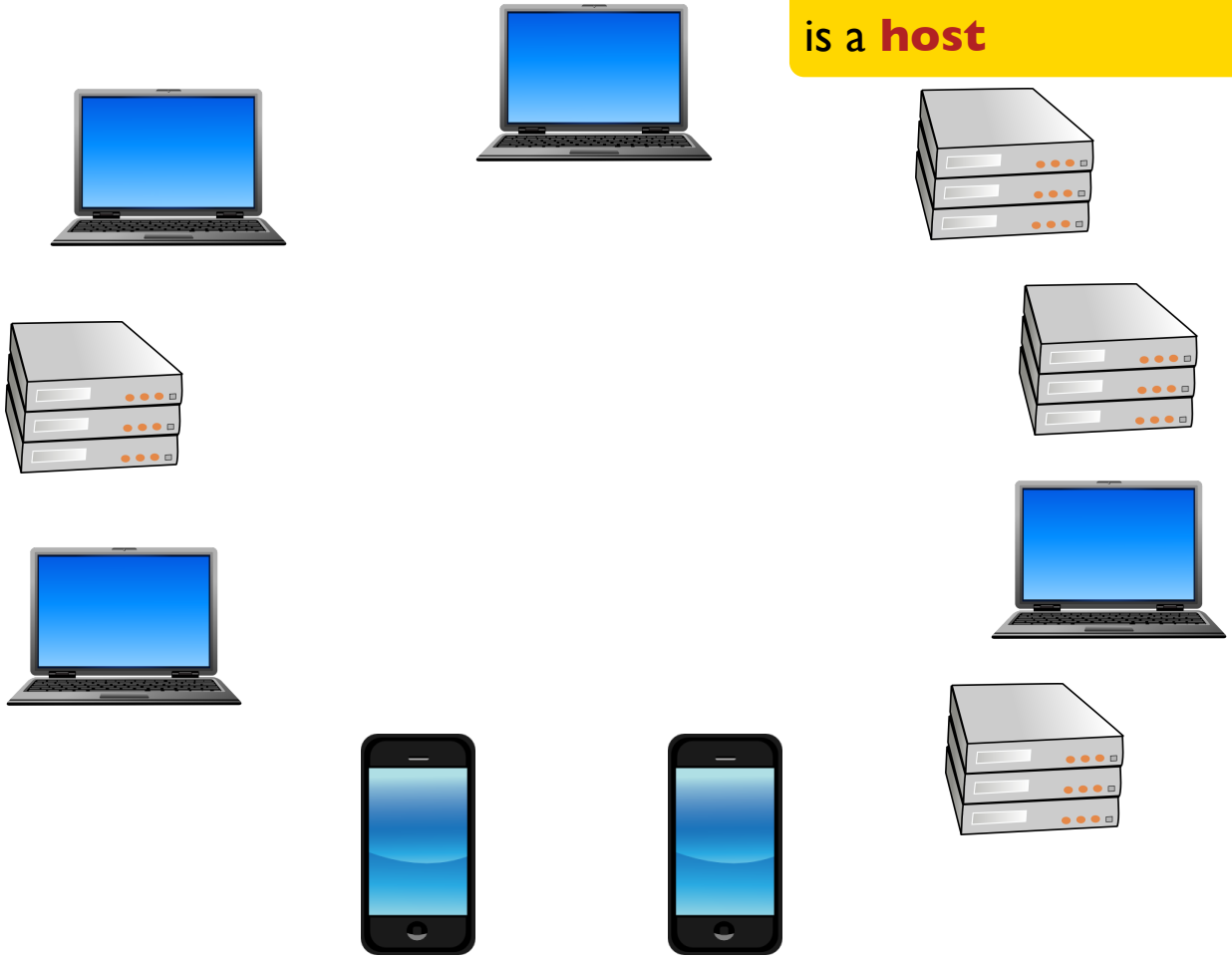
15,000,000,000 nodes

The Internet



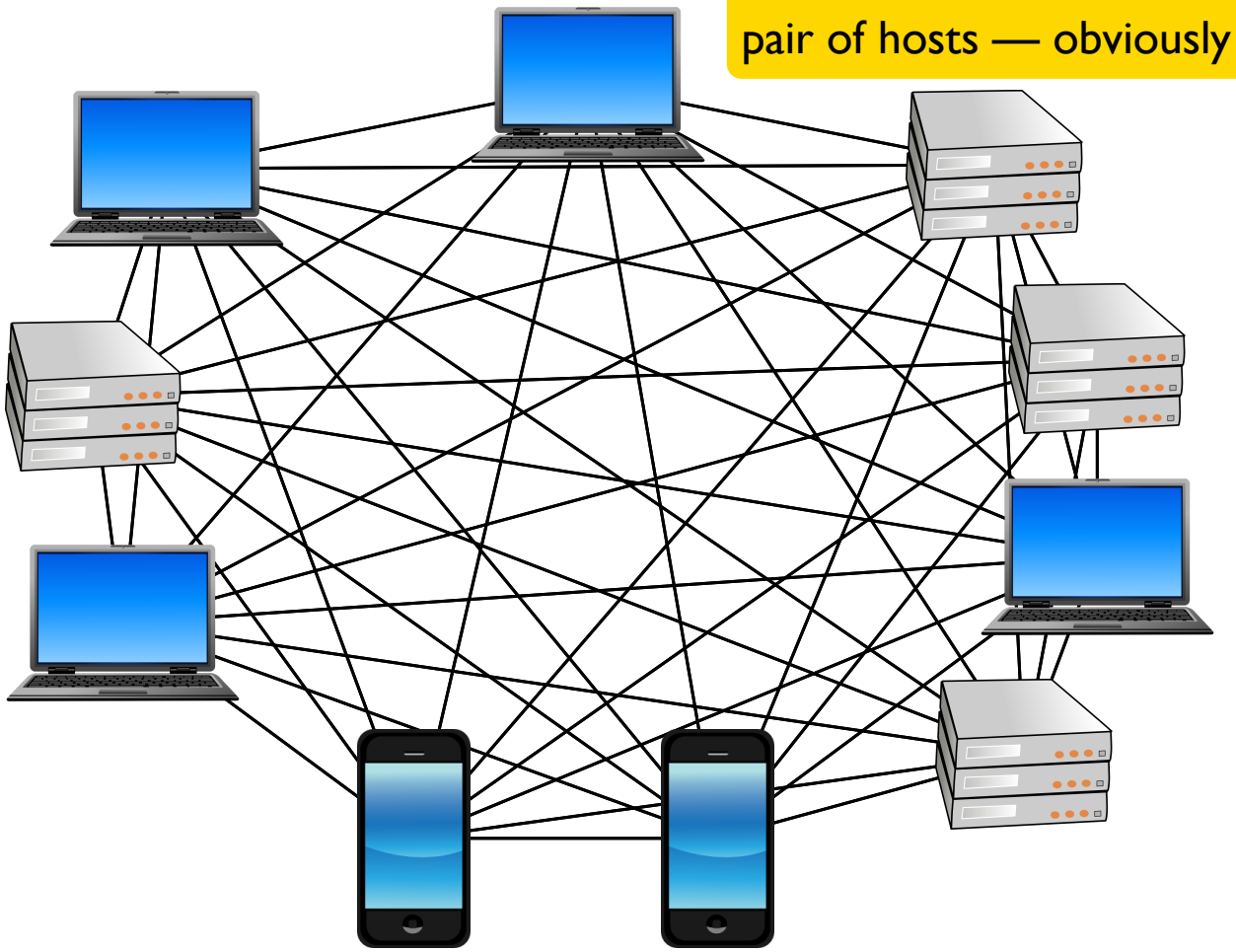
The Internet

Each **node** with applications is a **host**

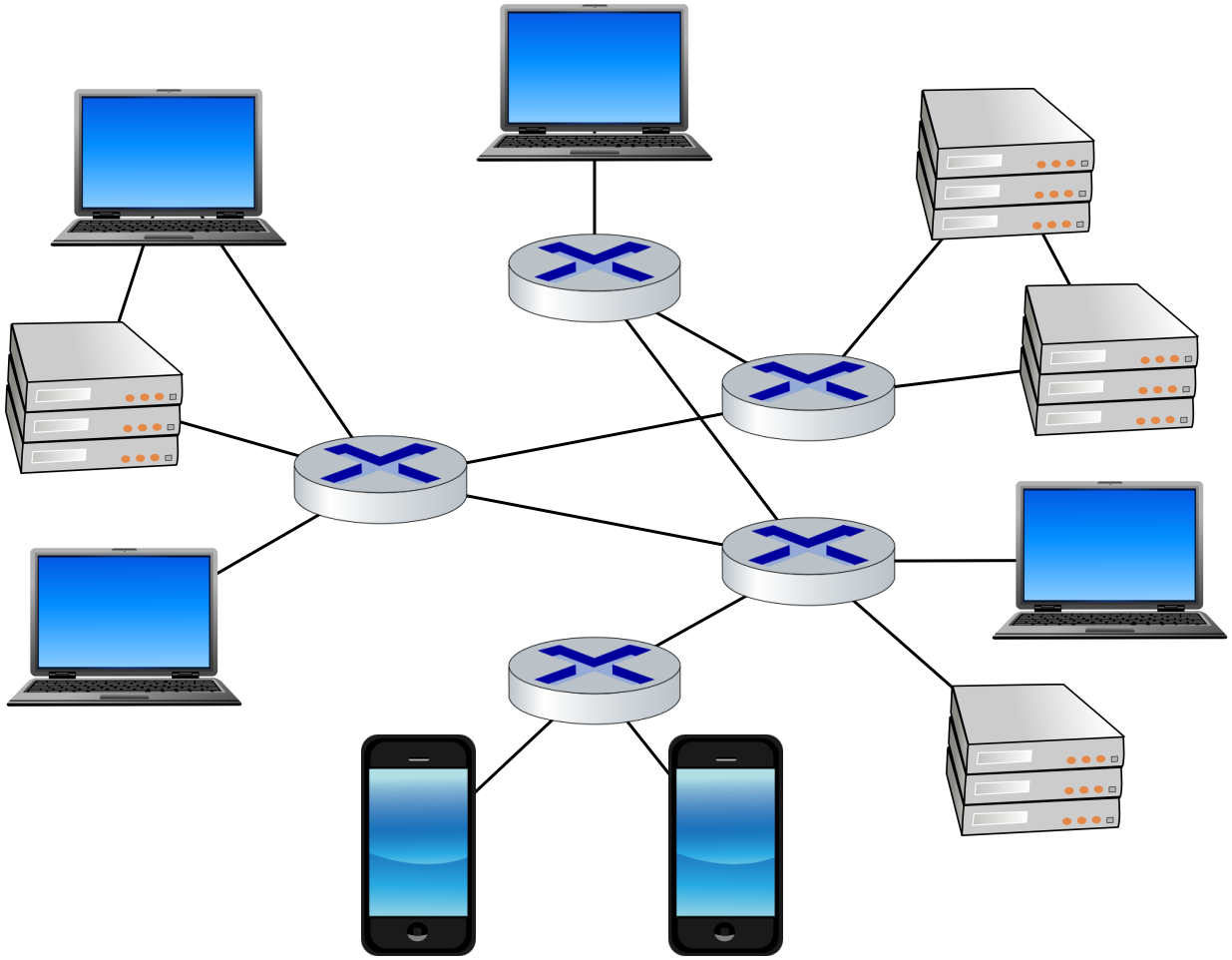


The Internet

Direct connection between every pair of hosts — obviously impractical

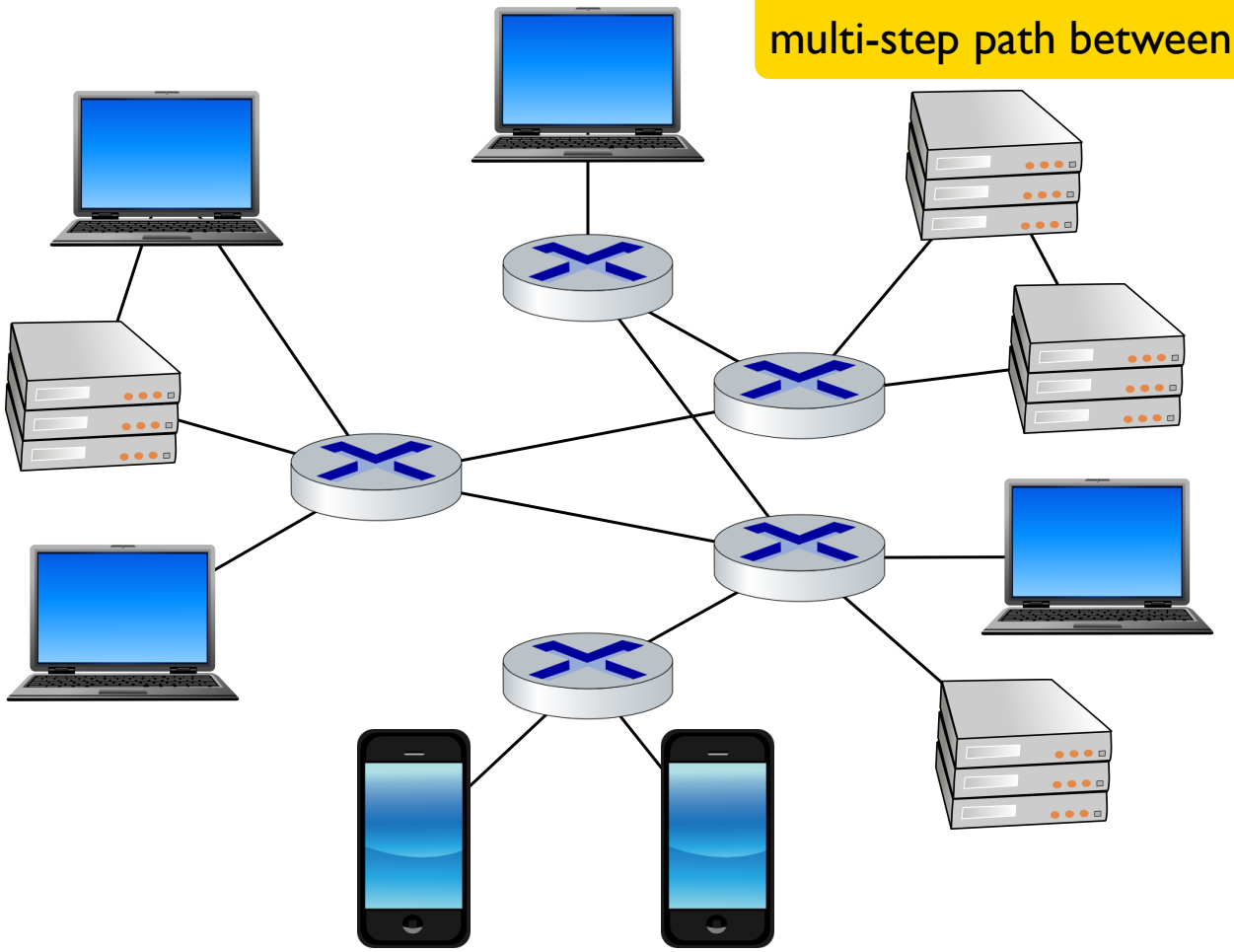


The Internet

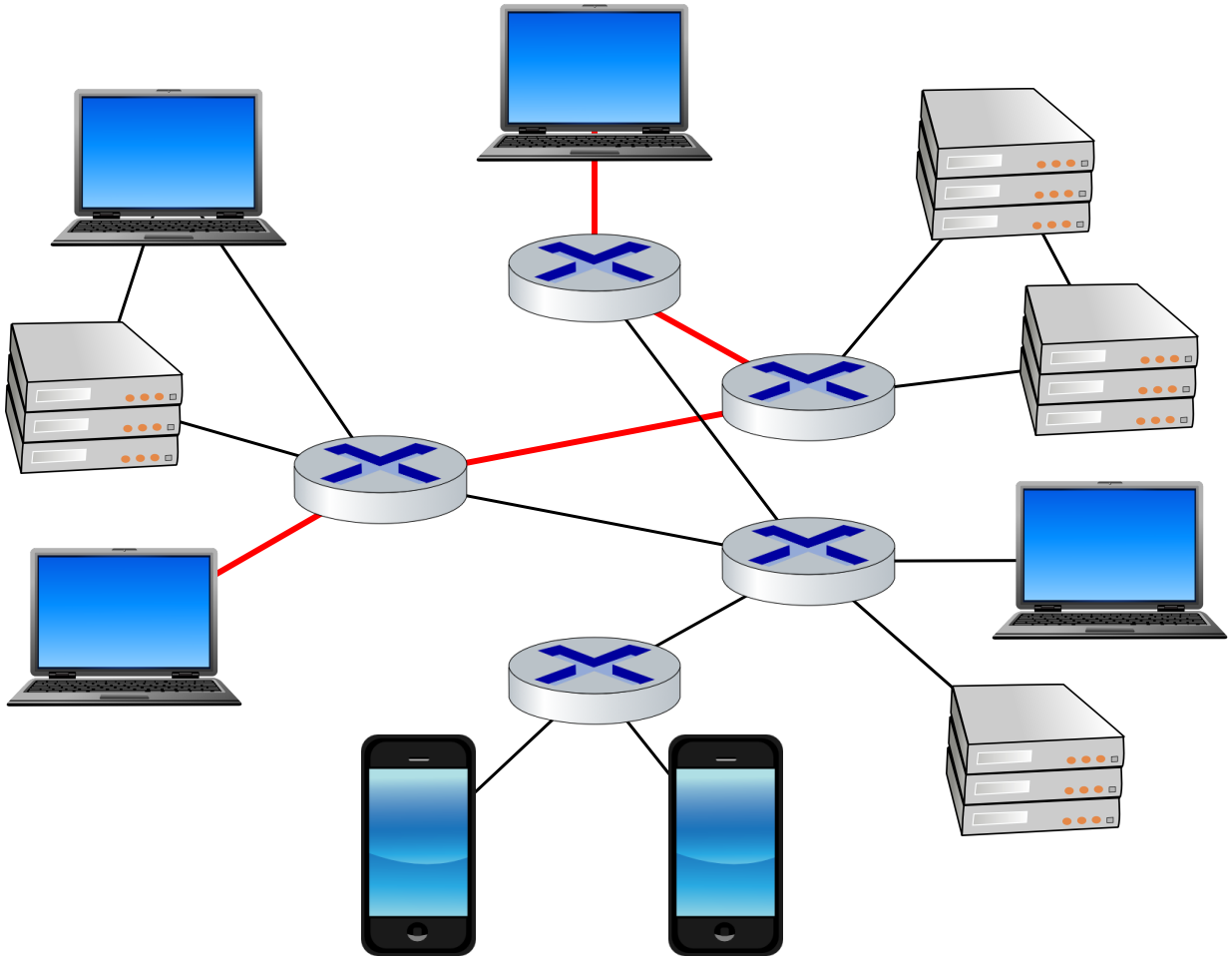


The Internet

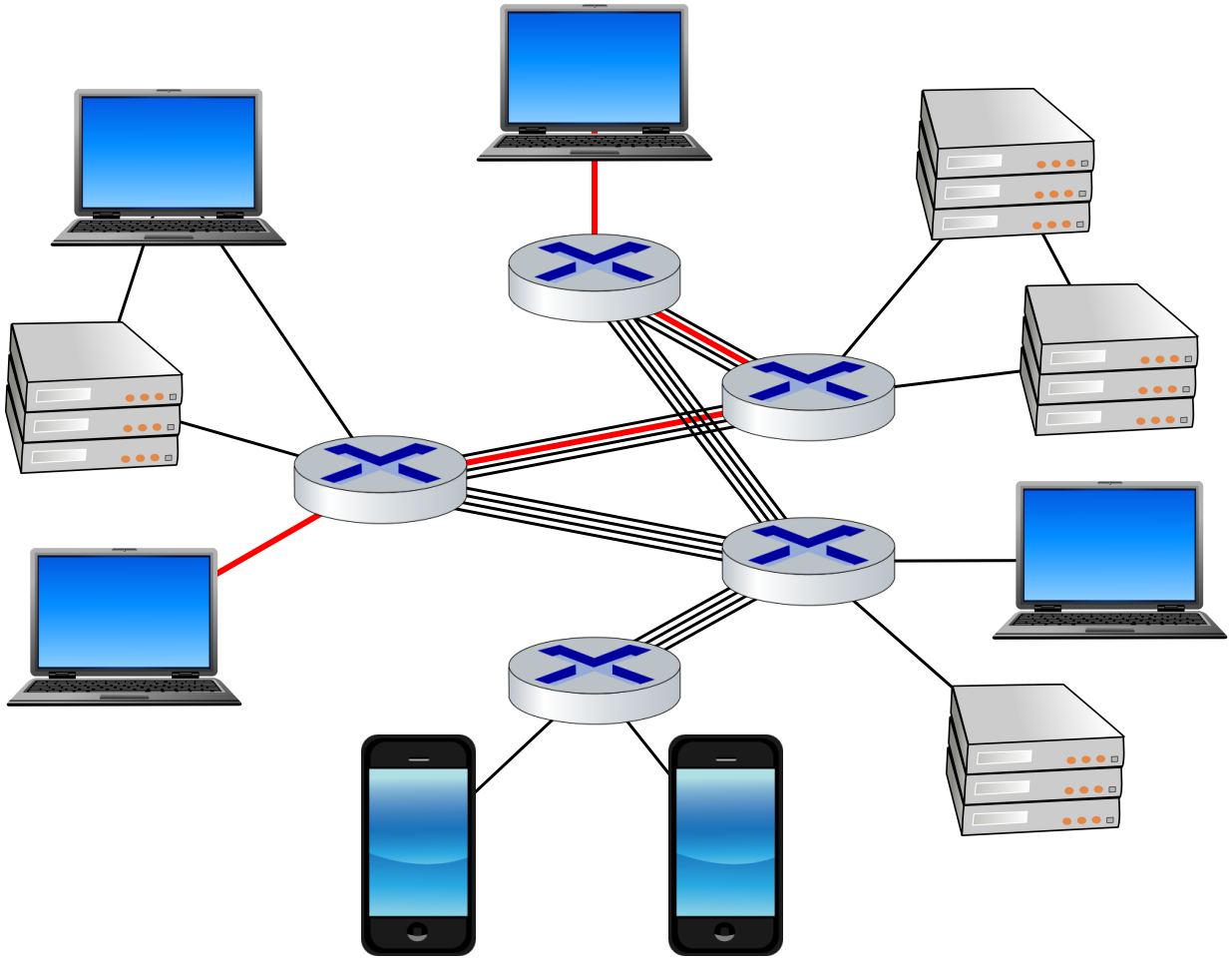
Routers enable a multi-step path between hosts



The Internet

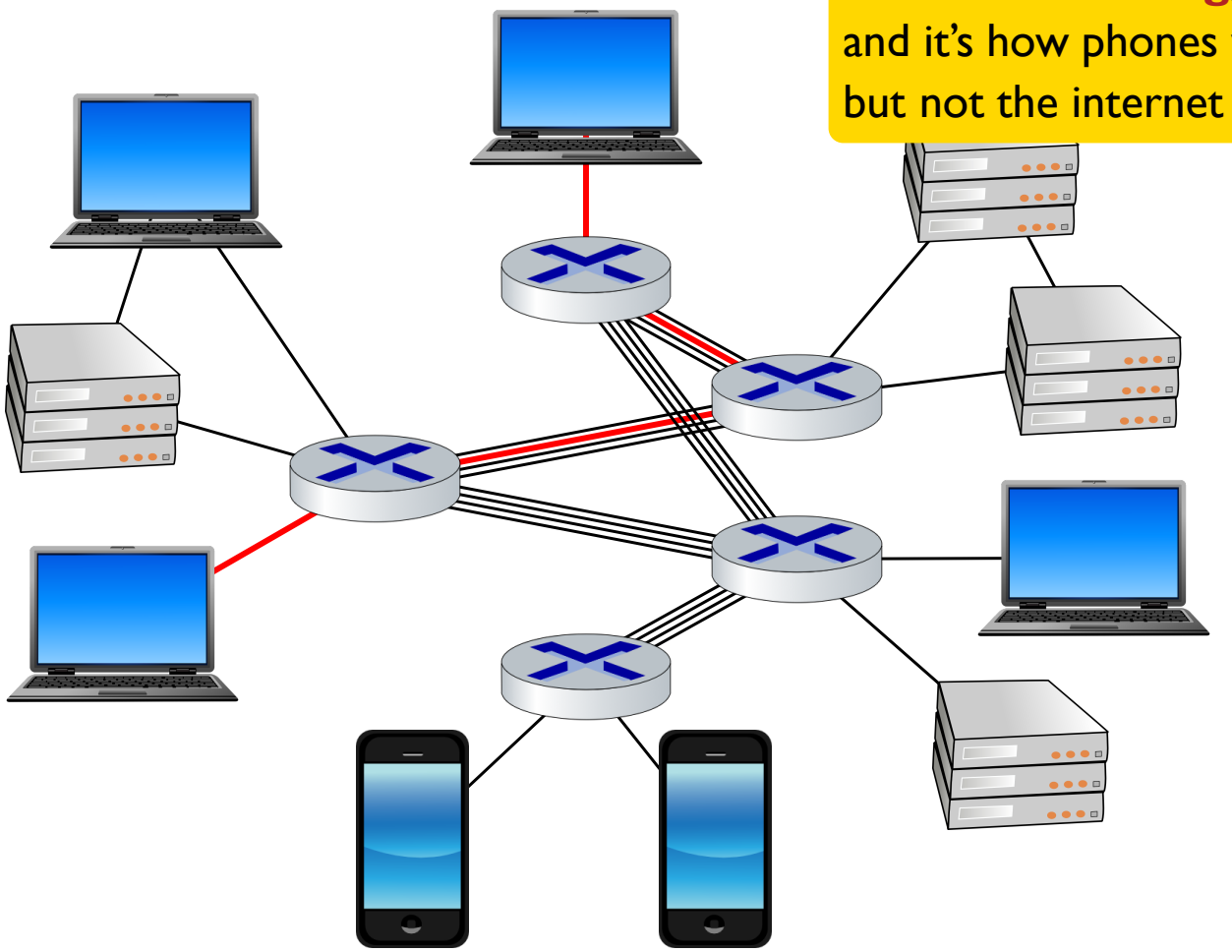


The Internet

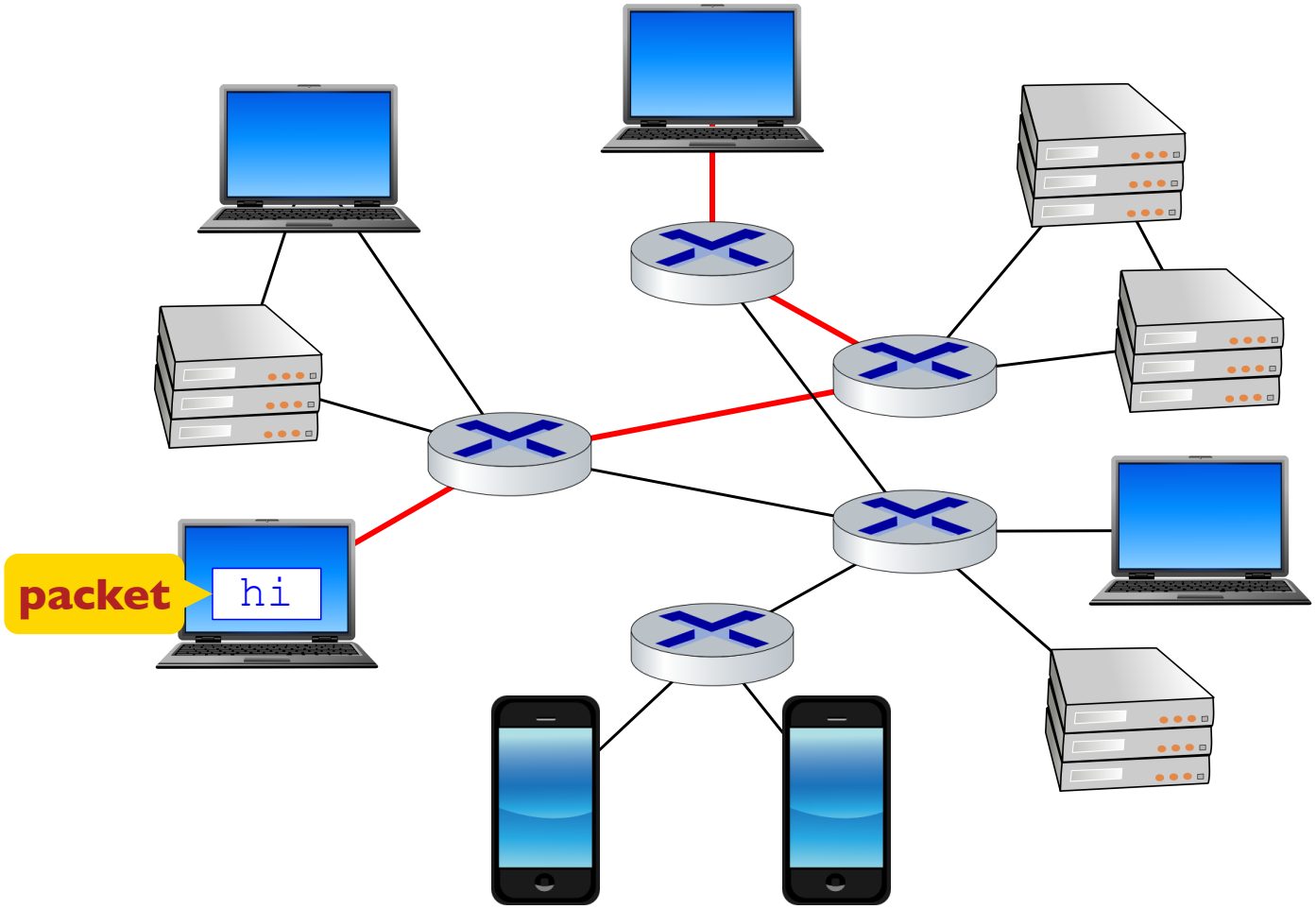


The Internet

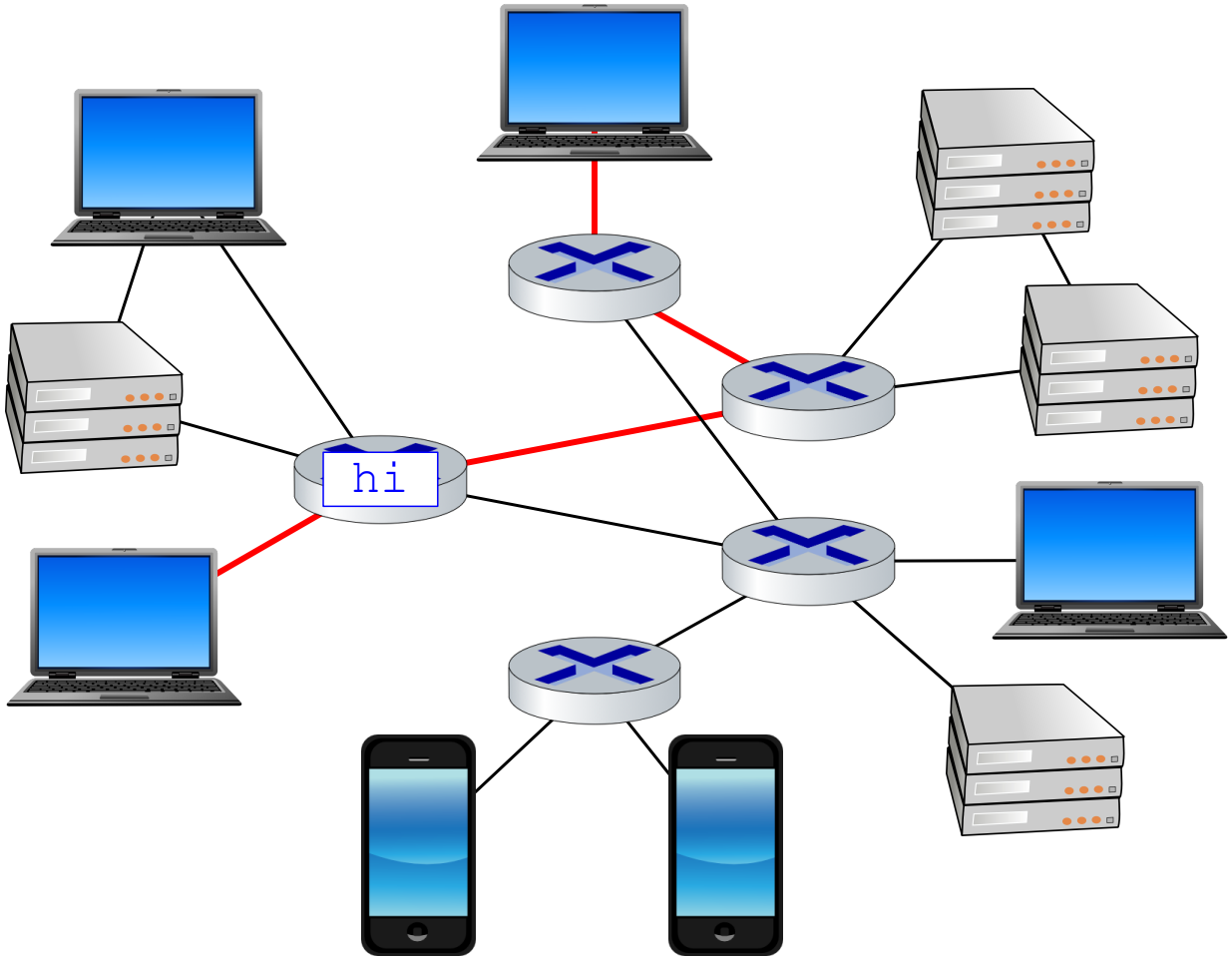
Reserving a path is **circuit switching**, and it's how phones worked, but not the internet



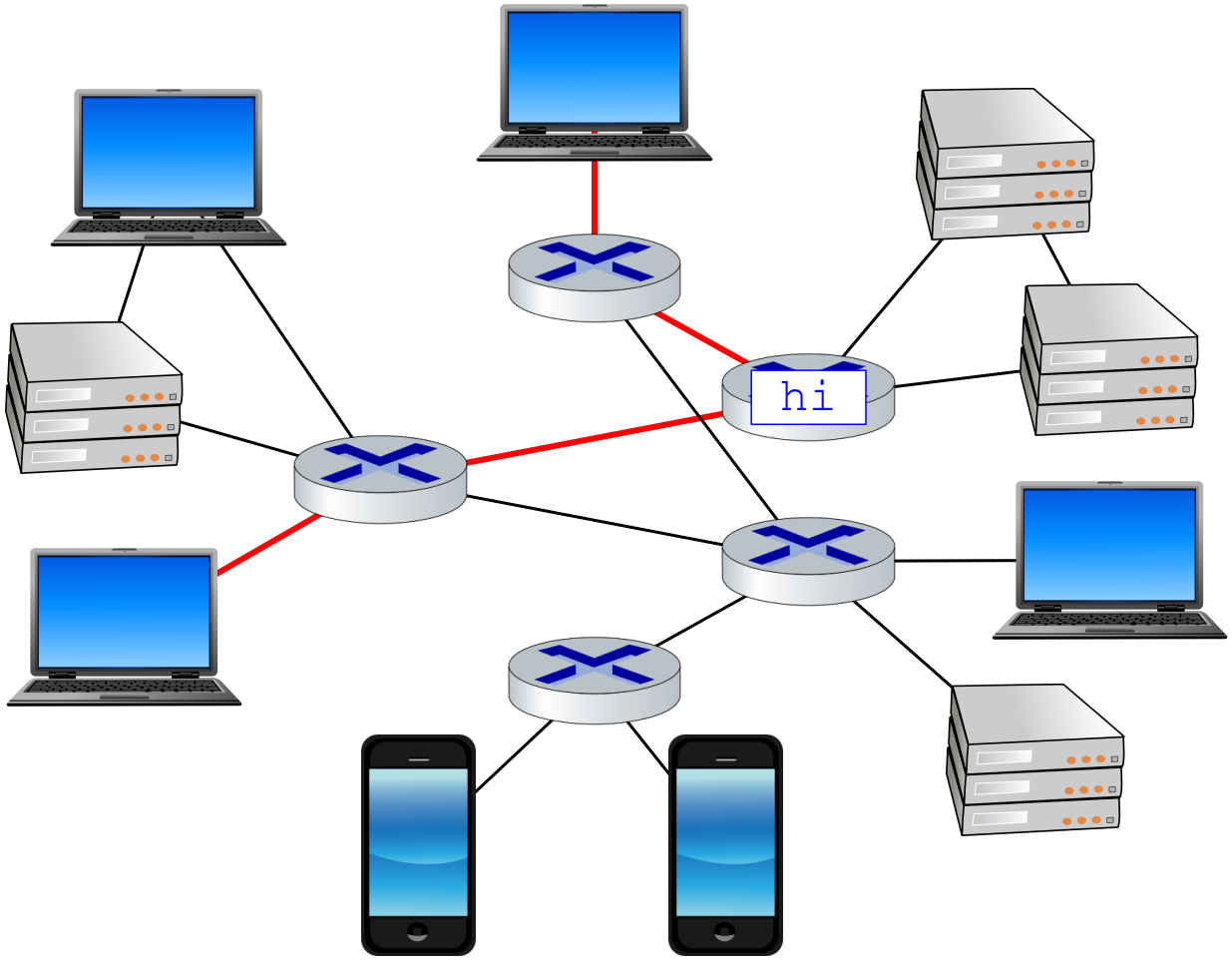
The Internet



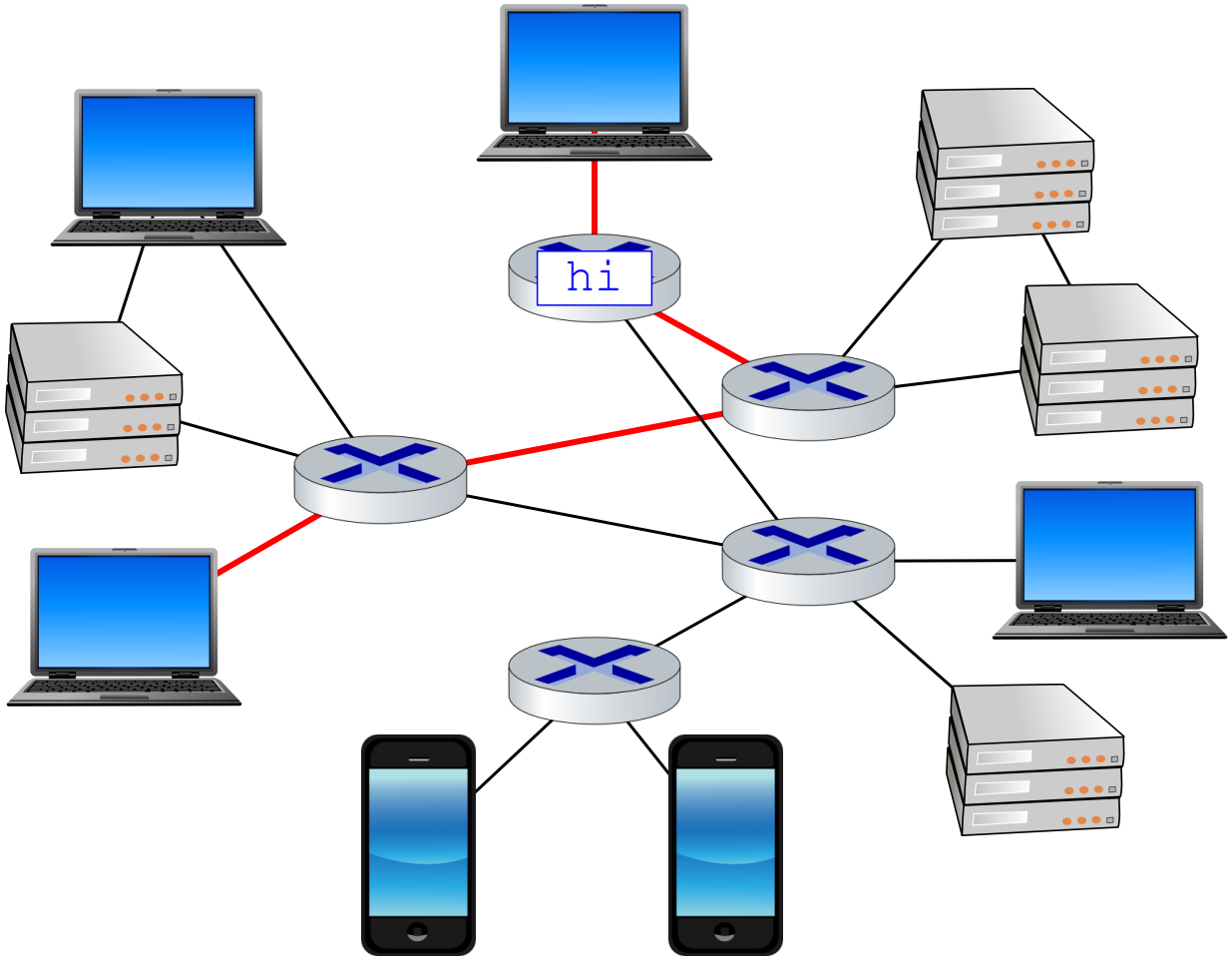
The Internet



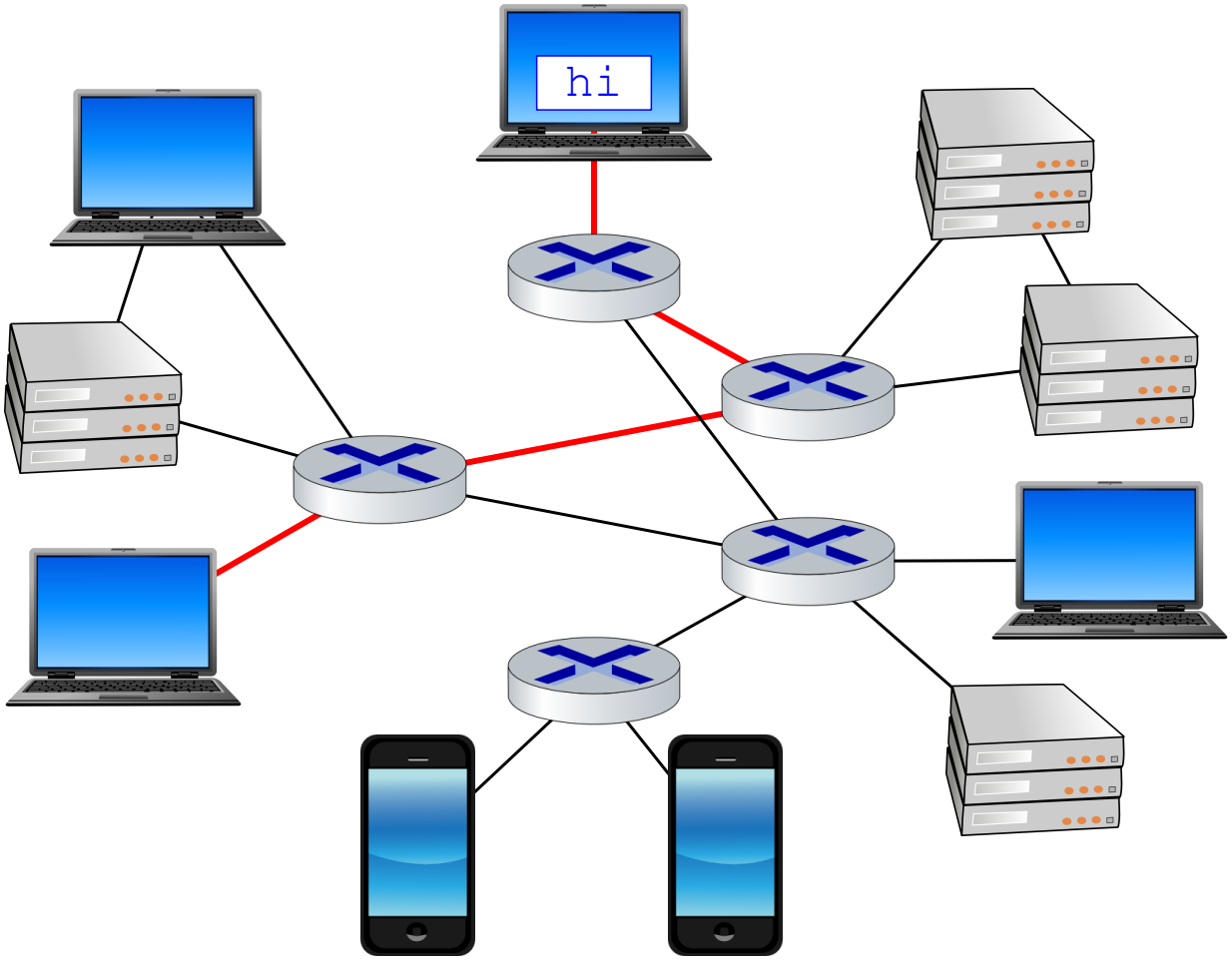
The Internet



The Internet

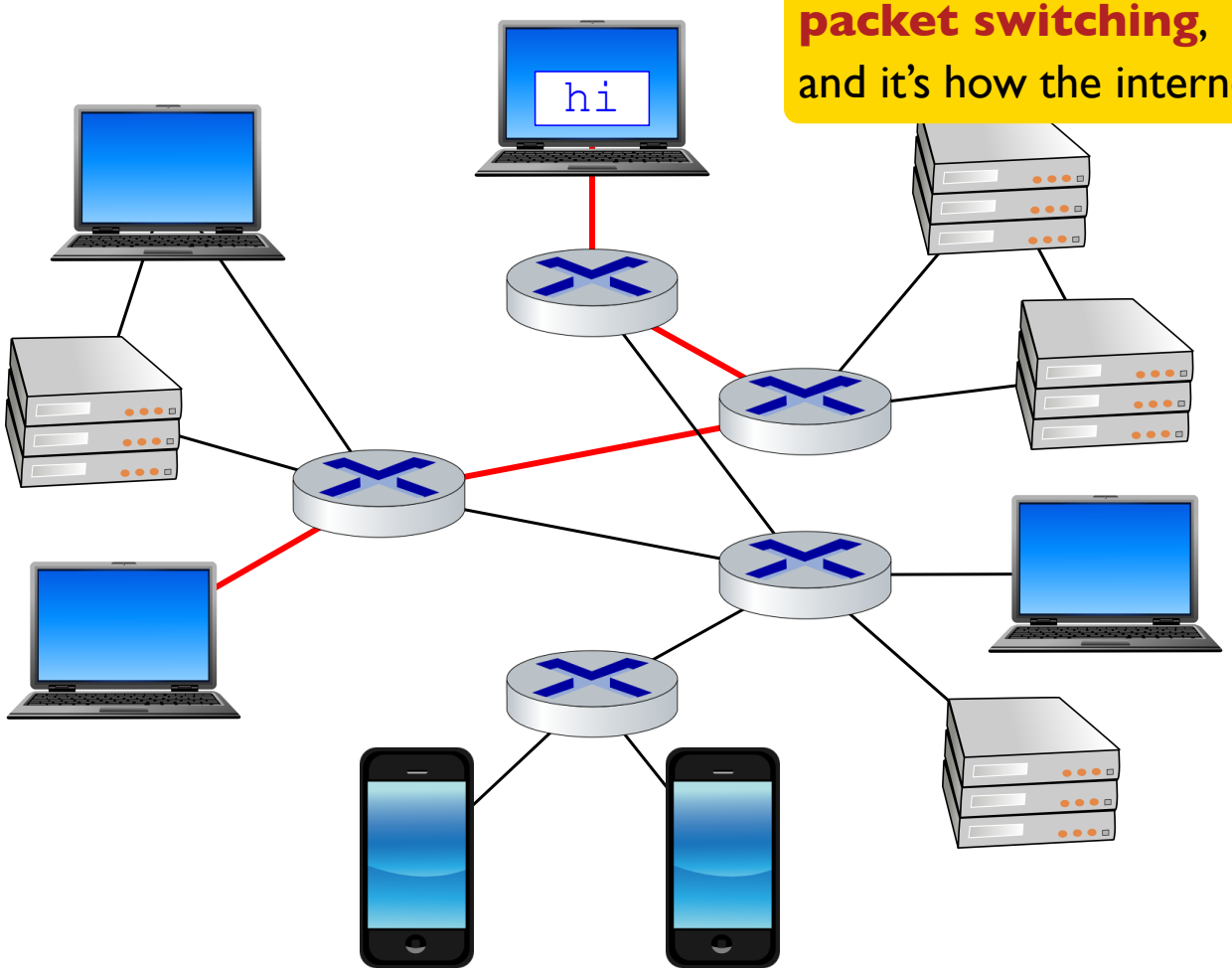


The Internet

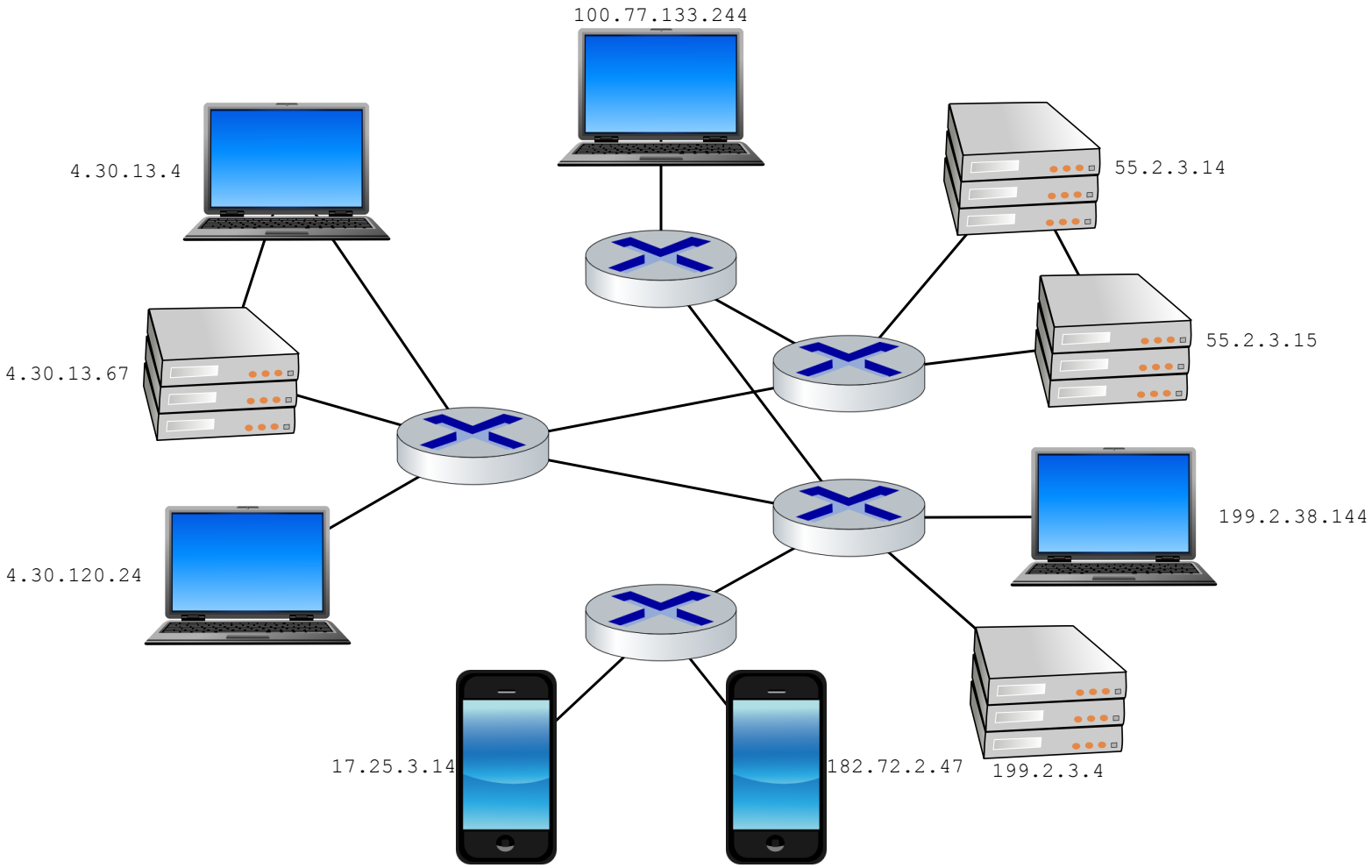


The Internet

Routing a single message is **packet switching**, and it's how the internet works

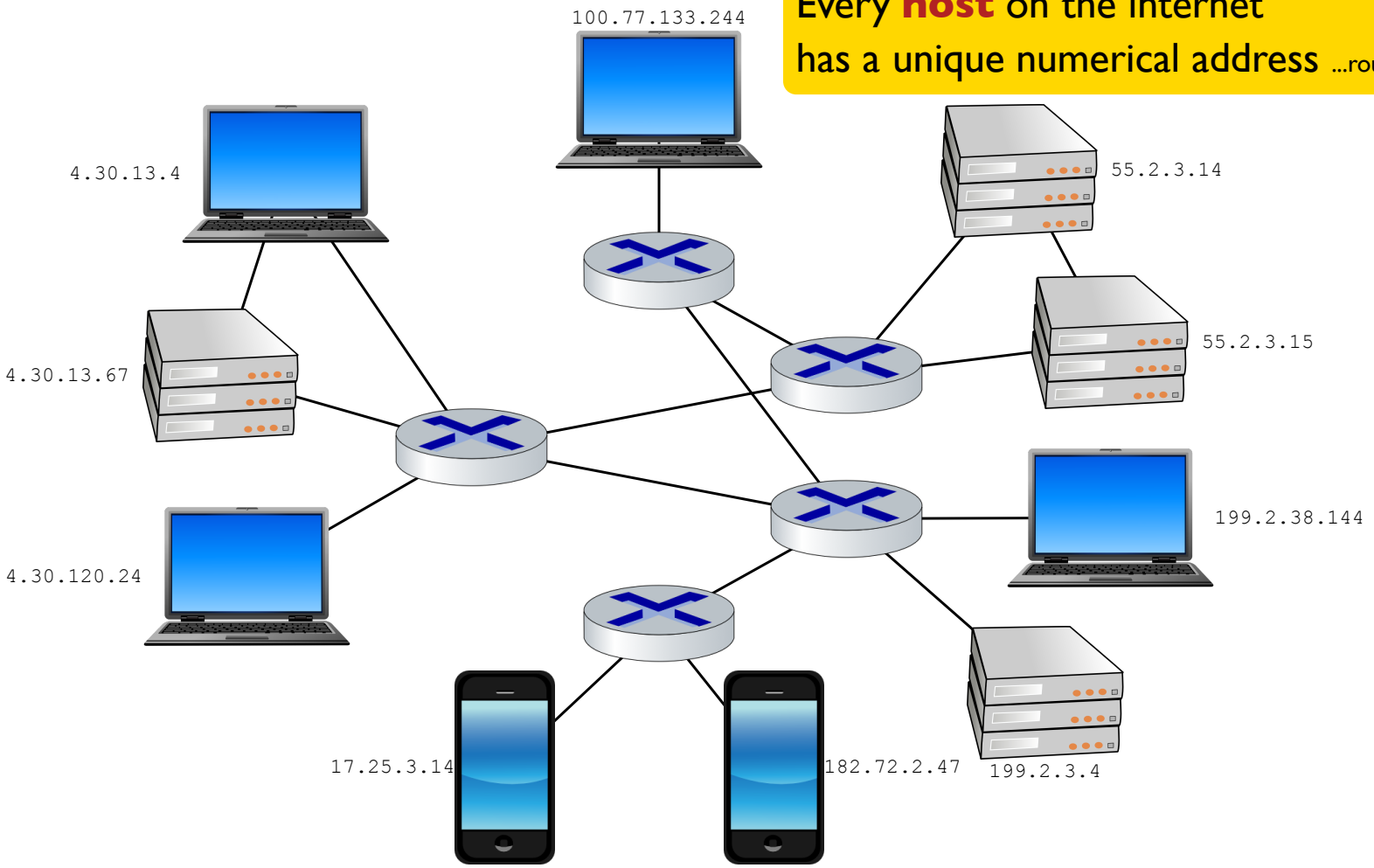


The Internet



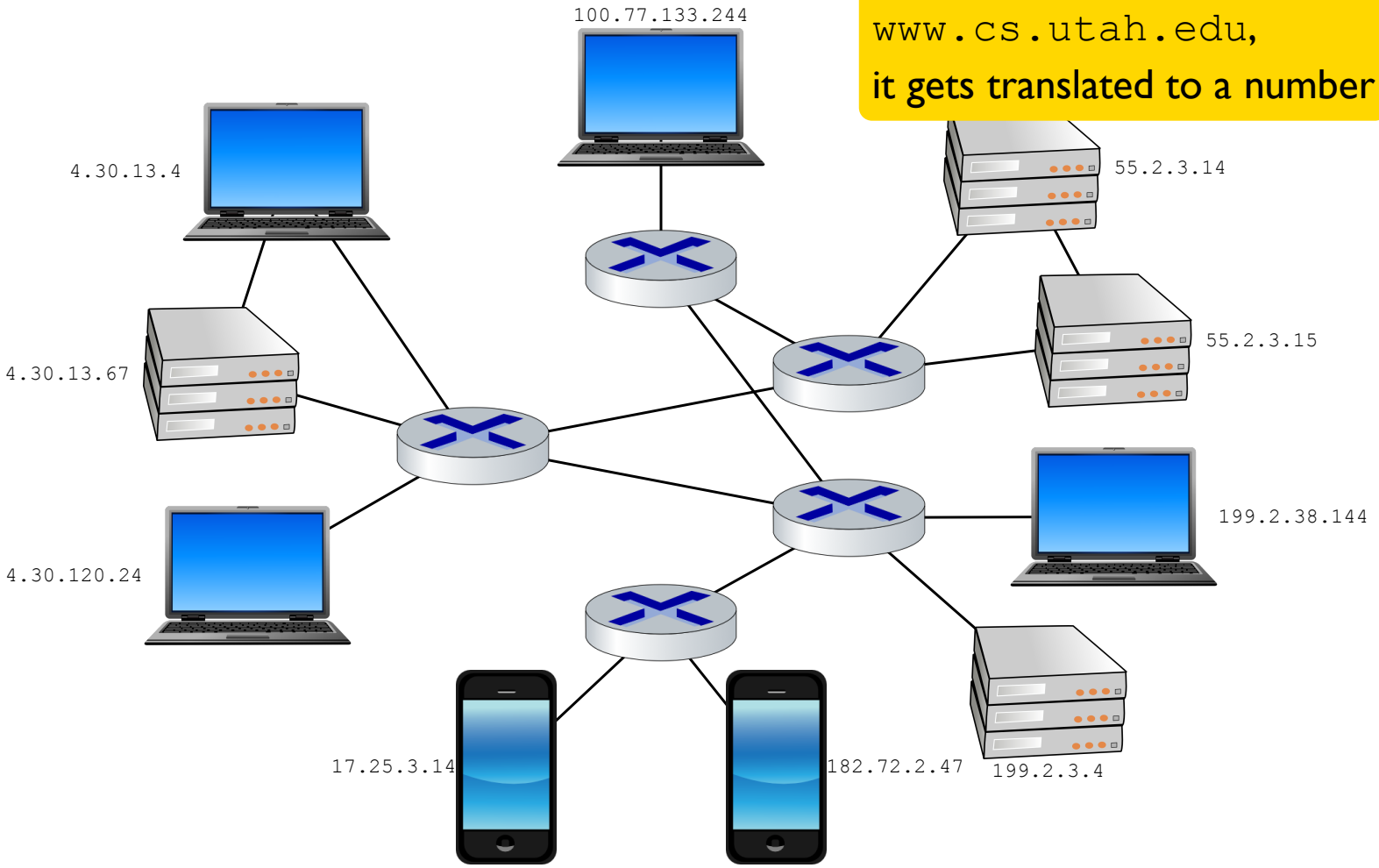
The Internet

Every **host** on the internet
has a unique numerical address ...roughly

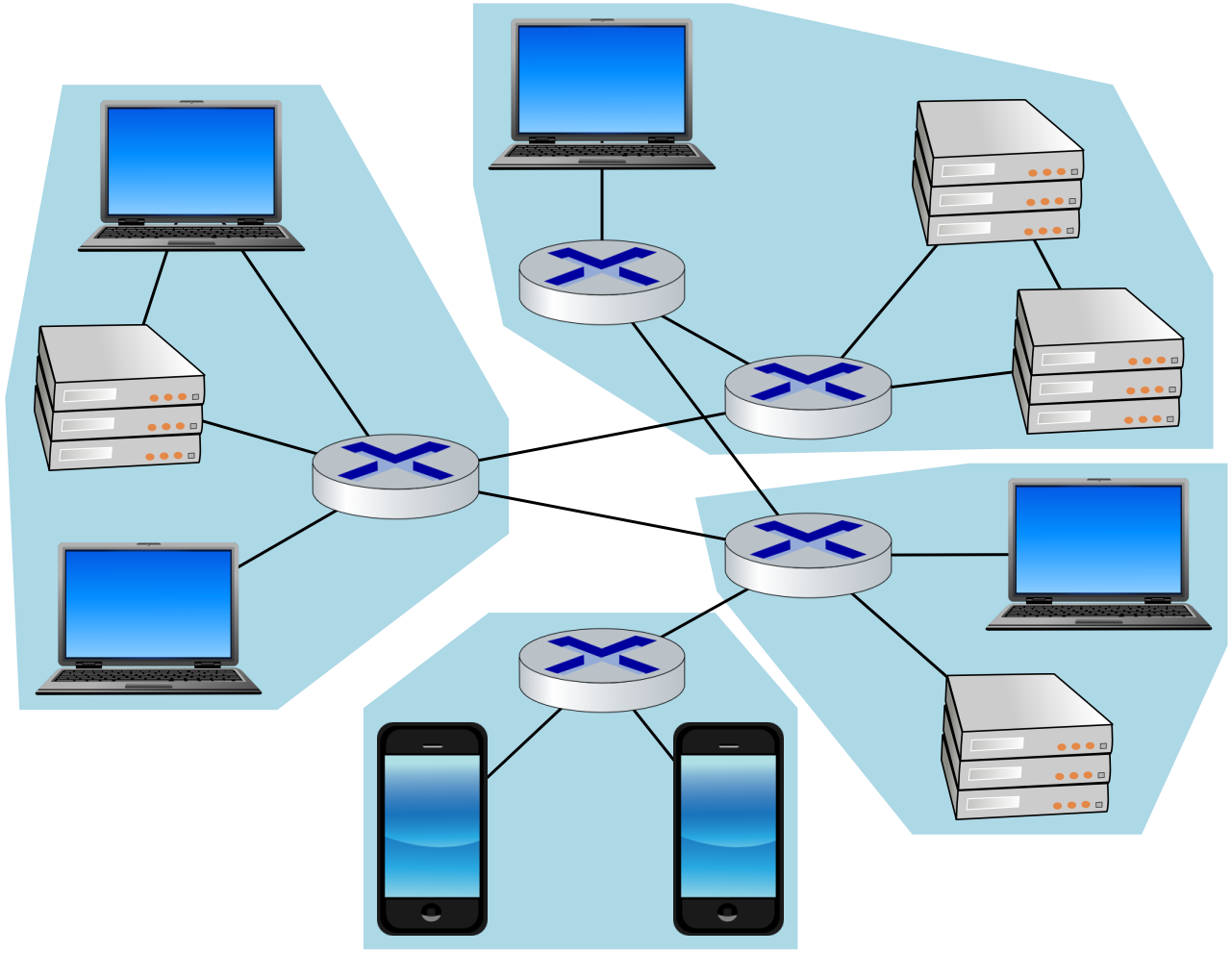


The Internet

When you use a name like
`www.cs.utah.edu`,
it gets translated to a number

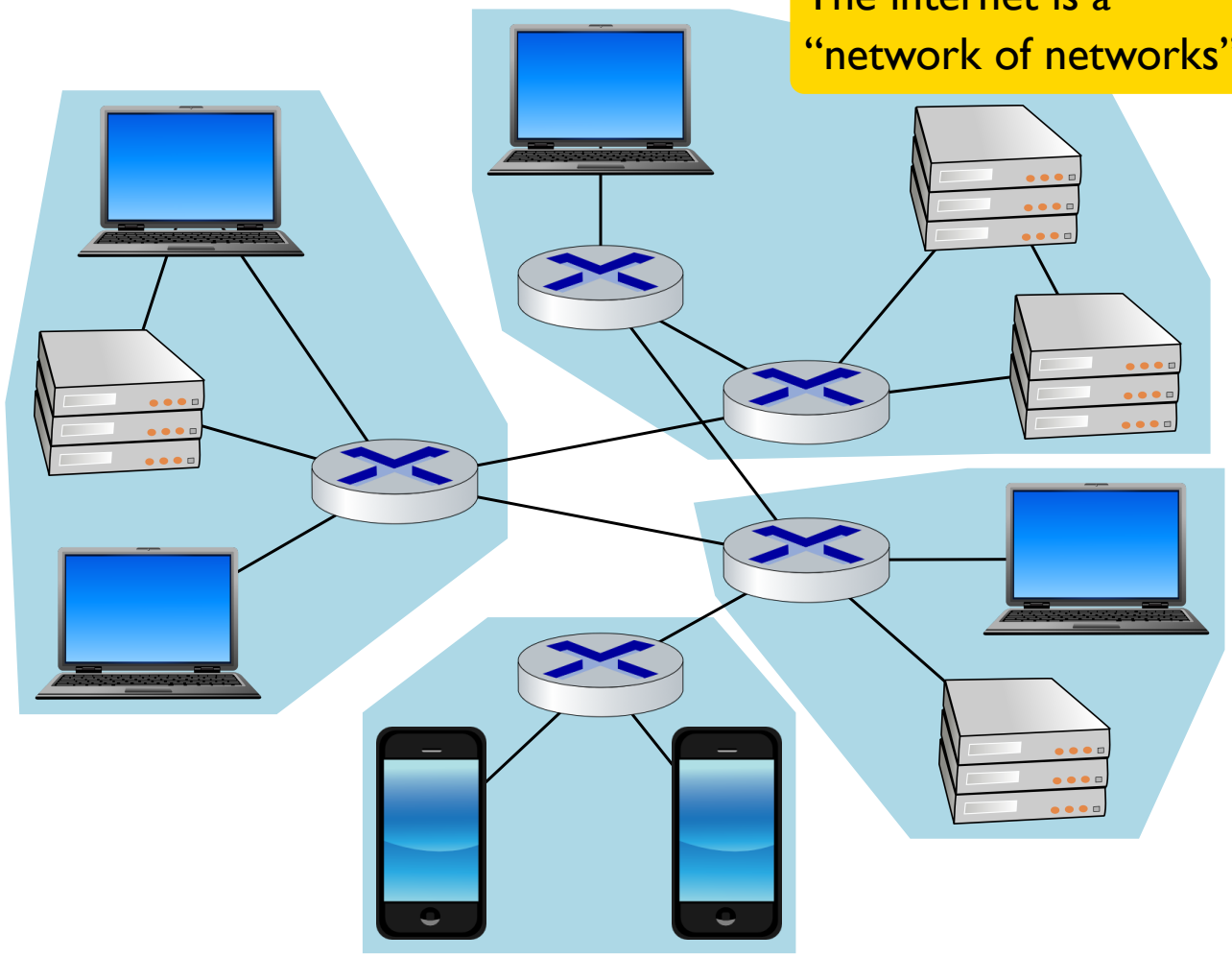


The Internet



The Internet

The internet is a "network of networks"



Routing

image from textbook slides

Routing

image from textbook slides

Hierarchy and Layers

Two main strategies for dealing with network complexity:

Hierarchical structure

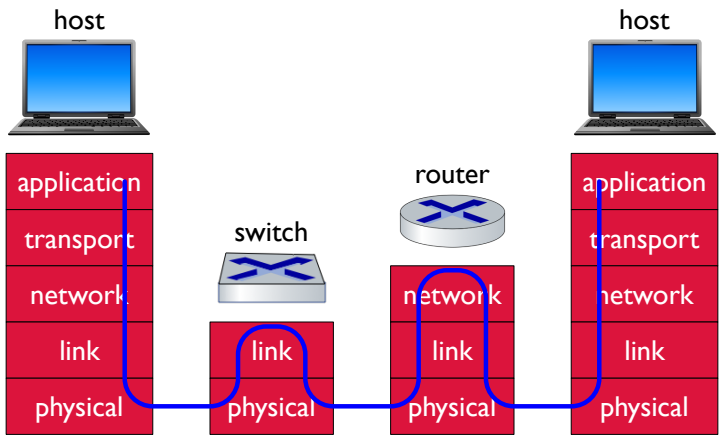
- addresses
- organizations

Layered implementation

- high-level protocols by applications
- lower-level protocols in operating systems
- hardware

Network Layers

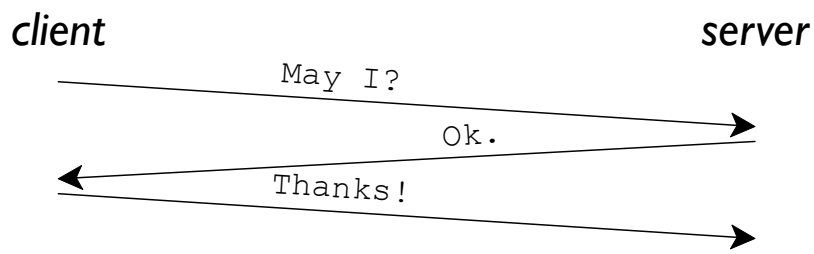
application	Firefox, `ping`, ...
transport	TCP, UDP, ...
network	IP
link	ethernet, WiFi, ...
physical	electrons, photons, ...



Network Layers

application	Firefox, `ping`, ...
transport	TCP, UDP, ...
network	IP
link	ethernet, WiFi, ...
physical	electrons, photons, ...

Each layer has its own **protocols**:

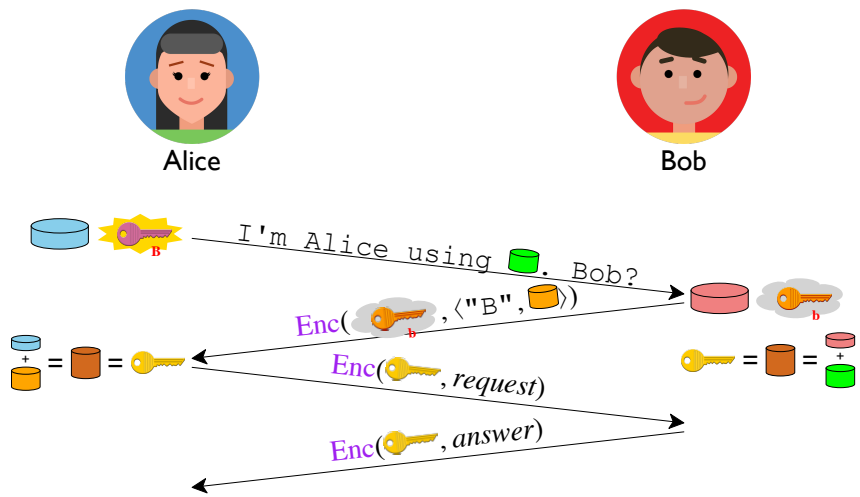


First ⅓ of the course explores these layers and protocols

Security and Cryptography

The internet was not designed with security in mind, so security requires extra layers

Secure communication ultimately relies on **cryptography**



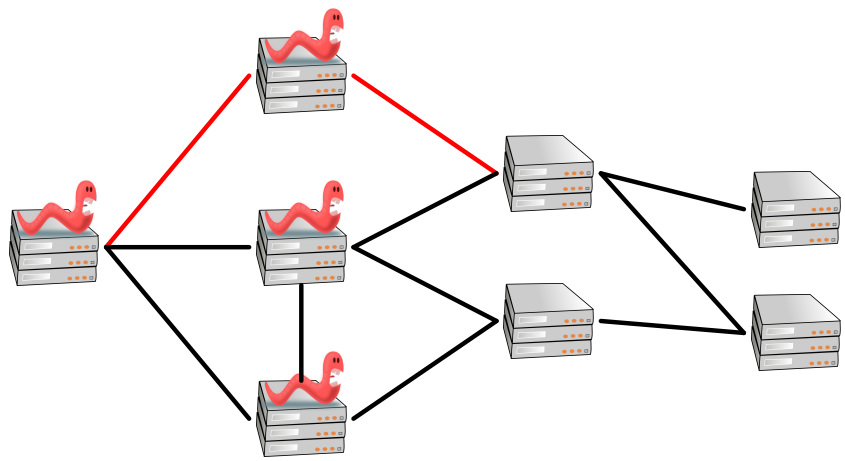
Middle ⅓ of the course is all about Alice, Bob, Eve, and Mallory

Computer and Network Security

Networking tells you what is possible for attackers in principle

Cryptography tells you what is possible for defenders in principle

Getting it right in practice is **computer and network security**



Last ⅓ of the course is about mistakes, consequences, and defense

Summary

The internet is a collection of connected **nodes**,
including applications at **host** nodes,
organized by a numeric **address** for each host,
communicating by **packets**,
organized hierarchically in a **network of networks**,
built in **layers**

Part 1: **network layers**:

application
transport
network
link
physical

Part 2: **cryptography**

Part 3: **computer and network security**