6.033 Spring 2017

Lecture #13

- **Wireless Networks**
  - **MAC Protocols (CSMA/CA, RTS/CTS)**
  - **Bit Rate Selection**
  - **Interactions with the Internet**

Internet of Problems

How do we **route** (and address) scalably, while dealing with issues of policy and economy?

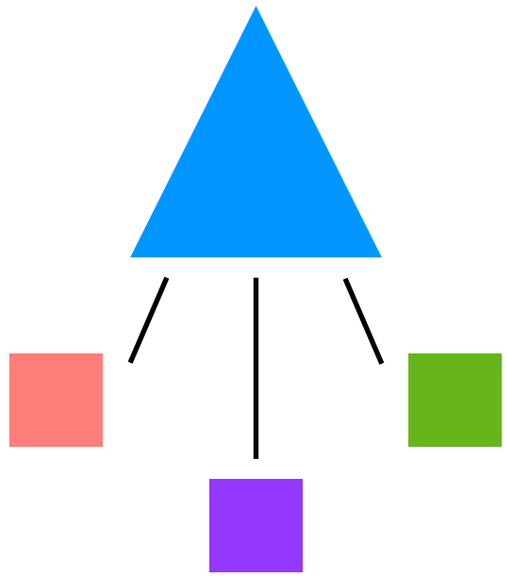
→ **BGP**

How do we **transport** data scalably, while dealing with varying application demands?

→ **TCP, in-network resource management**

How do we **adapt** new applications and technologies to an inflexible architecture?

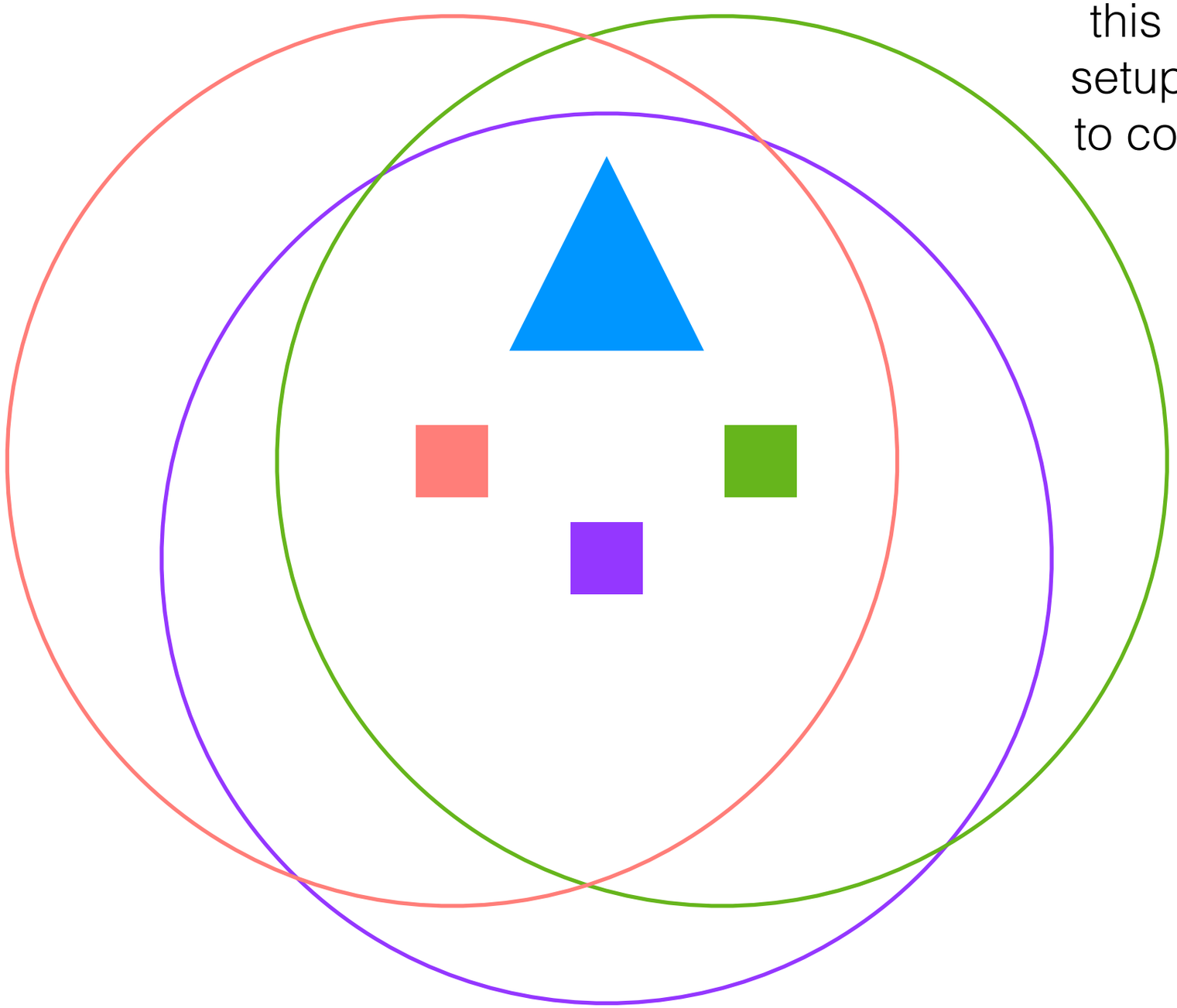
→ **P2P Networks, CDNs** (and more)



wired networks:

two nodes can communicate directly if there is a link between them, and no other nodes can overhear the communications on that link

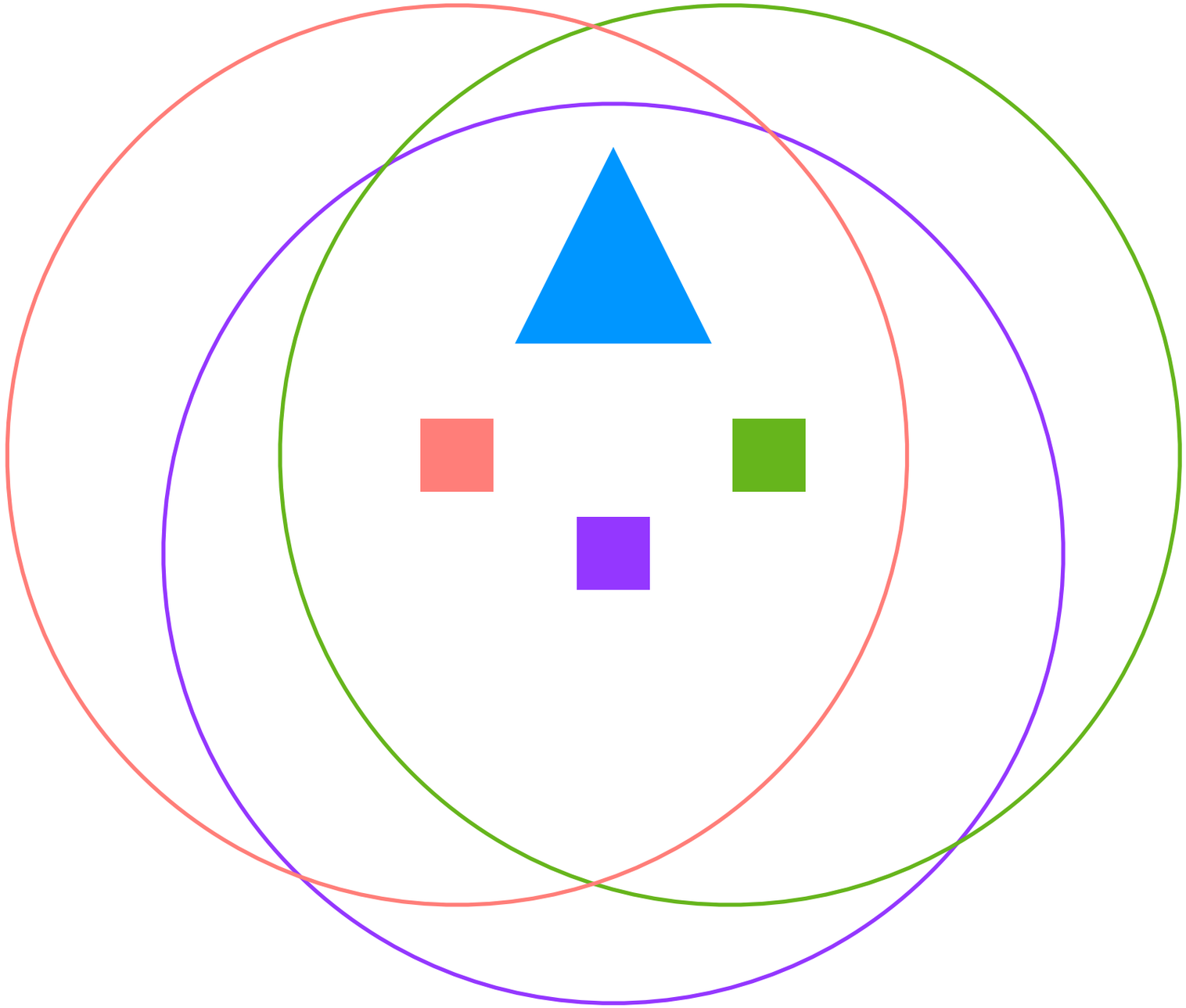
this is a typical 802.11 setup, with clients trying to communicate with an access point



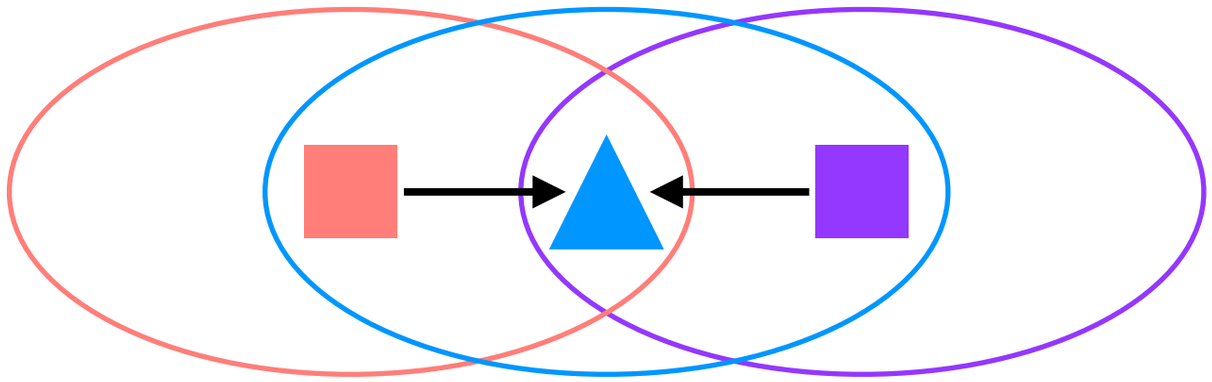
wireless networks:

wireless is a broadcast medium. nodes can overhear communications from other nodes

(*which* nodes depends on how their ranges overlap)



problem: if two (or more) nodes send at once, their packets will interfere (“collide”) and be lost where their ranges overlap

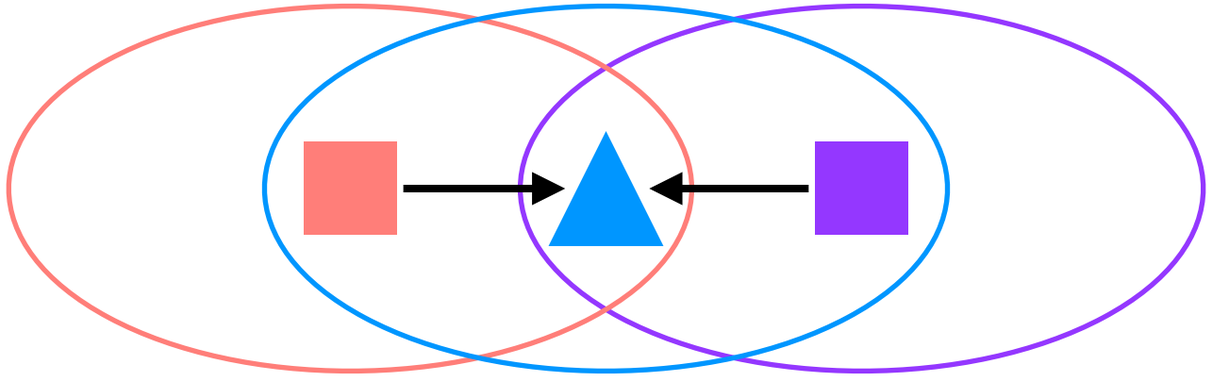


hidden terminals
clients will send when they shouldn't

problem: sensing happens at the sender, but interference at the receiver is what matters

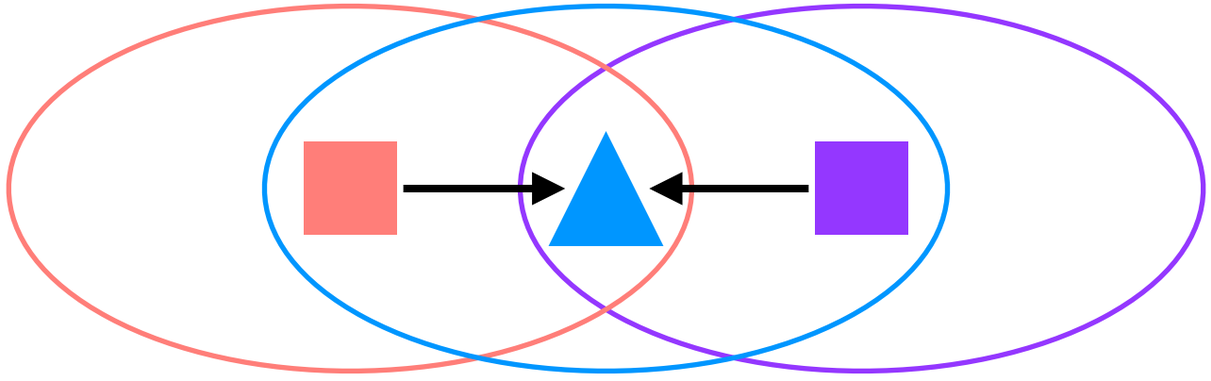
RTS/CTS: clients make a request to send (RTS), and send when they get a “clear to send” (CTS)

clients who overhear CTS messages for other clients **don’t** send



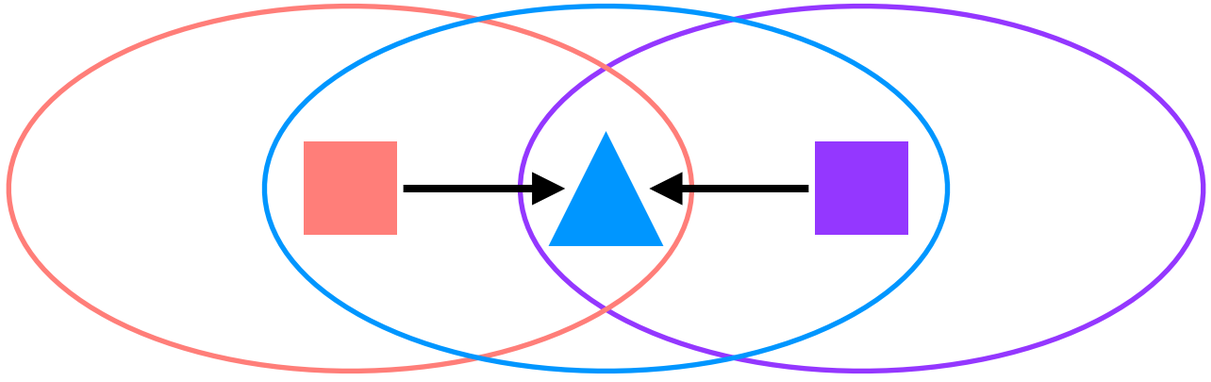
RTS/CTS: clients make a request to send (RTS), and send when they get a “clear to send” (CTS)

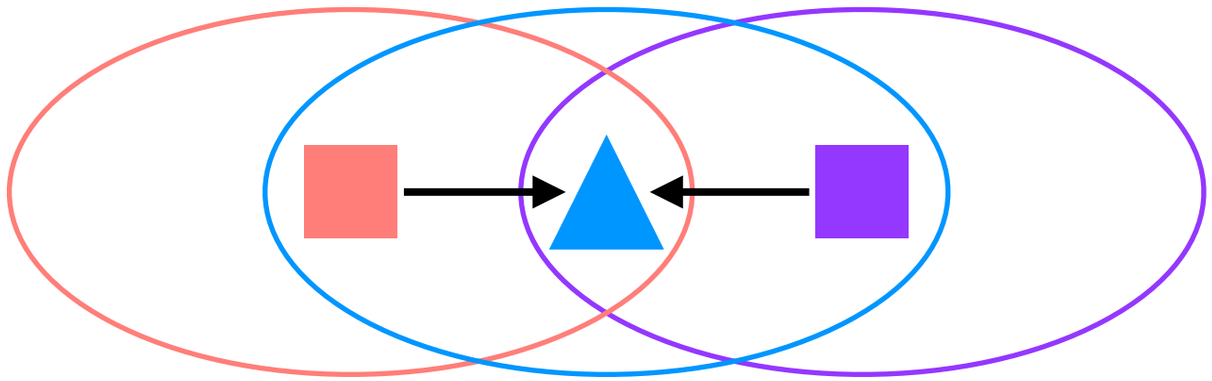
clients who overhear CTS messages for other clients **don’t** send



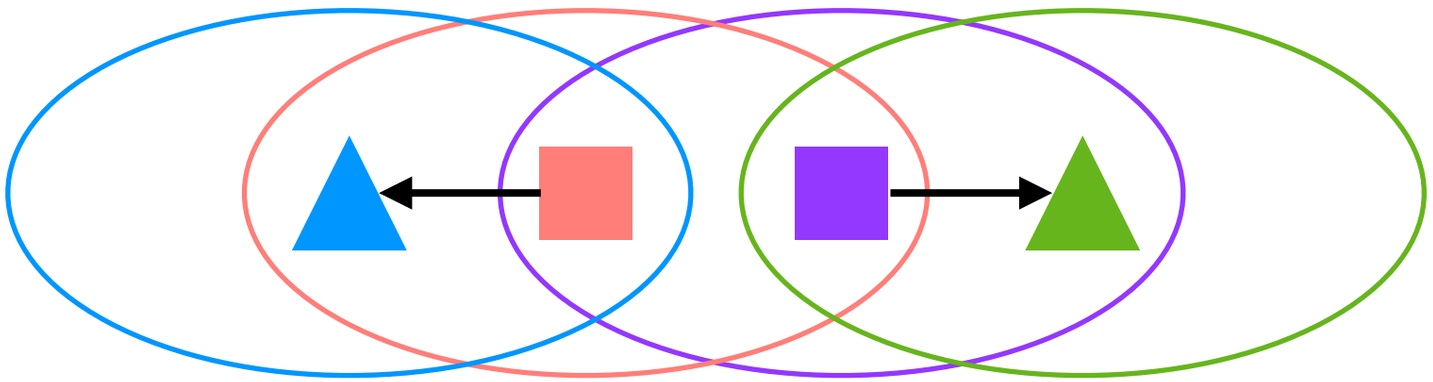
RTS/CTS: clients make a request to send (RTS), and send when they get a "clear to send" (CTS)

clients who overhear CTS messages for other clients **don't** send





hidden terminals
clients will send when they shouldn't

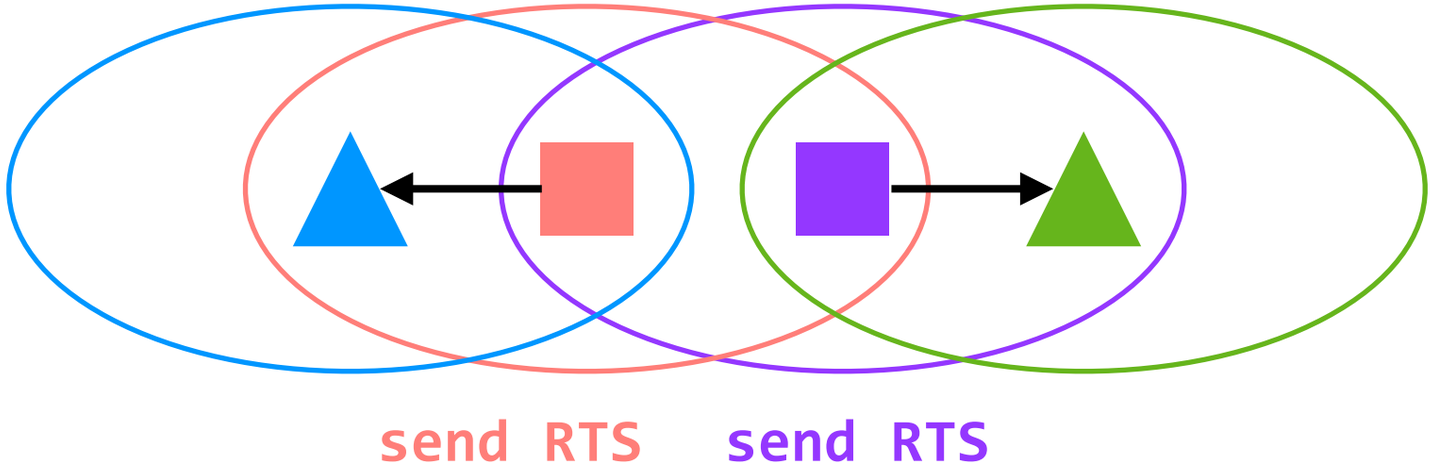


exposed terminals
clients won't send when they could

problem: sensing happens at the sender, but interference at the receiver is what matters

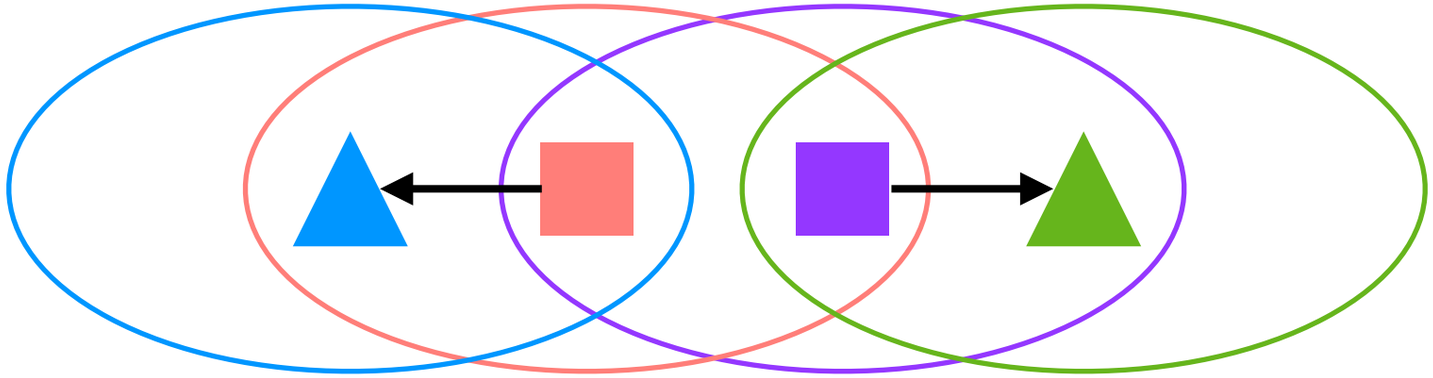
RTS/CTS: clients make a request to send (RTS), and send when they get a “clear to send” (CTS)

clients who overhear CTS messages for other clients **don’t** send



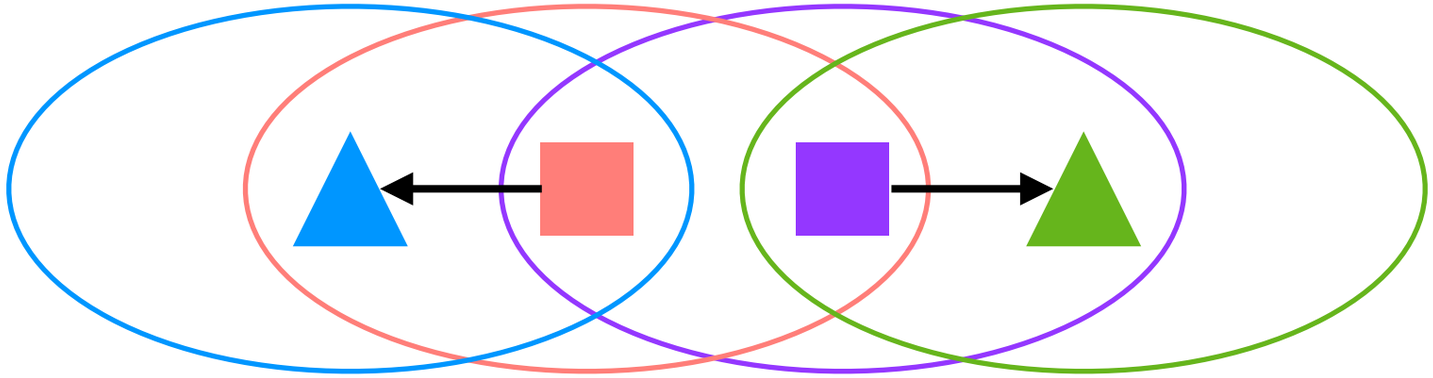
RTS/CTS: clients make a request to send (RTS), and send when they get a “clear to send” (CTS)

clients who overhear CTS messages for other clients **don’t** send

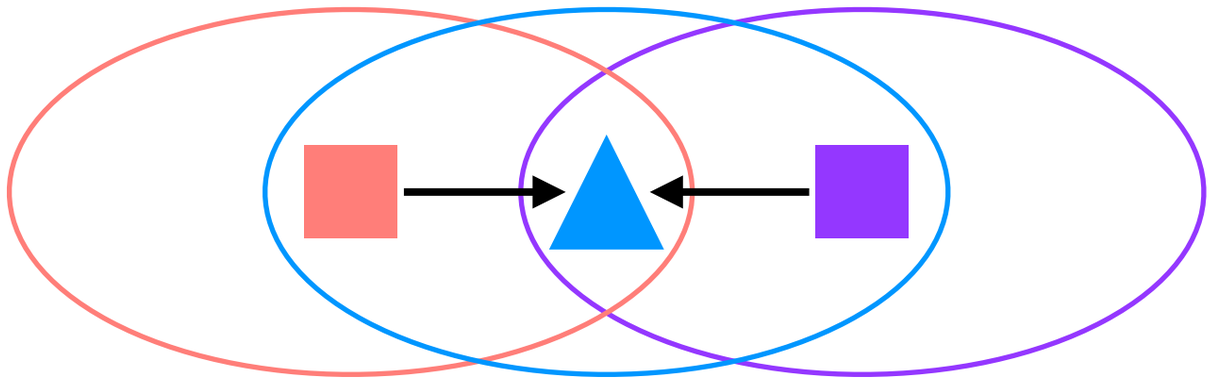


RTS/CTS: clients make a request to send (RTS), and send when they get a “clear to send” (CTS)

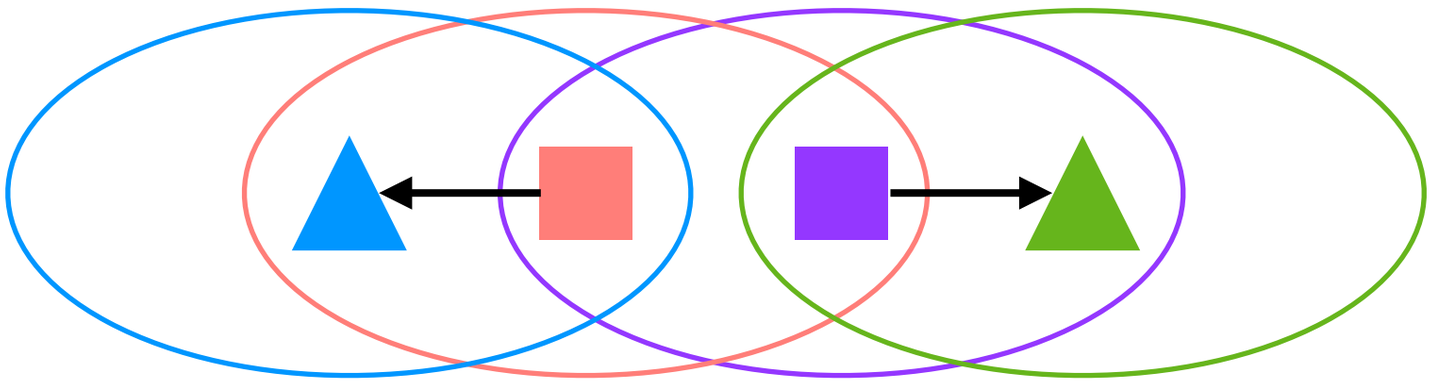
clients who overhear CTS messages for other clients **don’t** send



(neither overhear copies of the other’s CTS)



hidden terminals
clients will send when they shouldn't



exposed terminals
clients won't send when they could

RTS/CTS solve these problems in theory, but not always in practice; moreover, it adds a large amount of **overhead** to the common case

problem: there is still a lot of loss in wireless networks, and channel conditions can change rapidly

how does 802.11 interact with existing protocols?

- **(802.11) wireless** networks provide **broadcast** communication. They require (more complicated) **MAC protocols** to mitigate collisions, as well as **bit-rate-selection** algorithms to adapt to changing channel conditions.

- 802.11 networks cause some problems for existing protocols, such as TCP. But they also provide opportunities — mobility, mesh networks, etc. — that didn't exist when the Internet was designed.

after spring break: how do we build large, distributed systems in the face of random and targeted failures?

(also after spring break: a midterm)