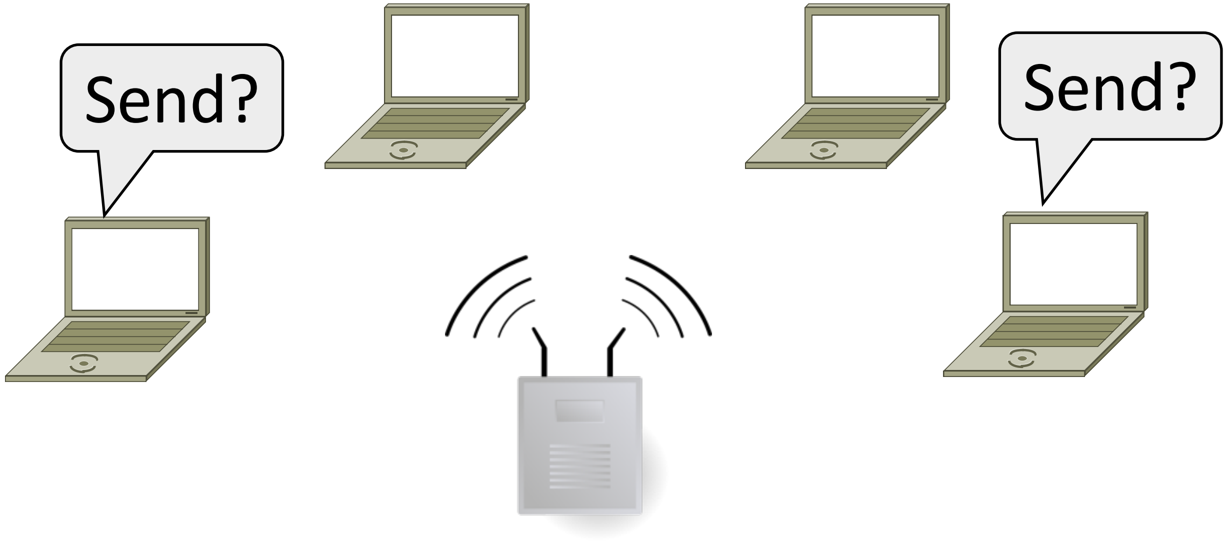
Wireless MACs

- How do wireless nodes share a single link? (Yes, this is WiFi!)
  - Build on our simple, wired model



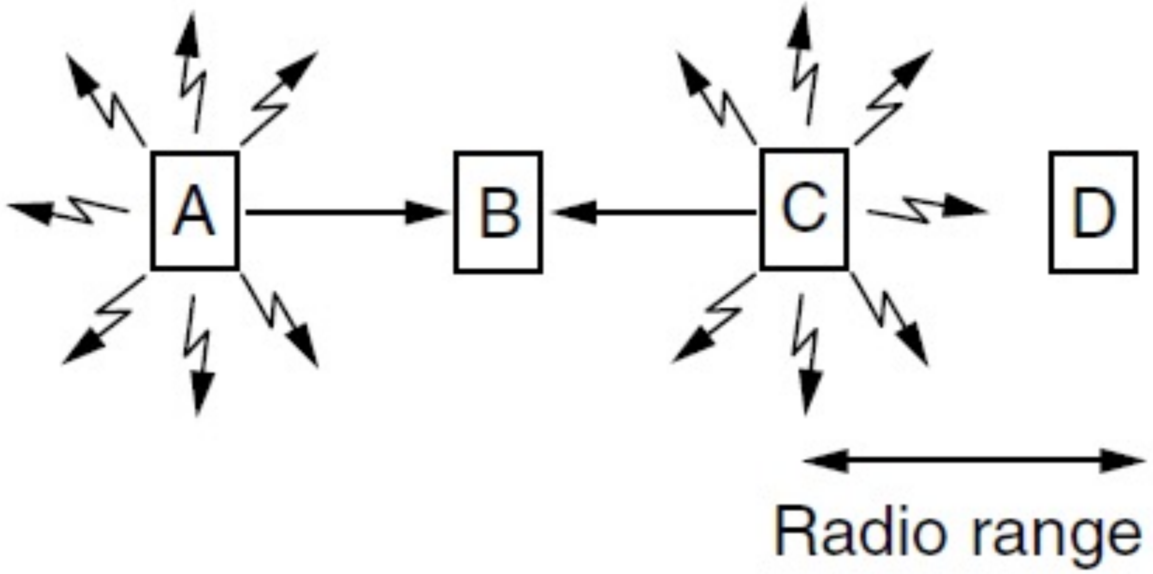
Wireless Complications

- Wireless is more complicated than wired (surprise!)
  1. Media is infinite – can’t reliably Carrier Sense
  2. Nodes usually can’t hear while sending – can’t Collision Detect

≠ CSMA/CD

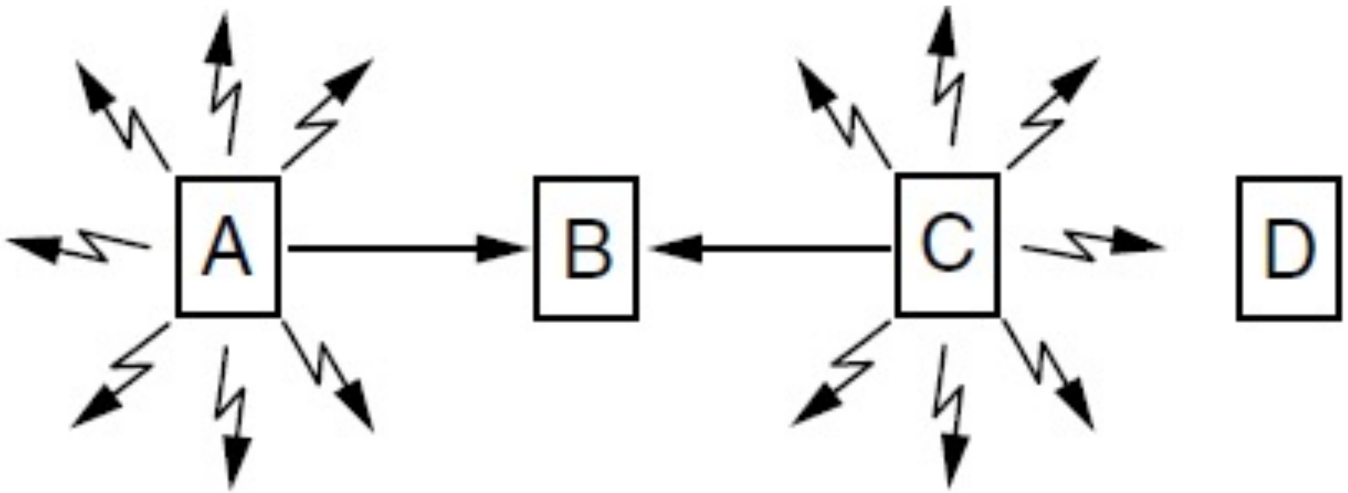
No CS: Different Coverage Areas

- Wireless signal is broadcast and received nearby, where there is sufficient SNR



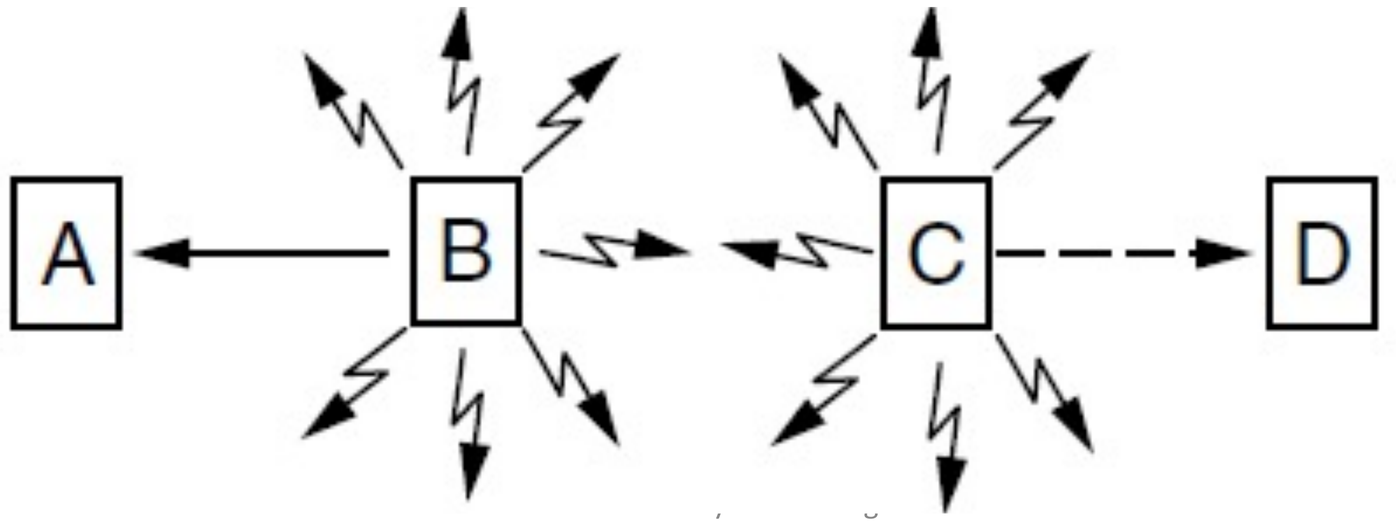
No CS: Hidden Terminals

- Node C is a <u>hidden terminal</u> when A sends to B
  - Similarly, A is a hidden terminal when C sends to B
  - A, C can’t hear each other (to coordinate) yet collide at B
  - We want to avoid the inefficiency of collisions



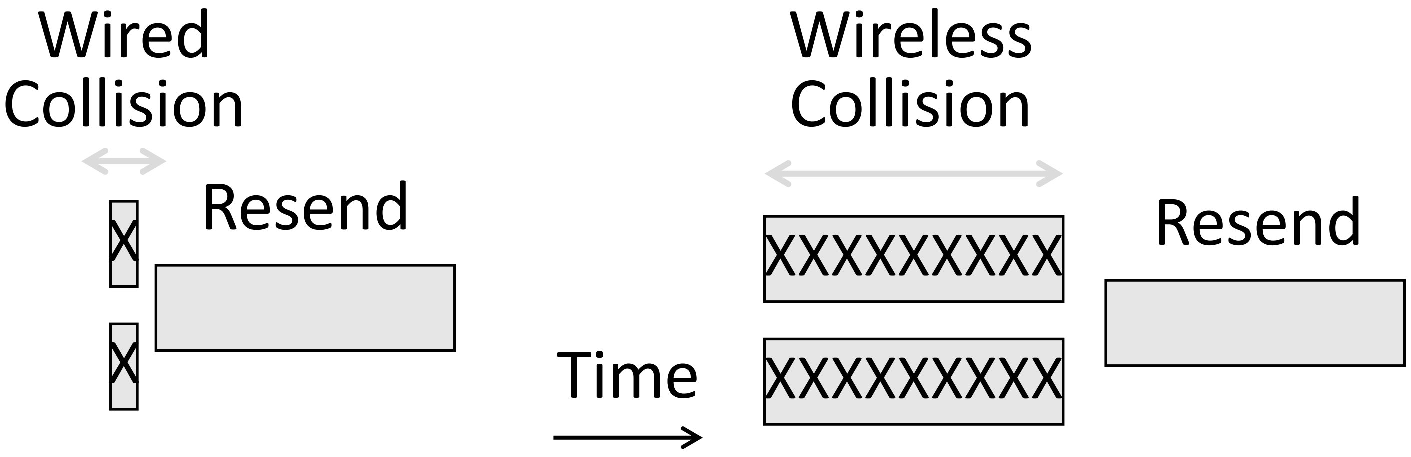
No CS: Exposed Terminals

- B, C are <u>exposed terminals</u> when sending to A, D
  - Can hear each other yet don’t collide at receivers A and D
  - We want to send concurrently to increase performance



Nodes Can’t Hear While Sending

- With wires, detecting collisions (and aborting) lowers their cost
- With wireless, more wasted time



Wireless Problems:

- Ideas?

MACA: Multiple Access w/ Collision Avoidance

- MACA uses a short handshake instead of CSMA (Karn, 1990)
  - 802.11 uses a refinement of MACA (later)

- Protocol rules:
  1. A sender node transmits a RTS (Request-To-Send, with frame length)
  2. The receiver replies with a CTS (Clear-To-Send, with frame length)
  3. Sender transmits the frame while nodes hearing the CTS stay silent

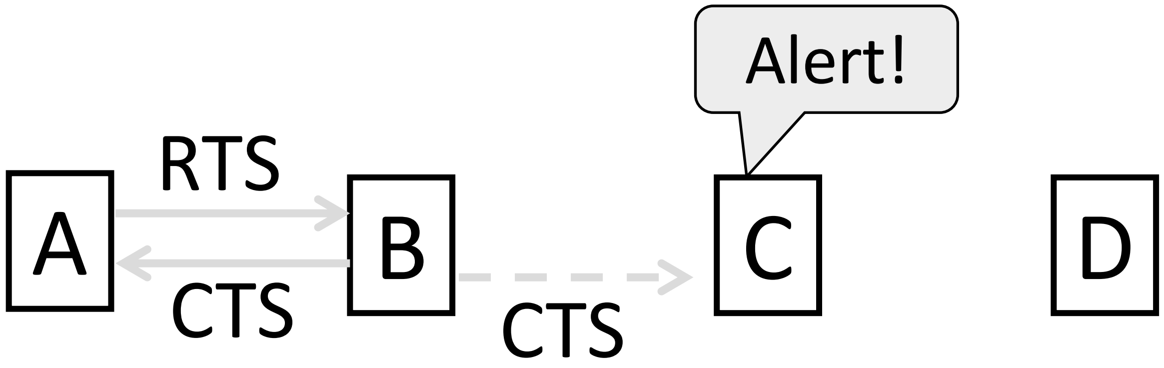
- Collisions on the RTS/CTS are still possible, but less likely

MACA – Hidden Terminals

- A→B with hidden terminal C
    1. A sends RTS, to B

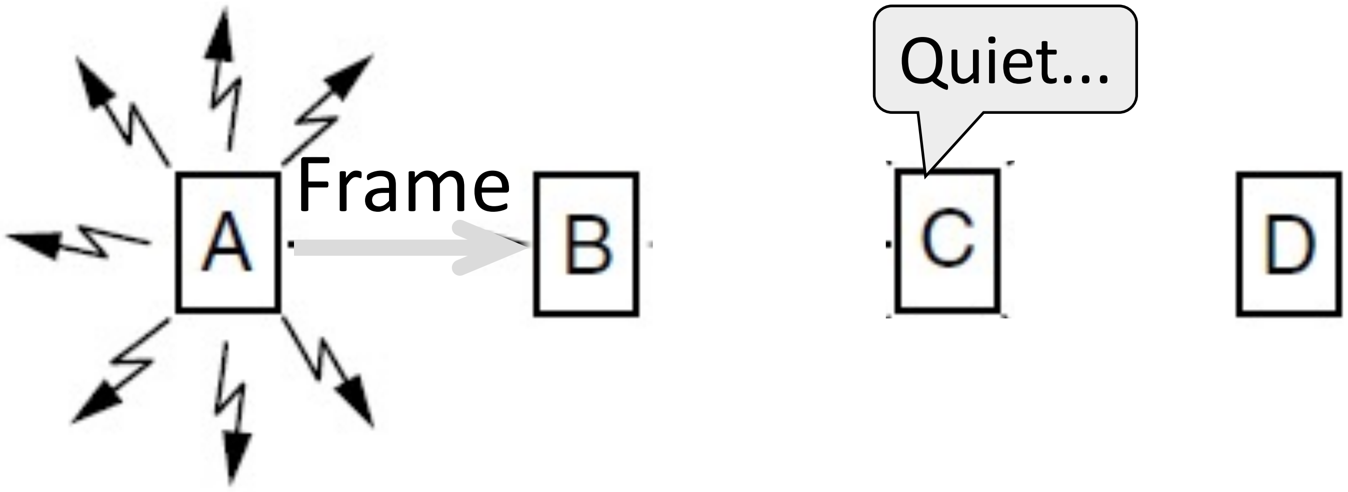
MACA – Hidden Terminals (2)

- A→B with hidden terminal C
    2. B sends CTS to A, and C overhears



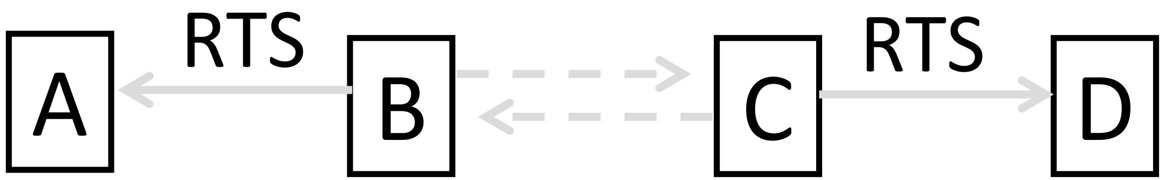
MACA – Hidden Terminals (3)

- A→B with hidden terminal C
  3. A sends frame while C defers



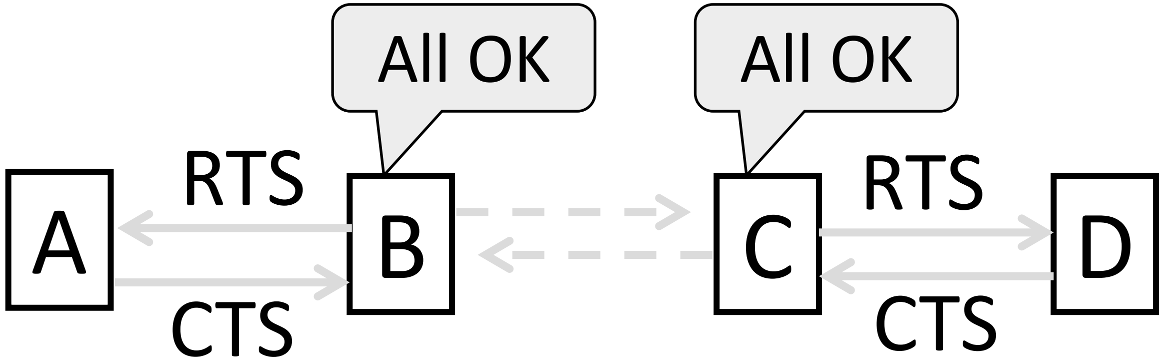
MACA – Exposed Terminals

- B→A, C→D as exposed terminals
  - B and C send RTS to A and D



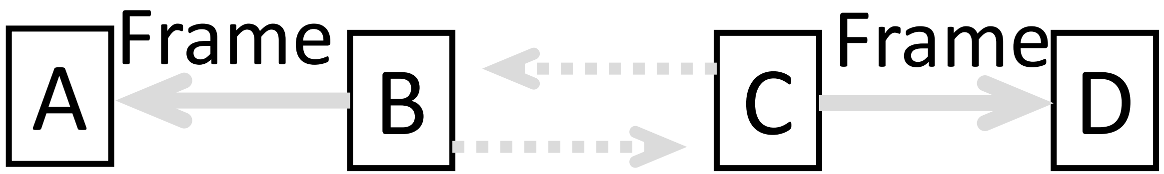
MACA – Exposed Terminals (2)

- B→A, C→D as exposed terminals
  - A and D send CTS to B and C



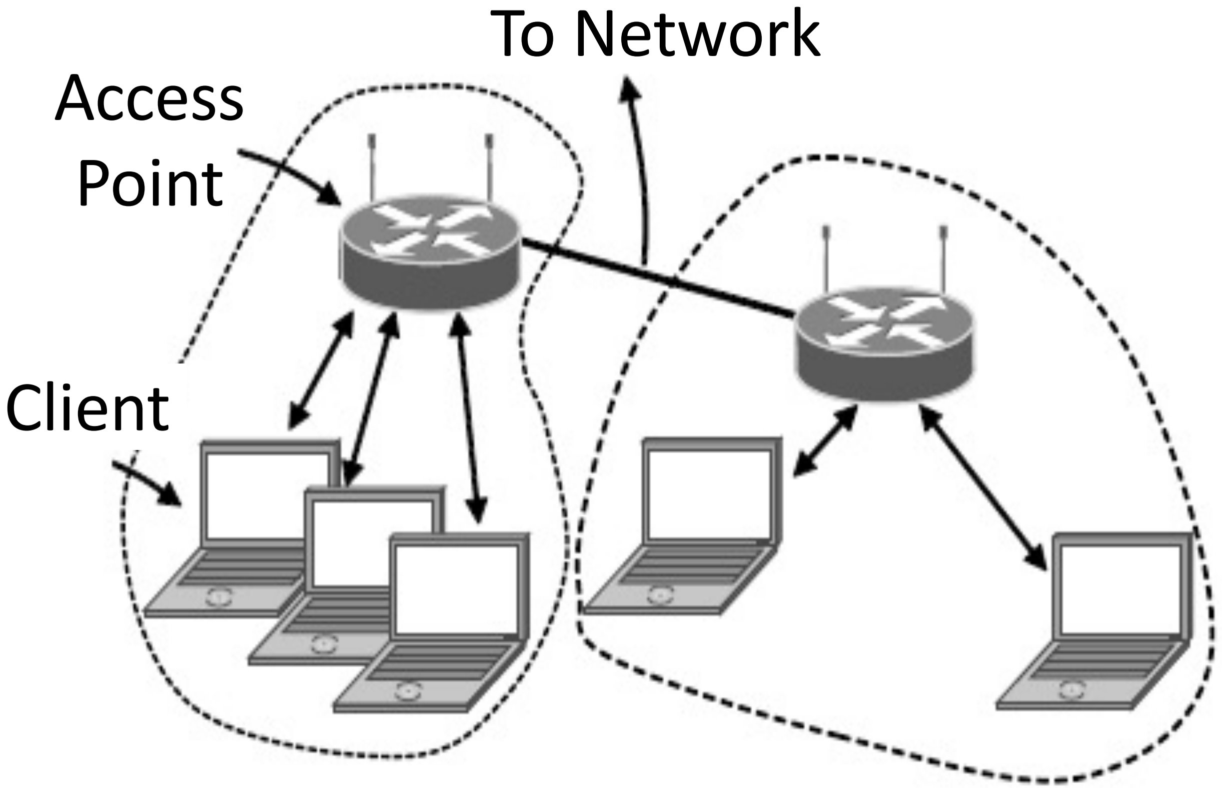
MACA – Exposed Terminals (3)

- B→A, C→D as exposed terminals
  - A and D send CTS to B and C



802.11, or WiFi

- Very popular wireless LAN started in the 1990s
- Clients get connectivity from a (wired) AP (Access Point)
- It’s a multi-access problem ☺
- Various flavors have been developed over time
  - Faster, more features



802.11 Physical Layer

- Uses 20/40 MHz channels on ISM (unlicensed) bands
  - 802.11b/g/n on 2.4 GHz
  - 802.11 a/n on 5 GHz
- OFDM modulation (except legacy 802.11b)
  - Different amplitudes/phases for varying SNRs
  - Rates from 6 to 54 Mbps plus error correction
  - 802.11n uses multiple antennas
    - Lots of fun tricks here

802.11 Link Layer

- Multiple access uses CSMA/CA (next); RTS/CTS optional
- Frames are ACKed and retransmitted with ARQ
- Funky addressing (three addresses!) due to AP
- Errors are detected with a 32-bit CRC
- Many, many features (e.g., encryption, power save)

Packet from Network layer (IP)

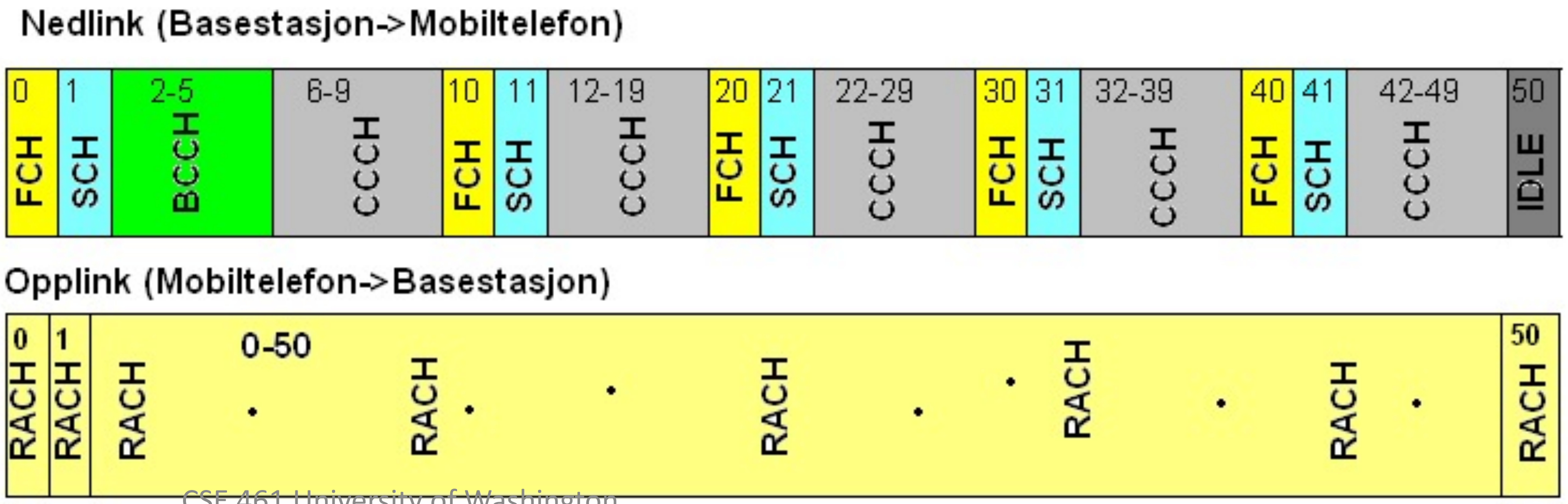
	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence
Bytes	2	2	6	6	6	2	0–2312	4

Centralized MAC: Cellular

- Spectrum suddenly very scarce
  - We can't waste all of it sending JAMs
- We have QoS requirements
  - Can't be as loose with expectations
  - Can't have traffic fail
- We also have client/server
  - Centralized control
  - Not peer-to-peer/decentralized

GSM MAC

- FDMA/TDMA
- Use one channel for coordination – Random access w/BEB (no CSMA, can't detect)
- Use other channels for traffic
  - Dedicated channel for QoS



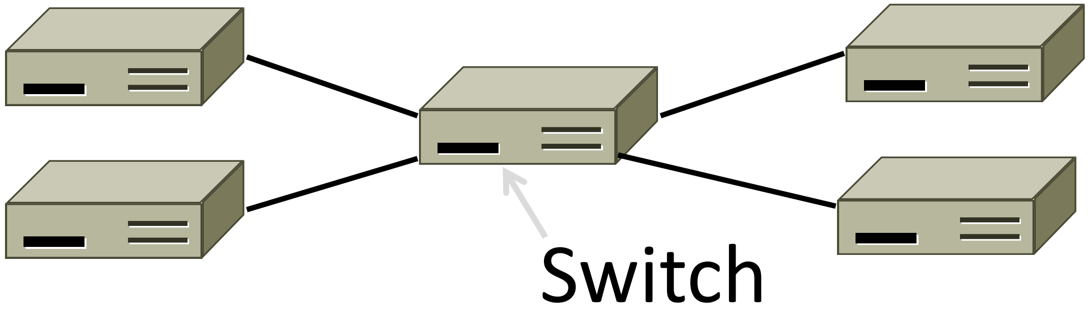
Recap: MAC layer ideas

- Random wait times upon collisions
- Carrier sense
  - Persistence
- Collision detection
- Binary exponential backoff
- RTS-CTS for hidden and exposed terminals

Link Layer: Switching

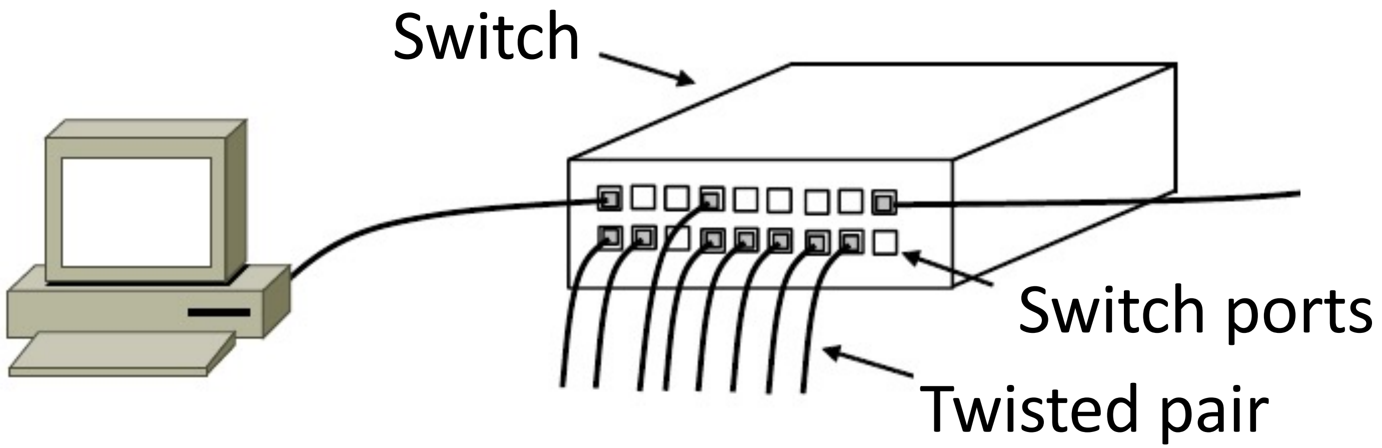
Switching

- How do we connect nodes with a switch instead of multiple access
  - Uses multiple links/wires
  - Basis of modern (switched) Ethernet



Switched Ethernet

- Hosts are wired to Ethernet switches with twisted pair
  - Switch serves to connect the hosts
  - Wires usually run to a closet



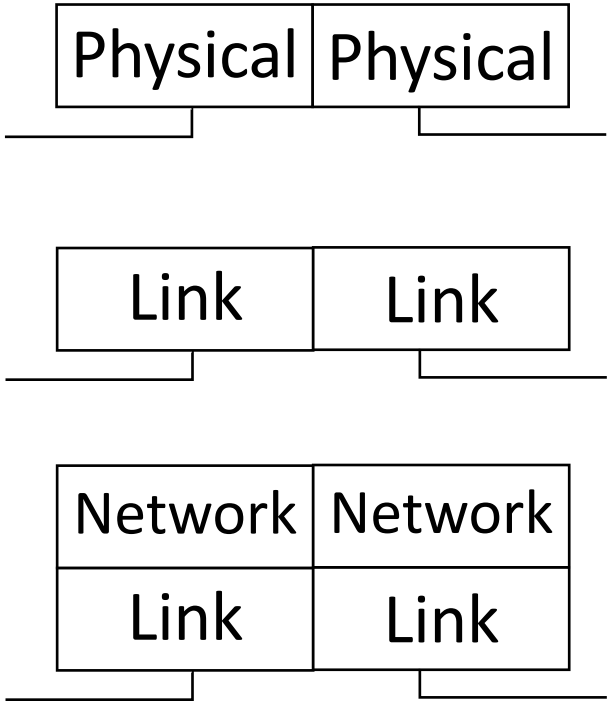
What's in the box?

- Remember from protocol layers:

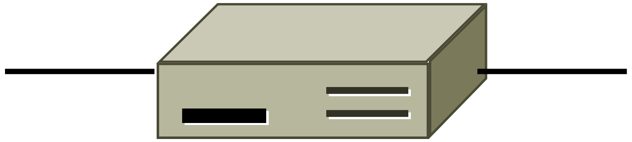
Hub, or repeater

Switch

Router

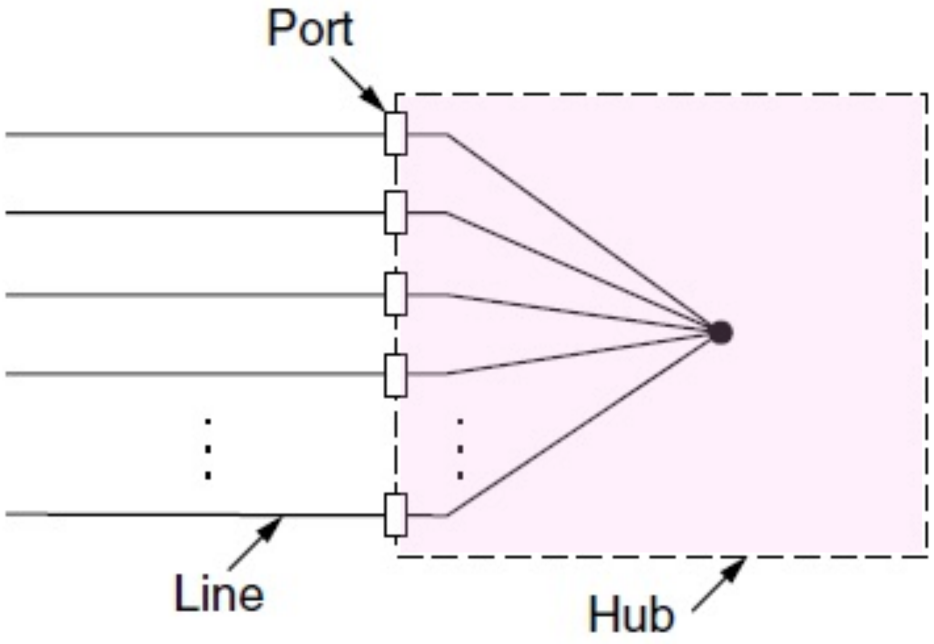


All look like this:

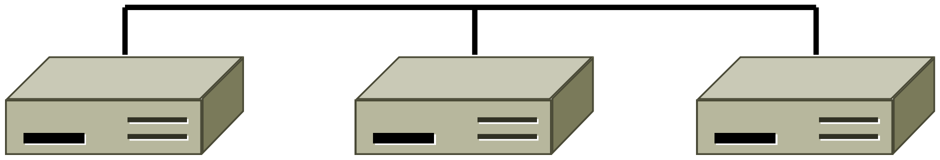


Inside a Hub

- All ports are wired together; more convenient and reliable than a single shared wire

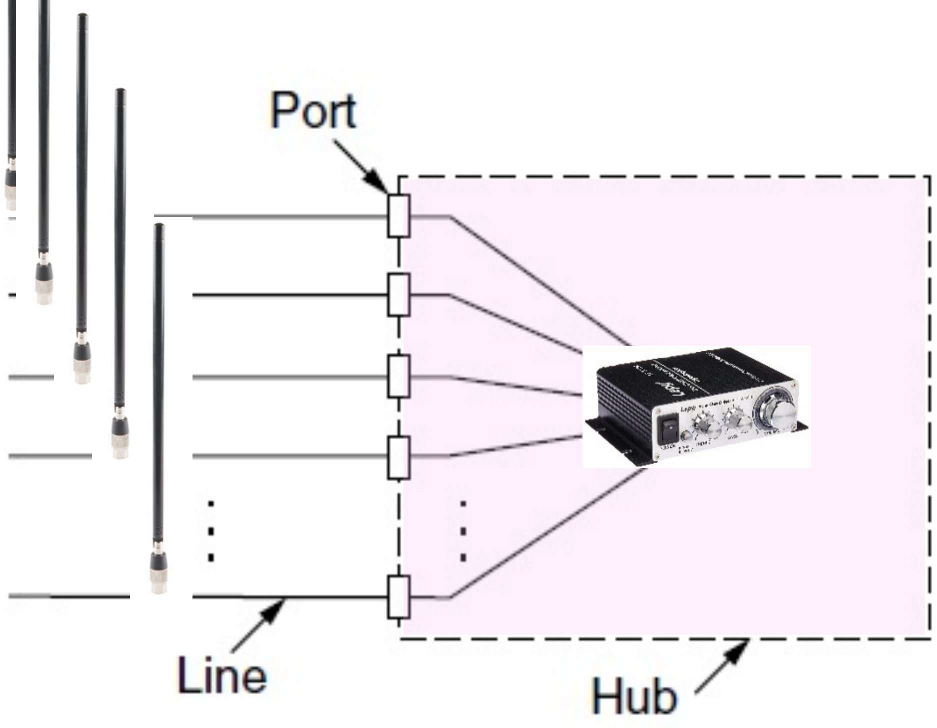


↔

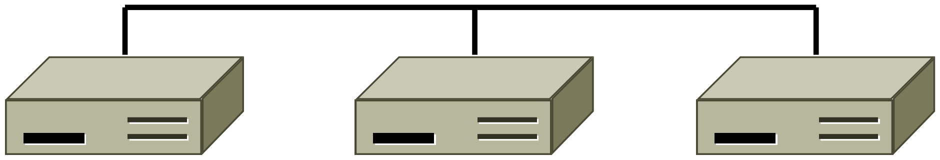


Inside a Repeater

- All inputs are connected; then amplified before going out

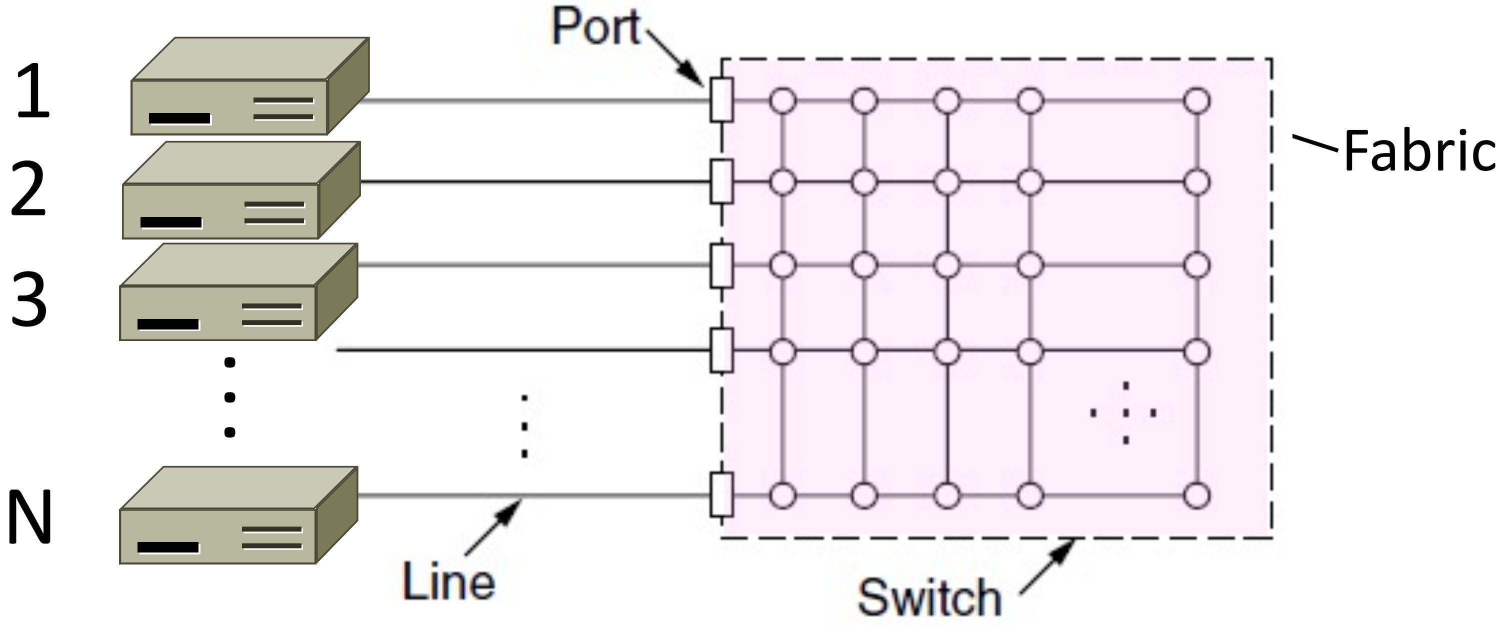


↔



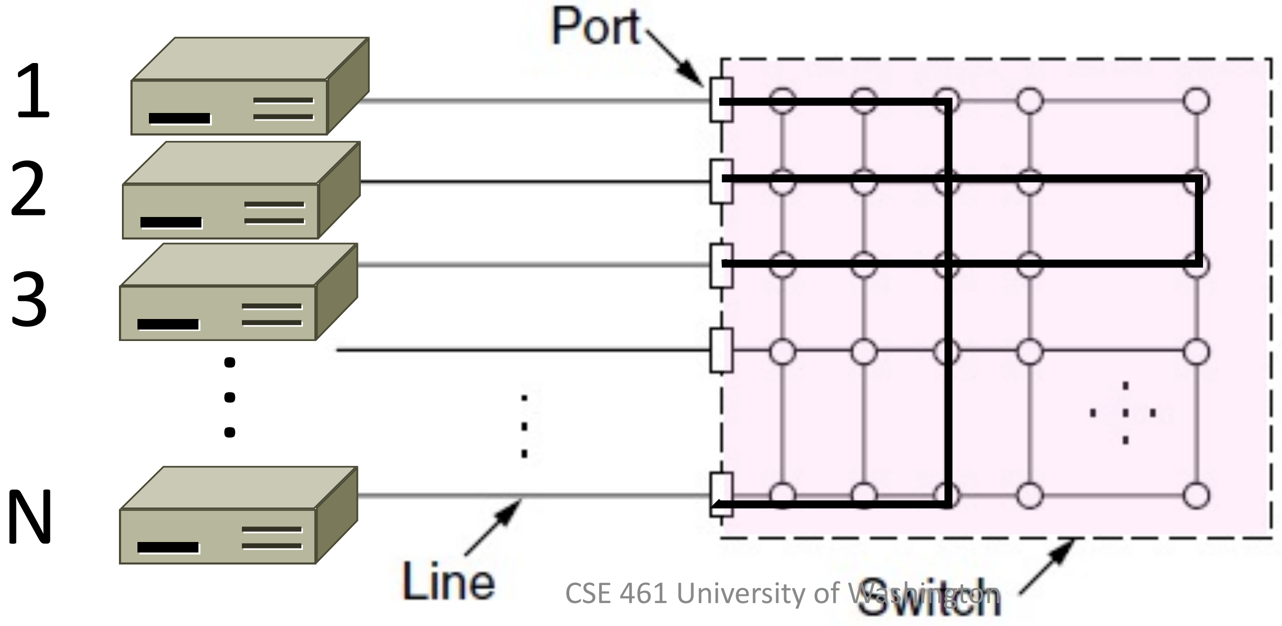
Inside a Switch

- Uses frame addresses (MAC addresses in Ethernet) to connect input port to the right output port; multiple frames may be switched in parallel



Inside a Switch (2)

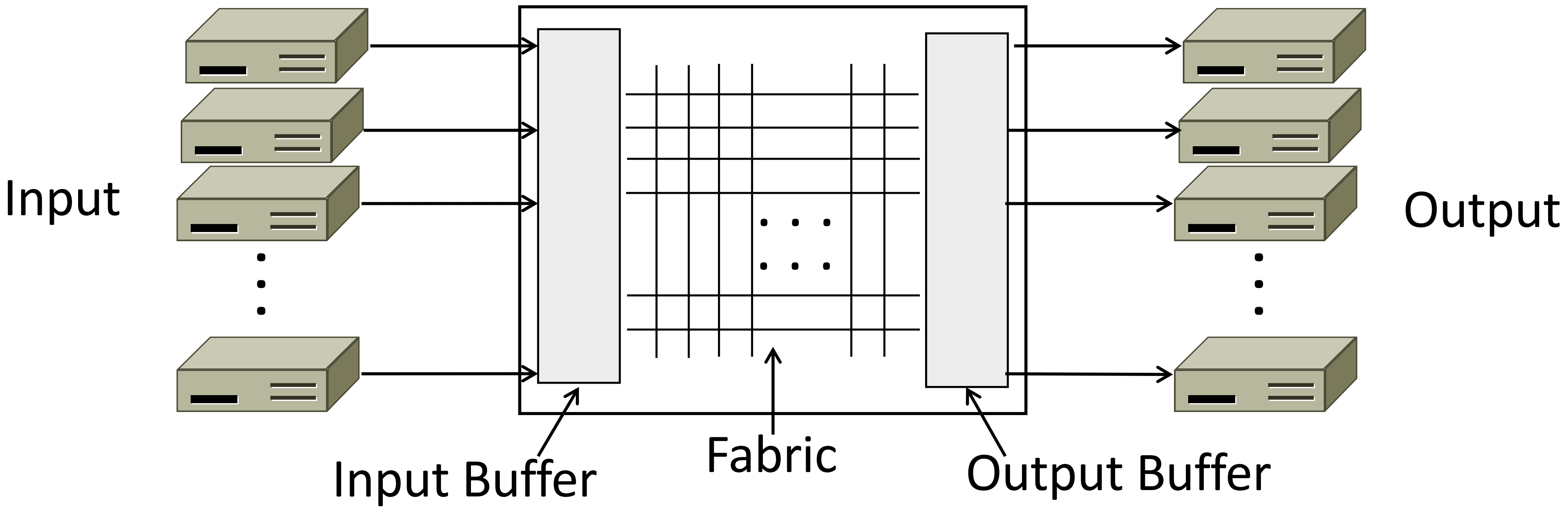
- Port may be used for both input and output (full-duplex)
  - Just send, no multiple access protocol



1 → 4
and
2 → 3

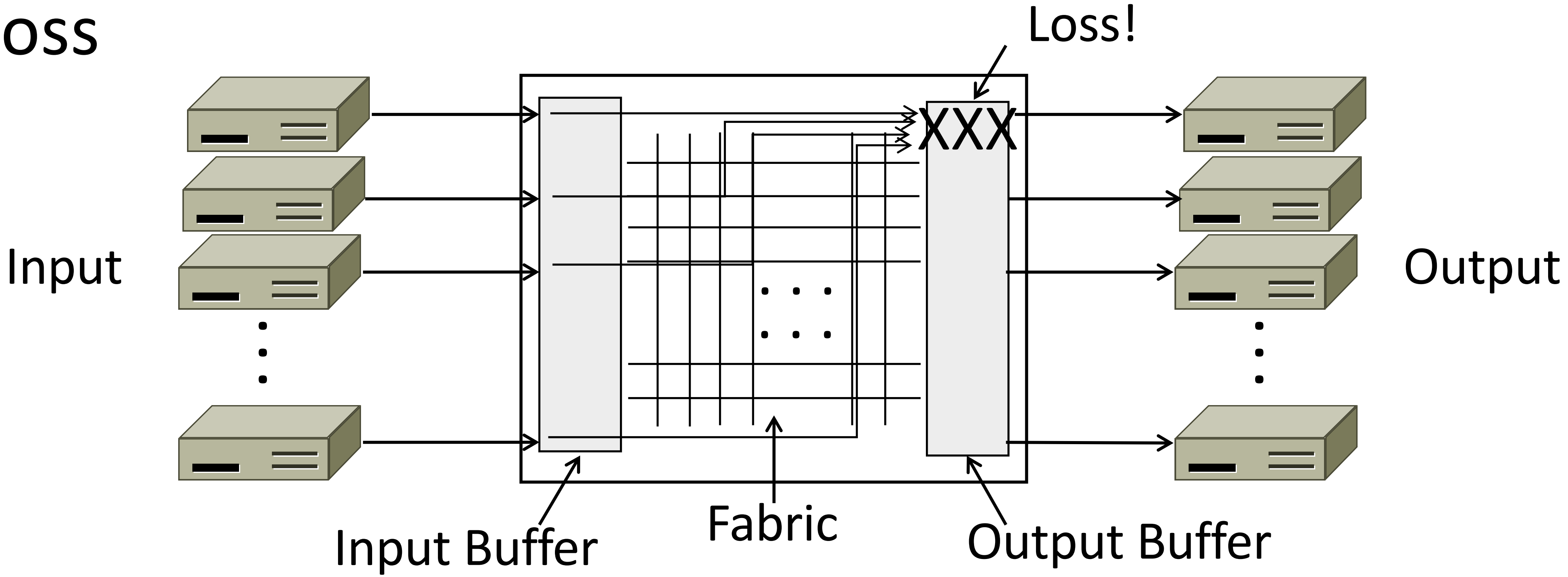
Inside a Switch (3)

- Need buffers for multiple inputs to send to one output



Inside a Switch (4)

- Sustained overload will fill buffer and lead to frame loss



Advantages of Switches

- Switches and hubs (mostly switches) have replaced the shared cable of classic Ethernet
  - Convenient to run wires to one location
  - More reliable; wire cut is not a single point of failure that is hard to find

- Switches offer scalable performance
  - E.g., 100 Mbps per port instead of 100 Mbps for all nodes of shared cable / hub