

# Computer Networks

## X\_400487

### Lecture 4

### Chapter 4: Medium Access Control



Lecturer: Jesse Donkervliet  
Includes slides from Vlad Cursaru



IEEE 802.3

IEEE 802.11

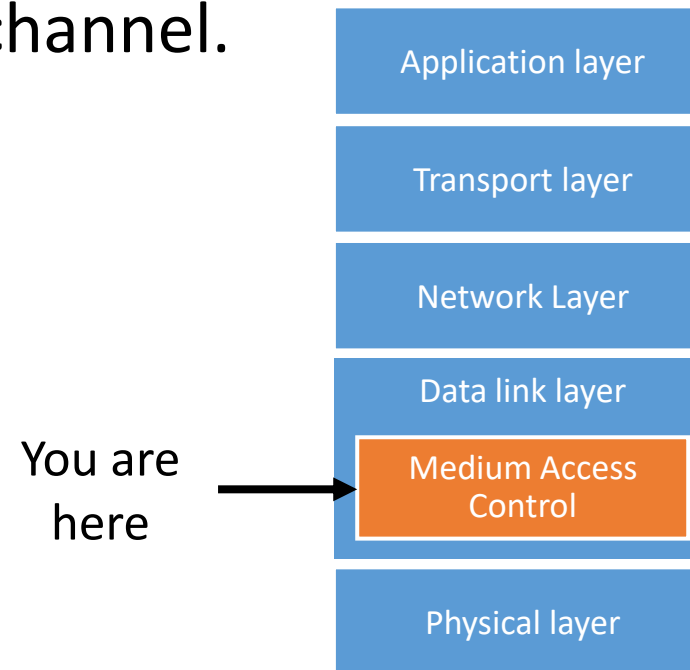


# The MAC sublayer

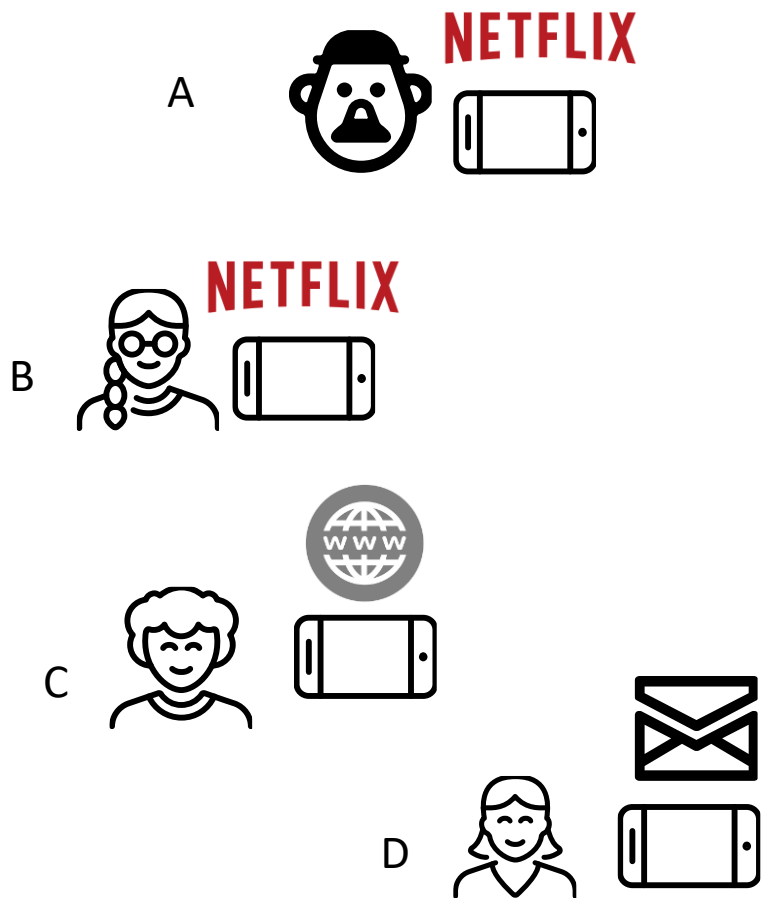
## Medium Access Control

Lower part of the Data link layer.

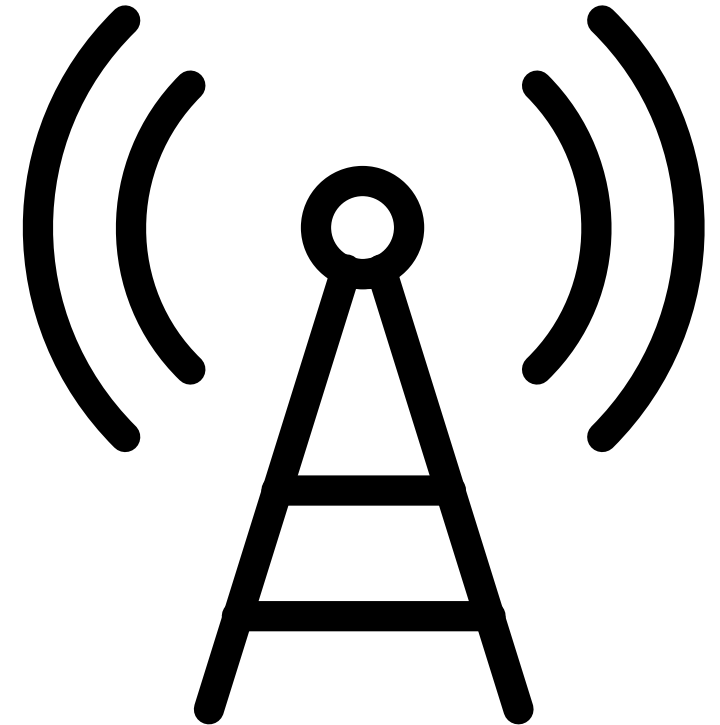
Responsible for deciding who can use the communication channel.



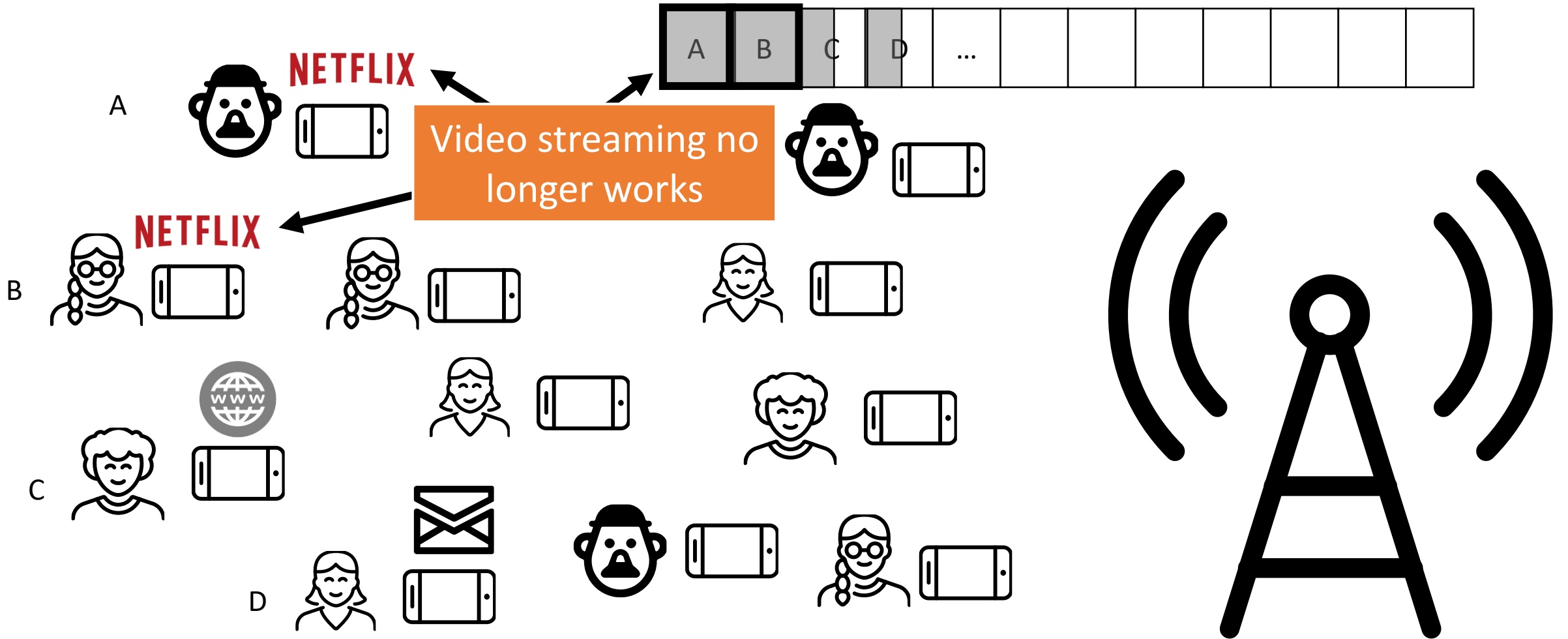
# Physical-Layer solution is insufficient!



Inefficient resource usage



# Physical-Layer solution is insufficient!



# MAC Sublayer Outline

ALOHA & Slotted ALOHA

CSMA

1-persistent

nonpersistent

p-persistent

CSMA/CD

**802.3 Ethernet**

Ethernet Switching

MAC for Wireless

Hidden Terminal

Exposed Terminal

CSMA/CA

**802.11 WiFi**

Collision-Free Protocols

Basic Bit-Map

Token Ring

Binary Countdown

# Two Approaches: Contend or Coordinate

## Contend

- If there is data to send, **send it!**
- Collisions are a fact of life.
- **Keep trying** until sending succeeds.

Q: When to apply which strategy?

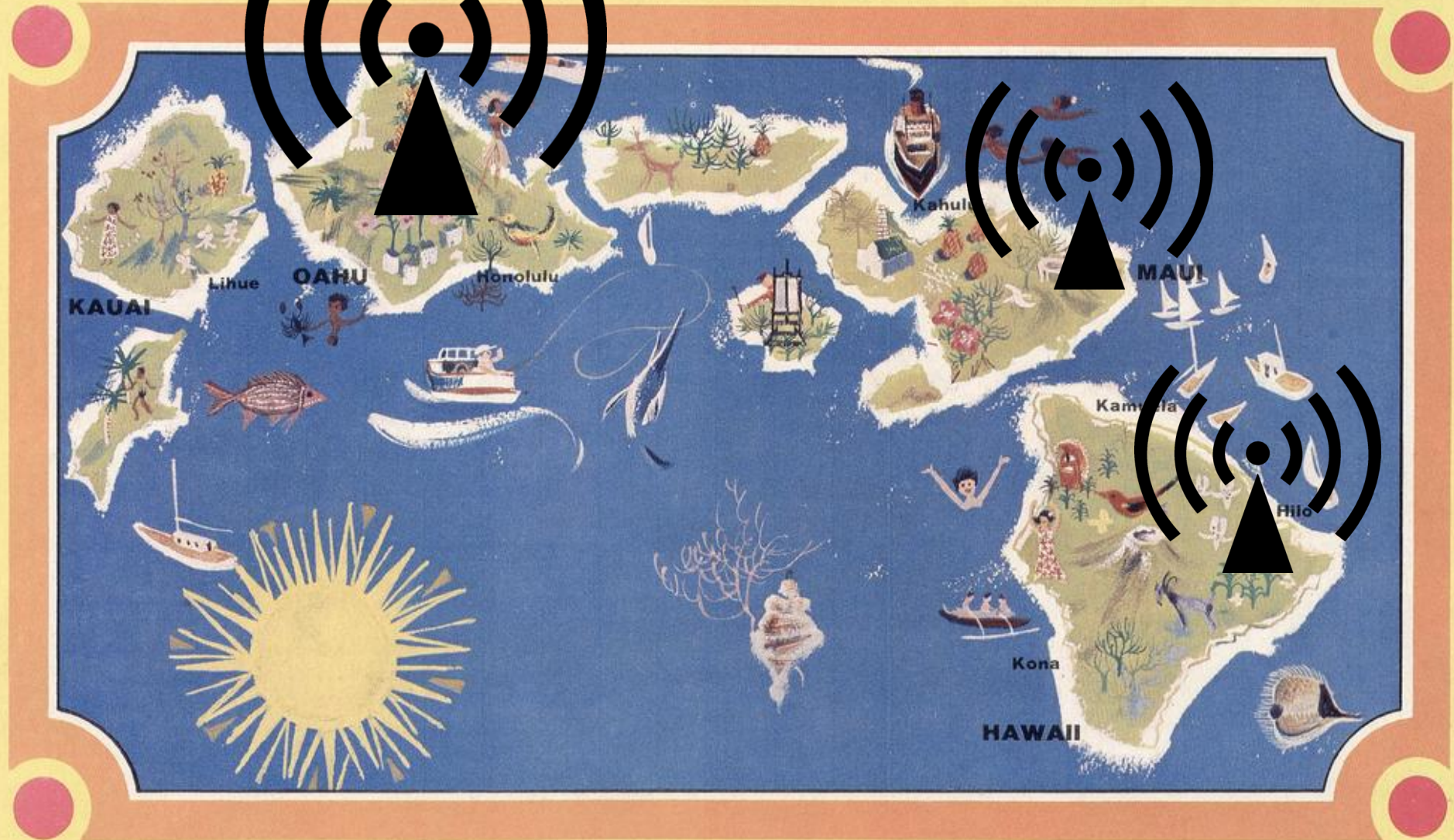
## Coordinate

- If there is data to send, let other stations know.
- Send **when it is your turn**.
- Patiently **wait** while other stations are sending.



Protocols somewhere along the spectrum

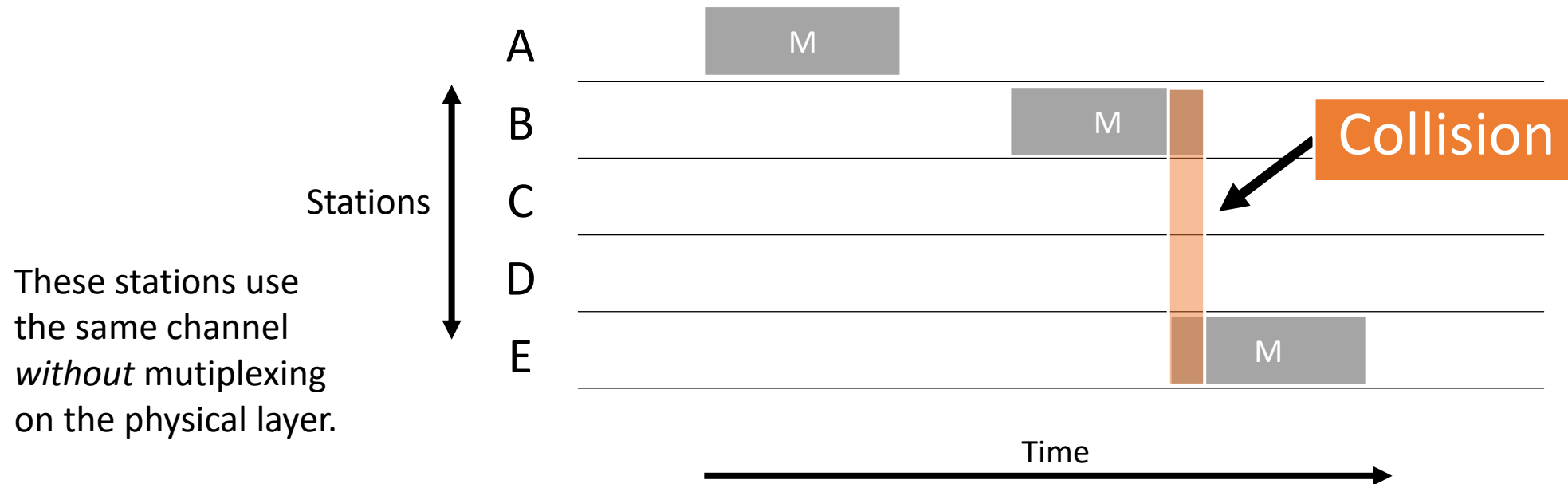
# HAWAII 1970



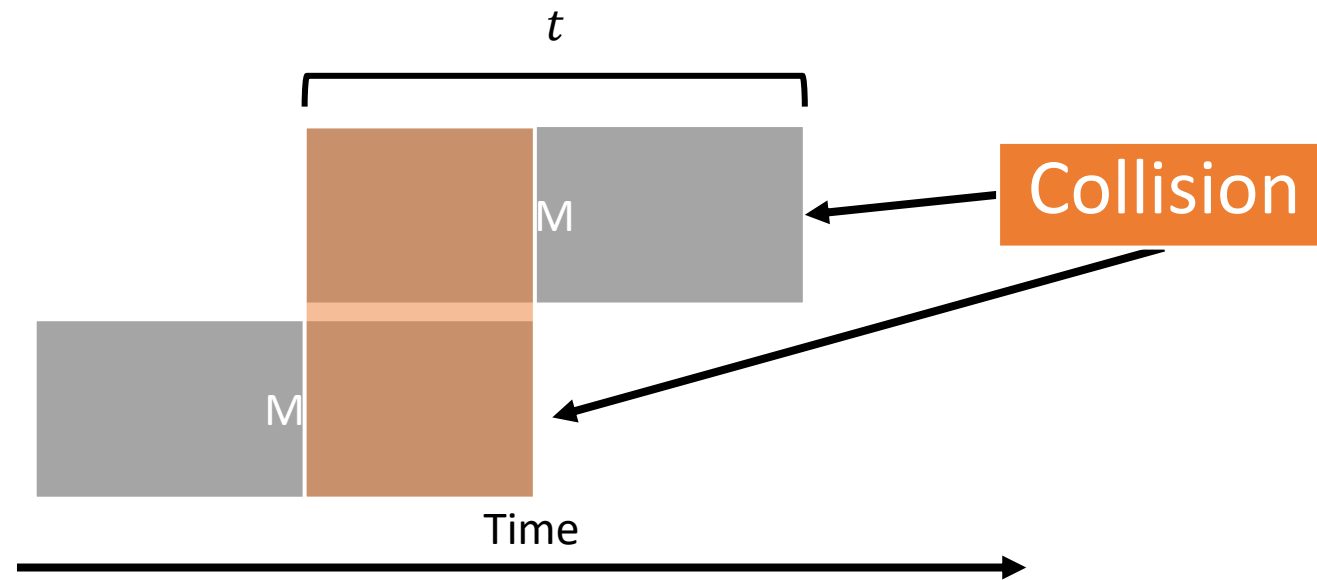
# ALOHA

Q: When does ALOHA perform well/badly?

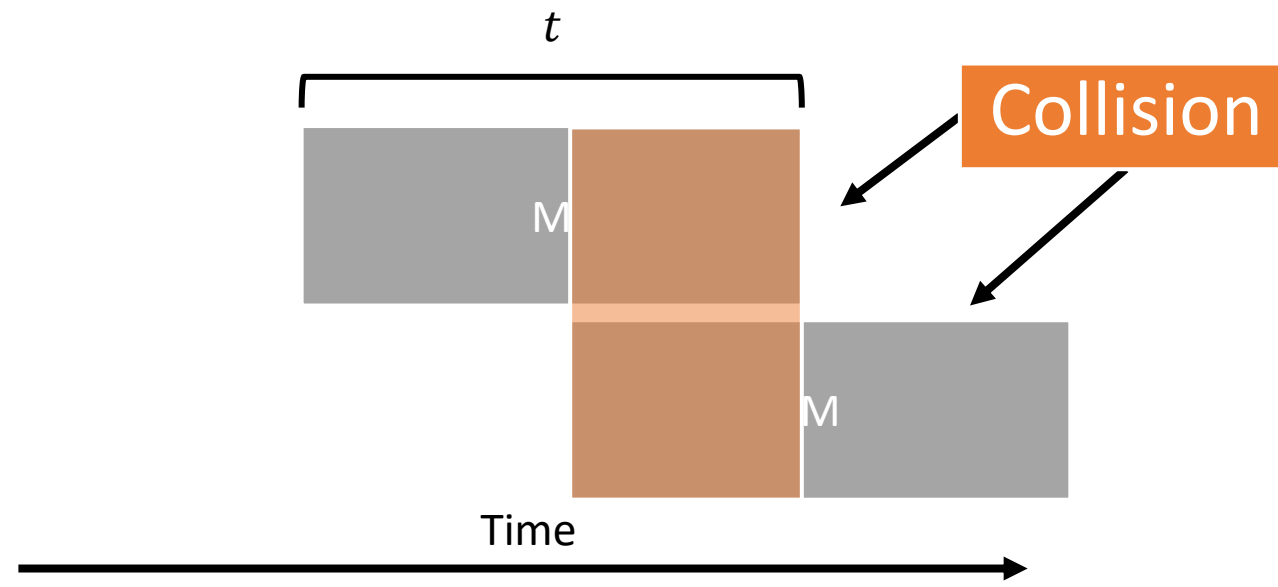
In pure ALOHA, users transmit frames *whenever they have data*; if a collision occurs, *users retry after a random delay*.



# Collisions in ALOHA



# Collisions in ALOHA

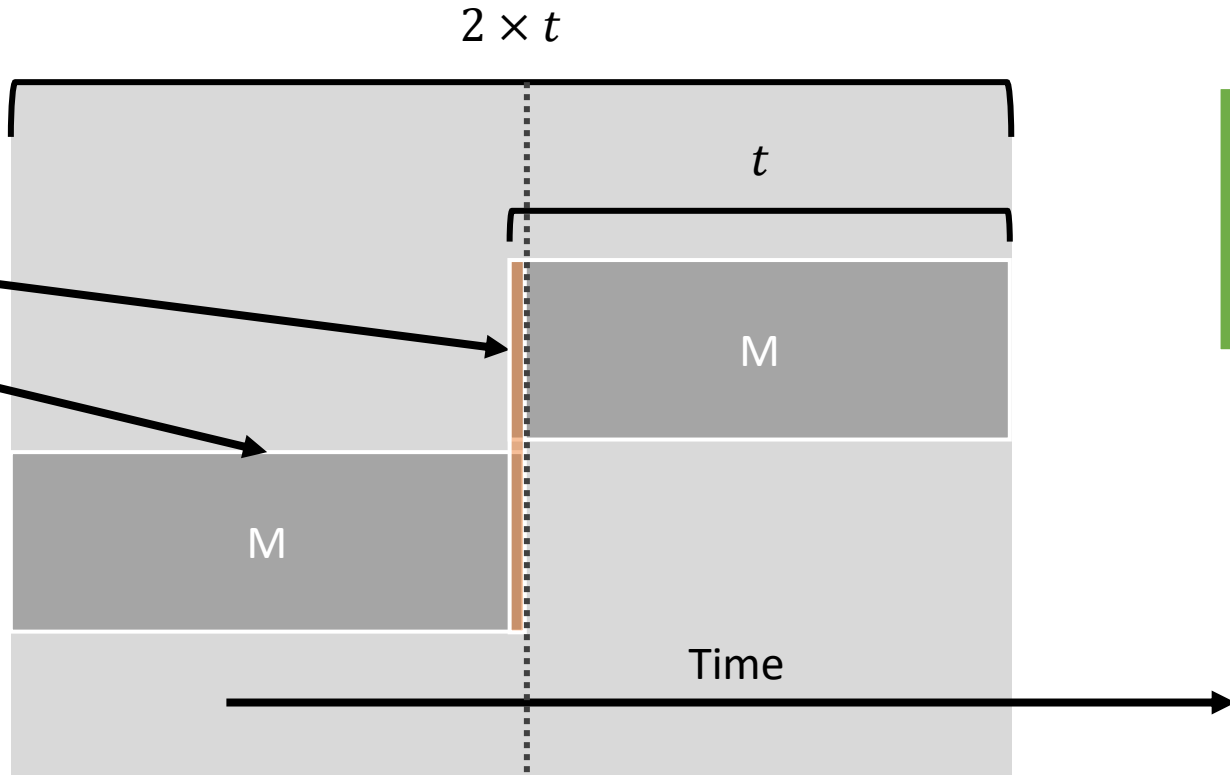


# Collisions in ALOHA

Frame collisions can occur anywhere within 2 times duration of transmission.



Collision

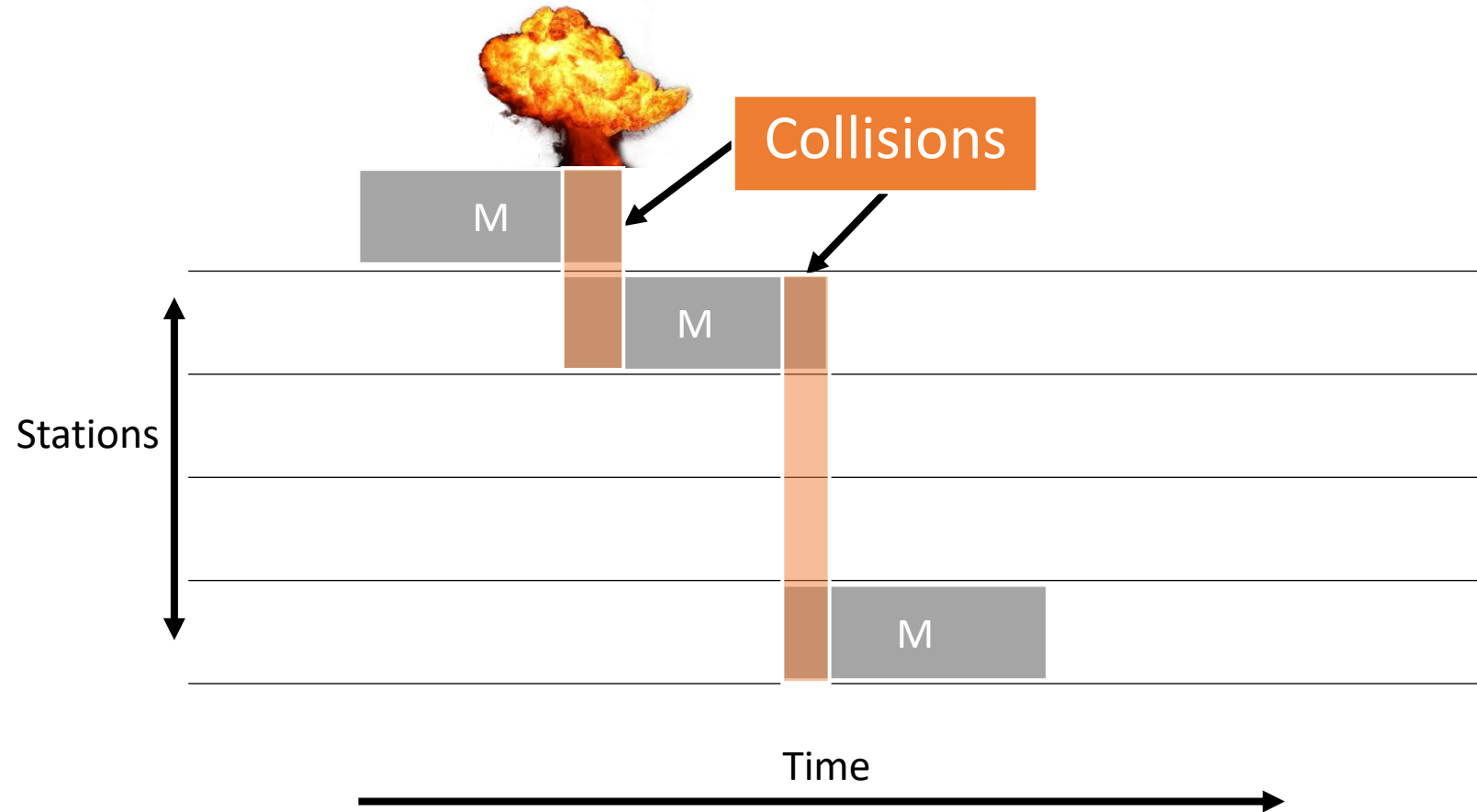


If another frame is sent anywhere in this period, a collision occurs

# Pure ALOHA

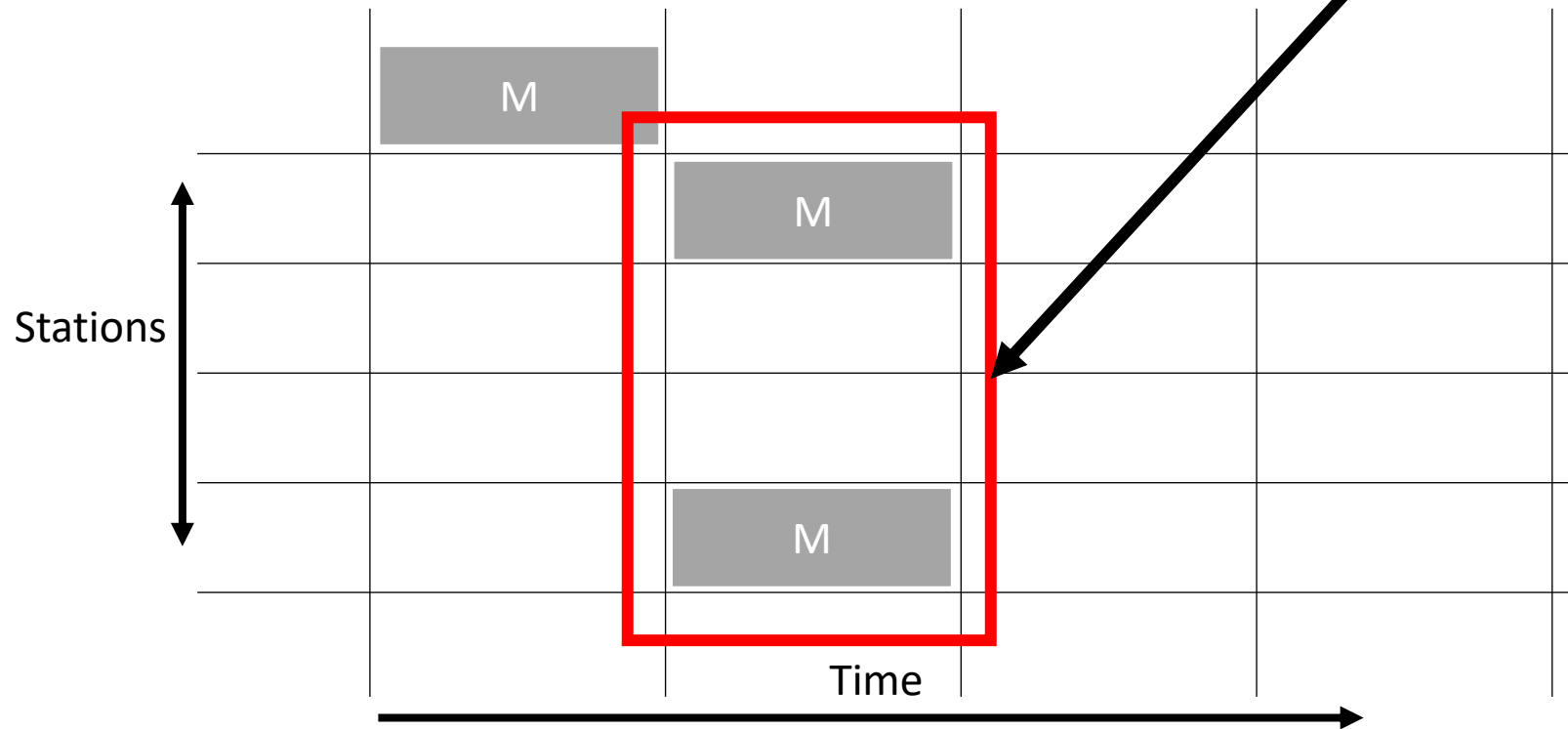
All of these messages will have to be retransmitted!

Q: How can we reduce the risk of collision?



# Slotted ALOHA

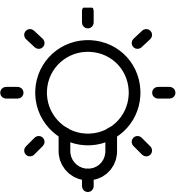
First frame sent successfully



These messages  
will have to be  
retransmitted!

Probability of frame collisions is reduced. Frames now overlap completely, or not at all.

# Carrier Sense Multiple Access



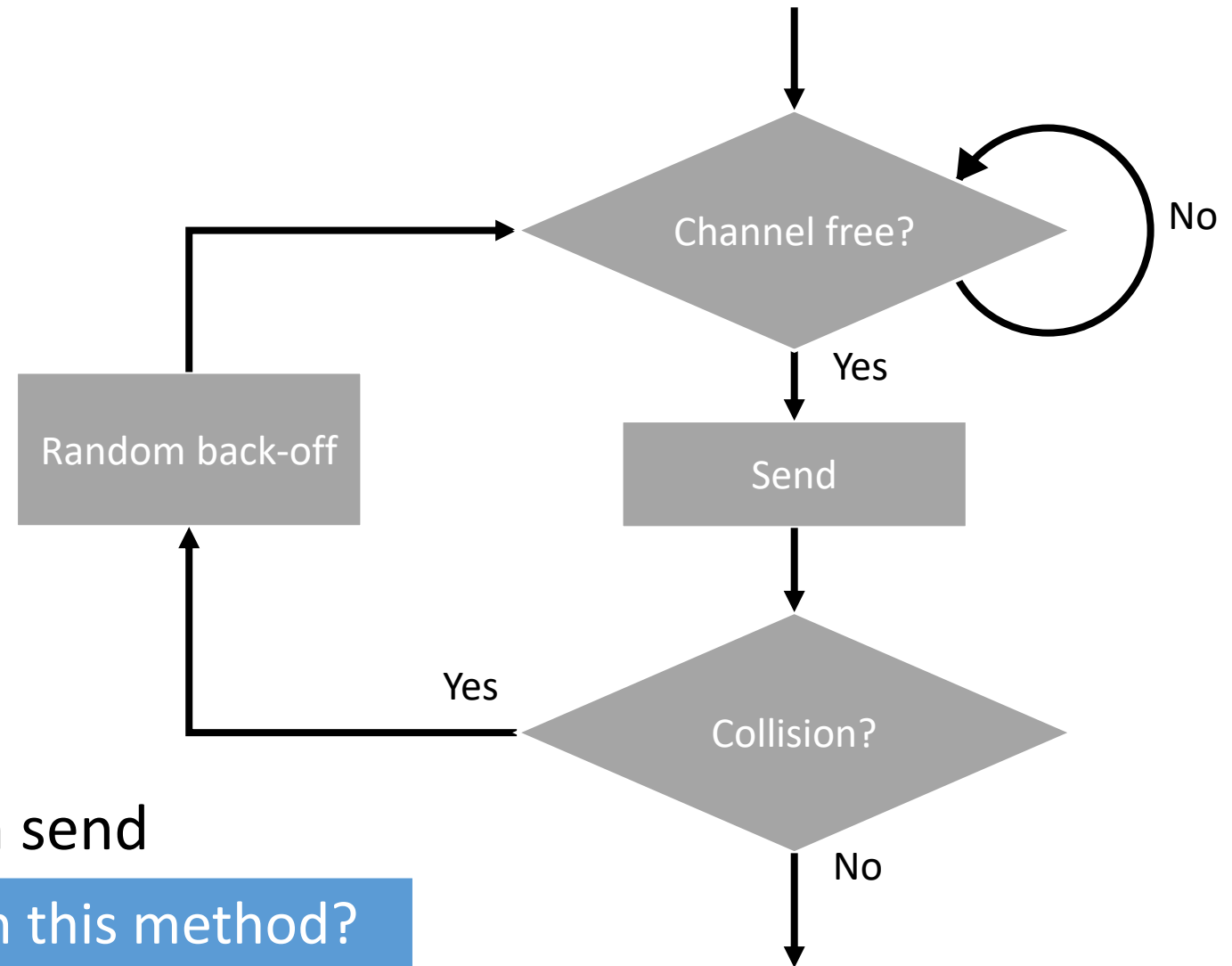
# Carrier-Sense Multiple Access

Senders detect (“sense”) if the channel is in use

Protocols that apply CSMA:

1. 1-persistent: wait for idle, then send. If collision, random back-off.
2. Nonpersistent: if busy, random back-off. Try again
3.  $p$ -persistent: if busy, wait for next slot  
if idle, send with probability  $p$

# 1-persistent CSMA



Wait until the channel is idle, then send

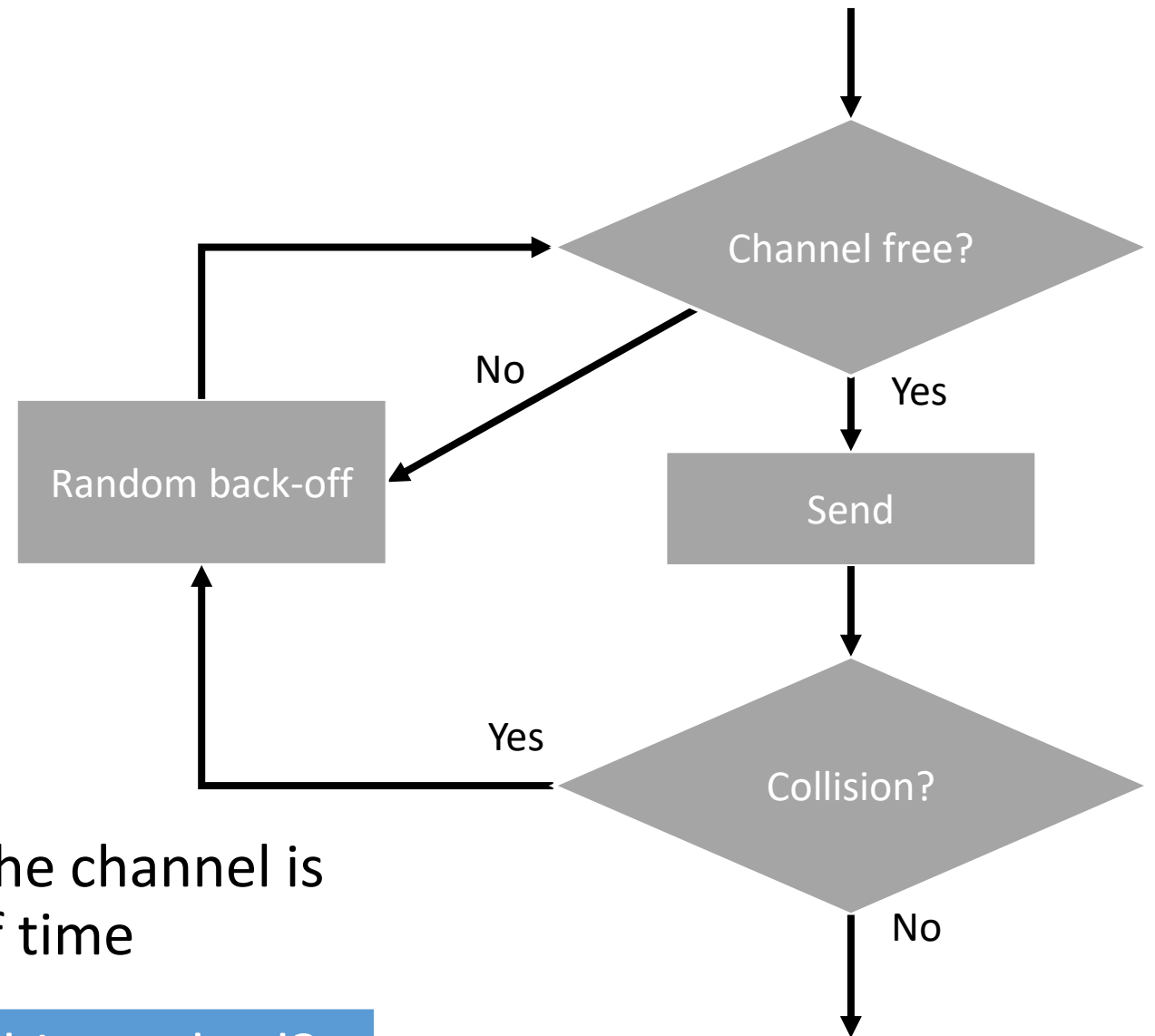
Q: Can you think of a problem with this method?

# Nonpersistent CSMA



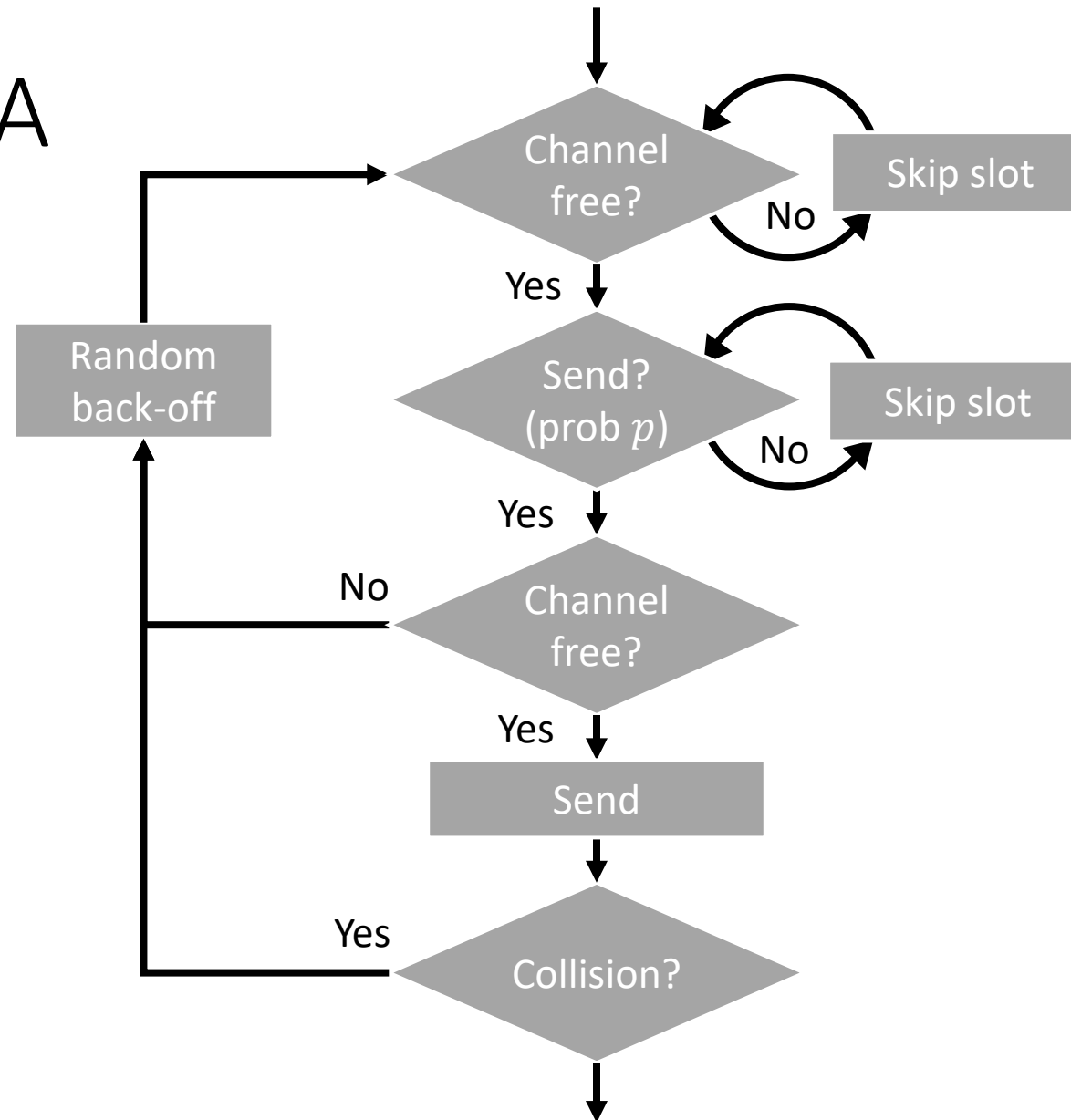
Nonpersistent CSMA is less greedy. If the channel is occupied, it waits a random amount of time

Q: Can you think of a problem with this method?



# $p$ -persistent CSMA

Applies to *slotted* channels.



Keeps waiting. Sends frame with probability  $p$

# Behavior of $x$ -persistent CSMA



Q: What trade-off do these protocols make?

Latency, bandwidth, (protocol) complexity

Early computer networks research evaluated protocol performance **theoretically**, using assumptions such as packet arrivals following **Poisson distributions**. Empirical research showed this **not to be the case**.<sup>\*</sup> We still(!) **lack mathematical tools** to describe the behavior of these systems, and instead **rely on observing the behavior** of these systems “in the wild.”



<sup>\*</sup>E.g., Paxson and Floyd, 1995; and Leland et al., 1994

# MAC Sublayer Outline

ALOHA & Slotted ALOHA

CSMA

1-persistent

nonpersistent

p-persistent

CSMA/CD

**802.3 Ethernet**

Ethernet Switching

MAC for Wireless

Hidden Terminal

Exposed Terminal

CSMA/CA

**802.11 WiFi**

Collision-Free Protocols

Basic Bit-Map

Token Ring

Binary Countdown

# CSMA/CD

Carrier Sense Multiple Access with Collision Detection



# CSMA/CD:

## CSMA with *Collision Detection*

Idea: when collision is detected, do not finish sending.  
Stop transmission instead.

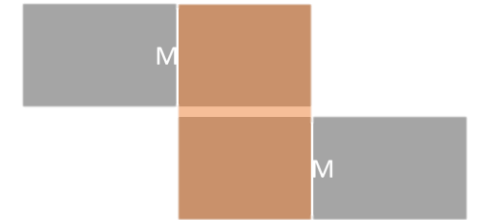
Separates **contention periods** from **transmission periods**.

Saves time and bandwidth

**Contention period:** check if it is safe to send data.

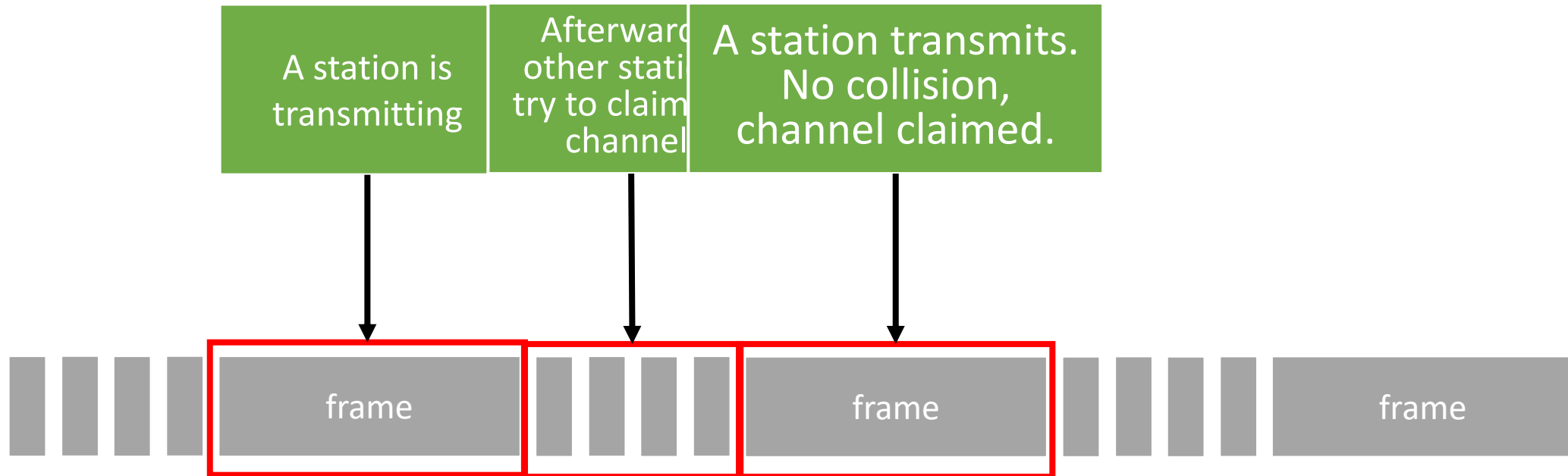
**Transmission period:** send data.

Remember?



# Collision detection

Abort transmission when collision is detected.



# Collision detection

Reduce contention period duration to improve throughput

Abort transmission when collision is detected.

Q: How do longer frames affect throughput? How about latency?



# MAC Sublayer Outline

ALOHA & Slotted ALOHA

CSMA

1-persistent

nonpersistent

p-persistent

CSMA/CD

**802.3 Ethernet**

Ethernet Switching

MAC for Wireless

Hidden Terminal

Exposed Terminal

CSMA/CA

**802.11 WiFi**

Collision-Free Protocols

Basic Bit-Map

Token Ring

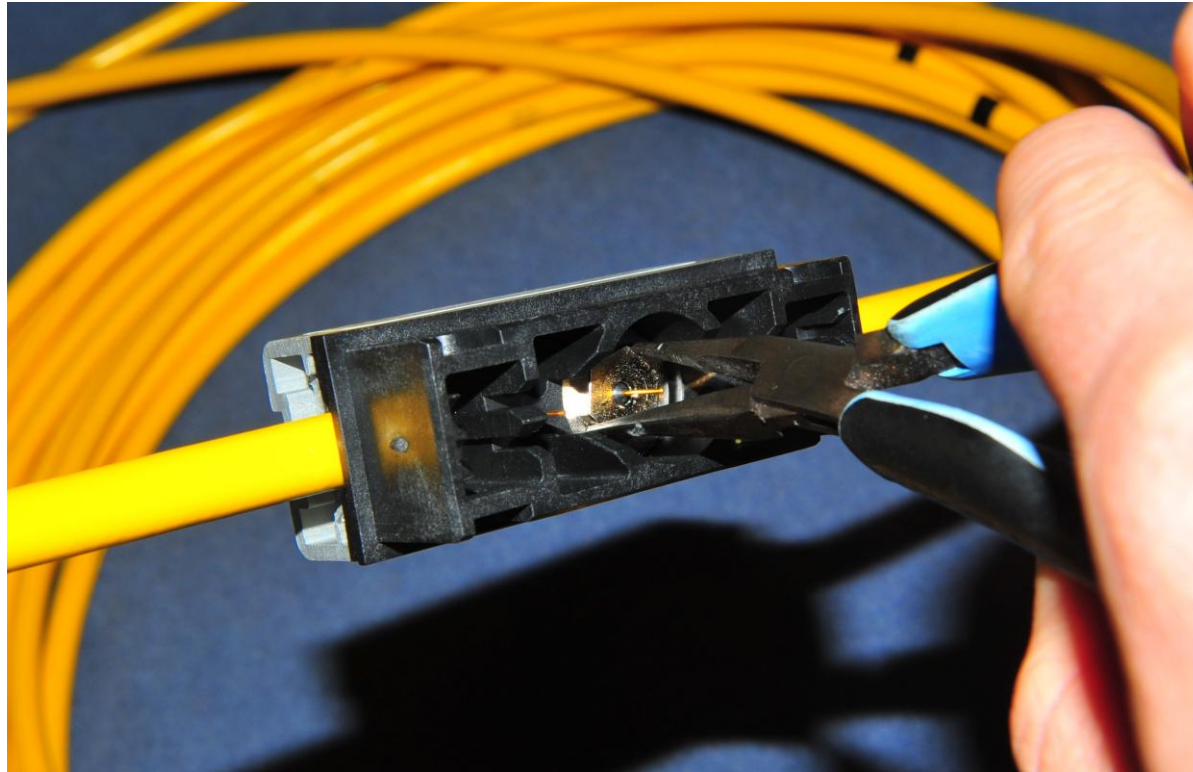
Binary Countdown

# Medium Access Control Classic Ethernet



# Medium Access Control in ... Classic Ethernet

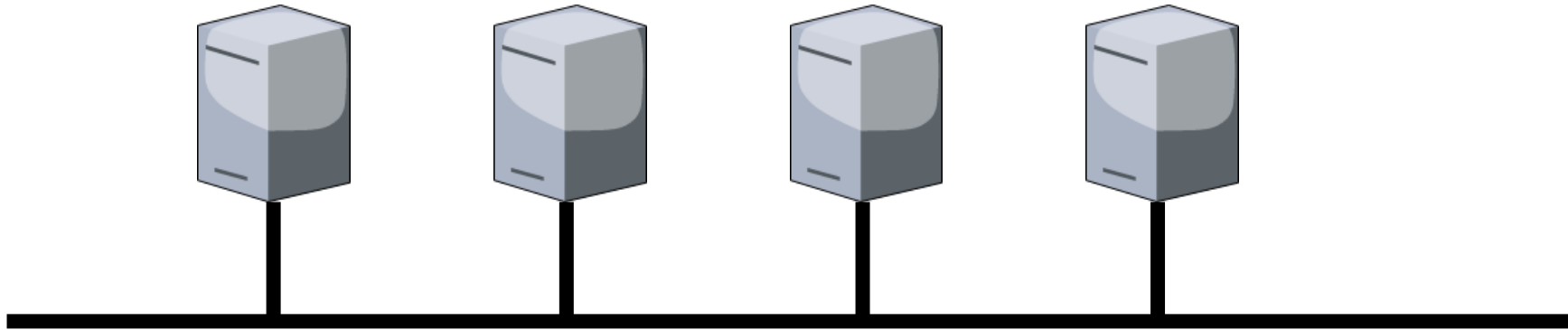
Multiple machines sharing a single Ethernet connection.



# Medium Access Control in ... Classic Ethernet

Multiple machines sharing a single Ethernet connection.

Q: Which MAC protocol should we use?



Newer versions of Ethernet (10-gigabit Ethernet and up) only support point-to-point full-duplex operation.

# Medium Access Control in ... Classic Ethernet

Uses **1-persistent CSMA/CD**.

Random delay (back-off) after collision is computed with Binary Exponential Back-off.

Failed Attempts	Maximum Delay	Random Delay Range
0	$2^0 - 1 = 0$	$w \in [0,0]$
1	$2^1 - 1 = 1$	$w \in [0,1]$
2	$2^2 - 1 = 3$	$w \in [0,3]$
3	$2^3 - 1 = 7$	$w \in [0,7]$
4	$2^4 - 1 = 15$	$w \in [0,15]$
...	...	...

Station waits  $w$  slots, where  $w$  between 0 and  $2^i - 1$ .  
 $i$  is the number of failed attempts.

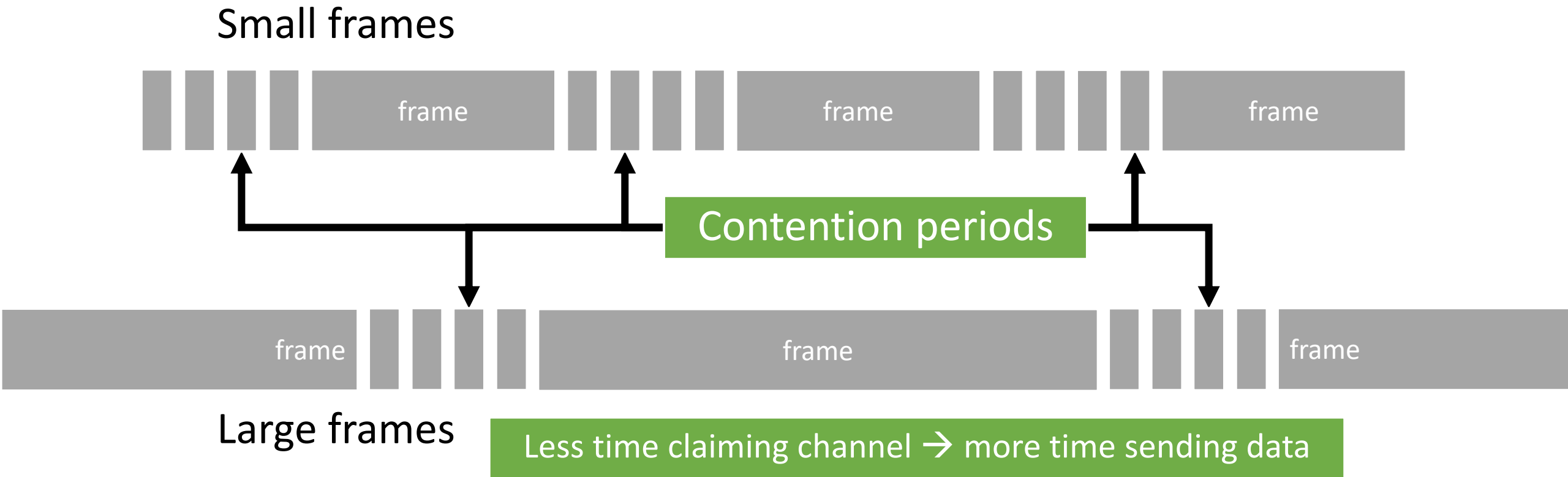
Q: What happens if more than 2 stations are trying to send a frame?

```
maxw = 0
collision = True
while collision:
    w = random.randint(0, maxw)
    collision = delayed_send(frame, w)
if collision:
    maxw = maxw << 1
    maxw = maxw | 1
```

# Ethernet performance

Q: What is more bandwidth efficient? Why?

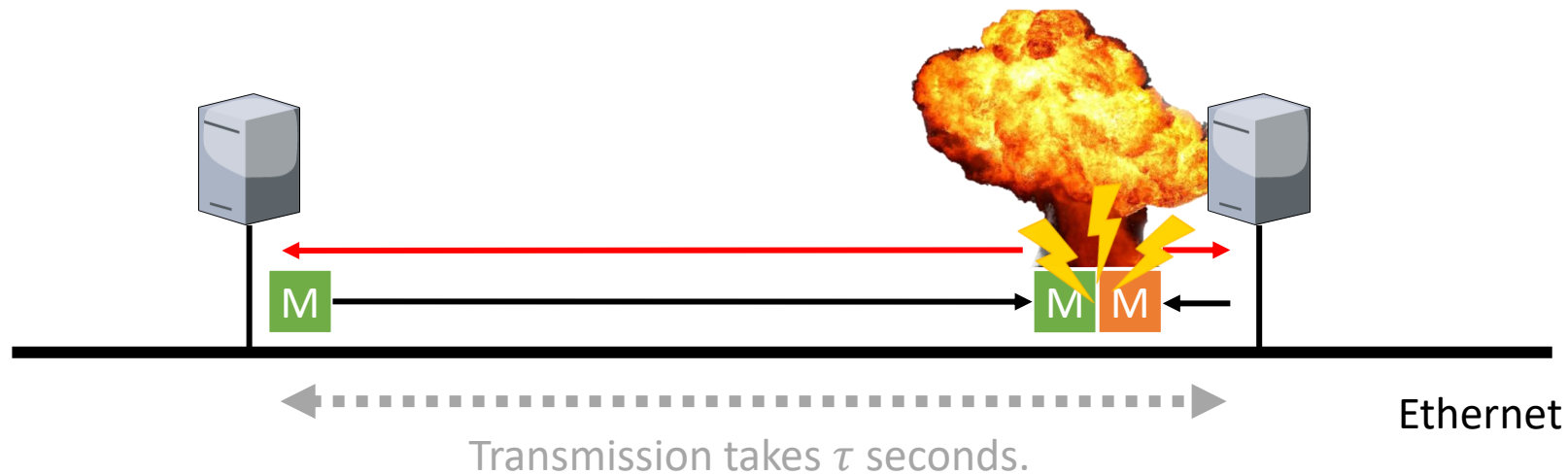
Q: Is there a trade-off here? Why?



# Classic Ethernet Collision detection

Q: Does the detection latency cause a problem?

Collisions can occur and take as long as  $2\tau$  to detect.  
 $\tau$  is the time it takes to propagate over the Ethernet.  
Leads to minimum packet size for reliable detection.

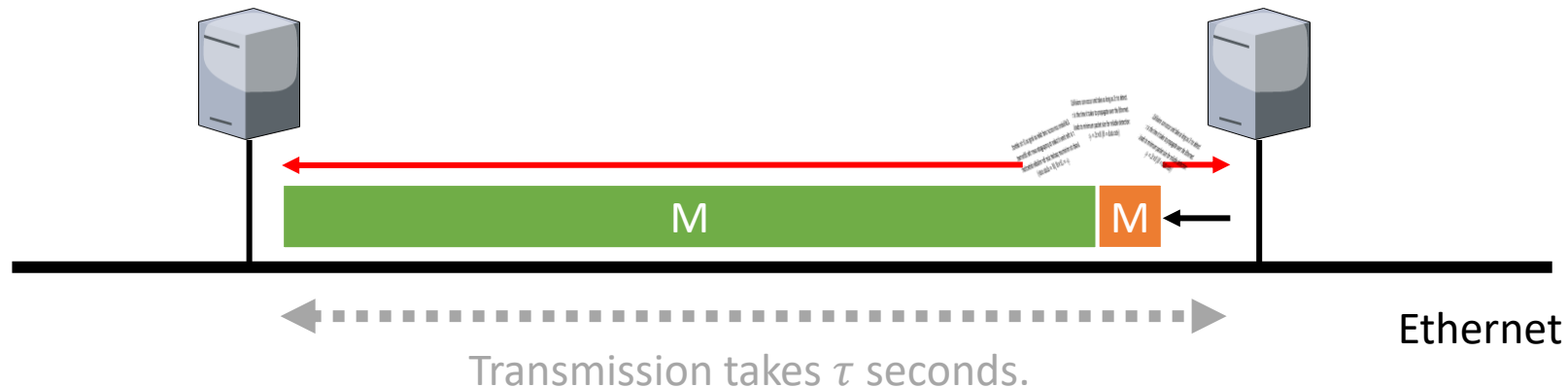


# Classic Ethernet Collision detection

Q: Does the detection latency cause a problem?

Collisions can occur and take as long as  $2\tau$  to detect.  
 $\tau$  is the time it takes to propagate over the Ethernet.  
Leads to minimum packet size for reliable detection:

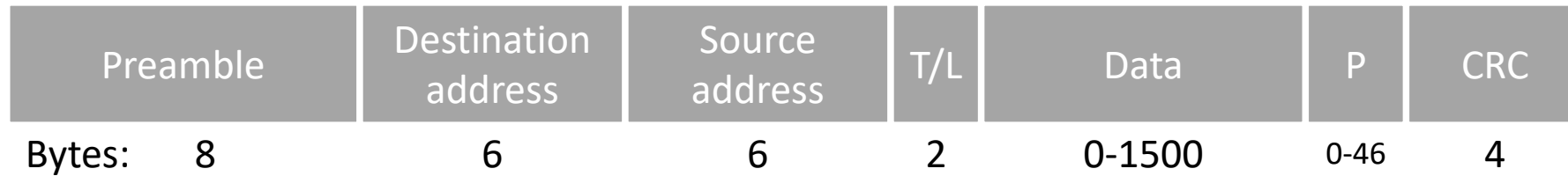
$$s_f = 2\tau \times R \quad (R = \text{data rate})$$



$$\tau = 5\mu\text{s}, R = 500\text{Mbps}, s_f = 2 \times 5\mu\text{s} \times 500\text{Mbps} = 5000 \text{ bits}$$

# Ethernet frames

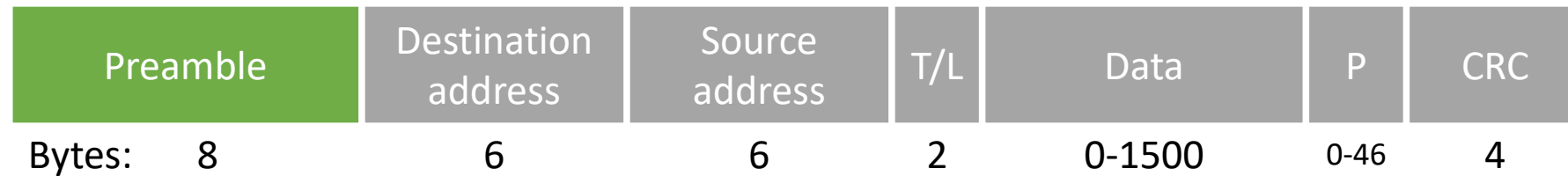
Frame format still used in modern versions of Ethernet.\*



\*VLAN-aware packets from 802.1Q use a slightly modified header.

# Ethernet frames

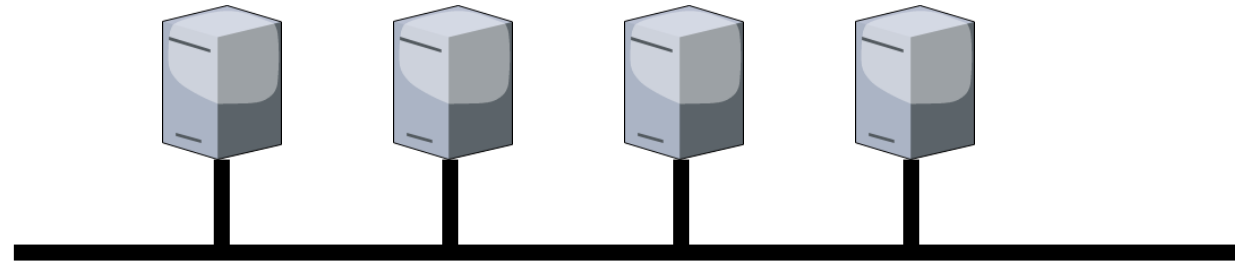
Frame format still used in modern versions of Ethernet.\*



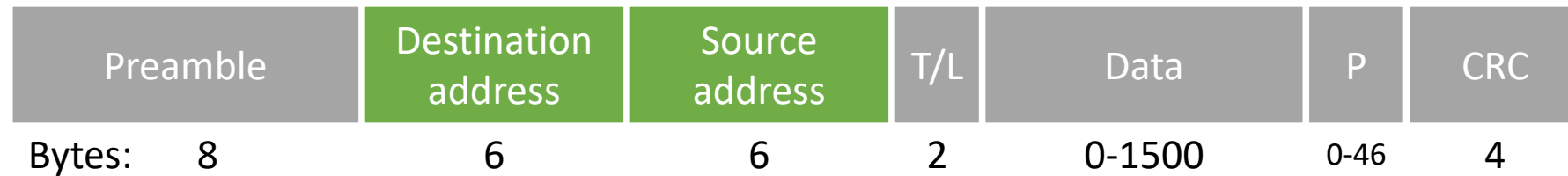
Bit-sequence used to indicate start of frame.

\*VLAN-aware packets from 802.1Q use a slightly modified header.

# Ethernet frames



Frame format still used in modern versions of Ethernet.\*



Source and destination addresses.

Q: Why needed over a single link?

Q: What is the name of this address? What is it assigned to?

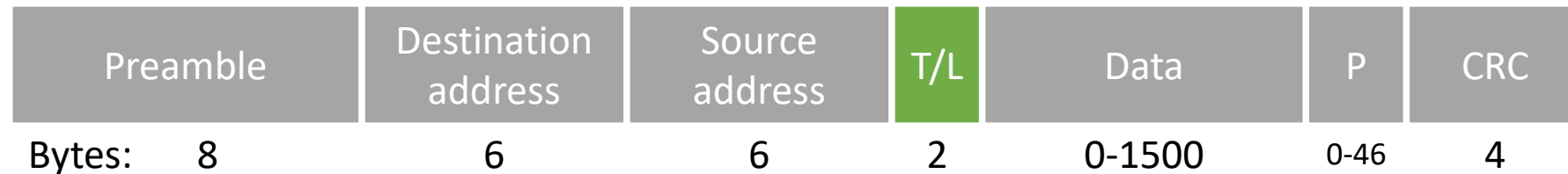
\*VLAN-aware packets from 802.1Q use a slightly modified header.

# Ethernet frames

Q: How is frame length determined?

Answer in physical layer:  
See 8B/10B encoding in book

Frame format still used in modern versions of Ethernet.\*



Type/length field:

Indicates to which network layer protocol the data should be sent.

Values less than 0x600 (1536) can be interpreted as length.  
(IEEE 802.3 only)

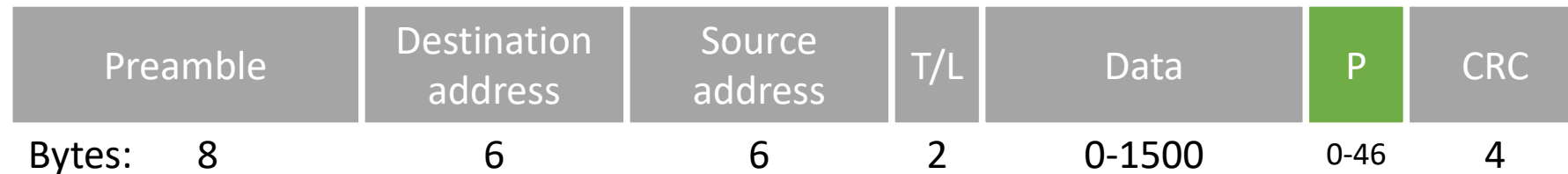
\*VLAN-aware packets from 802.1Q use a slightly modified header.

# Ethernet frames

Q: How to differentiate data and padding?

Problem for network layer: IP packet has length field

Frame format still used in modern versions of Ethernet.\*



Pad field:

Used if data causes frame to be less than the minimum frame length.

\*VLAN-aware packets from 802.1Q use a slightly modified header.

# Ethernet frames

Q: Reliable delivery?

Frame format still used in modern versions of Ethernet.\*



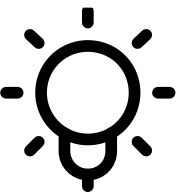
32-bit Cyclic Redundancy Check used for error detection.

Q: Error detection/correction?

Q: How long is the generator polynomial?

\*VLAN-aware packets from 802.1Q use a slightly modified header.

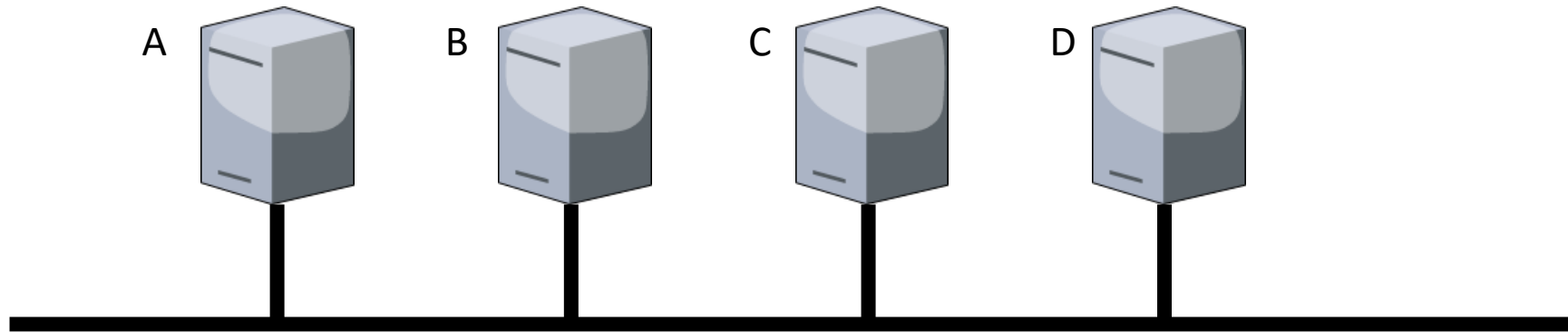
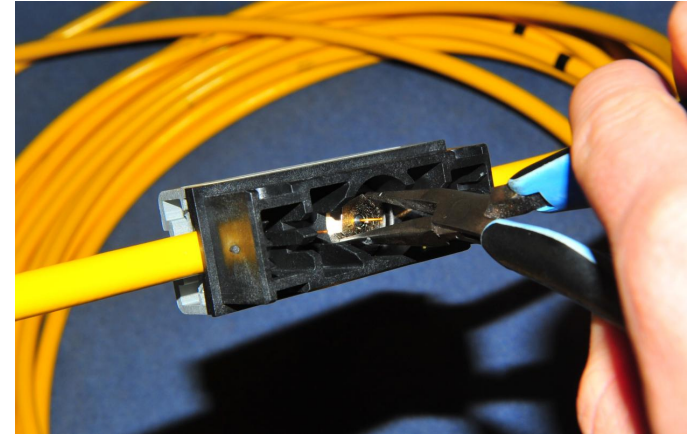
# Data Link Layer Switching



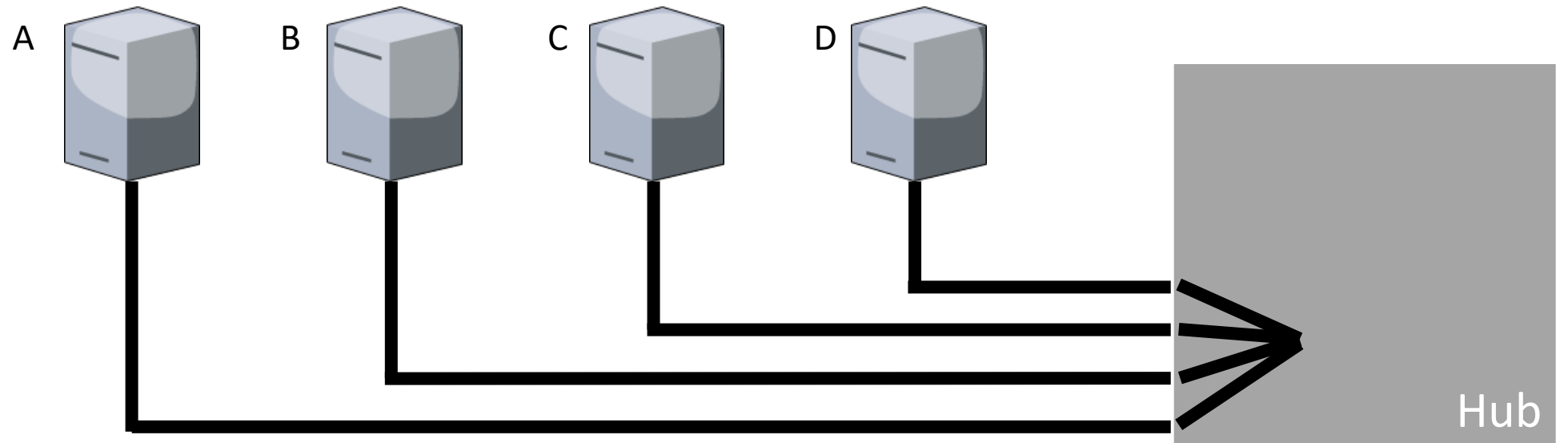
# Classic Ethernet

Maximum data rate: 3 to 10 Mbps

Remember?



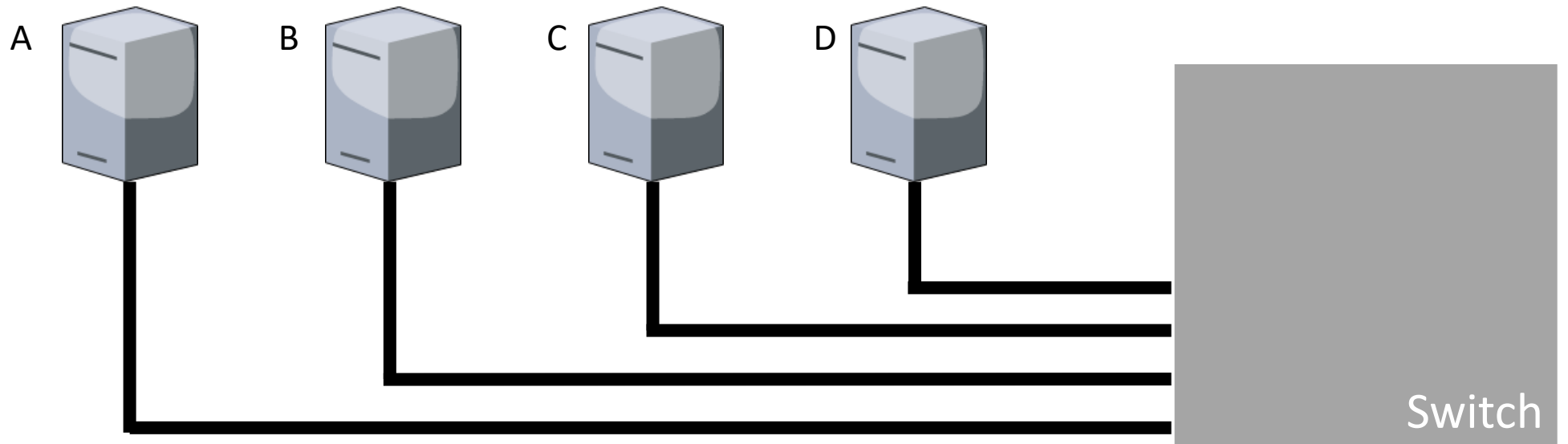
# Classic Ethernet with Hubs



# Ethernet with ✨ Switches ✨

Q: Do we still need MAC?

Same network topology, but MAC protocol no longer needed, if the channel is duplex!

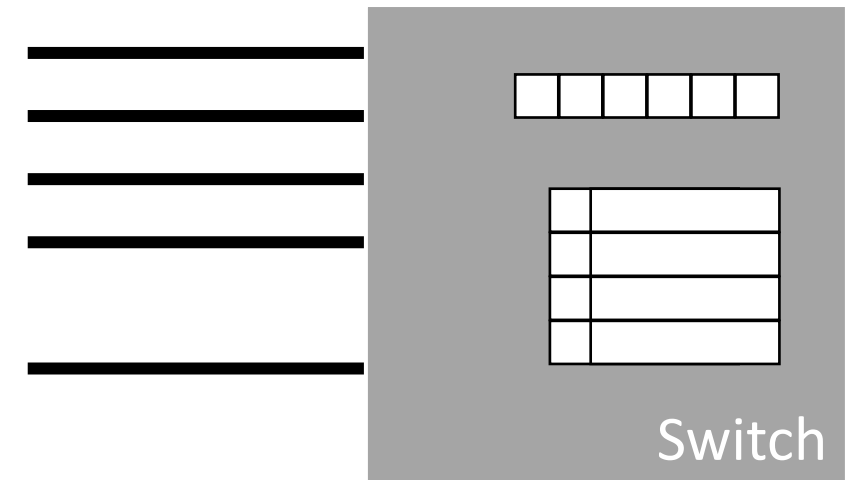
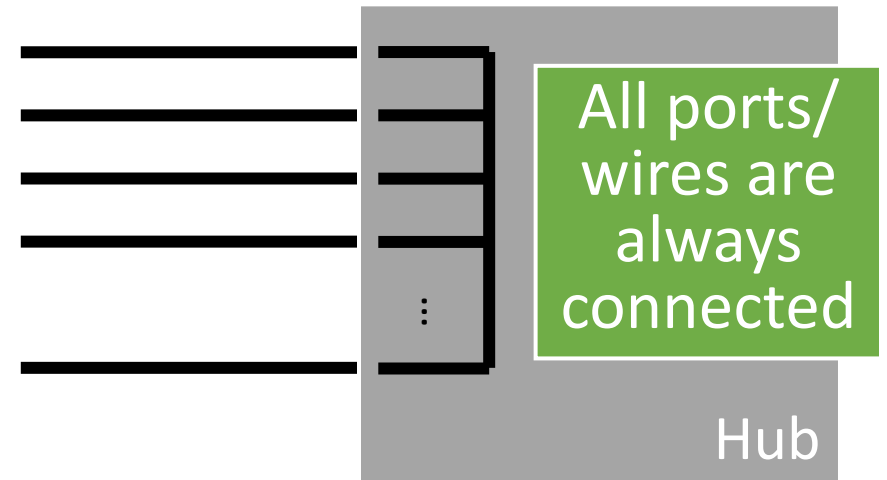


# Ethernet evolution

## From hubs to switches

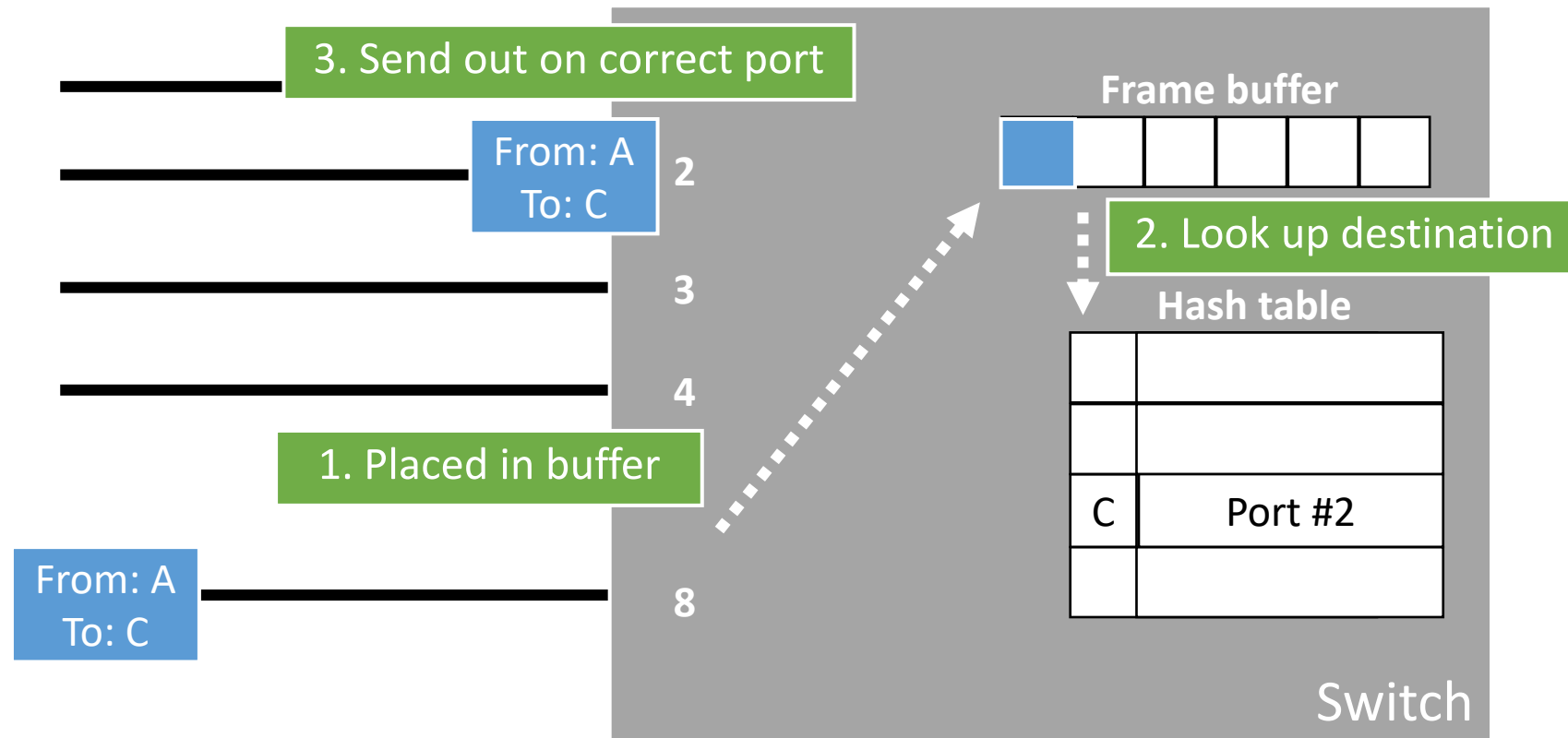
1. Classic Ethernet: 3 to 10 Mbps
2. Fast Ethernet: 100 Mbps
3. Gigabit Ethernet: 1000 Mbps
4. 10-Gigabit Ethernet: 10,000 Mbps
5. 40-Gigabit Ethernet: ...
6. 100-Gigabit Ethernet: ...

Switched versions of Ethernet



# Ethernet switch

Q: Advantages of switches?



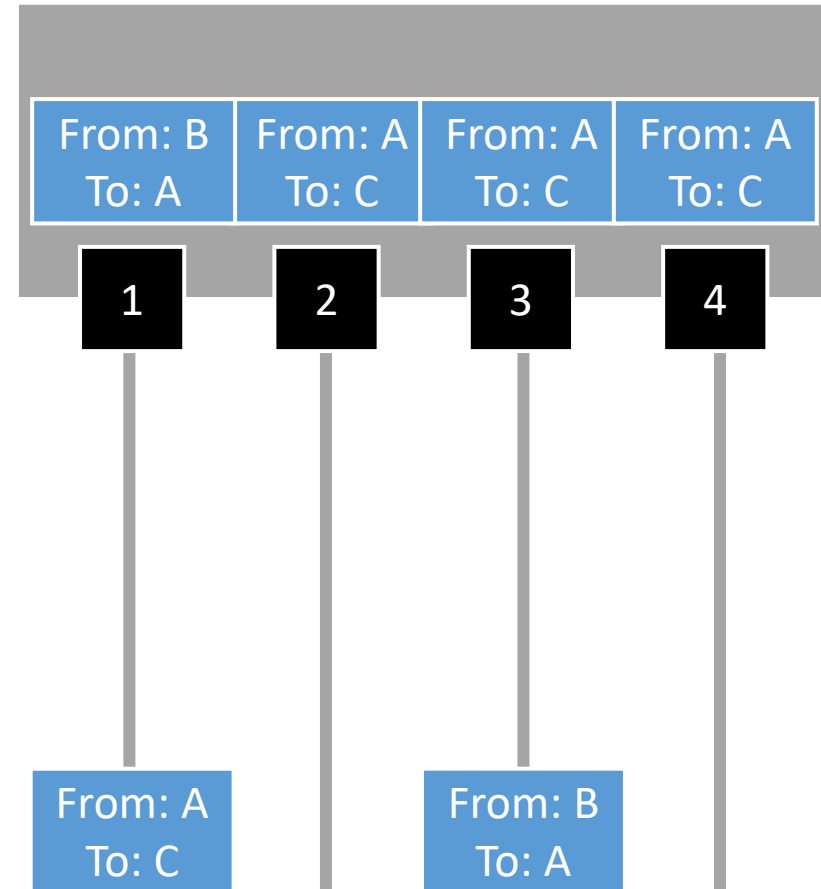
# Learning bridges

## Backwards learning

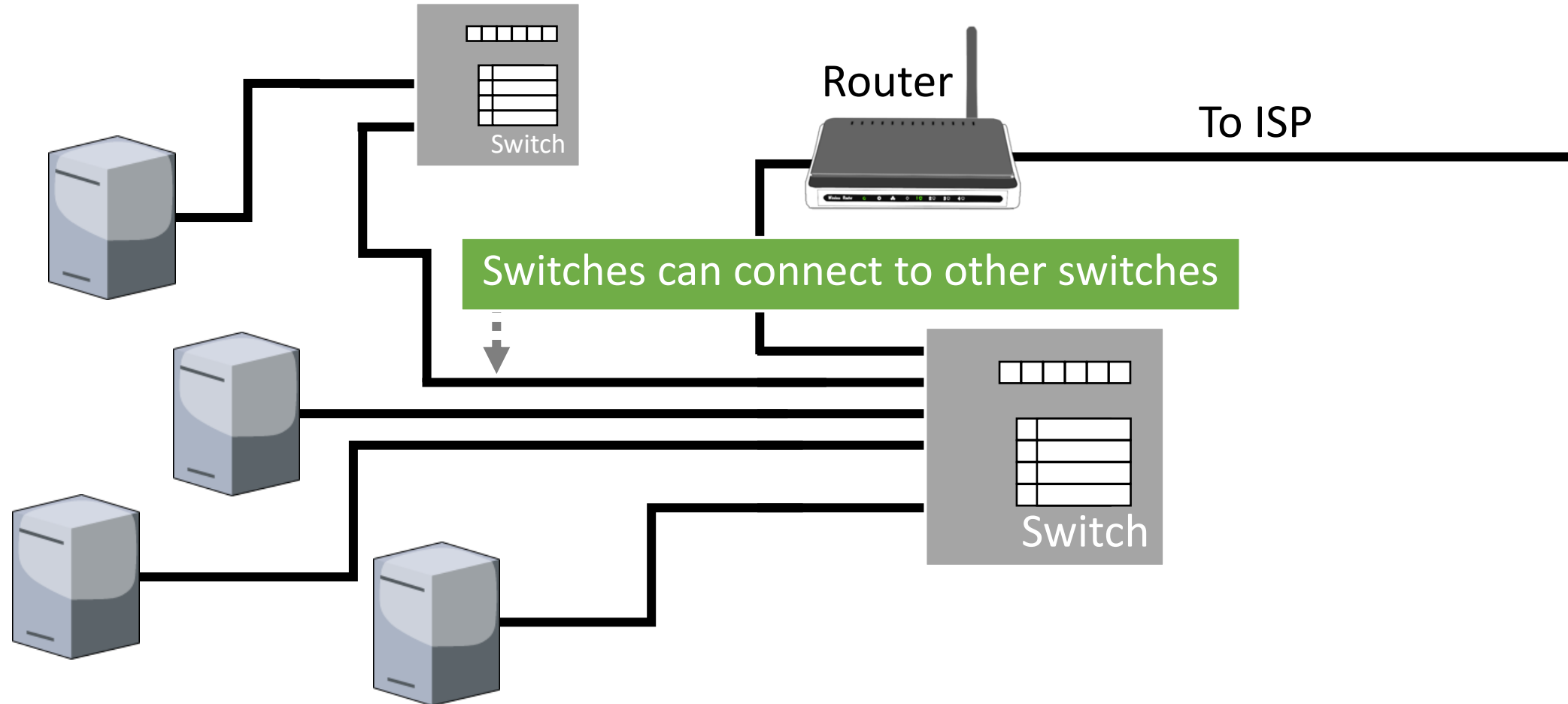
Hash table:

A:1

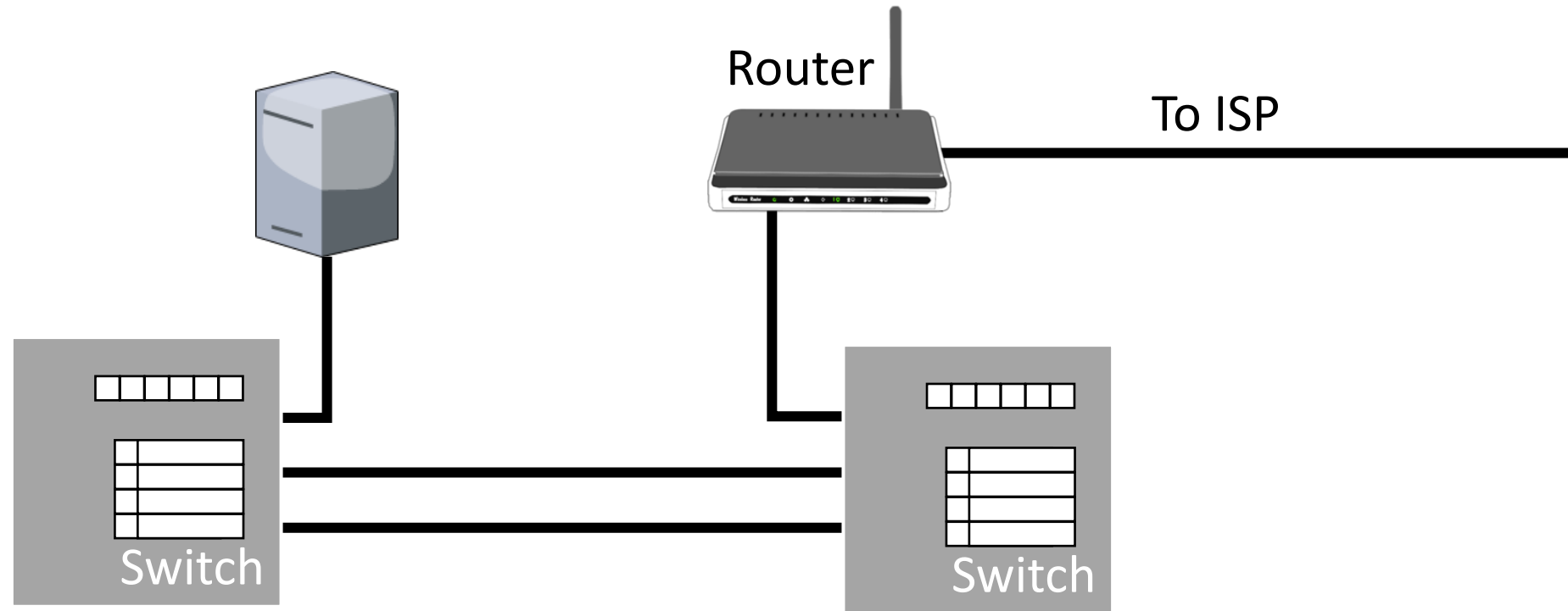
B:3



# Ethernet Wiring pattern



# Learning bridges Topology with loops

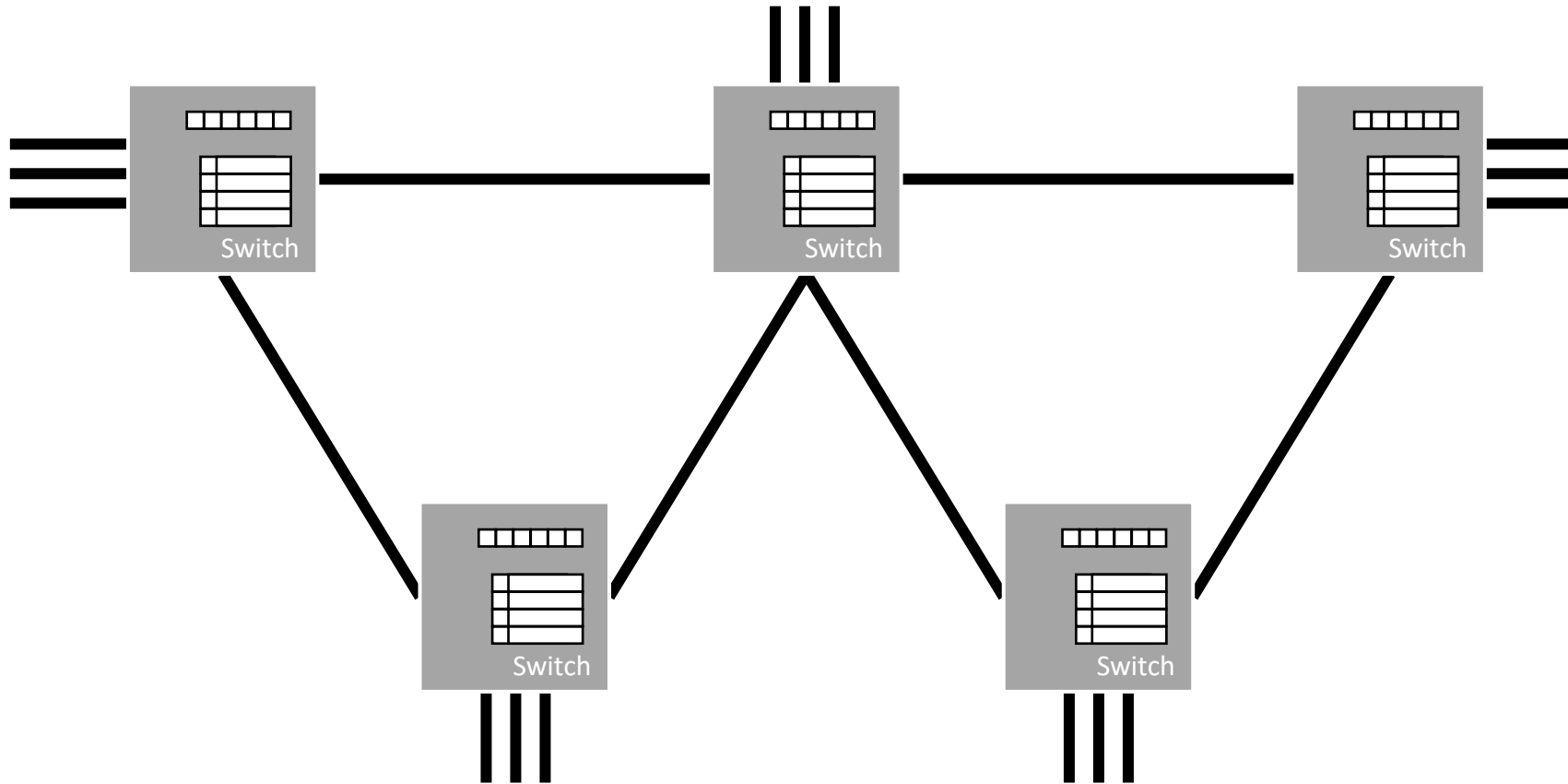


Network contains a loop

Q: What kind of problem can this cause?

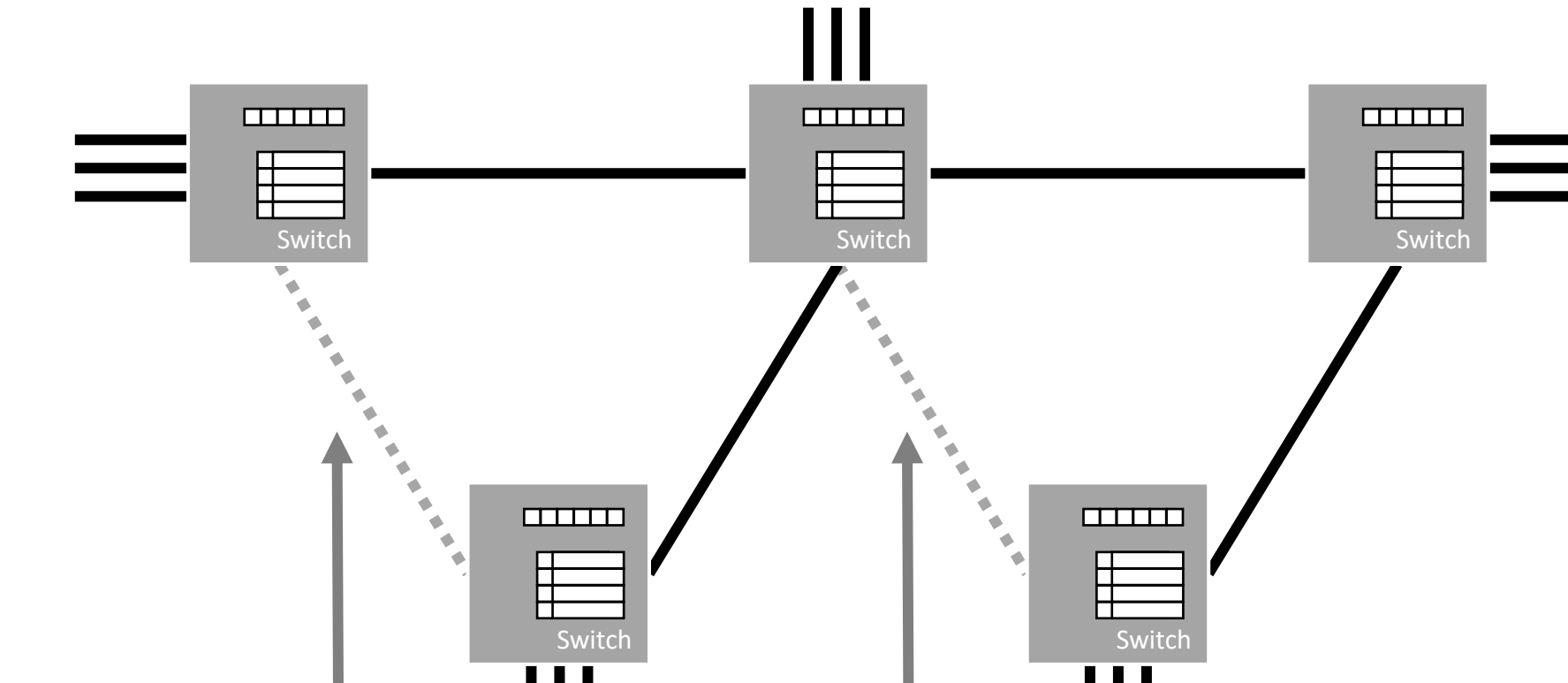
# Spanning tree Example

No direct loops



# Spanning tree Example

No direct loops



Only links in spanning tree are used. Others ignored

# Spanning tree algorithm

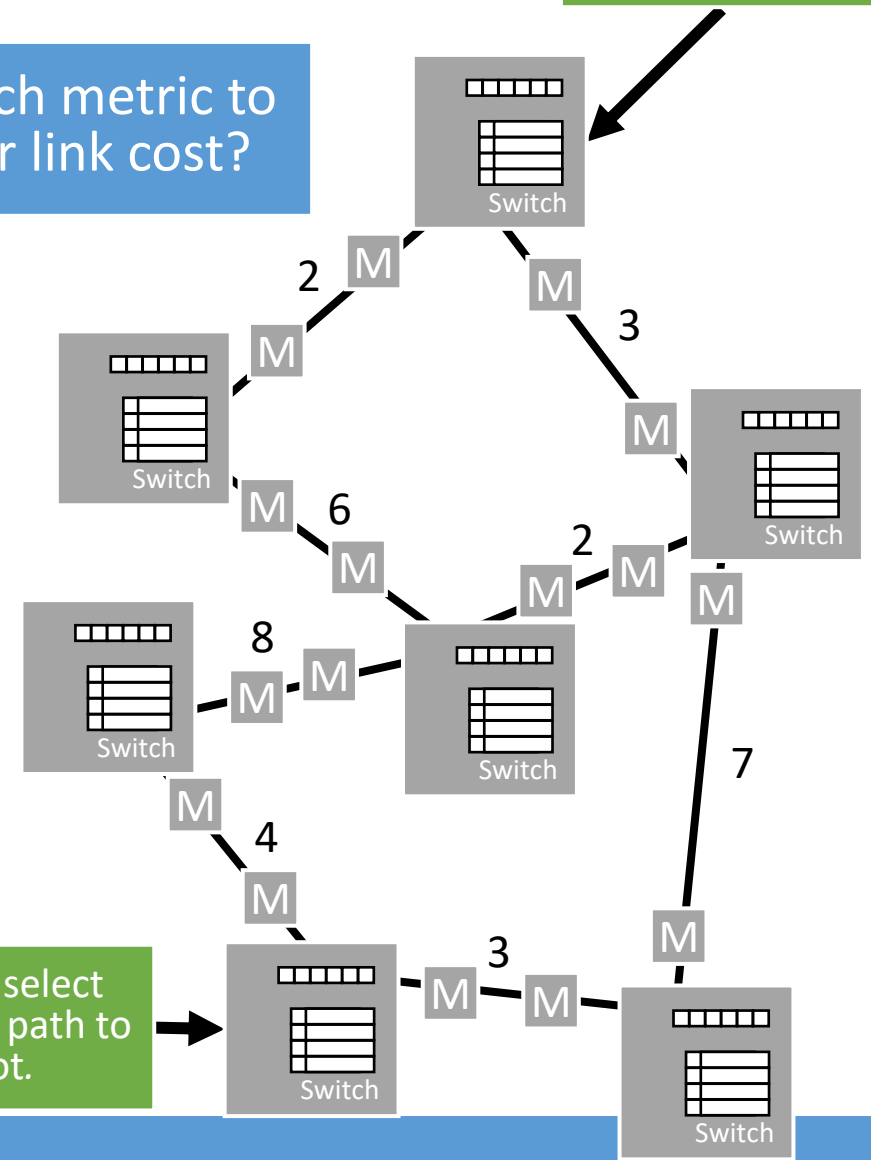
## As a poem

I think that I shall never see  
A graph more lovely than a tree.  
A tree whose crucial property  
Is loop-free connectivity.  
A tree which must be sure to span.  
So packets can reach every LAN.  
First the Root must be selected  
By ID it is elected.  
Least cost paths from Root are traced  
In the tree these paths are placed.  
A mesh is made by folks like me  
Then bridges find a spanning tree.  
— Radia Perlman, 1985.

Q: Which metric to use for link cost?

Nodes select shortest path to root.

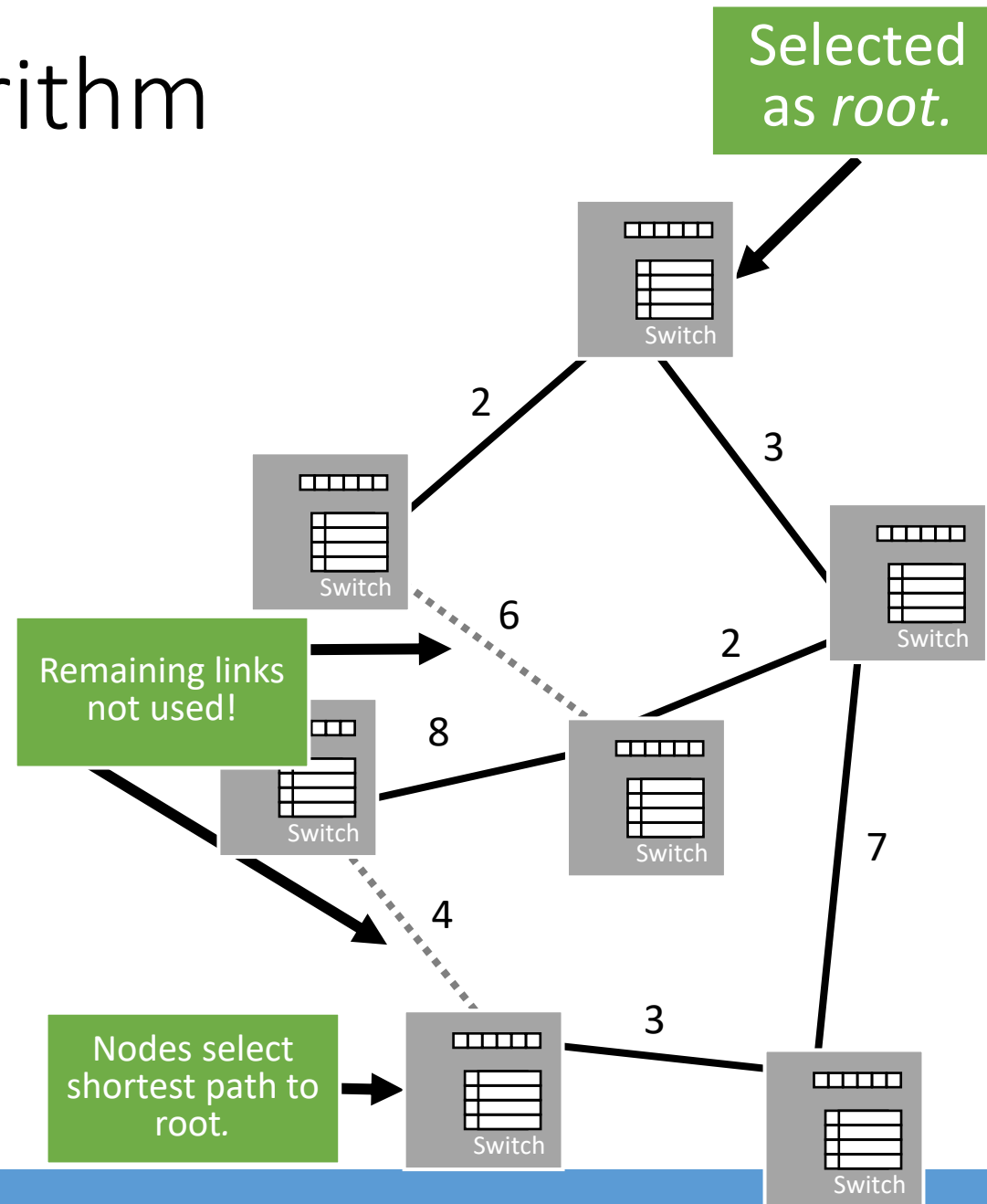
Selected as root.



# Spanning tree algorithm

## As a poem

I think that I shall never see  
A graph more lovely than a tree.  
A tree whose crucial property  
Is loop-free connectivity.  
A tree which must be sure to span.  
So packets can reach every LAN.  
First the Root must be selected  
By ID it is elected.  
Least cost paths from Root are traced  
In the tree these paths are placed.  
A mesh is made by folks like me  
Then bridges find a spanning tree.  
— Radia Perlman, 1985.



# MAC Sublayer Outline

ALOHA & Slotted ALOHA

CSMA

1-persistent

nonpersistent

p-persistent

CSMA/CD

**802.3 Ethernet**

Ethernet Switching

MAC for Wireless

Hidden Terminal

Exposed Terminal

CSMA/CA

**802.11 WiFi**

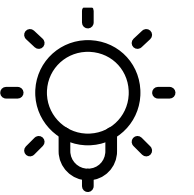
Collision-Free Protocols

Basic Bit-Map

Token Ring

Binary Countdown

# Medium Access Control for Wireless Channels



# Properties of Wireless Channels Affect MAC Protocol Design

The good news: no more wires.

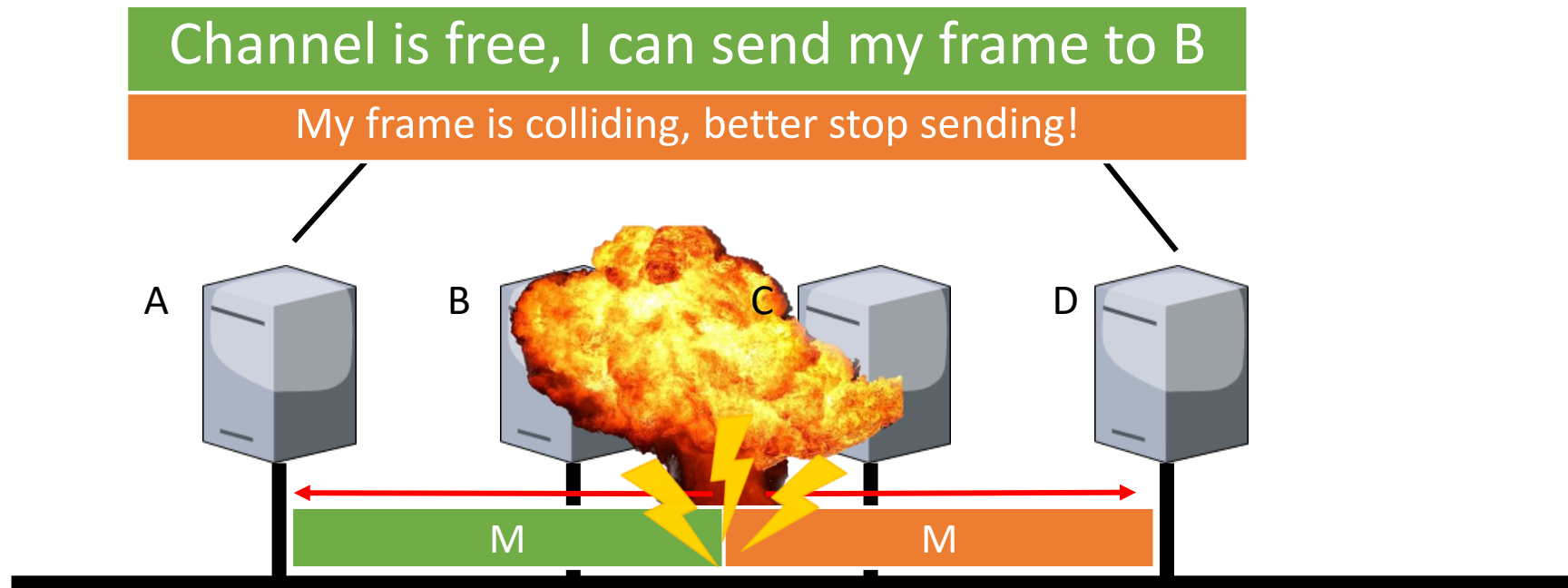
The bad news:

1. Nodes cannot detect collisions while sending.  
(you cannot talk and listen at the same time!)
2. *Hidden* and *exposed* terminals.

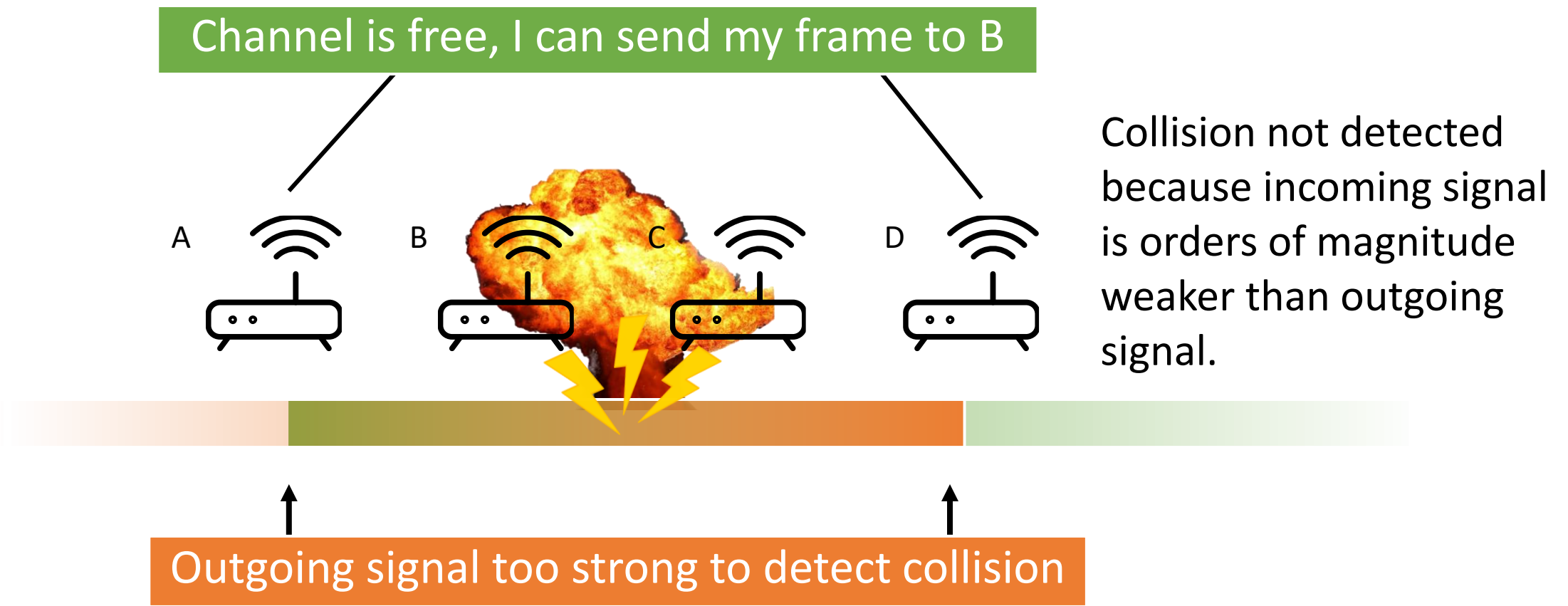
We cannot detect collisions while transmitting!



# MAC for Wireless Channels: No Collision Detection

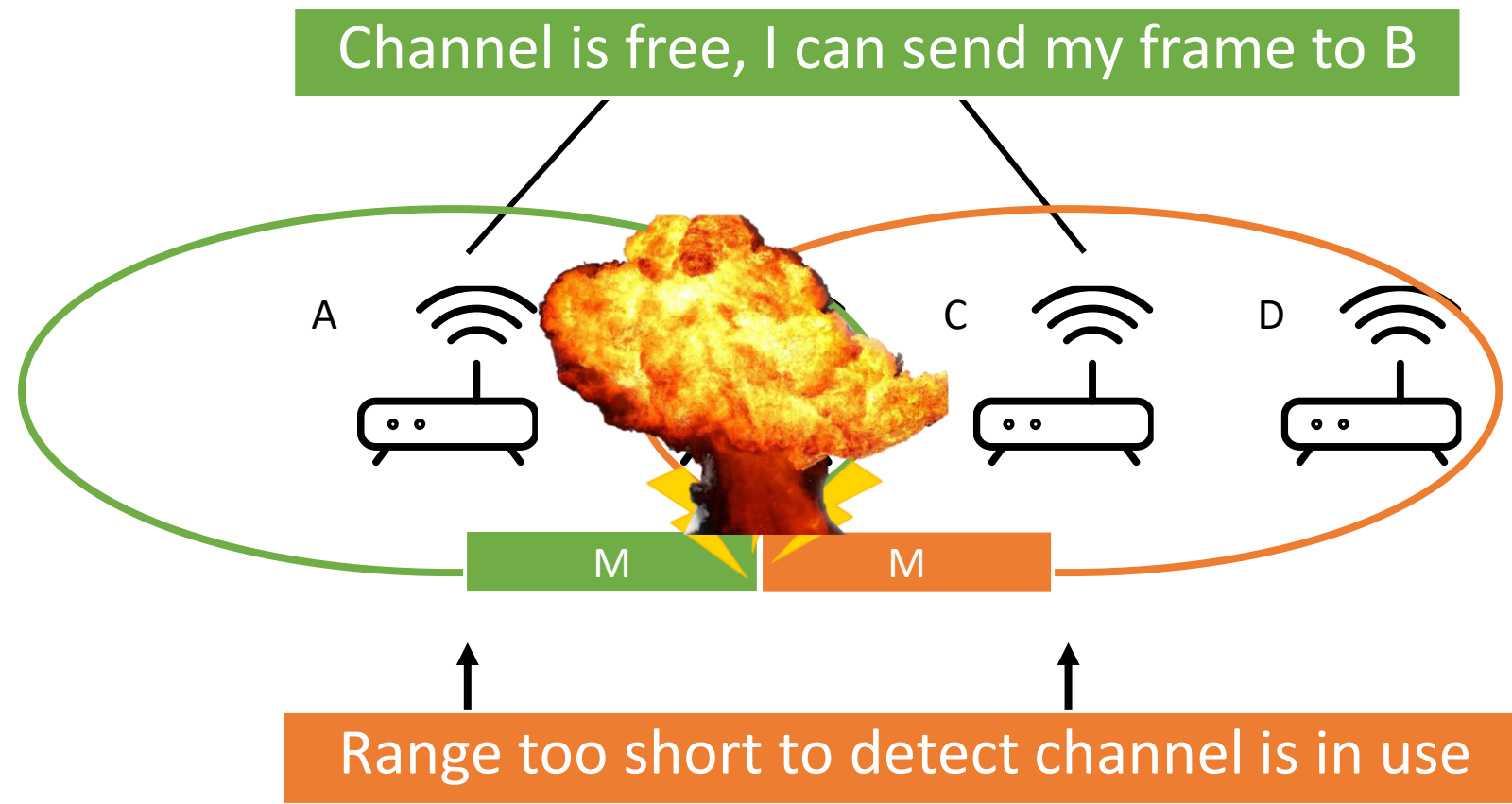


# MAC for Wireless Channels: No Collision Detection



# MAC for Wireless Channels: Carrier Sense has Limited Range

## Hidden Terminal



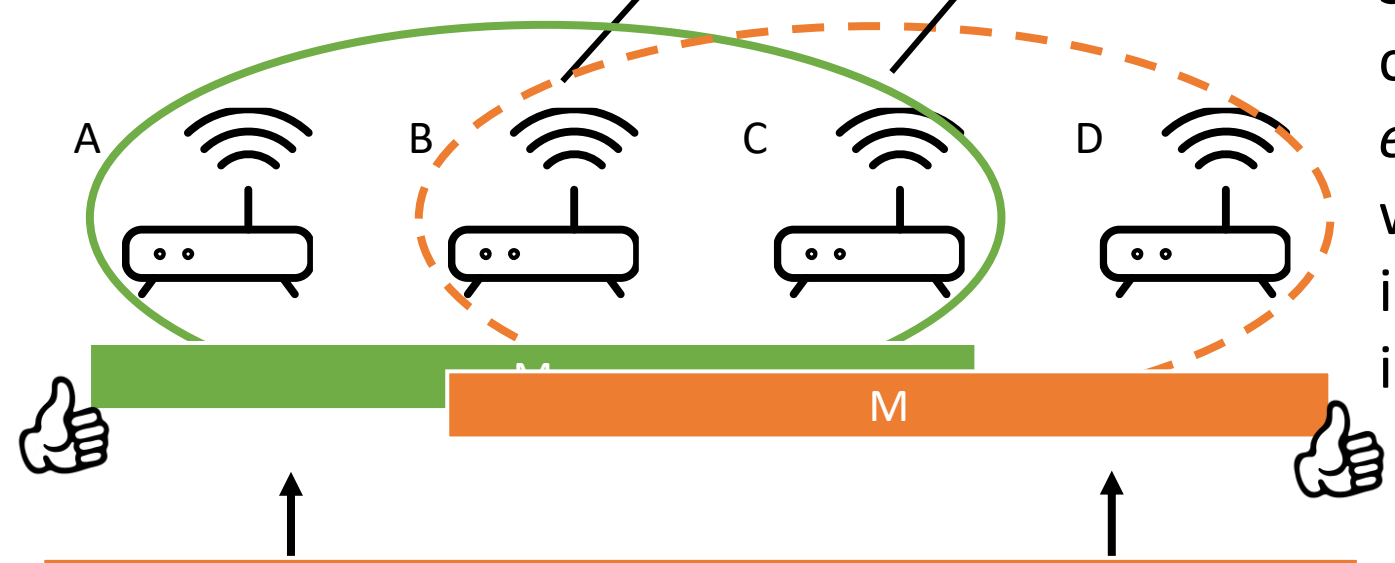
Stations sense that channel is idle, but their range is too short to detect a transmitting *hidden terminal*.

# MAC for Wireless Channels: Carrier Sense has Limited Range

**Exposed Terminal**

Channel is free, I can send my frame A

Channel is in use, I cannot send my frame to D



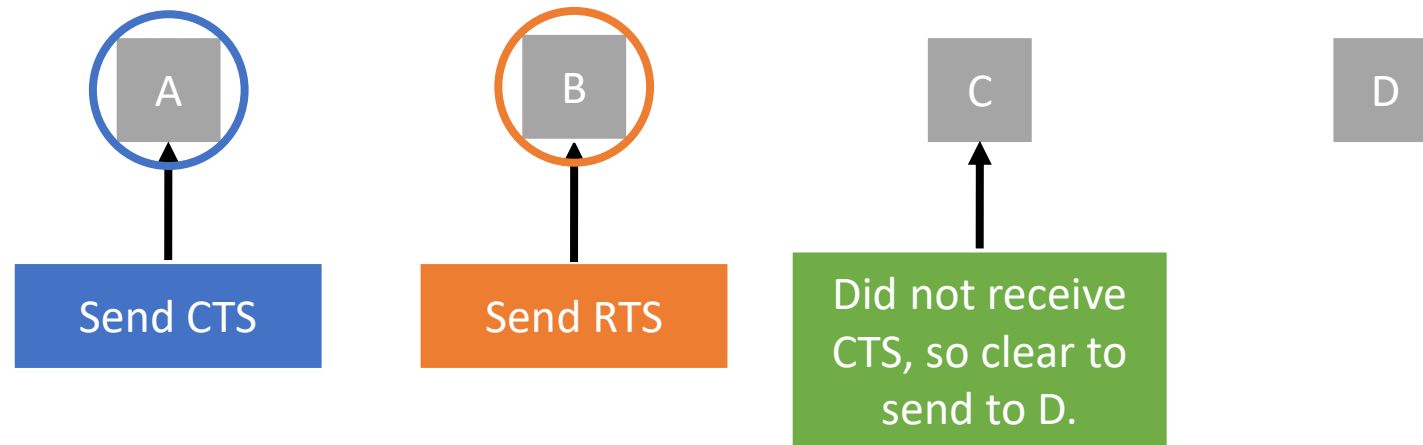
Stations sense that channel is in use, but the *exposed terminal's* signal would not reach and interfere with the intended recipient.

There would be no collision at recipients

# Multiple Access with Collision Avoidance (MACA)

An approach to solve the hidden terminal and exposed terminal problem.

Example: B wants to send to A.



# MAC Sublayer Outline

ALOHA & Slotted ALOHA

CSMA

1-persistent

nonpersistent

p-persistent

CSMA/CD

**802.3 Ethernet**

Ethernet Switching

MAC for Wireless

Hidden Terminal

Exposed Terminal

CSMA/CA

**802.11 WiFi**

Collision-Free Protocols

Basic Bit-Map

Token Ring

Binary Countdown

# Medium Access Control in ... 802.11

Stations cannot detect collisions while they occur.  
Relies on ACKs to determine if collision occurred.

If ACK is lost, sender assumes frame was lost;  
retransmits frame

Can use RTS/CTS, but usually does not.

Instead uses a protocol called **CSMA/CA**.  
CA: Collision Avoidance.

# CSMA/CA (Collision Avoidance)

## **Physical channel sensing.**

Sense if the channel is in use. Wait for channel to become idle.

## ***Virtual channel sensing.***

Frames carry a Network Allocation Vector (NAV) that indicates the length of the exchange.



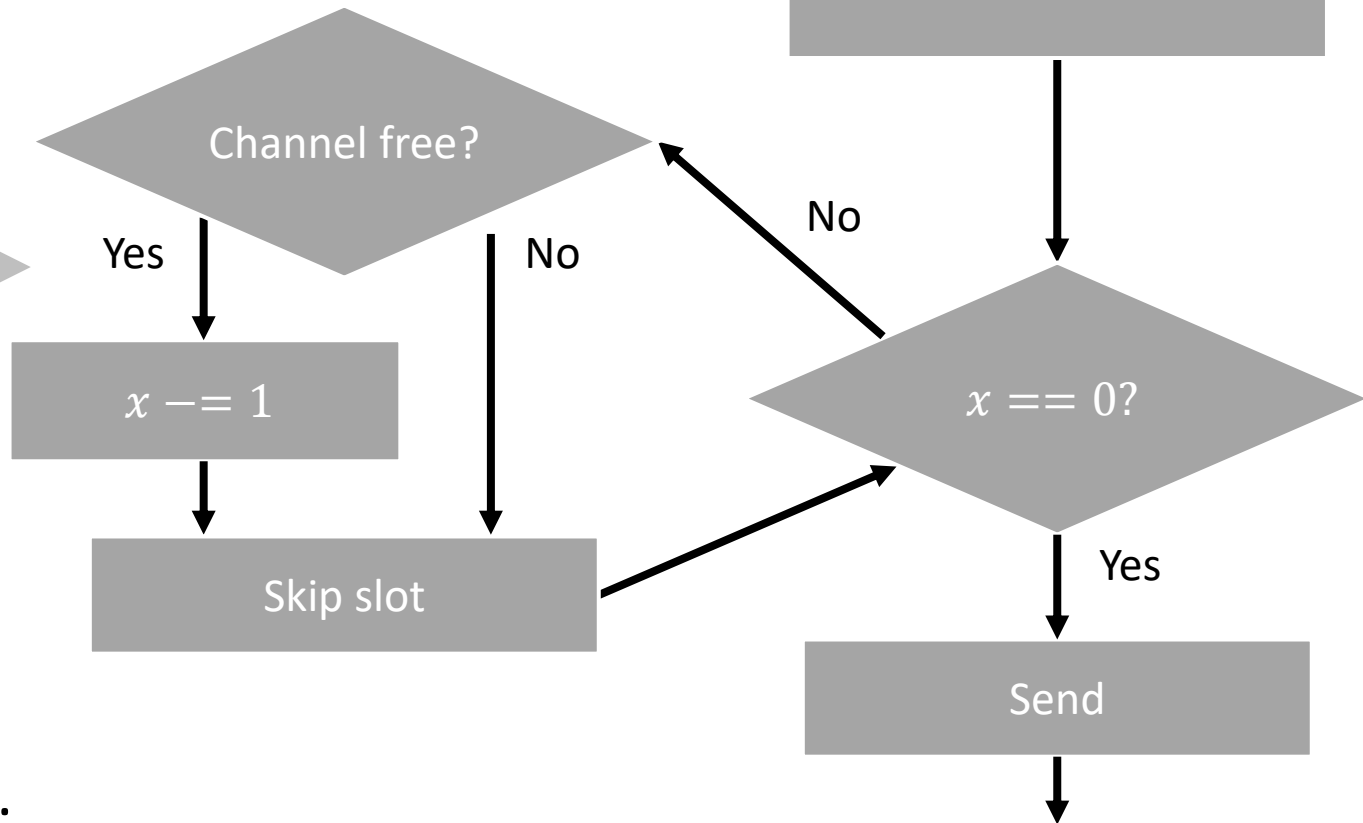
Data + Ack

Wait for end of exchange.

# CSMA/CA

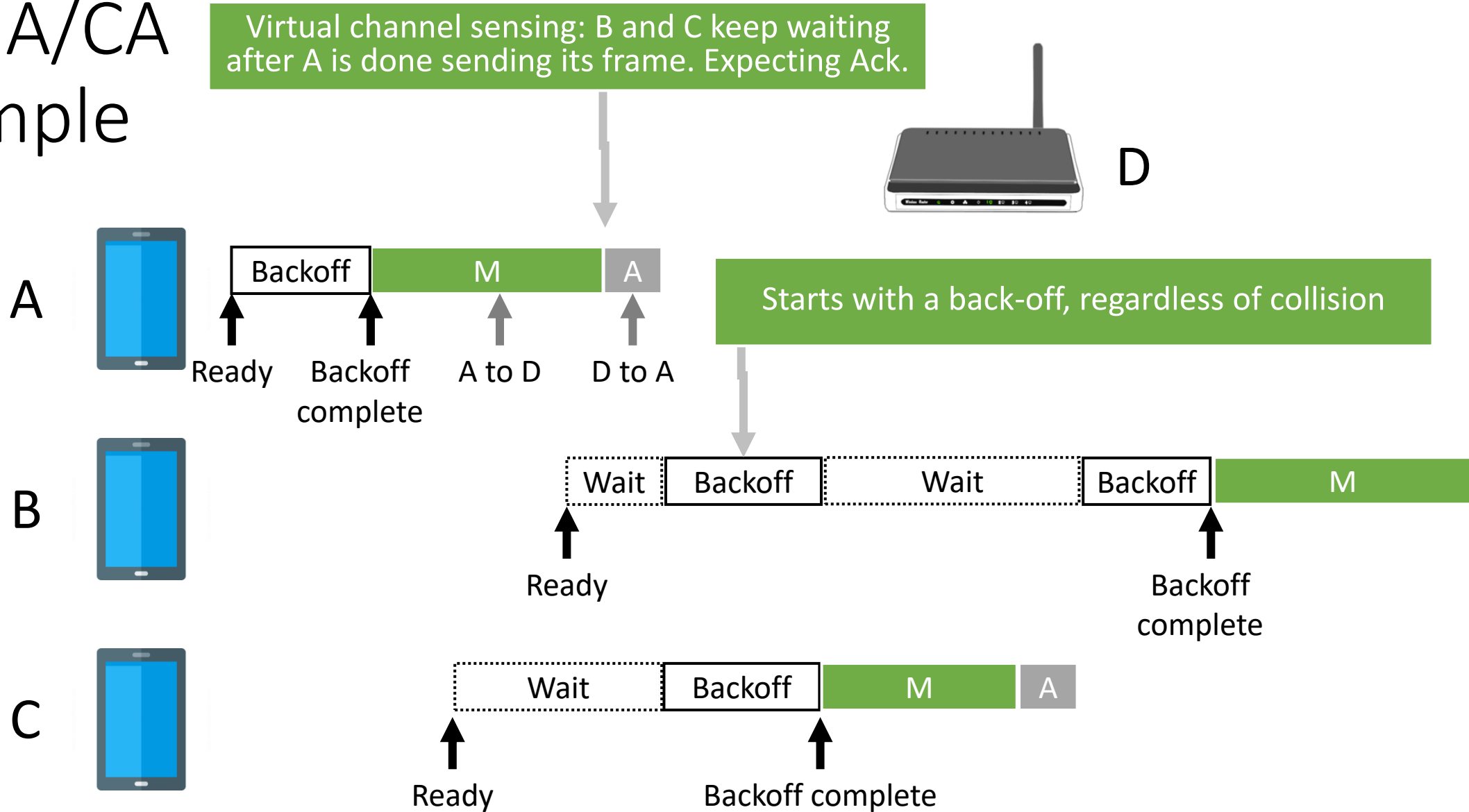
Starts with a back-off, regardless of collision

Countdown paused when other channel is occupied

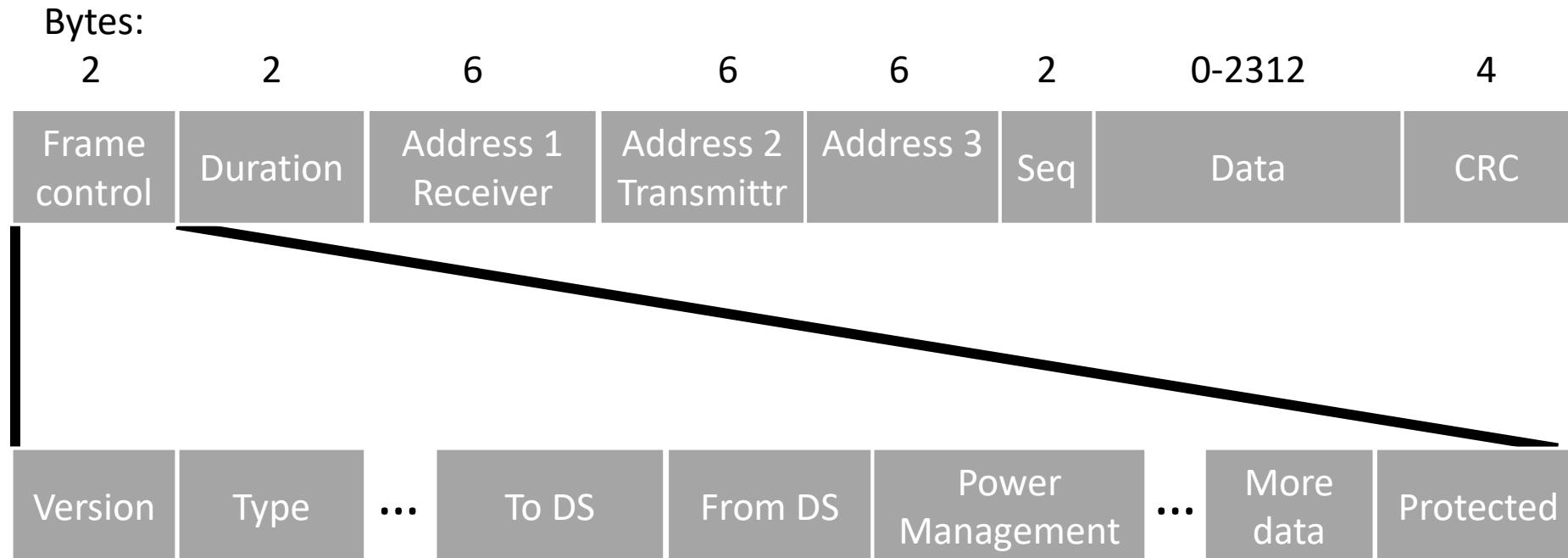


Backoff by selecting and counting down  $x$ .

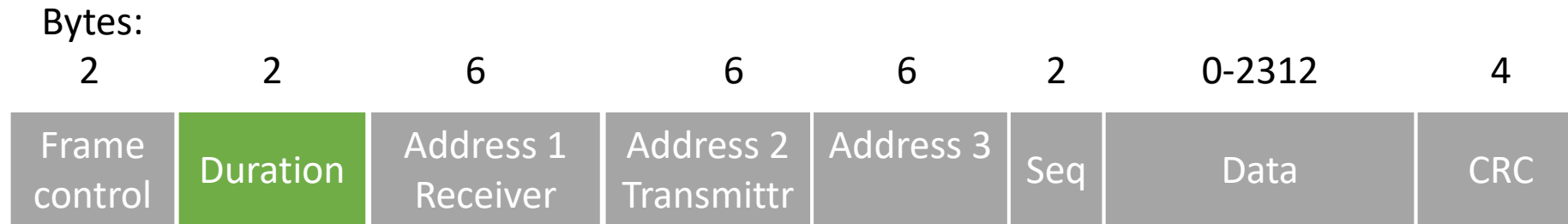
# CSMA/CA Example



# 802.11 frames

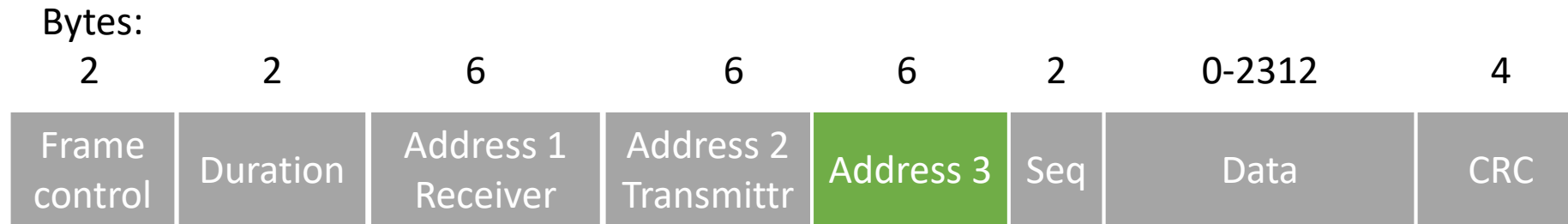


# 802.11 frames



Stations use the duration to update their Network Allocation Vector (NAV).

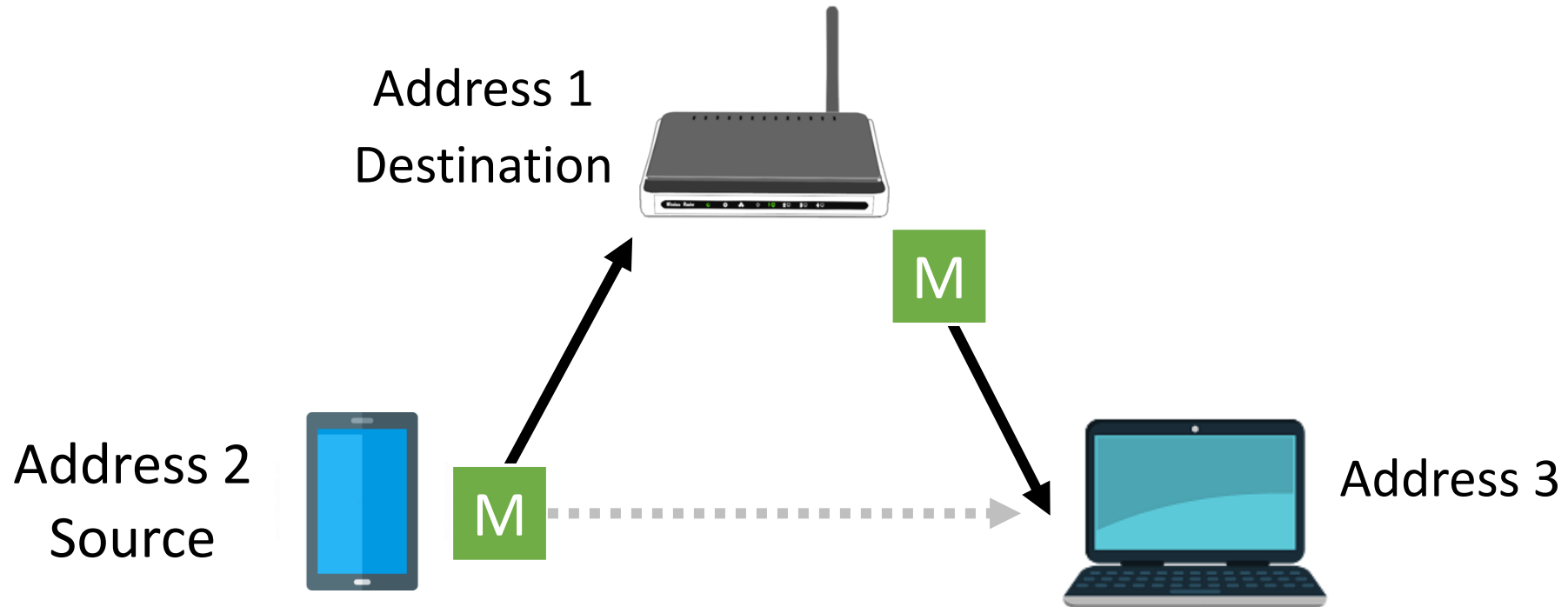
# 802.11 frames



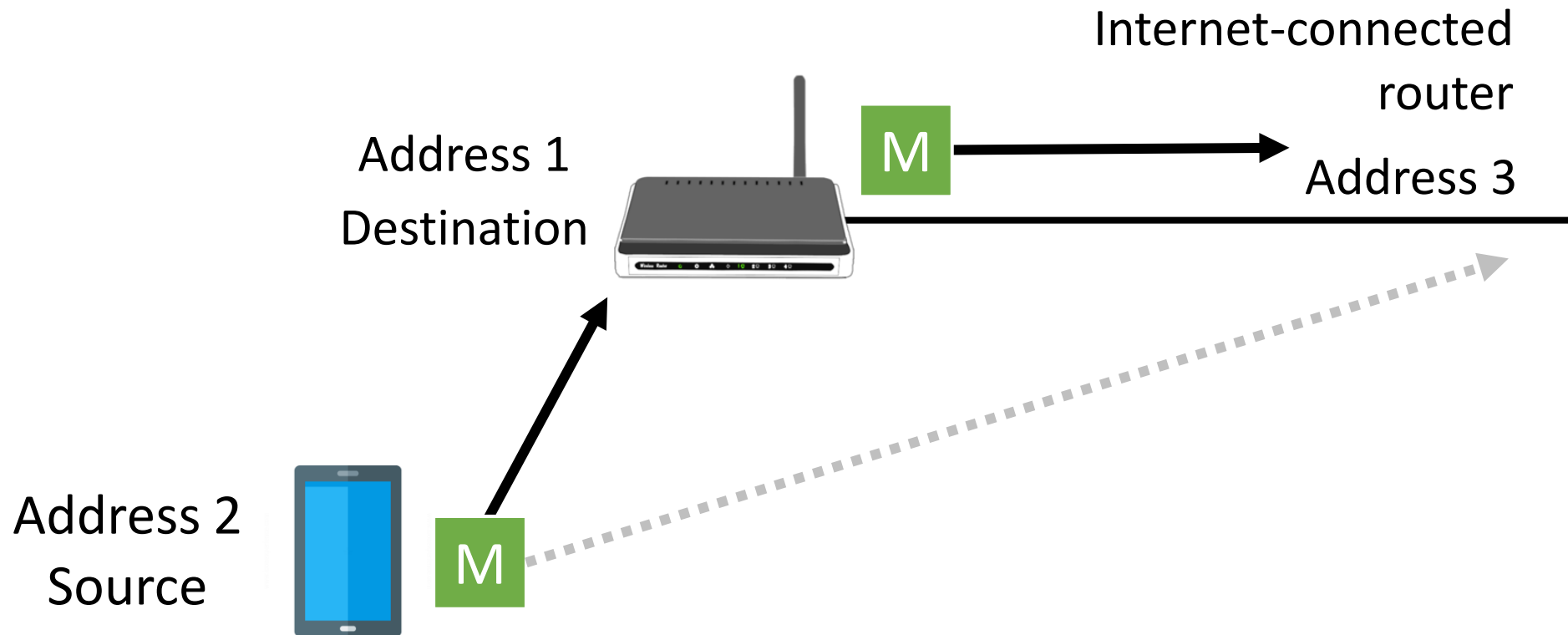
Q: Why a third address?

Third address is destination (Address 2 is access point)

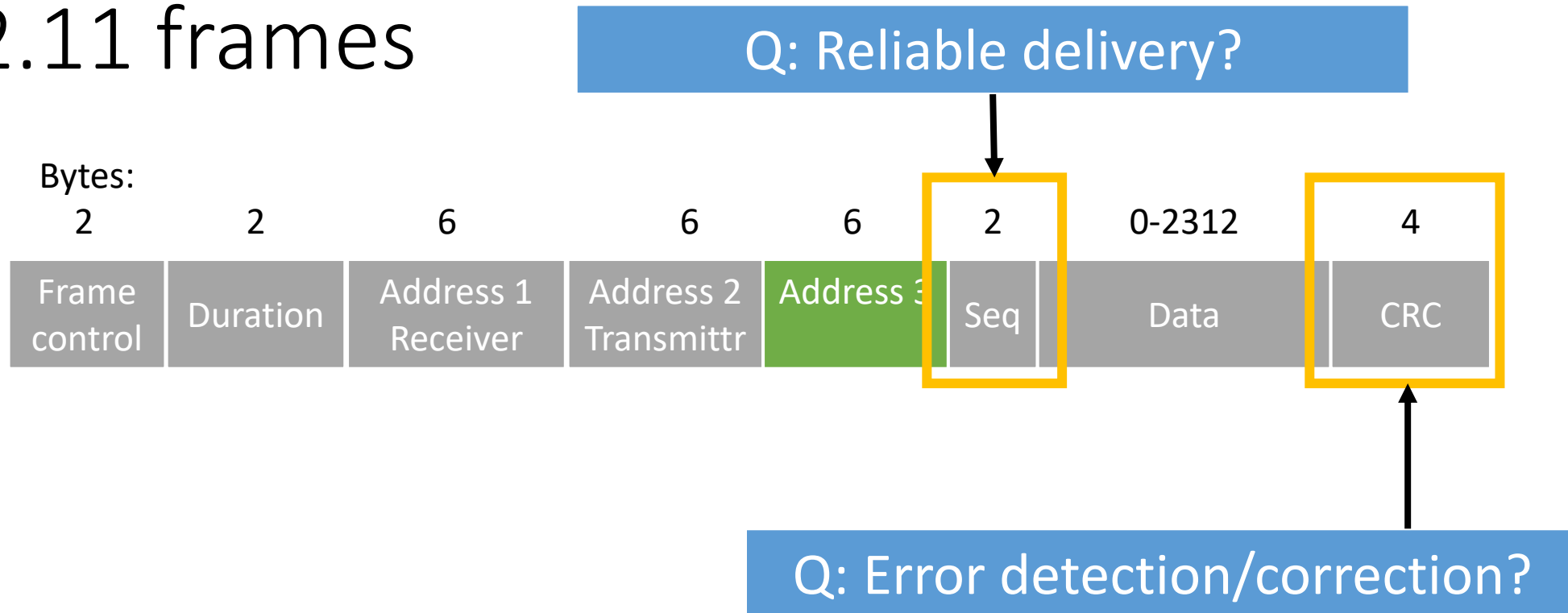
# Access point forwards frame to recipient



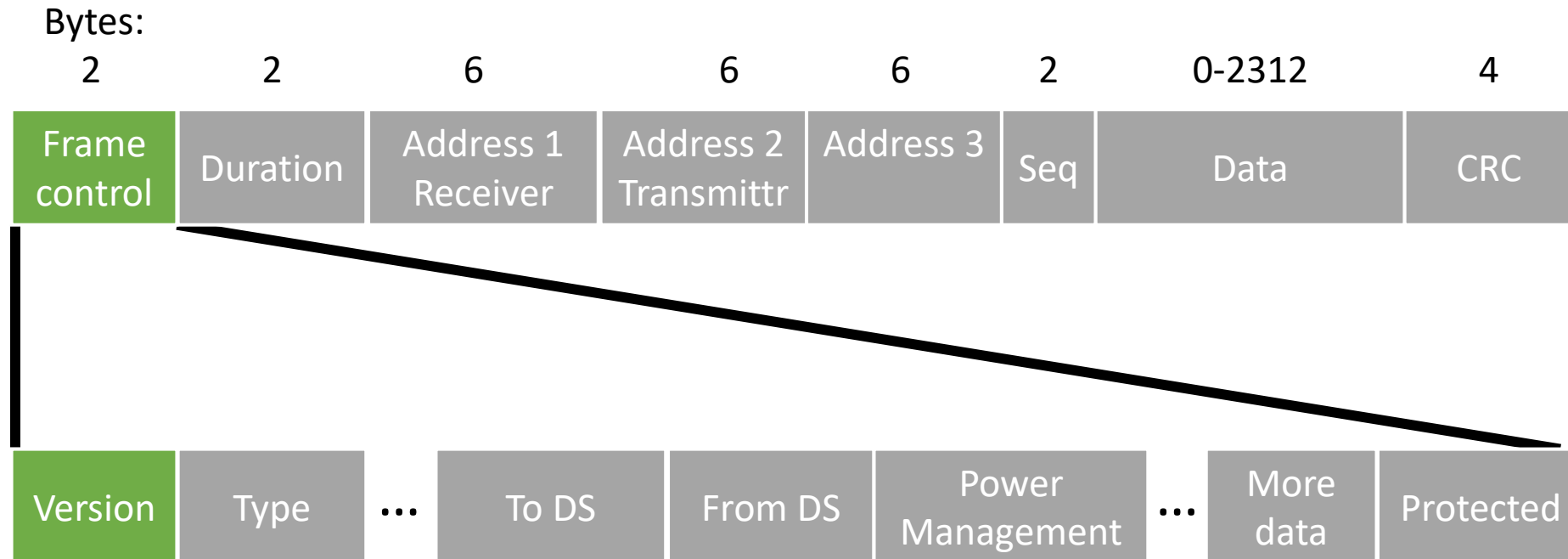
# Access point forwards frame to recipient



# 802.11 frames

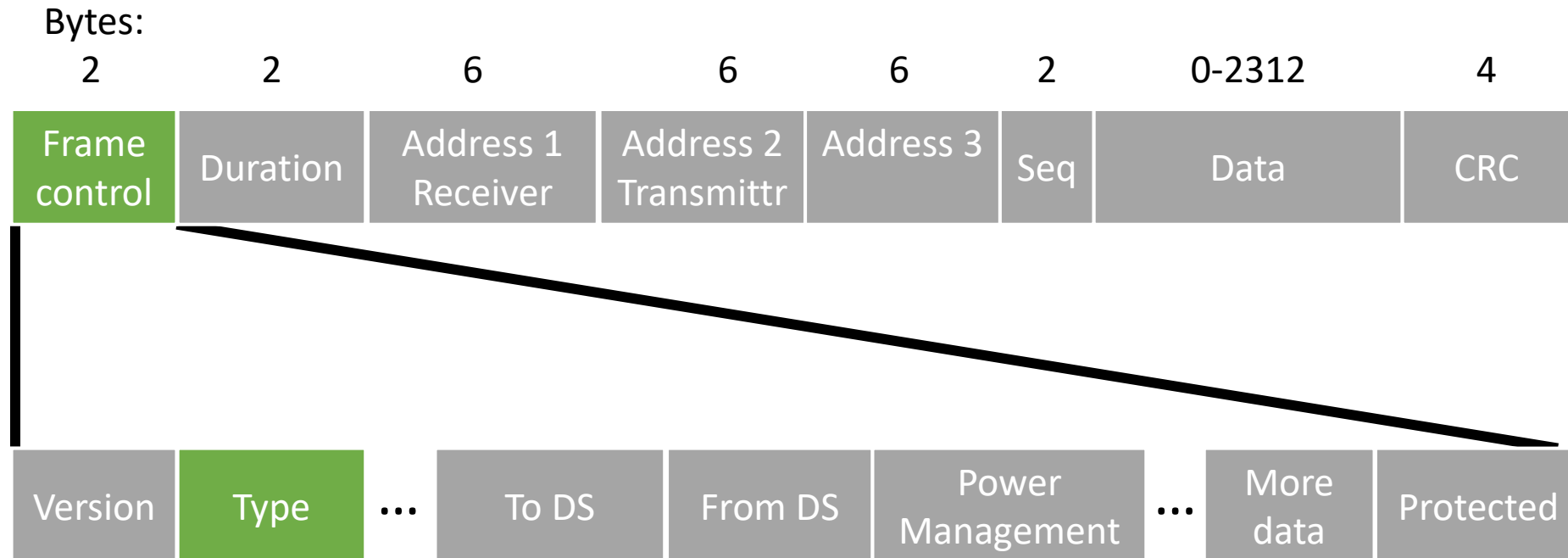


# 802.11 frames



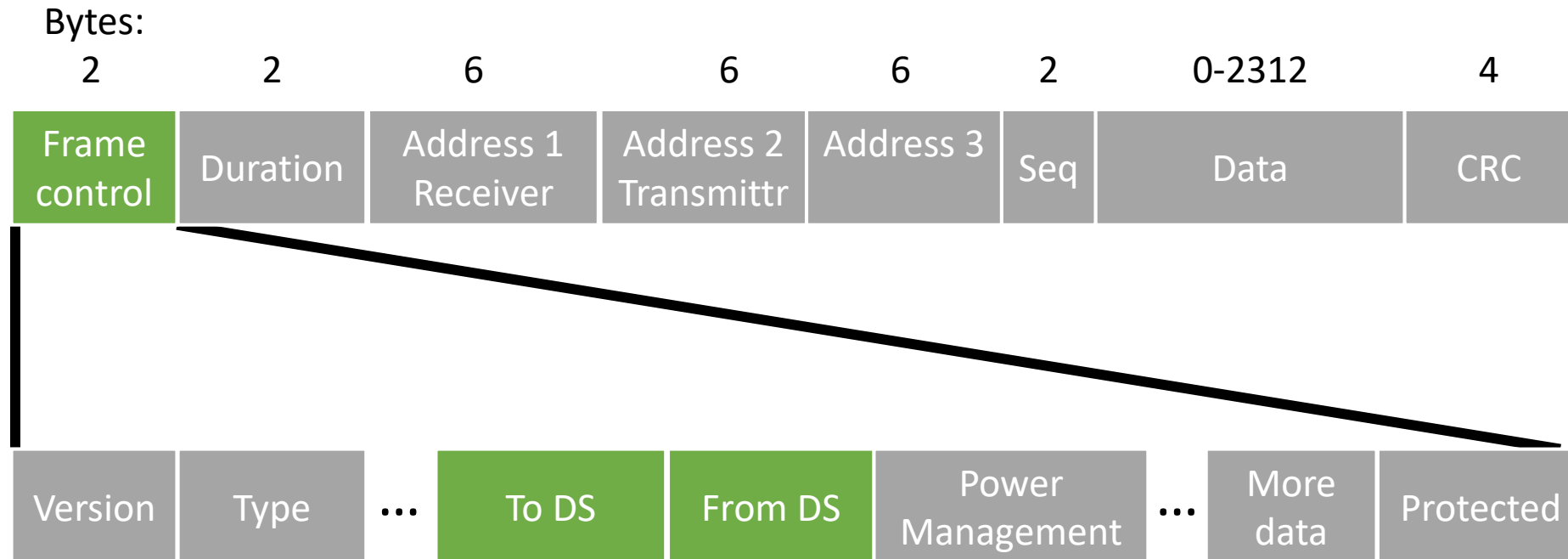
Available for other types of frames in future versions of the protocol.

# 802.11 frames



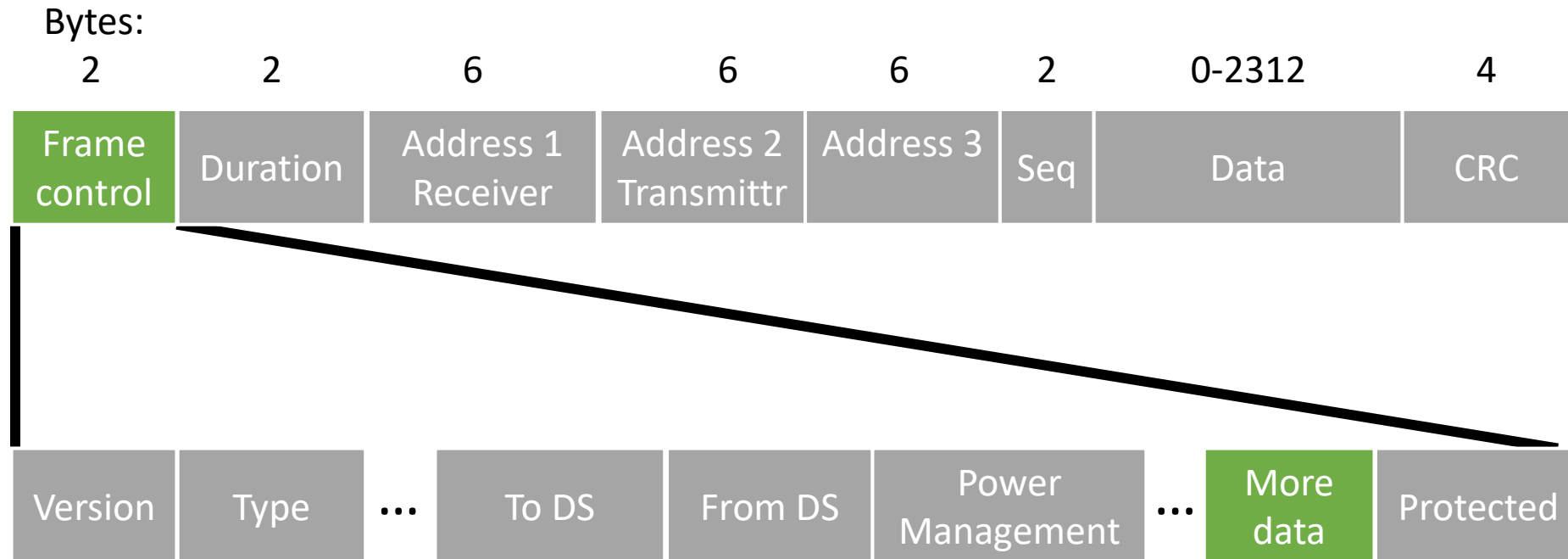
Indicates a control, management, or data frame.

# 802.11 frames



Indicates frames to and from the access points (distribution system) respectively.

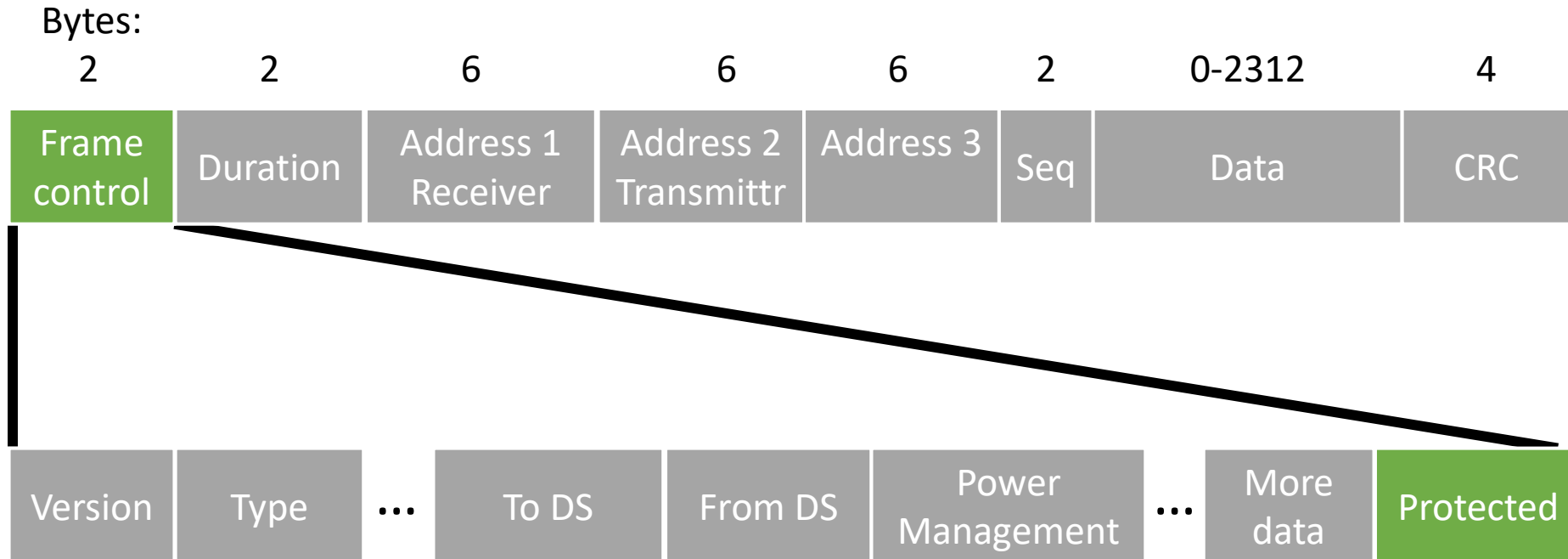
# 802.11 frames



Indicates that the sender has more frames for the receiver.

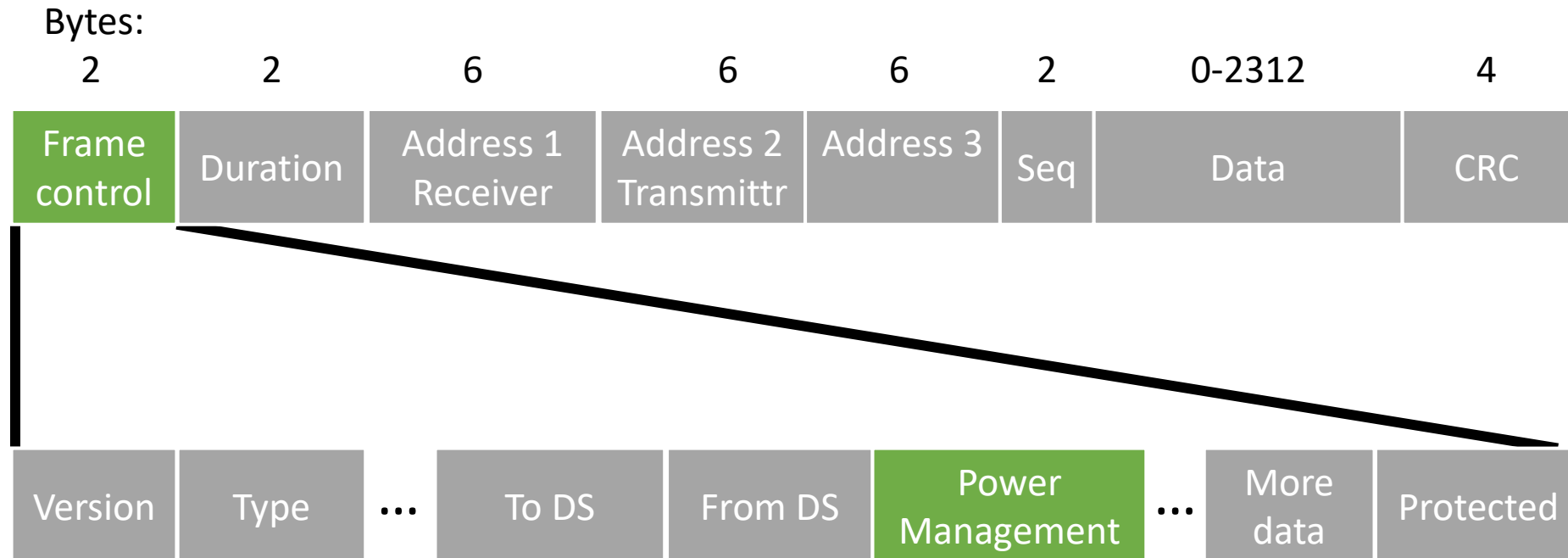
# 802.11 frames

Authentication uses username+password (e.g., Eduroam), or only a password (e.g., your wireless network at home).



Indicates that the data is encrypted.

# 802.11 frames

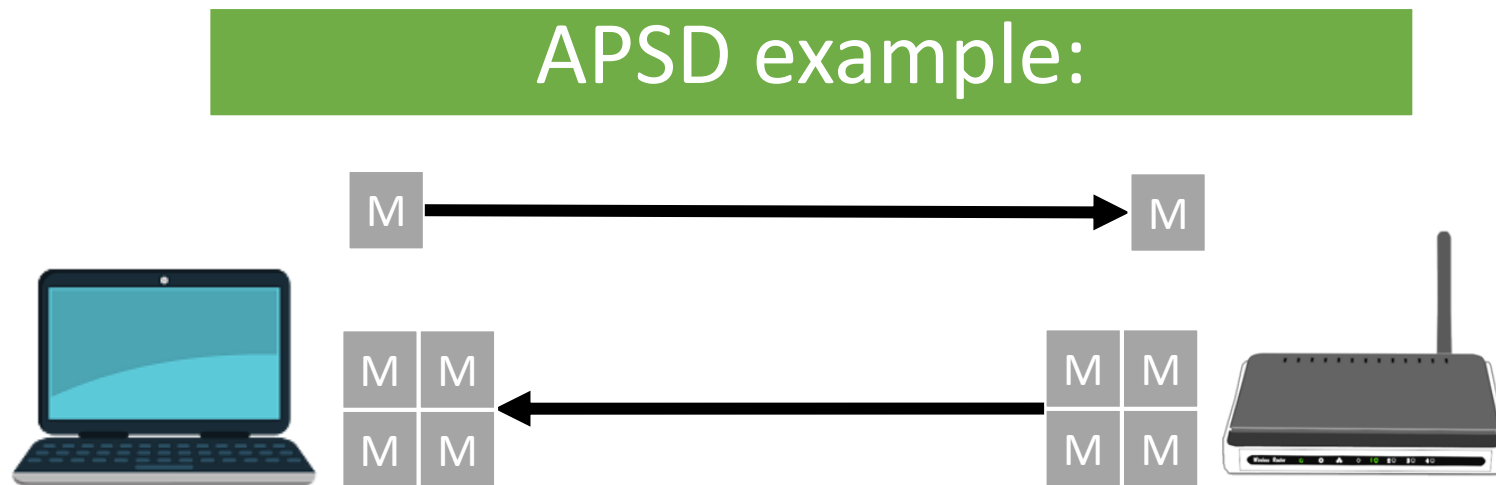


Indicates that the sender will enter power save mode.

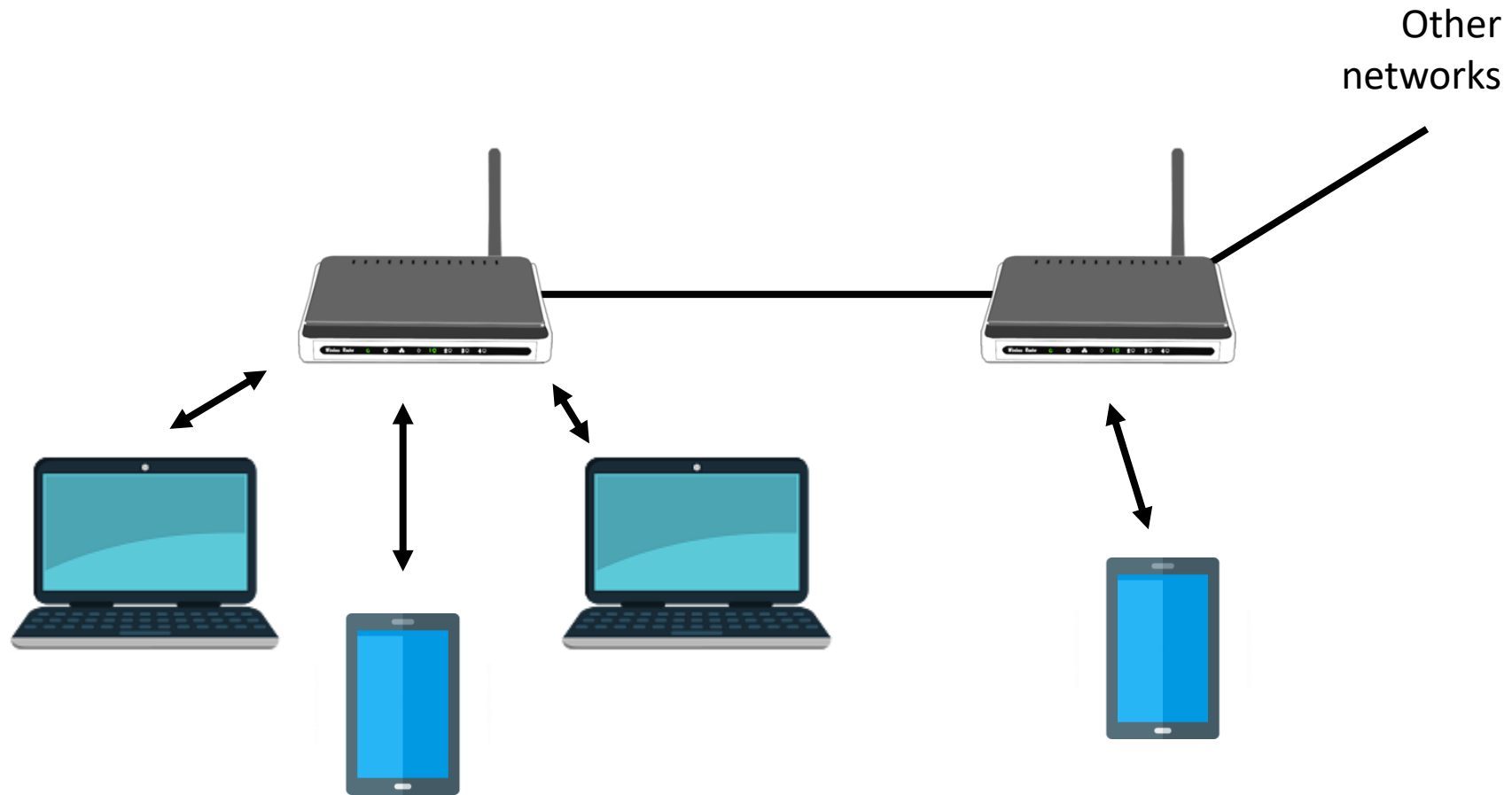
# Power saving in 802.11

Multiple methods possible

- Beacon frames
- Automatic Power Save Delivery (APSD)
- ...

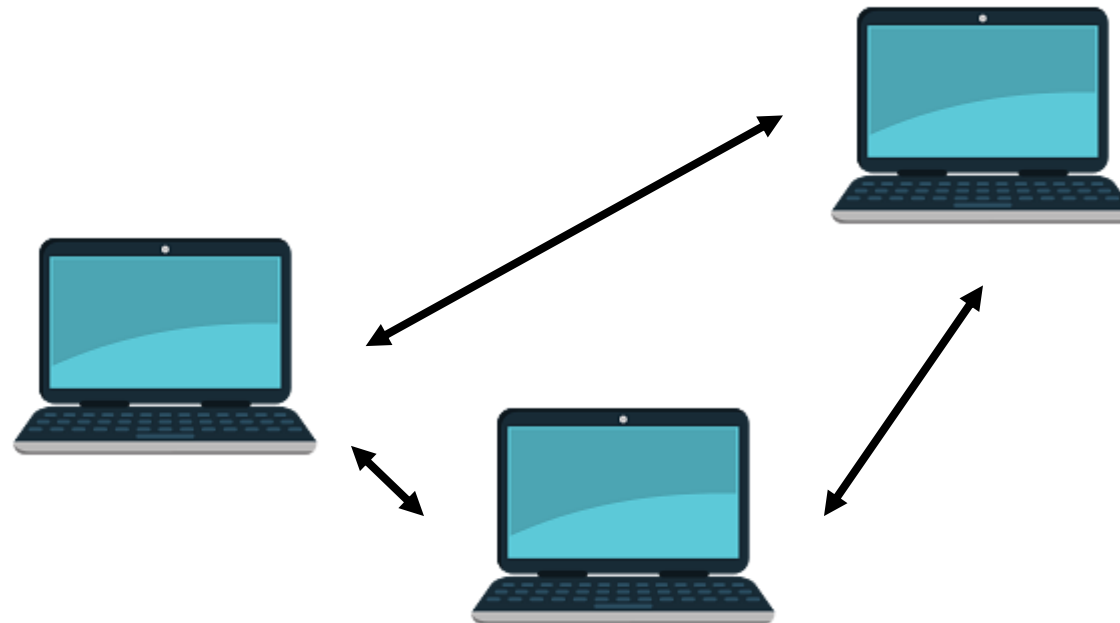


# 802.11 Infrastructure mode



# 802.11 Ad-hoc networks

Q: Can you think of a (dis)advantage?



# MAC Sublayer Outline

ALOHA & Slotted ALOHA

CSMA

1-persistent

nonpersistent

p-persistent

CSMA/CD

**802.3 Ethernet**

Ethernet Switching

MAC for Wireless

Hidden Terminal

Exposed Terminal

CSMA/CA

**802.11 WiFi**

**Collision-Free Protocols**

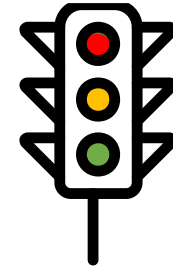
Basic Bit-Map

Token Ring

Binary Countdown

# Collision-Free Protocols

Replacing *contention* with *coordination*



Instead of detecting collisions, why not prevent collisions?

Protocol examples:

1. Basic Bit-Map Protocol
2. Token Ring
3. Binary Countdown

# The Basic Bit-Map Protocol

Q: What is the efficiency of this protocol?

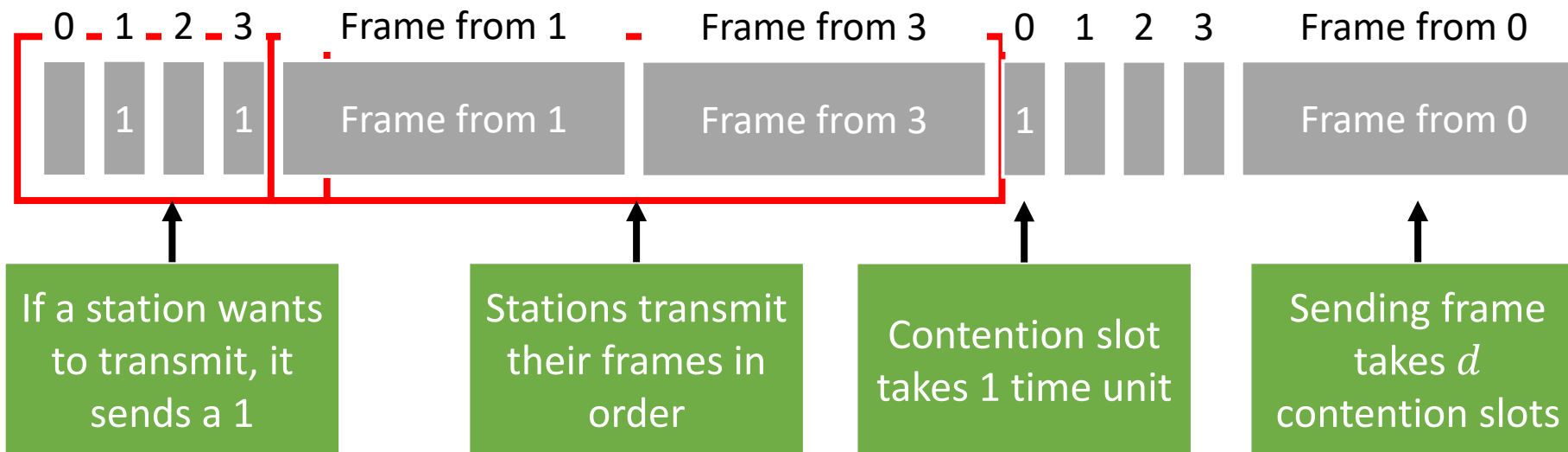
An example of a *collision-free* protocol.

Stations that want to transmit send a '1' in their slot.

With  $n$  stations,

$$e_H = \frac{nd}{n+nd} = \frac{d}{1+d}$$

Efficiency increases if frame size increases/contention slot size decreases ( $d$  increases)



$$e_L = \frac{d}{n + d}$$

# Token Ring

Station with token is allowed to send frame, pass on token

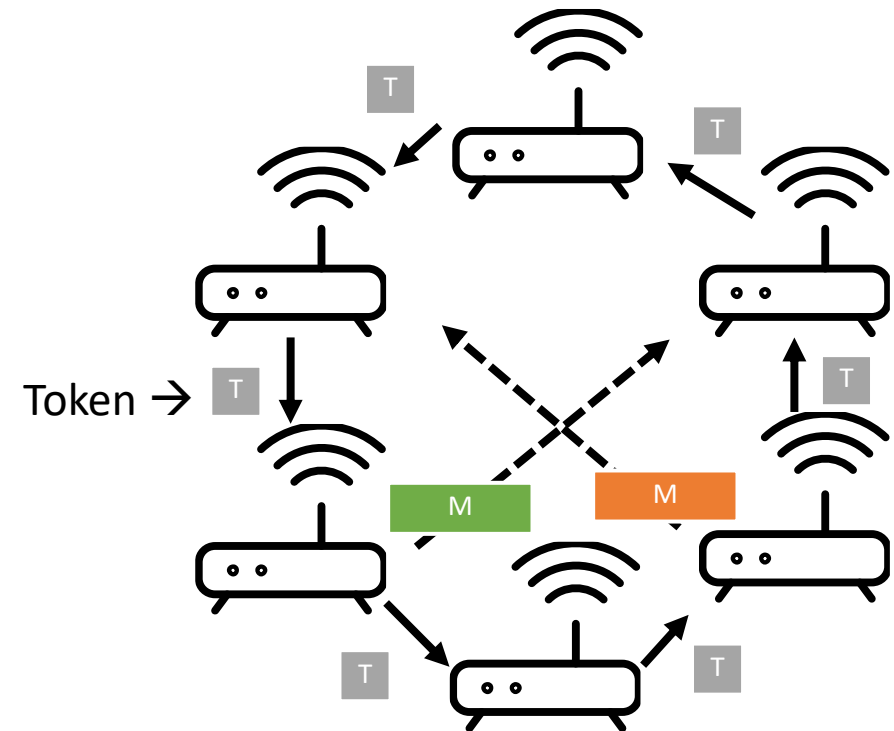
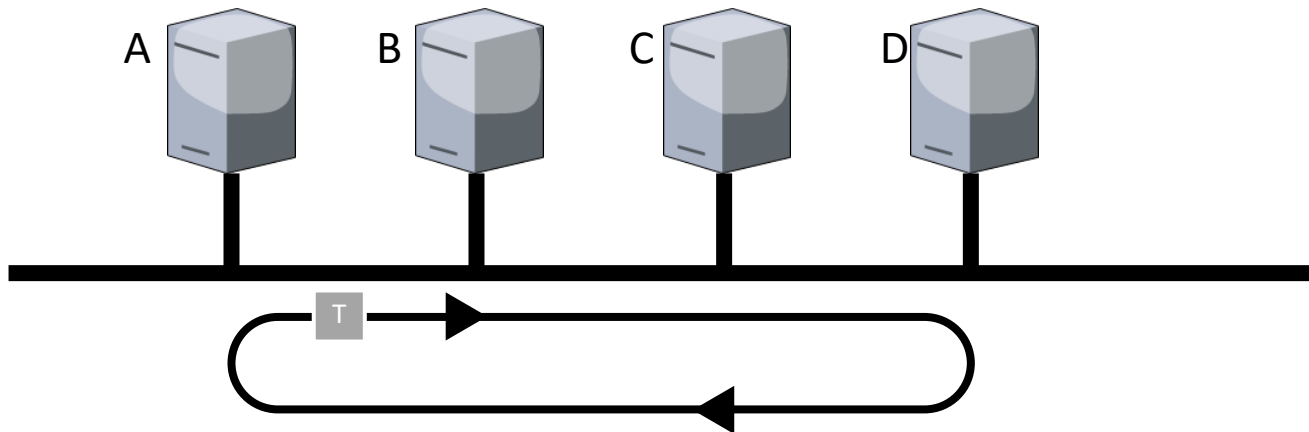
Q: What is the efficiency of this protocol?

A *collision-free* protocol.

Similar to the basic bit-map protocol.

All stations send in a predefined order.

Physical network layout need not be a ring



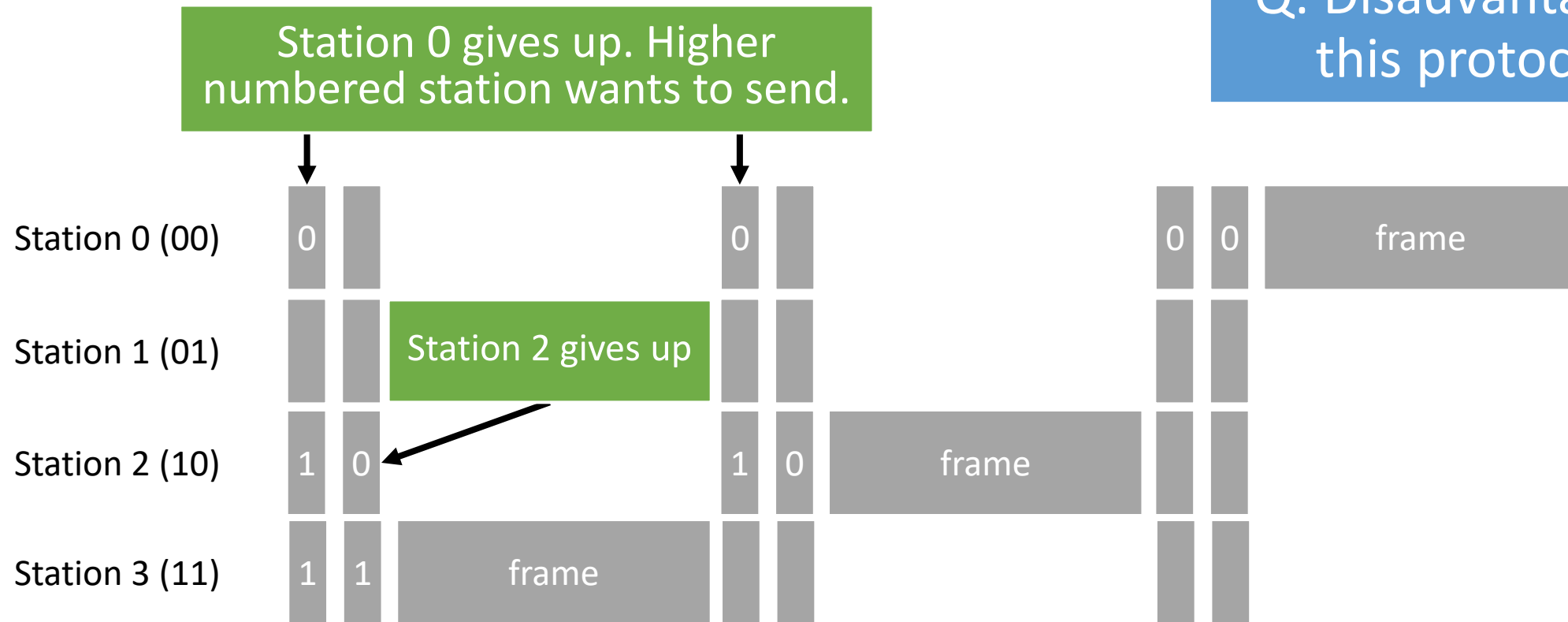
# Binary countdown

Q: What is the trade-off these protocols make?

$$e = \frac{\log_2(n) \text{ overhead, } d}{d + \log_2 n}$$

Example: Stations 0, 2, and 3 want to send a frame

Q: Disadvantage of this protocol?



# MAC Layer Summary



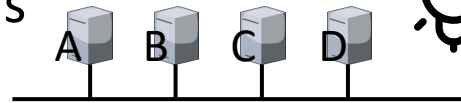
Multiplexing on the link layer **Q: Why useful?**

- Contention and coordination **Q: Which is better?**
- Centralized and decentralized protocols
- Properties: bandwidth efficiency, latency, complexity.



Protocols and mechanisms

- Carrier Sense
- Collision Detection, 1-persistent, nonpersistent, p-persistent **Q: Why not used on wireless channels?**
- Collision Avoidance, MACA, CSMA/CA
- Collision-free protocols, Basic bitmap, Token ring, Binary countdown



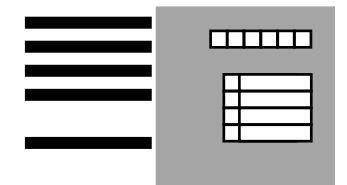
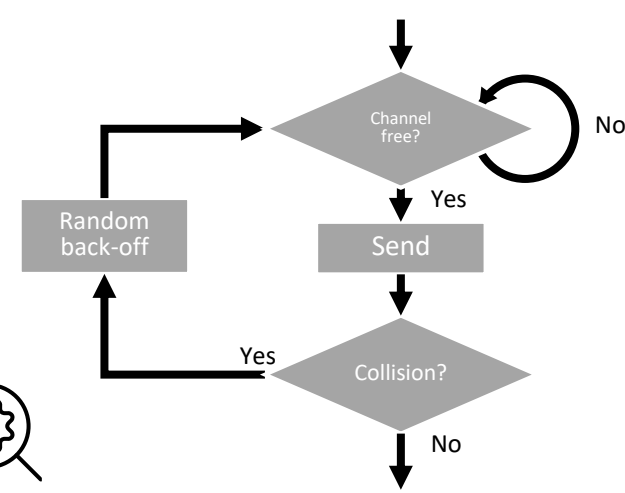
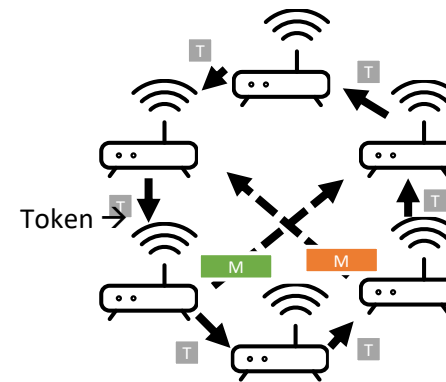
Wireless Channels

- Limited Radio Range
- Hidden terminals and Exposed terminals



Switching

- Routing on the link layer **Q: How to know where to send frames?**
- No MAC protocol needed when used on full-duplex wired channels



# Computer Networks

## X\_400487

### Lecture 5

### Chapter 4: Medium Access Control



Lecturer: Jesse Donkervliet  
Includes slides from Vlad Cursaru



Extra Slides 

# Medium Access Control Bluetooth

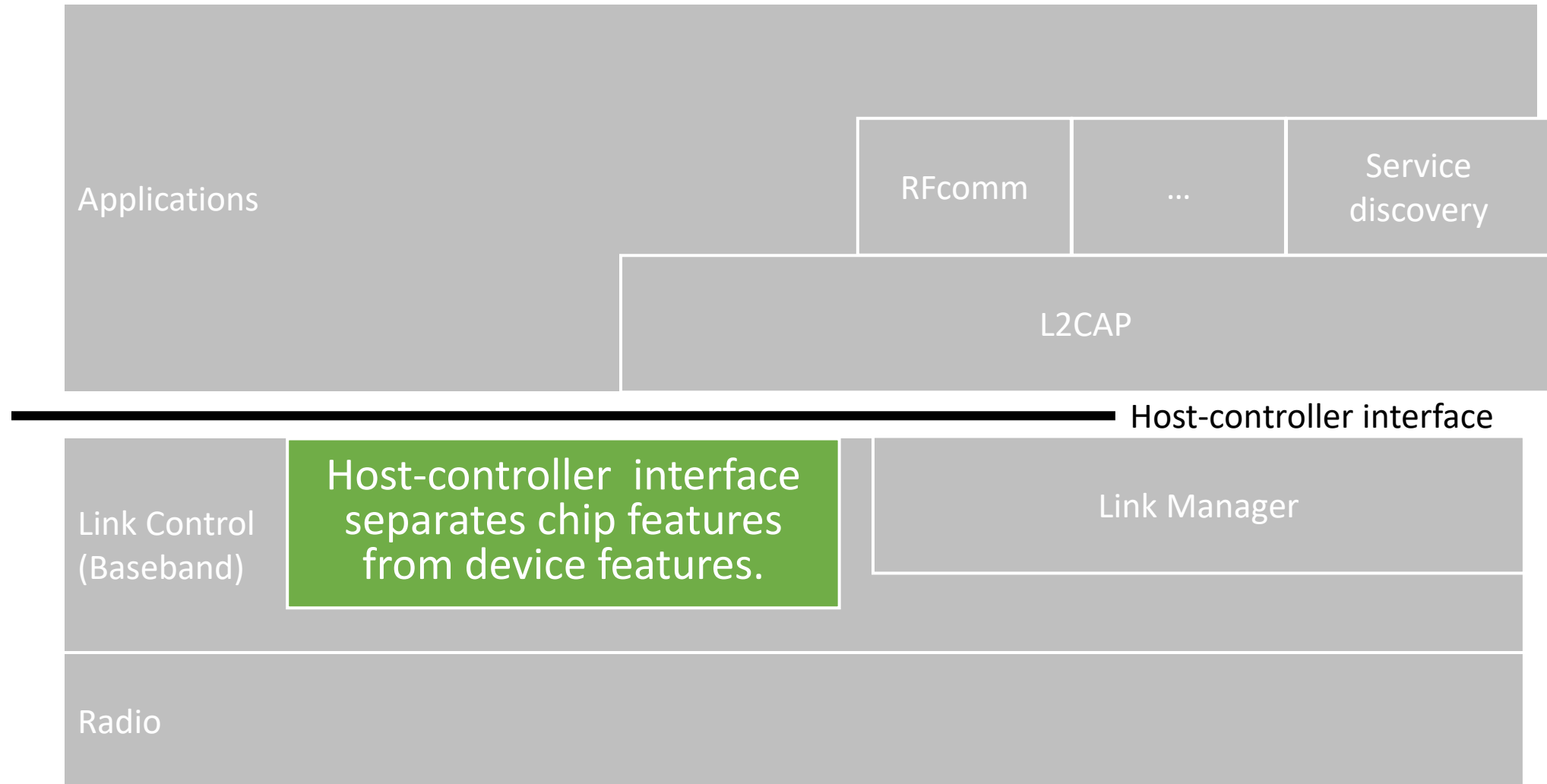


# Bluetooth Protocol Stack

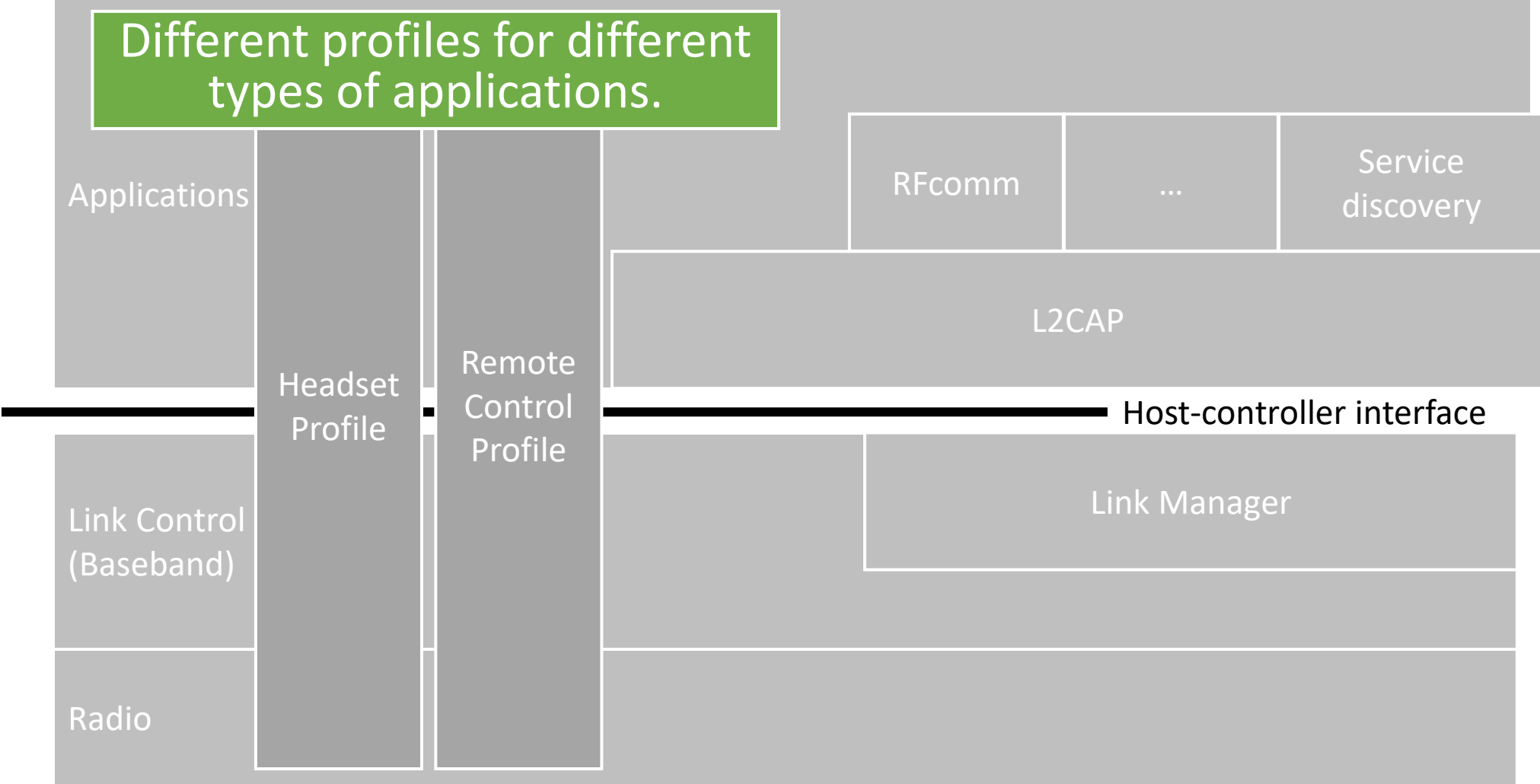
No fixed set of protocols. Instead, **profiles** define the set of protocols for a given application.

25 profiles, including headset, intercom, streaming audio, remote control, personal area network, and others.

# Bluetooth Protocol Stack



# Bluetooth Protocol Stack



# Medium Access Control in ... Bluetooth

## Radio layer

Q: How to prevent interference with 802.11?

Uses adaptive frequency hopping in 2.4GHz band.

## Link layer

Connectionless or connection-oriented  
depending on the application.

TDM with timeslots for master and slaves.

*Synchronous CO* for periodic slots in each direction.

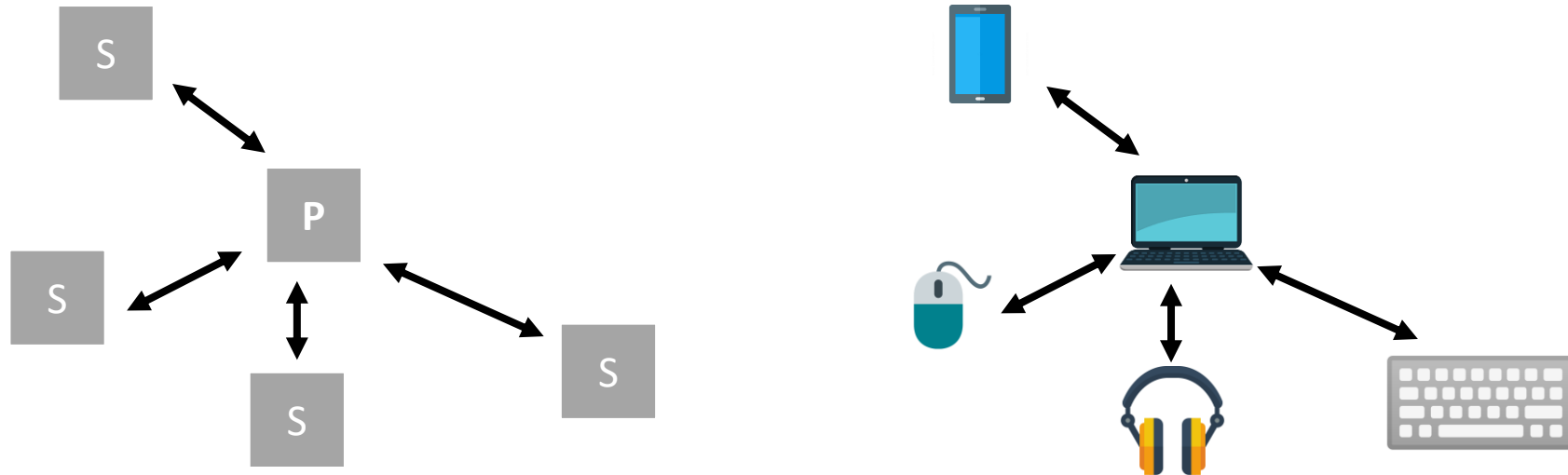
*Asynchronous CL* for packet-switched data.

Links undergo pairing (user confirms passkey/PIN) to authorize them before use.

# Medium Access Control in ... Bluetooth

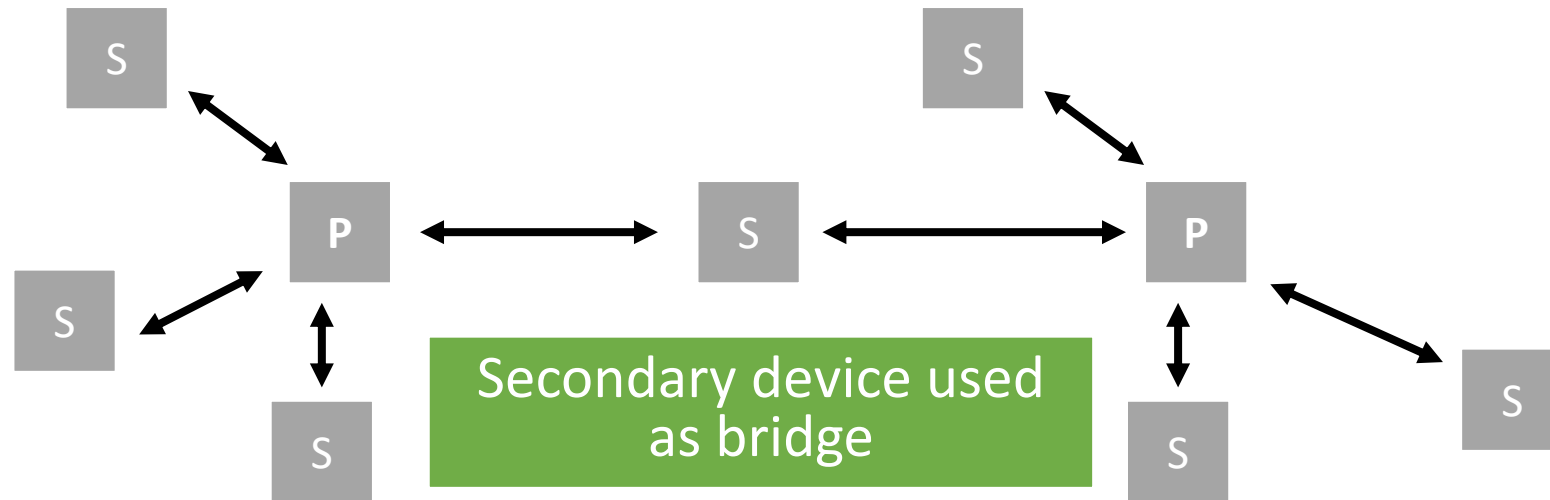
A Bluetooth network is called a *piconet*.

Secondaries may be asleep (parked) to save power.



# Bluetooth piconet

Two piconets can be bridged into a *scatternet*.



# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



# Bluetooth frames

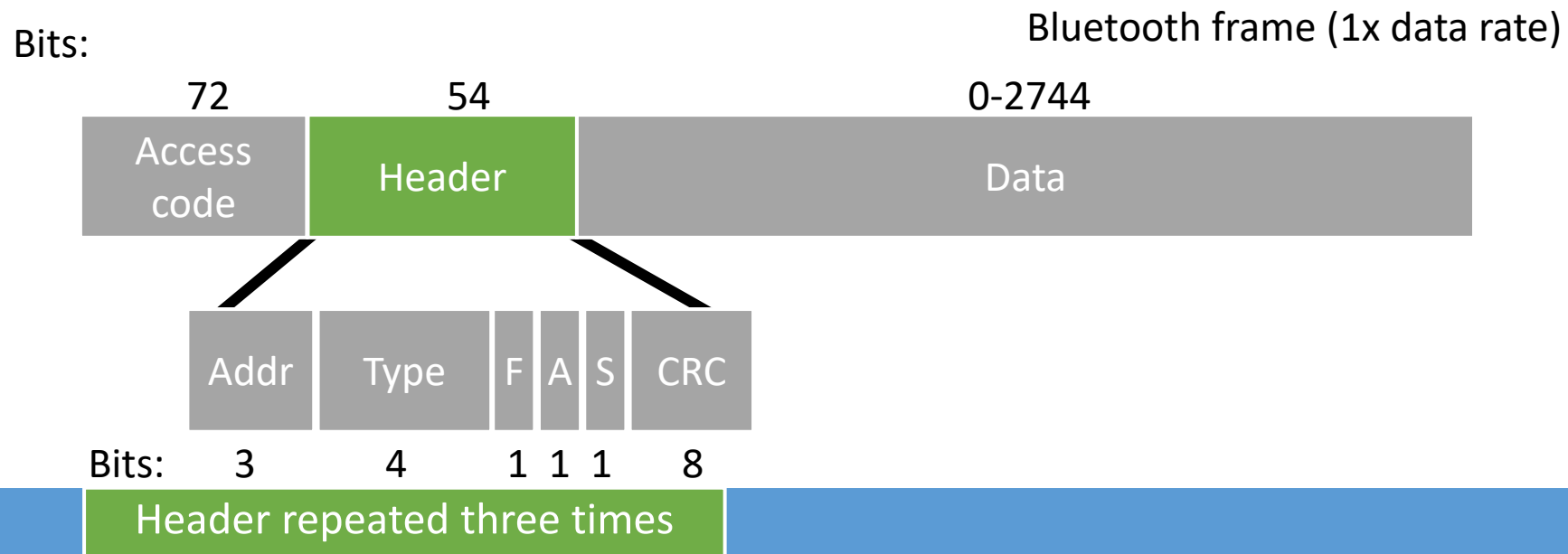
Uses multiple types of frames, similar to 802.16.



Used to identify *primary* device.

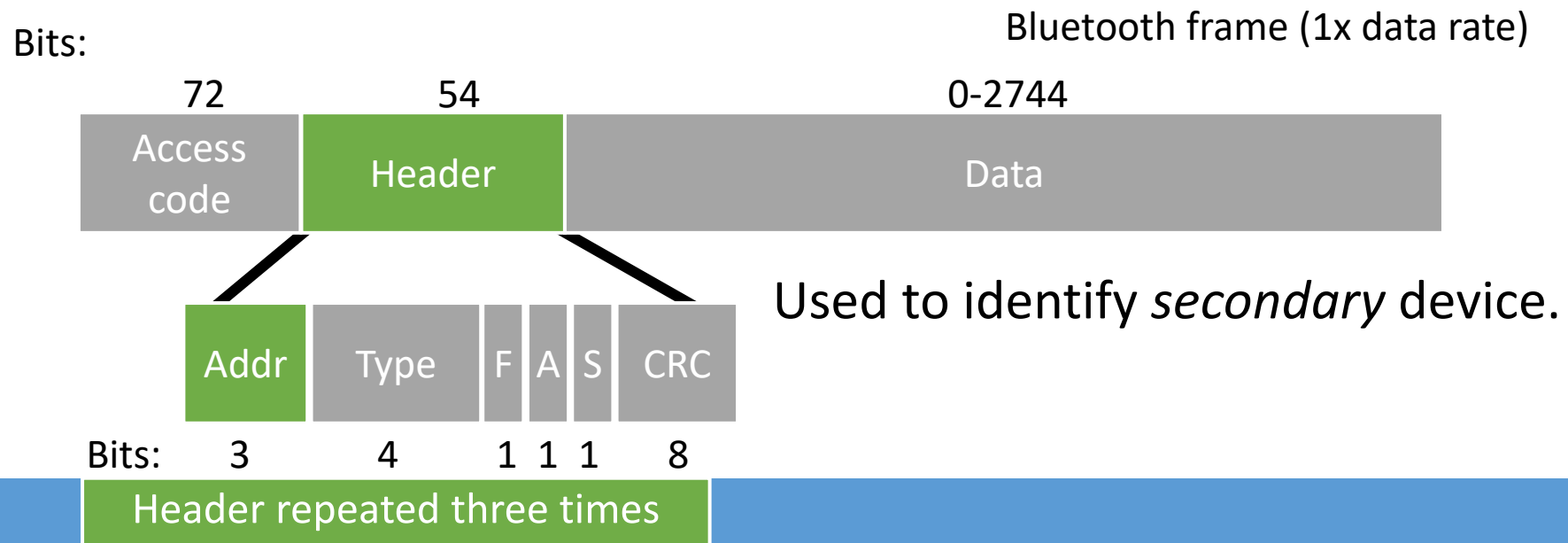
# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



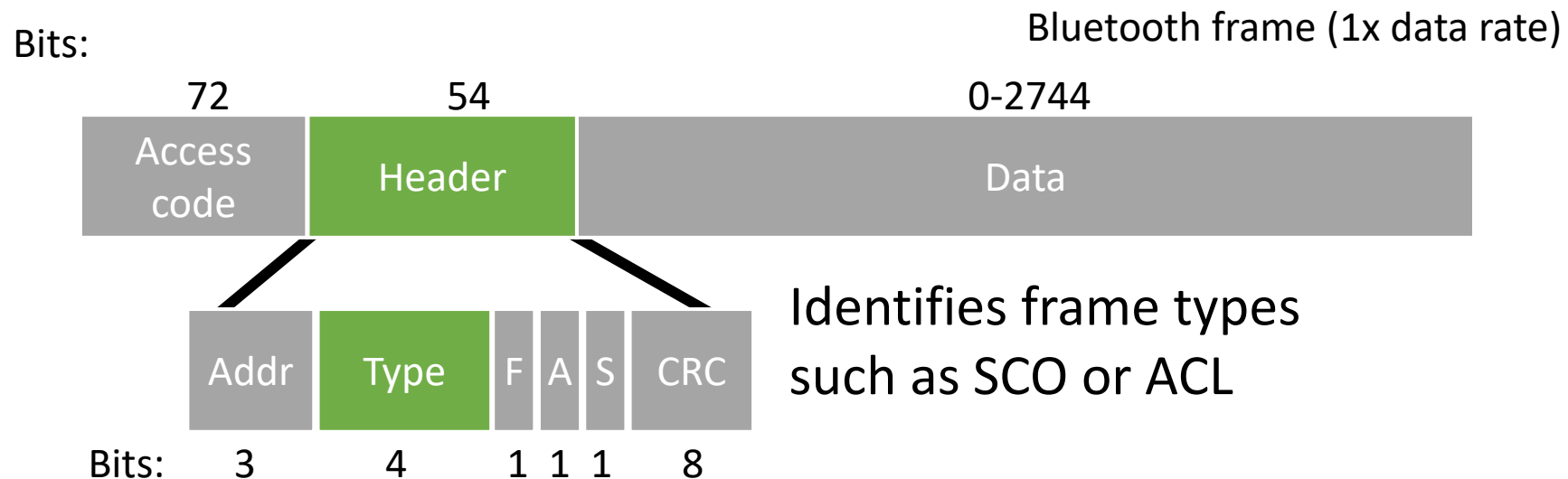
# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



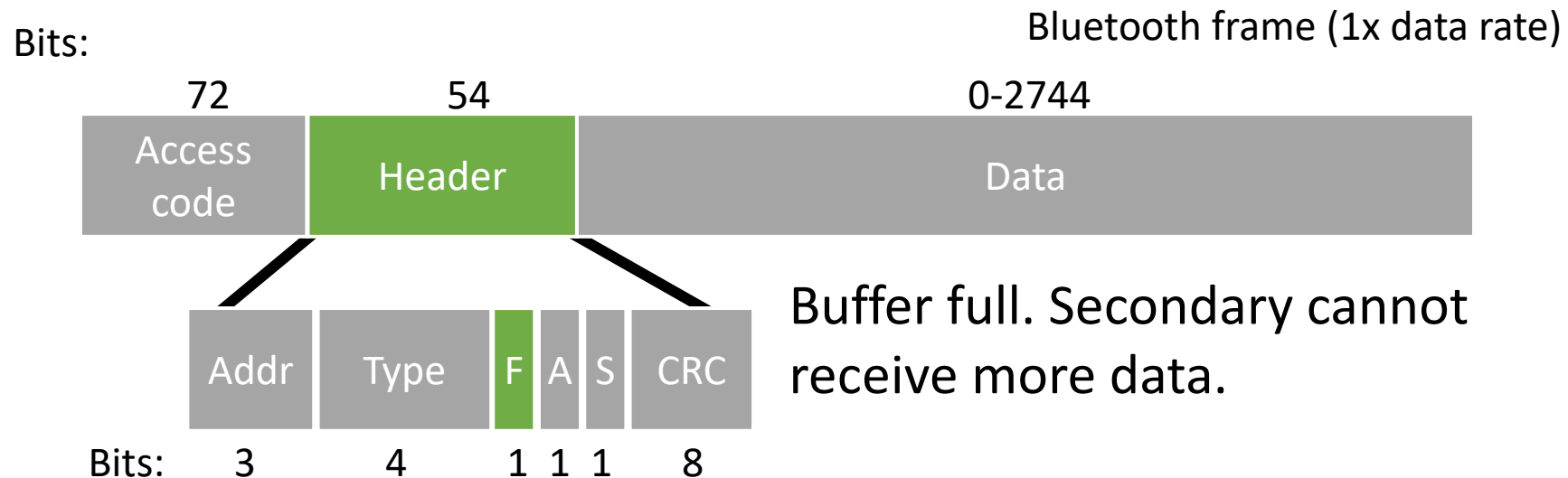
# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



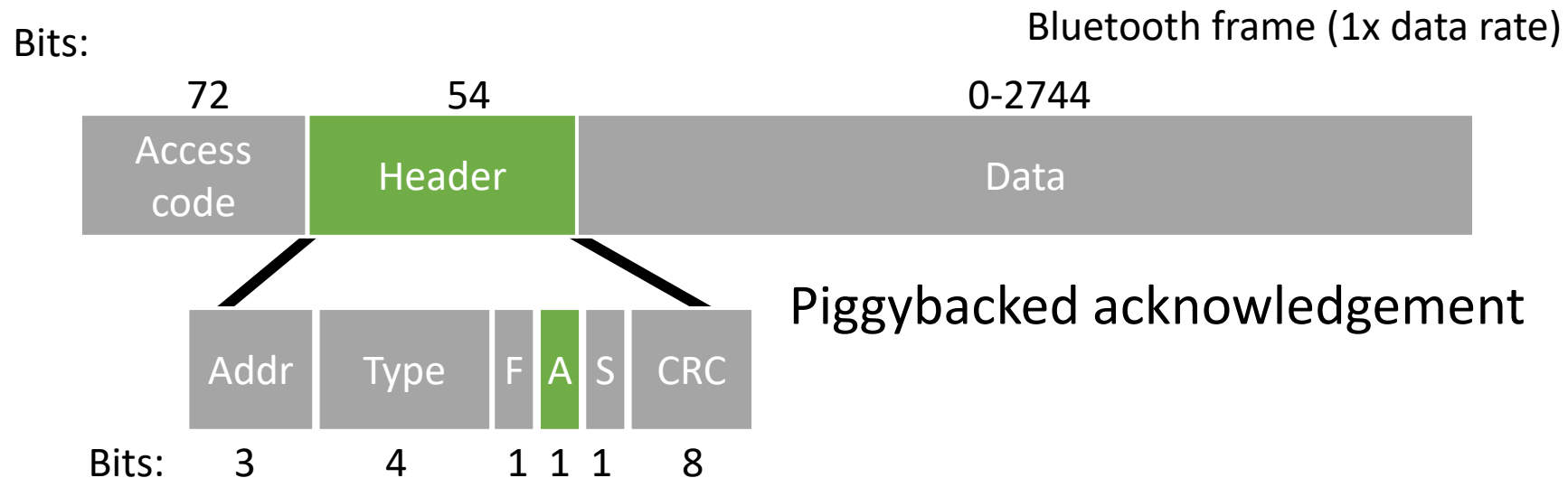
# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



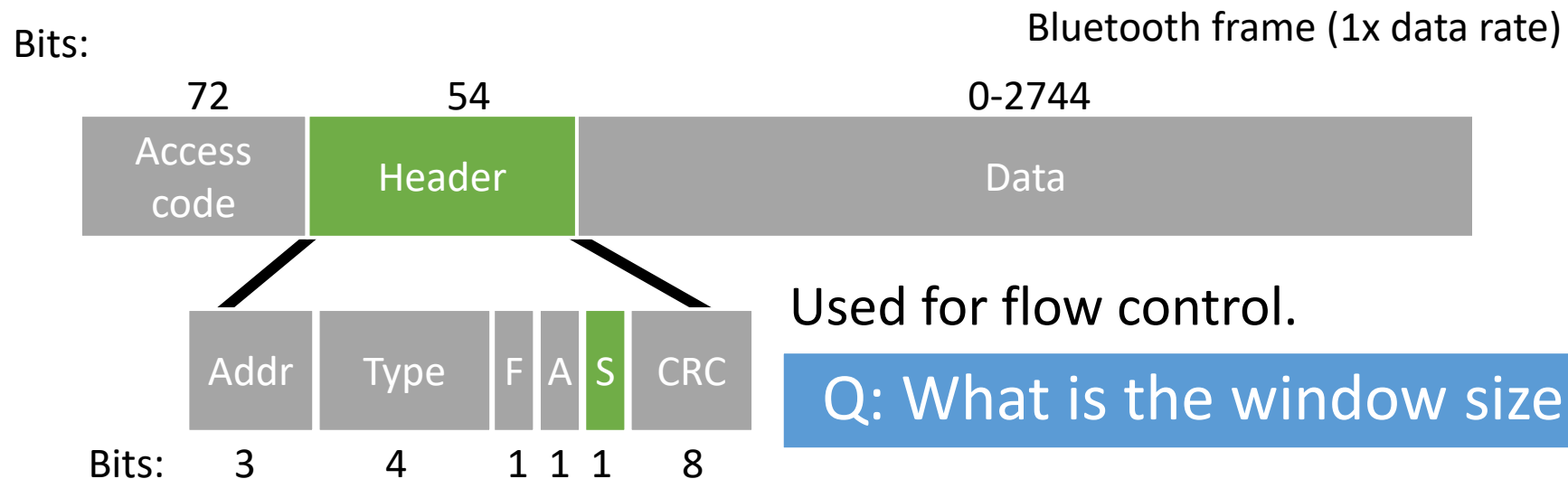
# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



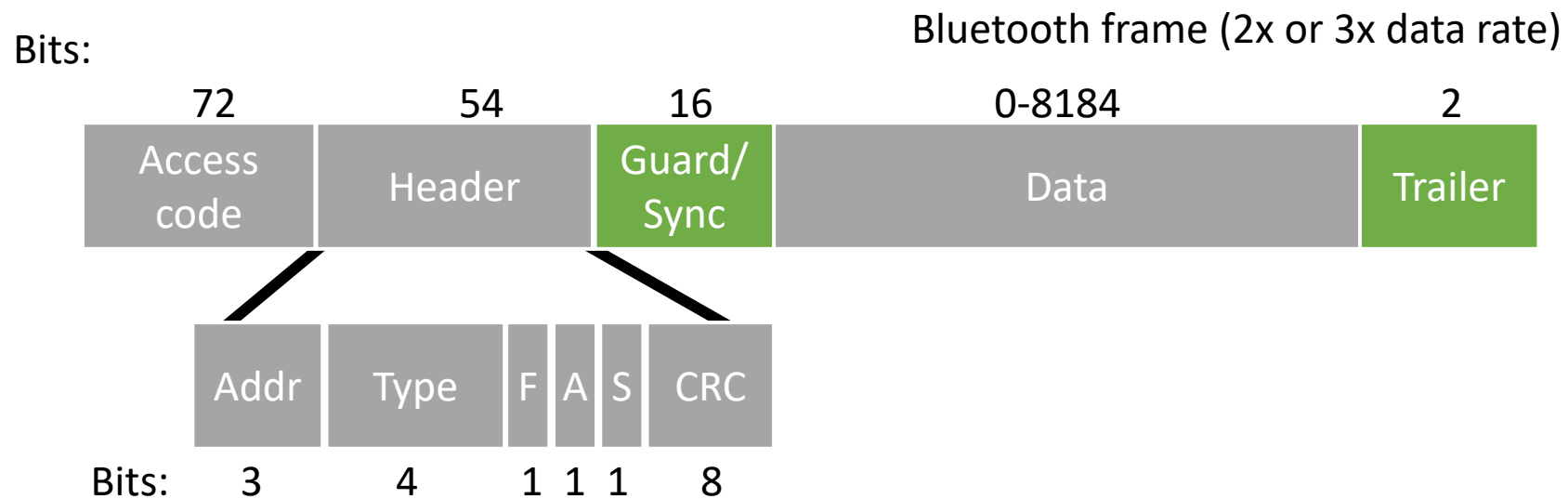
# Bluetooth frames

Uses multiple types of frames, similar to 802.16.



# Bluetooth frames

Enhanced data rates send faster but for the same time.



# Medium Access Control RFID



# RFID Readers

Stationary reader



Mobile reader



# Medium Access Control in ... RFID

RFID uses **readers** and **tags**. Reader in charge of medium access control. Tags reply to requests.



# Medium Access Control in ... RFID

RFID uses **readers** and **tags**. Reader in charge of medium access control. Tags reply to requests.

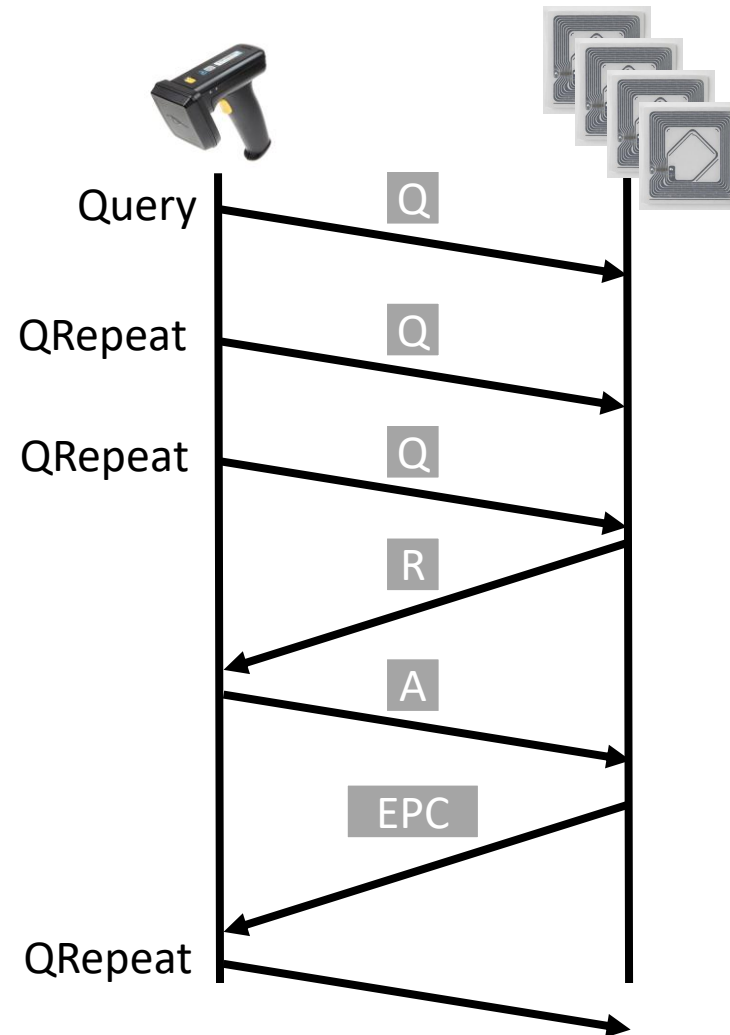


Q: Similar to a method we have seen last lecture?

# RFID communication example

Generation 2 Tag identification.

1. Reader sends query and sets slot structure.
2. Tags reply (RN16) in a random slot; may collide.
3. Reader asks one tag for its identifier. (ACK)
4. Process continues until no tags are left.



# RFID request frame

RFID uses multiple types of frames.  
Example of a request-frame:

Bits:



# RFID request frame

RFID uses multiple types of frames.  
Example of a request-frame:

Bits:



Used to configure physical layer properties (e.g., data rate).

# RFID request frame

RFID uses multiple types of frames.  
Example of a request-frame:

Bits:



Used to keep track of which tag is identified by which reader.  
Allows tags to reply to multiple readers in the same area.

# RFID request frame

RFID uses multiple types of frames.  
Example of a request-frame:

Bits:



Limits random backoff values available to the tags.

Tag responds in a slot between 0 and  $2^Q - 1$