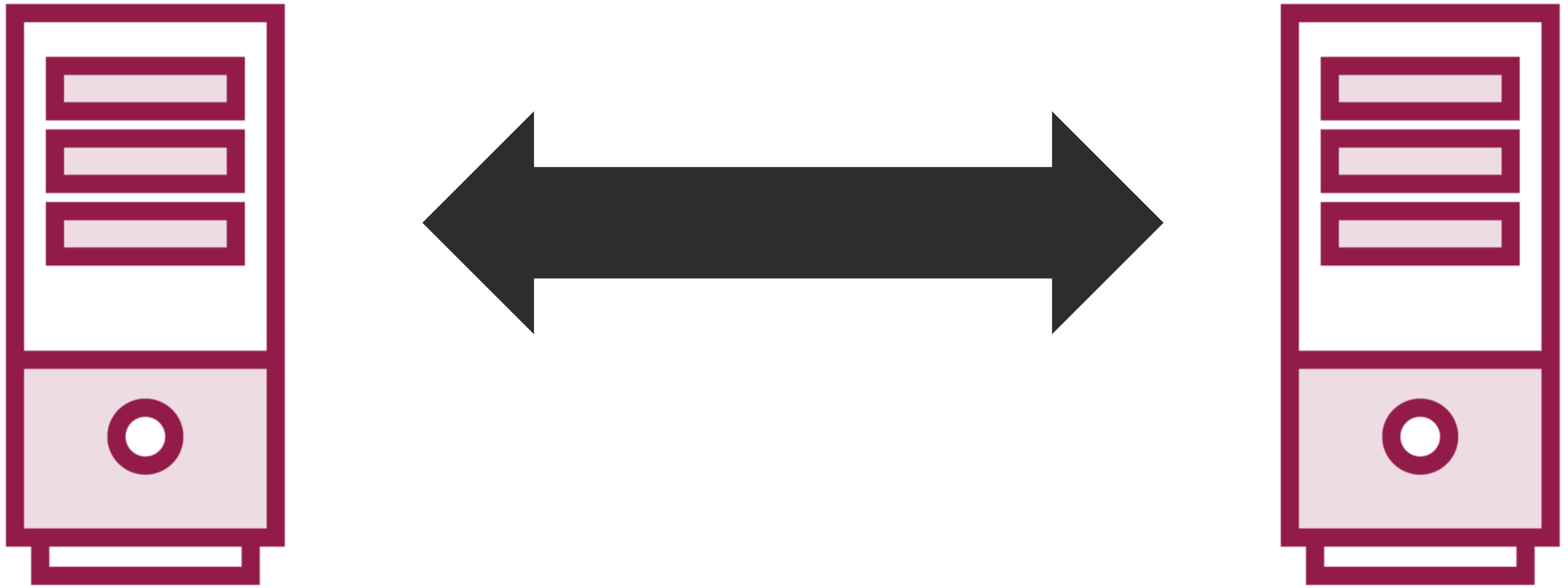
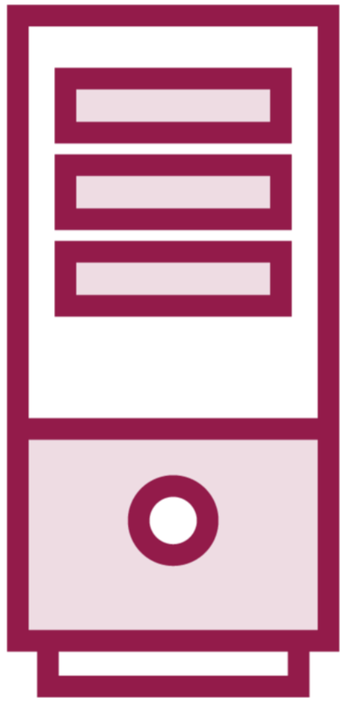
Understanding the 3-way Handshake

Dale Meredith

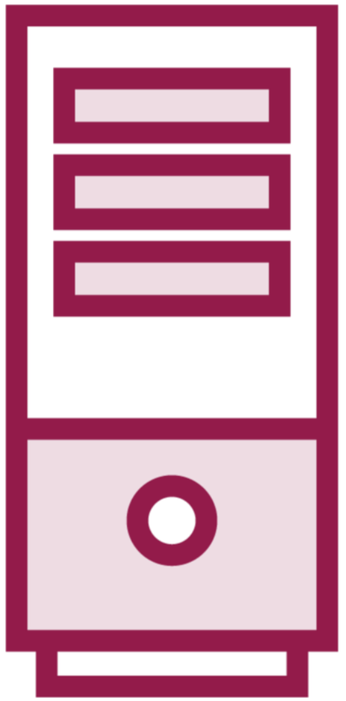
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith



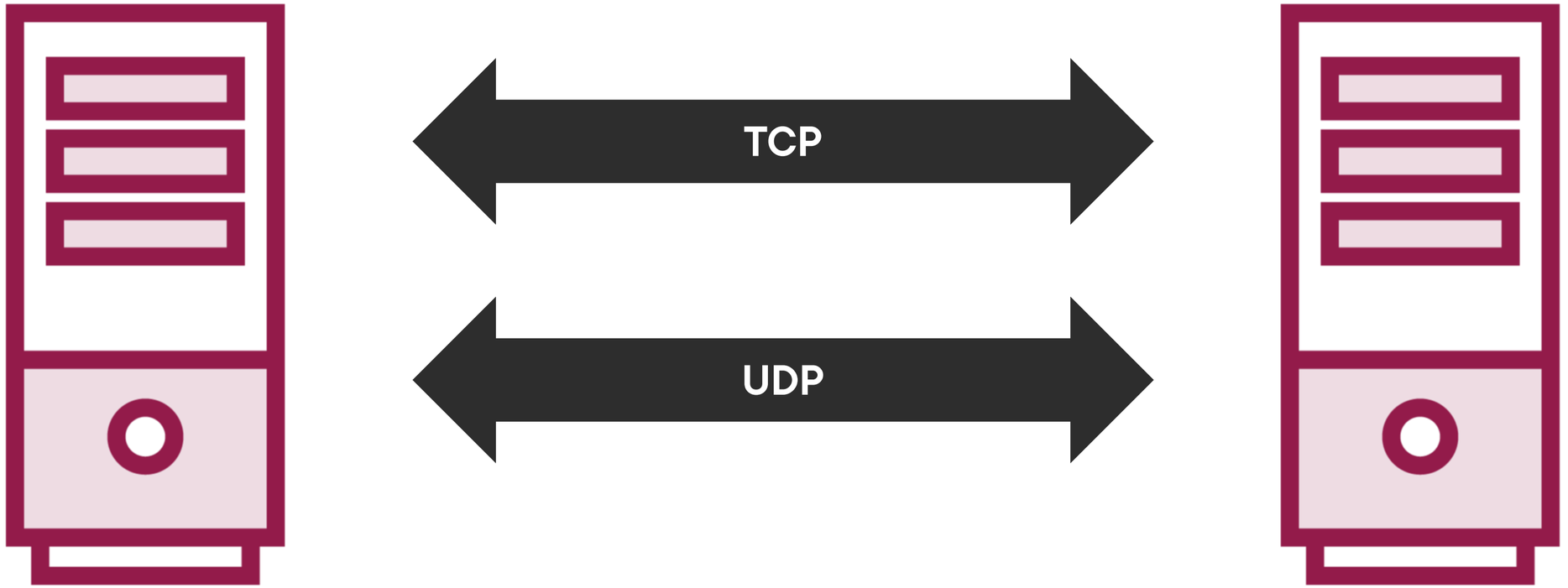


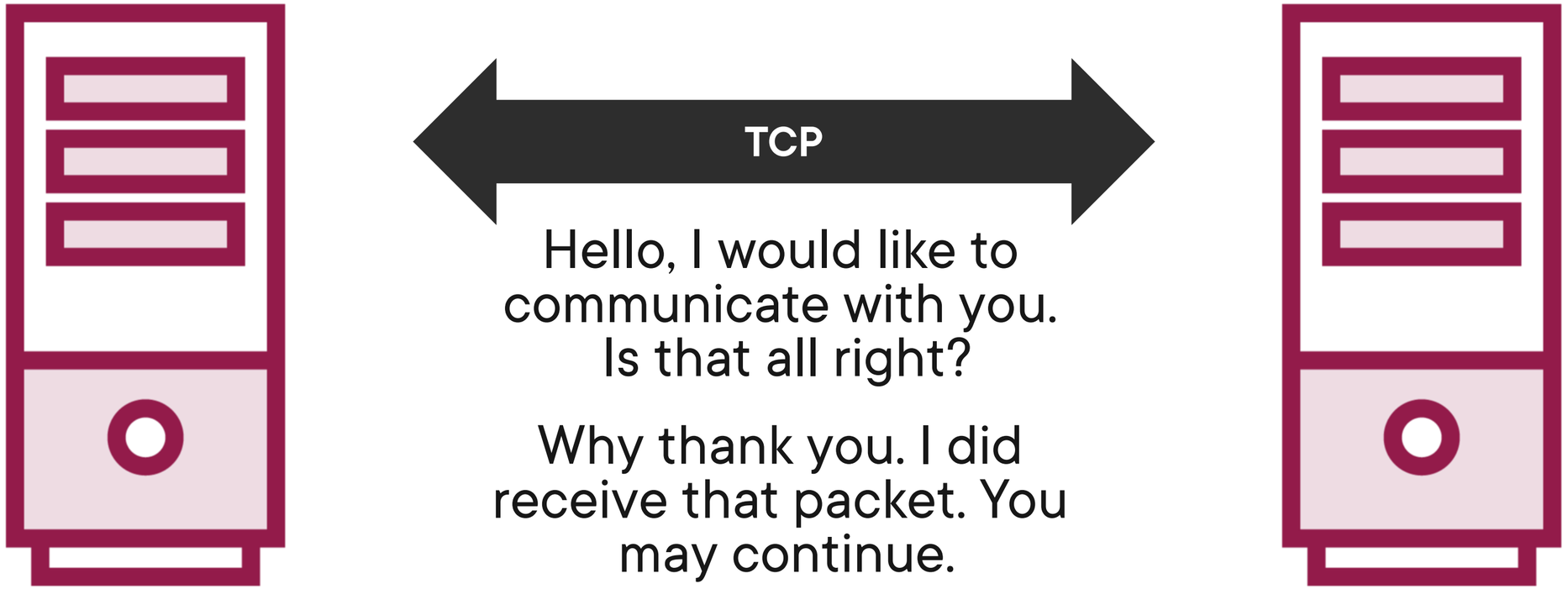
3-way Handshake



I don't remember who came up with the handshake idea, but it was a great one.

Mike O’Cain





Acknowledges the packet was received

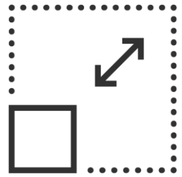
Retransmits packets that fail to deliver

Conducts a in-order delivery

Controls congestion

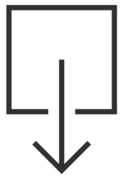
TCP

Retransmissions, in-order delivery, congestions control, and delivery acknowledgments impacts it's speed



Utilizes 20 bytes vs UDP's 8 bytes

Utilizes a larger overhead than UDP



Uses stream-orientation to send packets

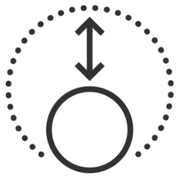
Requires three packets to set up a socket connection

UDP 3-Way Handshakes

UDP

Connectionless based

Does not guarantee delivery



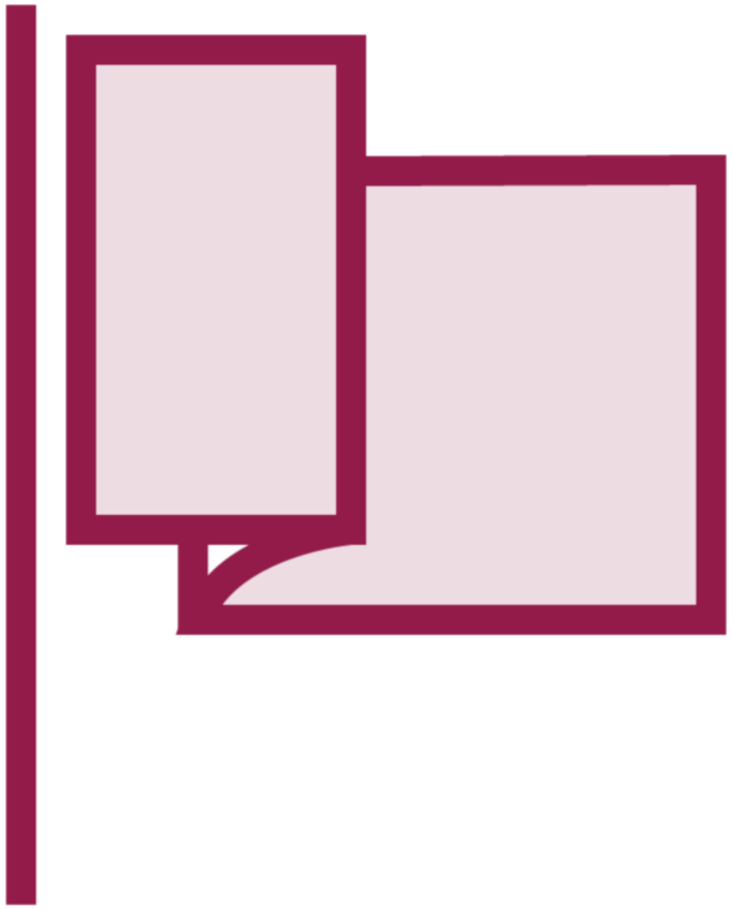
Utilizes smaller packets (8 bytes)

Extremely fast

Message-oriented

TCP Header Flags

There's a Flag on the Play!



SYN

- Synchronize (Includes a seq #)

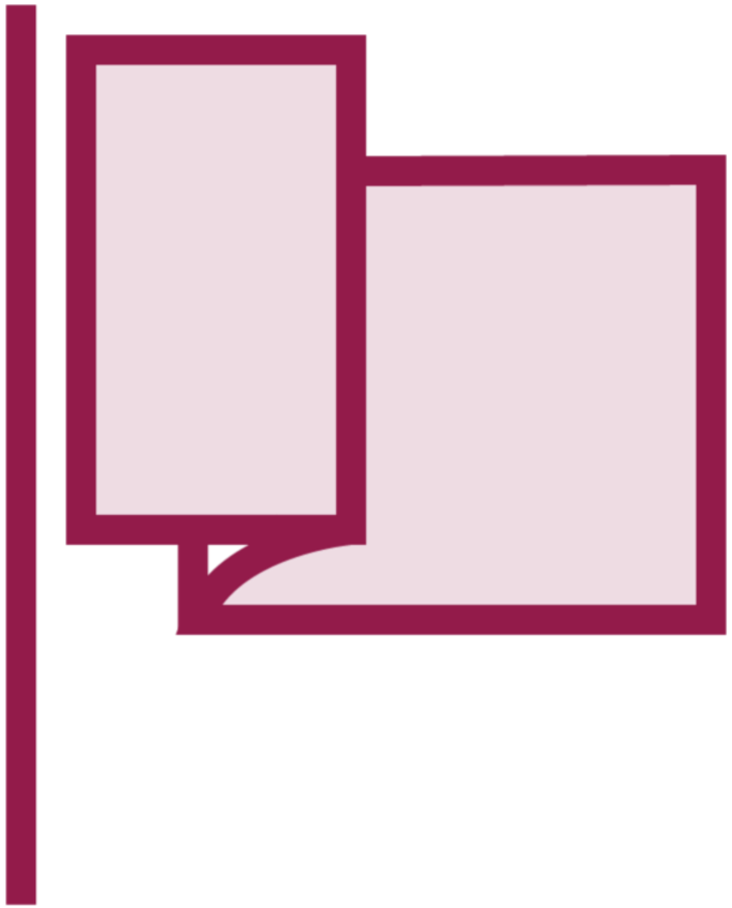
ACK

- Acknowledgement

FIN

- Finish

There’s a Flag on the Play!



PSH

- Push

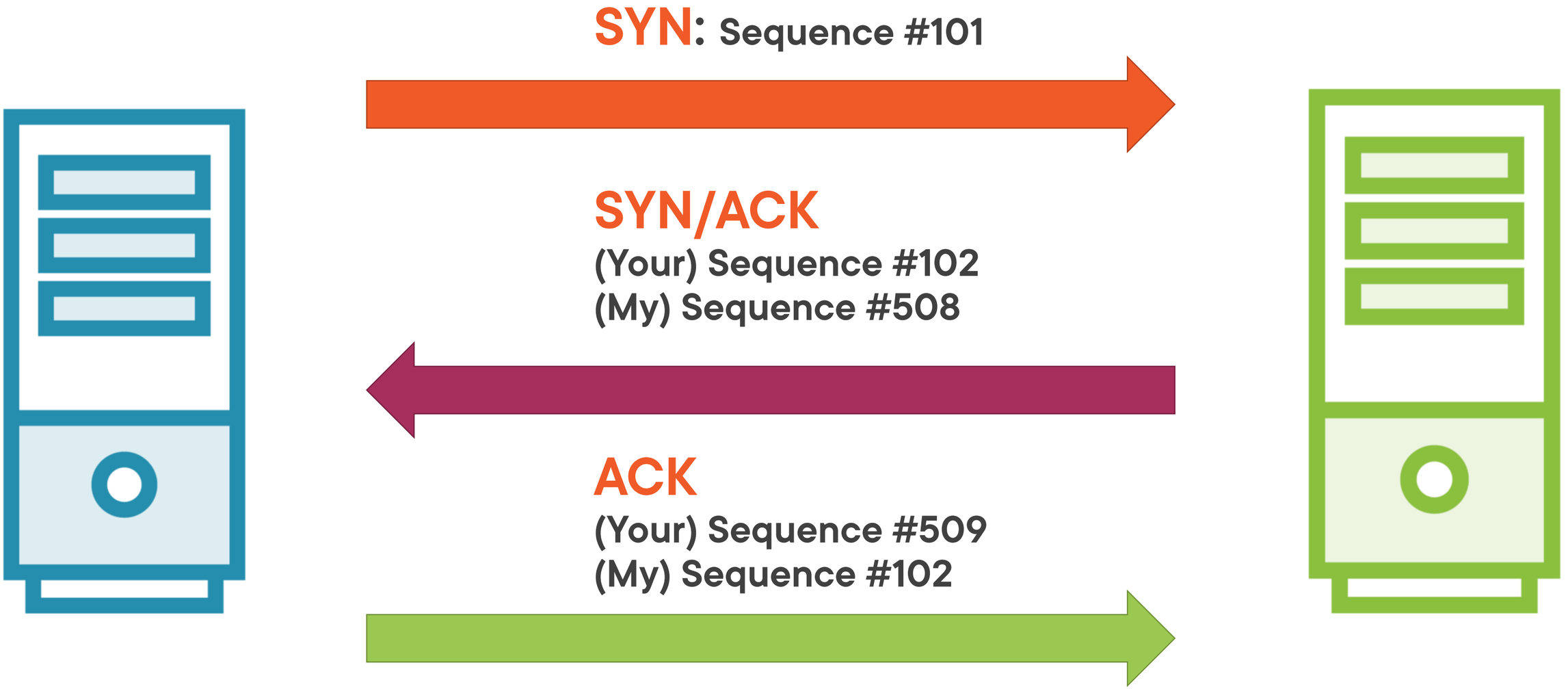
URG

- Urgent

RST

- Reset

Let's Put It All Together Now



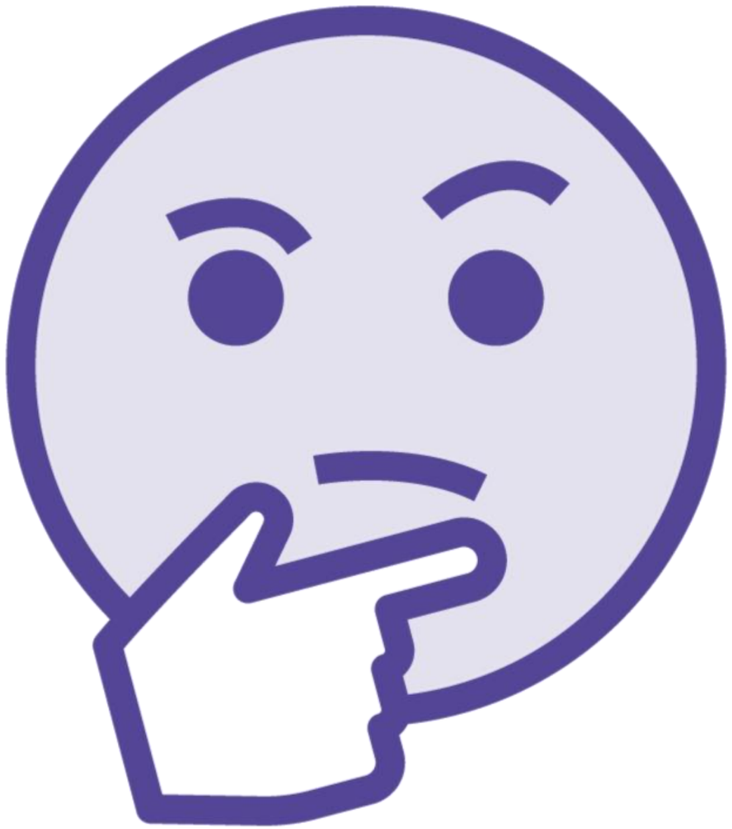
Let's Put It All Together Now

Demo

Let’s see the 3-way handshake

What If…

Think Outside the Box



SYN / SYN-ACK / ACK
FIN / ACK-FIN /ACK

What would happen if your first packet was

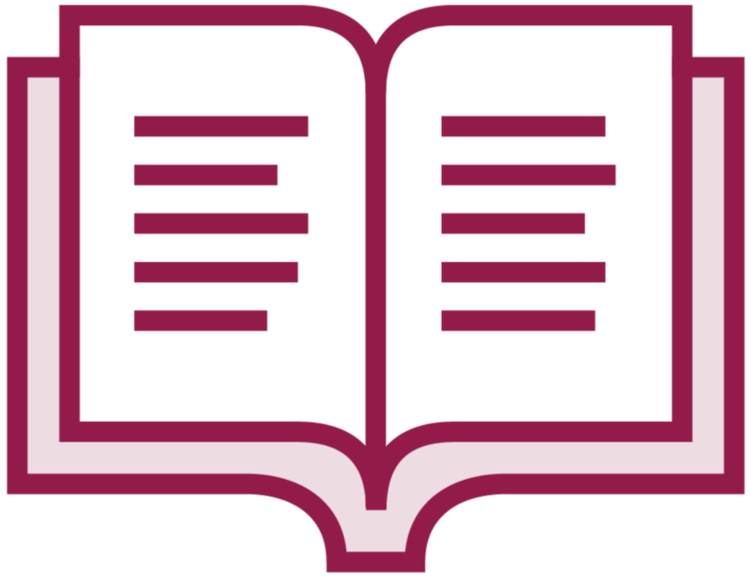
- **a SYN/ACK**
- **FIN**

What would happen if you shot a gun in space?

Learning Check

Learning Check

- UDP
- SYN-ACK
- PSH
- RST
- Connection-based



Next Up:
Classifying the Types of Scanning