Using Wireshark to Analyze ARP

Chris Greer
NETWORK ANALYST

@packetpioneer www.packetpioneer.com

Module Overview

ARP

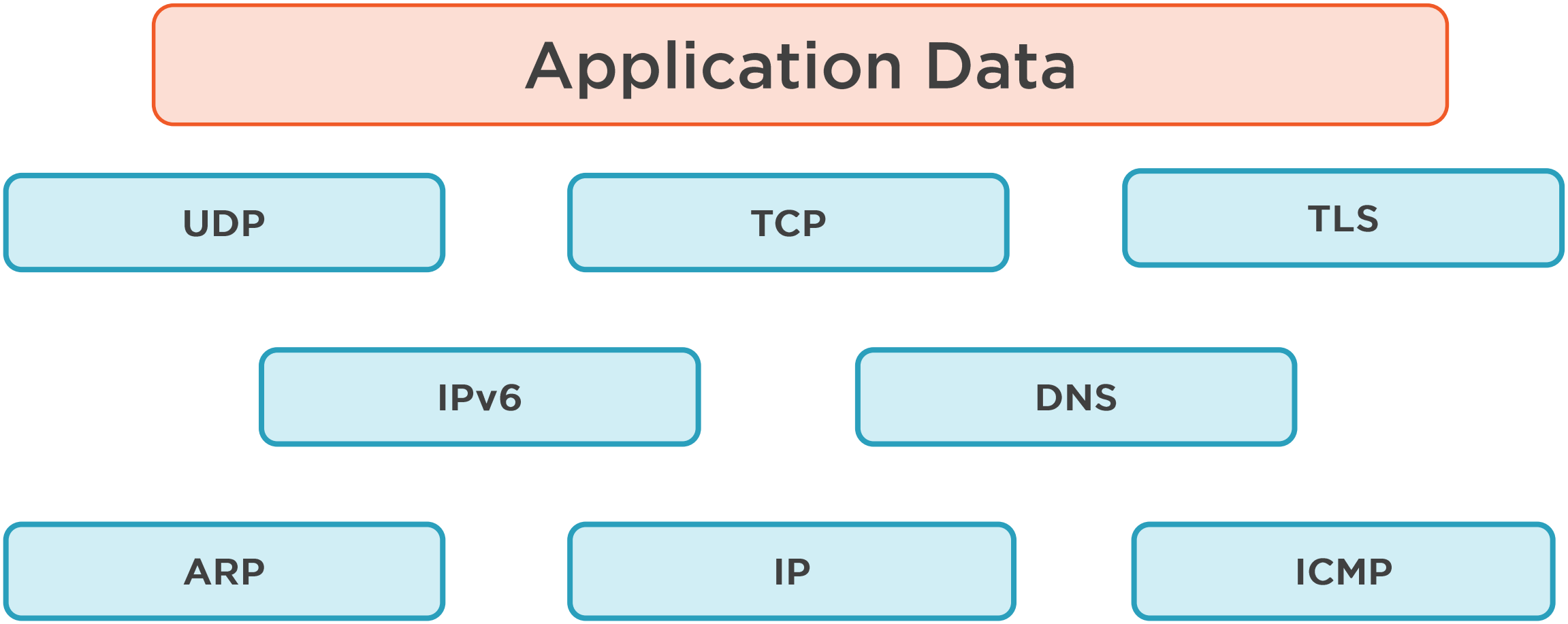
- Why is it needed?
- How does it work?

How can we tell if it is not working?

- What symptoms will we see?

Hands-on practice

Core Protocols - ARP



ARP Resolves Addresses

Layer Two Techs/Protocols

Ethernet

Token Ring

FDDI

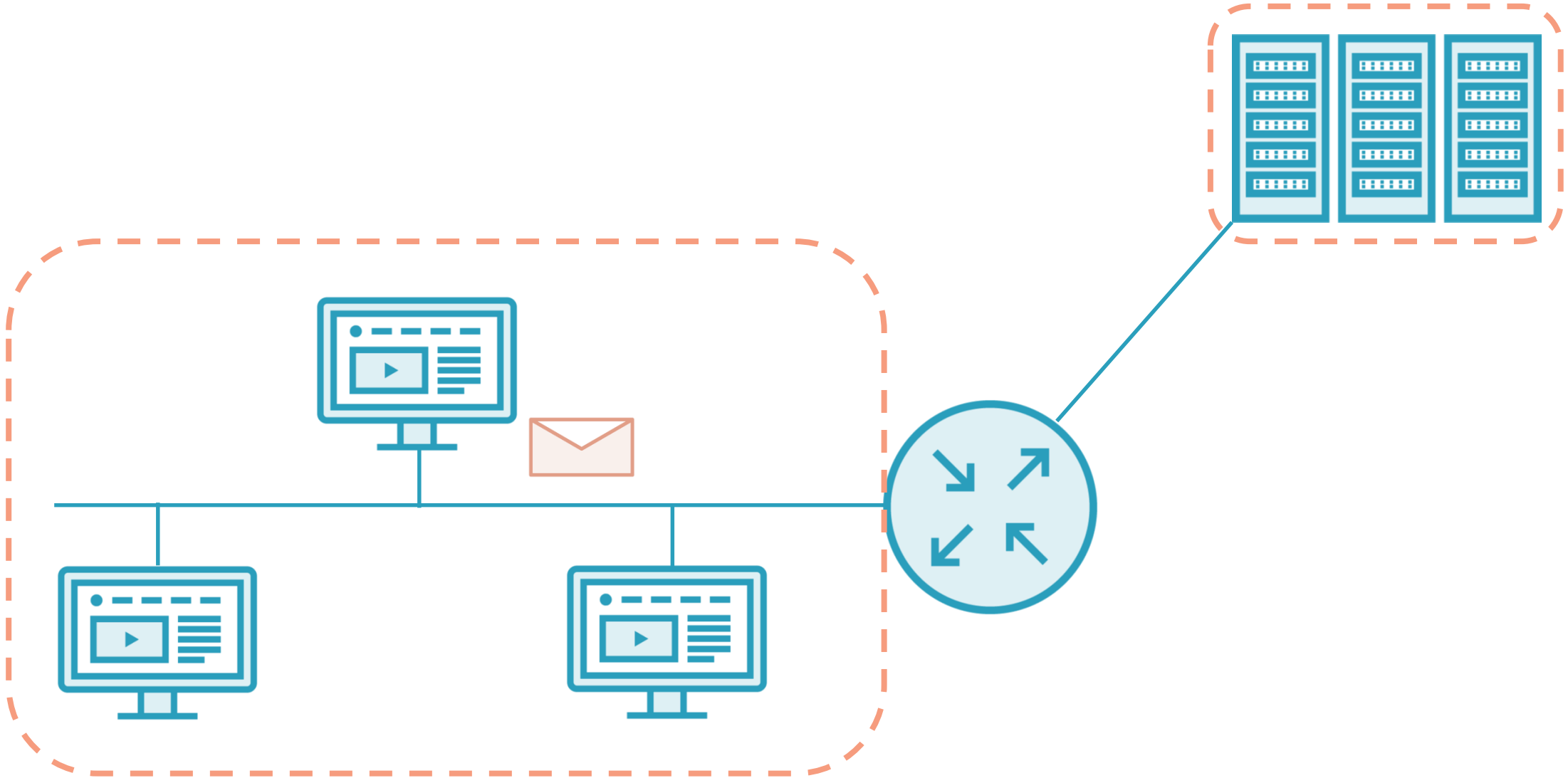
ATM

Layer Three Protocols

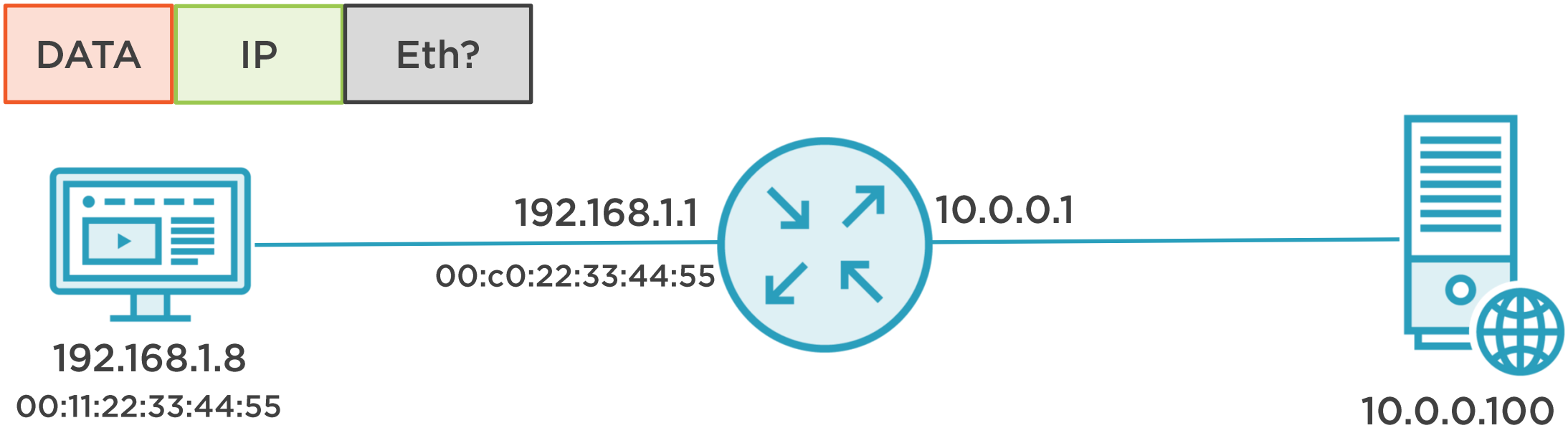
IP

IPv6 does not use ARP

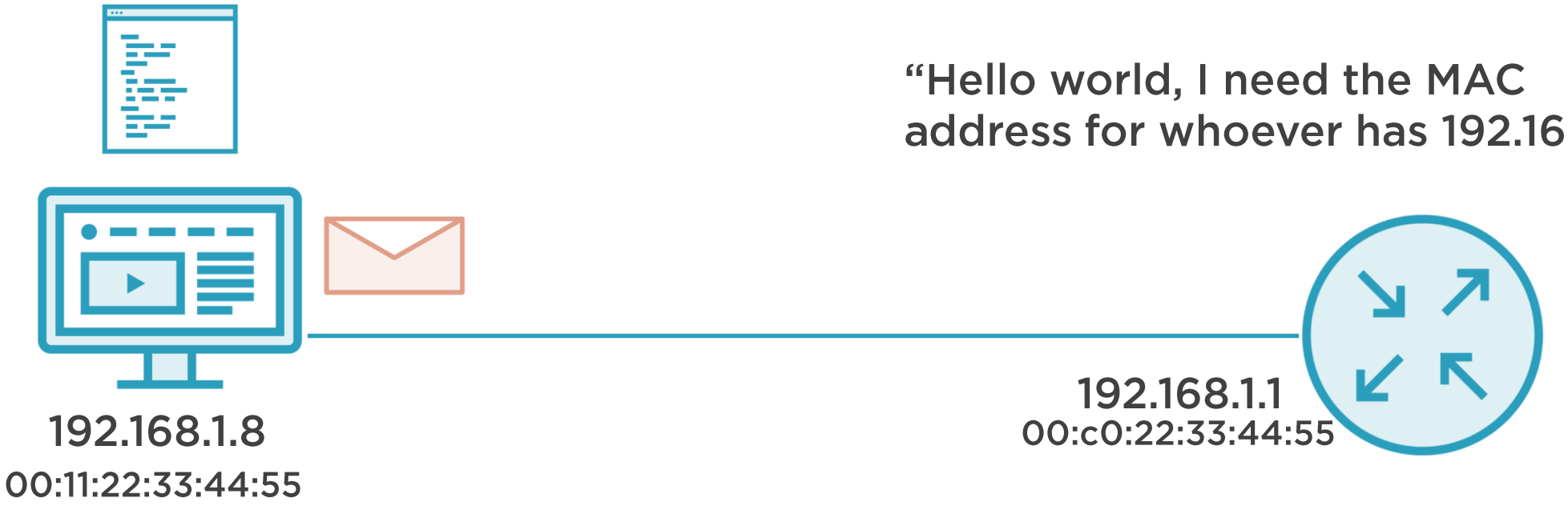
Network Communications



Simple Layer 2/3 Encapsulation



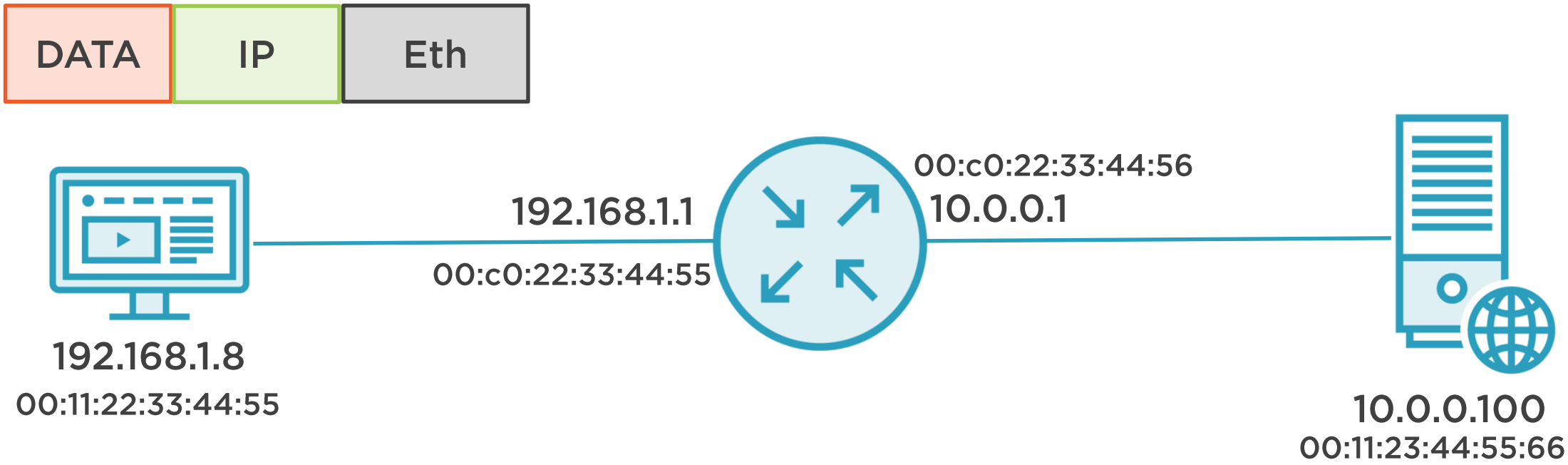
Address Resolution Protocol



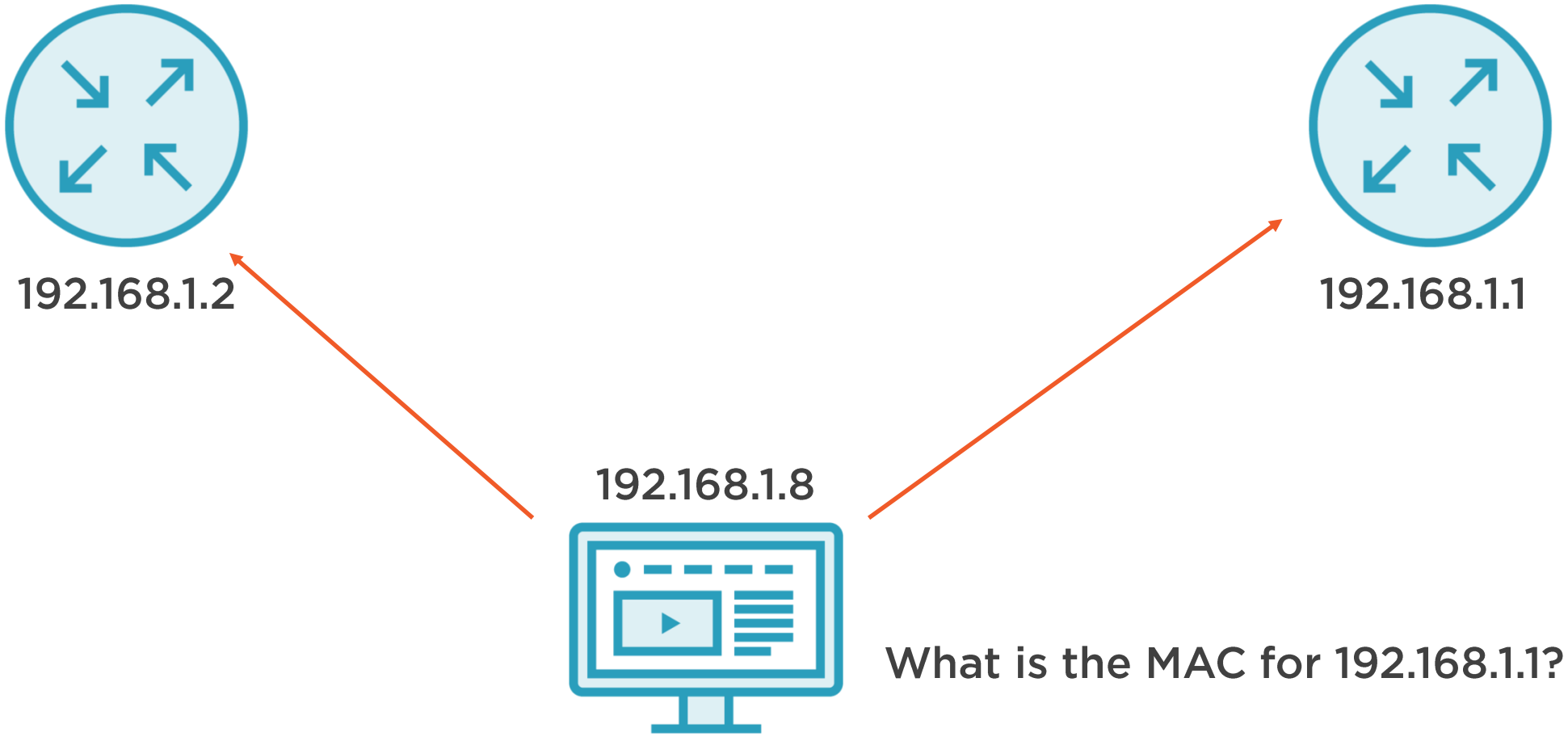
Address Resolution Protocol

"Sure client – here is my MAC address"

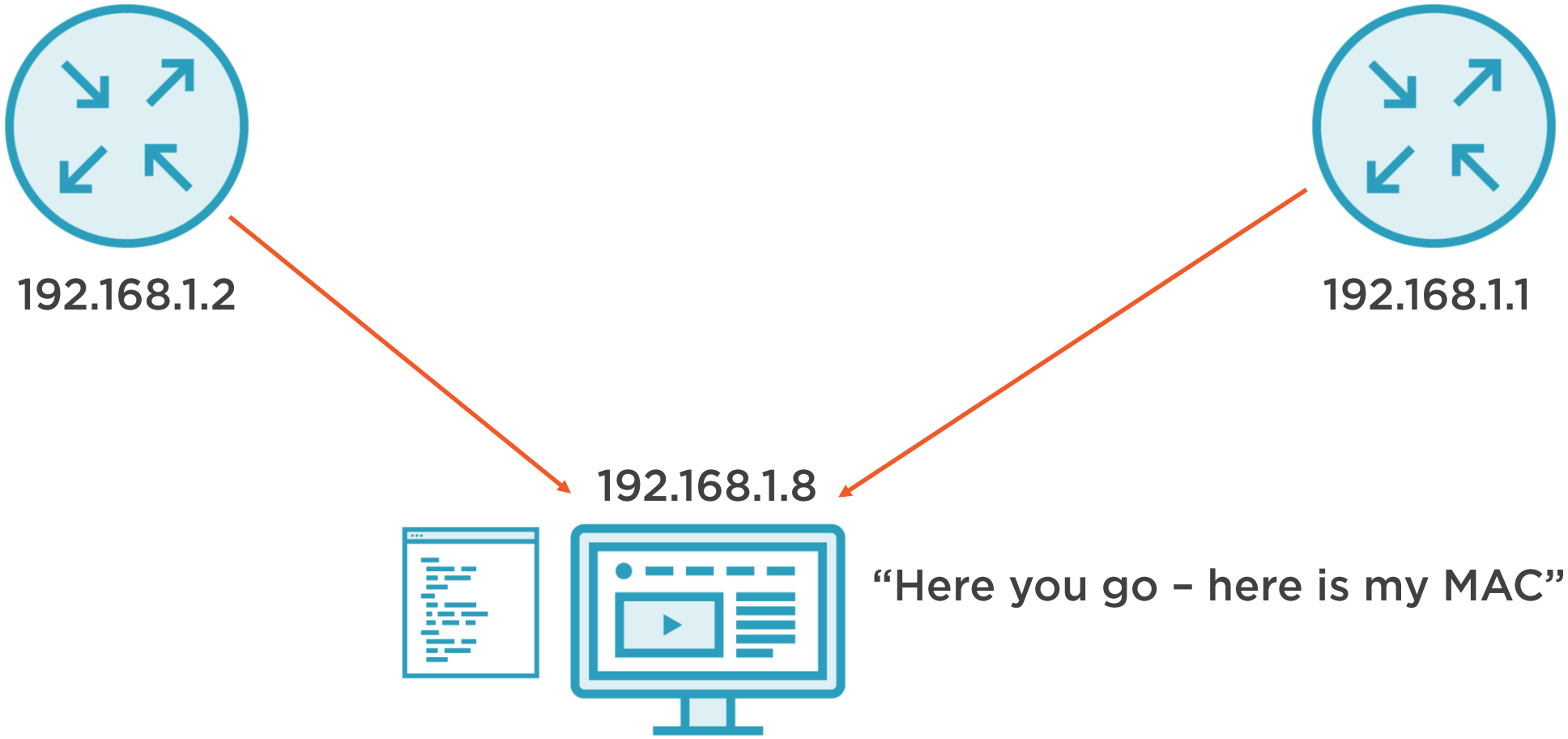
Simple Layer 2/3 Encapsulation

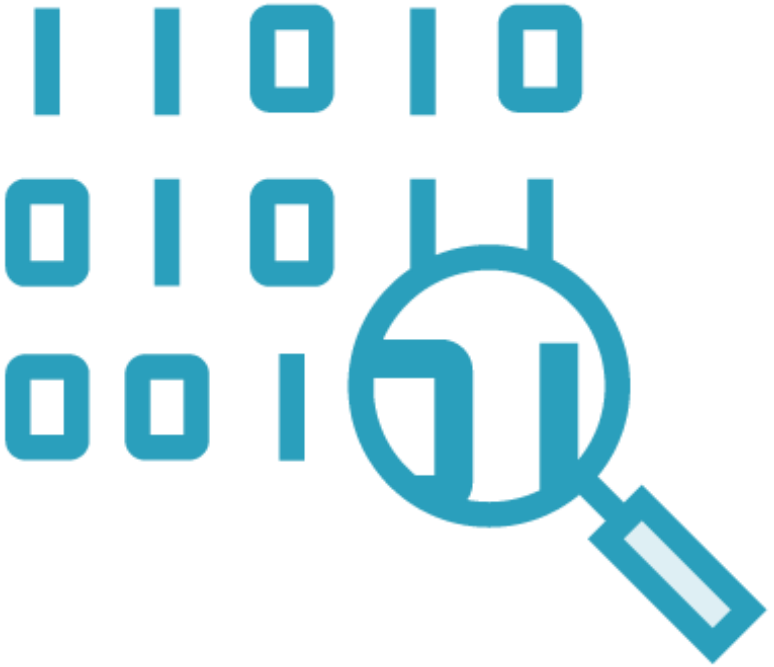


Troubleshooting with ARP



Troubleshooting with ARP





Check the ARP protocol if you see:

- Problems connecting to an application
- Intermittent connectivity
- Unicast flooding

Demo

Let's look at ARP in action!

- Learn more about how ARP works
- Create a profile
- Remove ARP from traces