Using Wireshark to Analyze Core Services - UDP, DHCP, and DNS

Chris Greer
NETWORK ANALYST

@packetpioneer www.packetpioneer.com

Module Overview

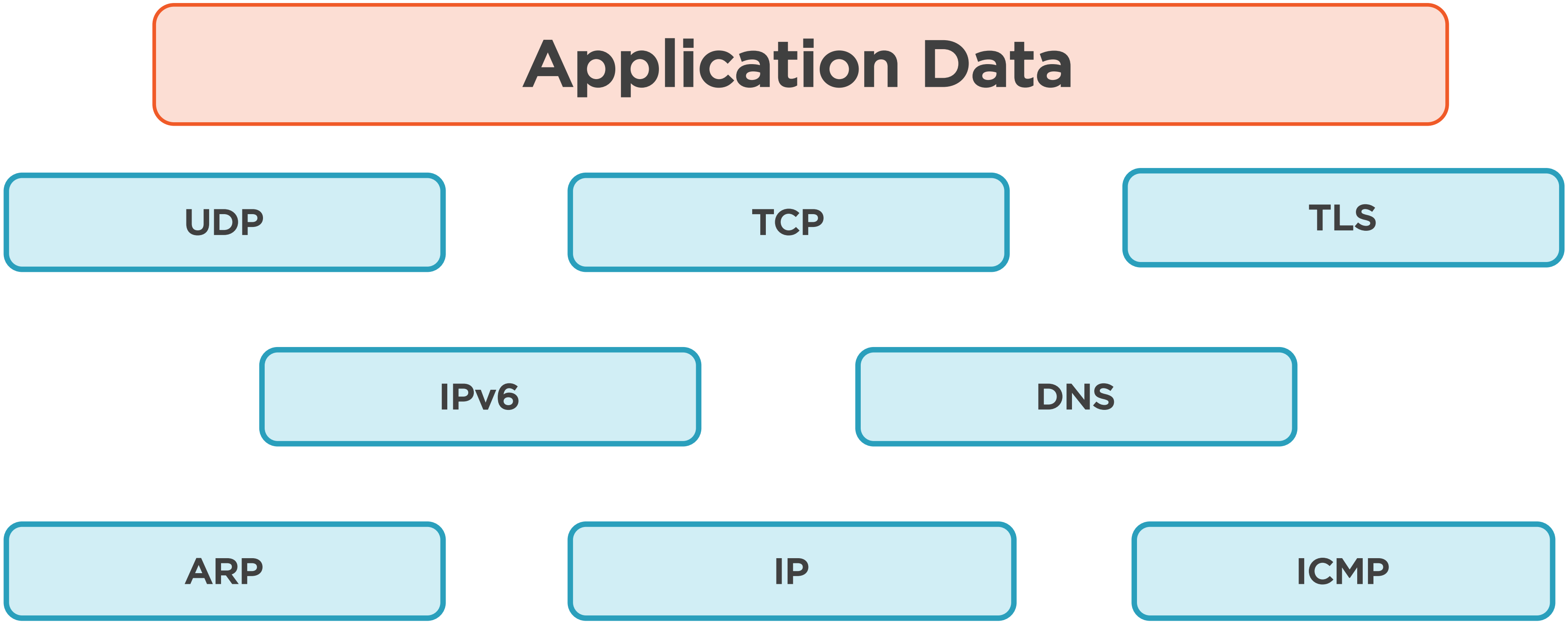
Let’s talk UDP

- Connectionless communication

Analyzing DHCP

Analyzing DNS

Core Protocols - UDP



Application Data

UDP

TCP

TLS

IPv6

DNS

ARP

IP

ICMP

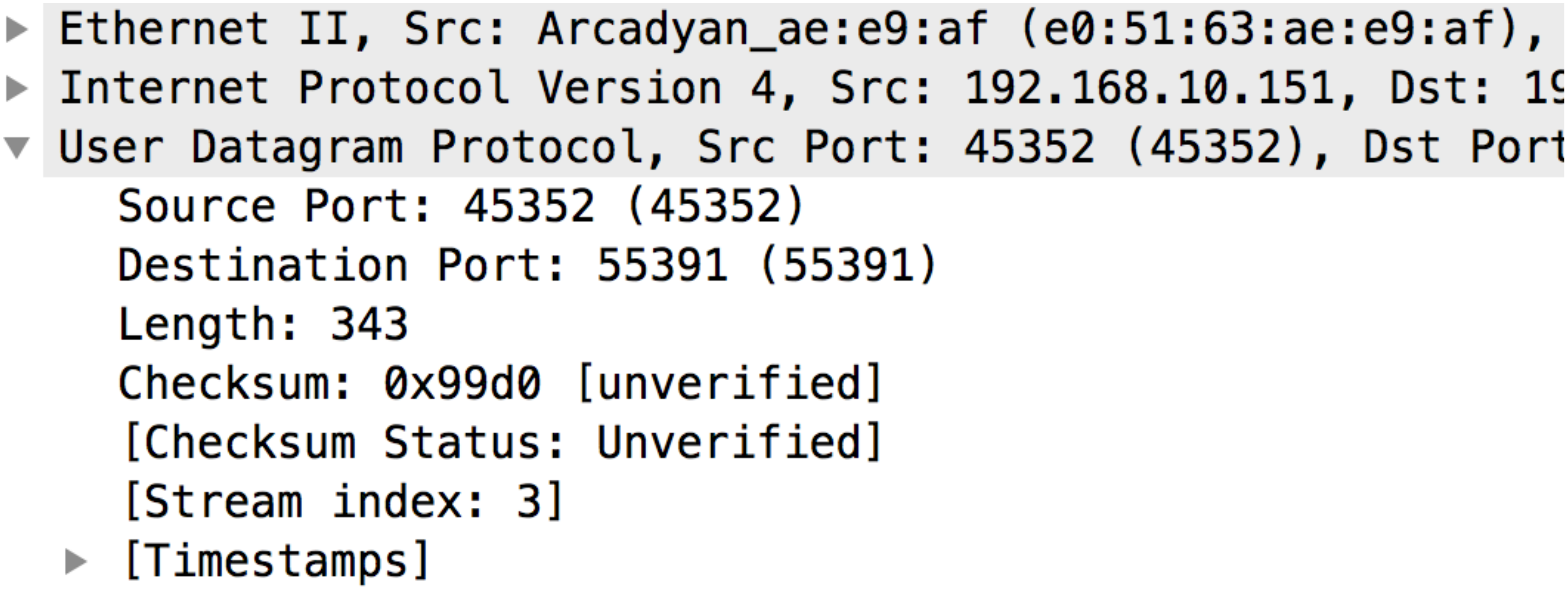
The User Datagram Protocol

No connection necessary

Time sensitive applications

Simple – no options

The UDP Header



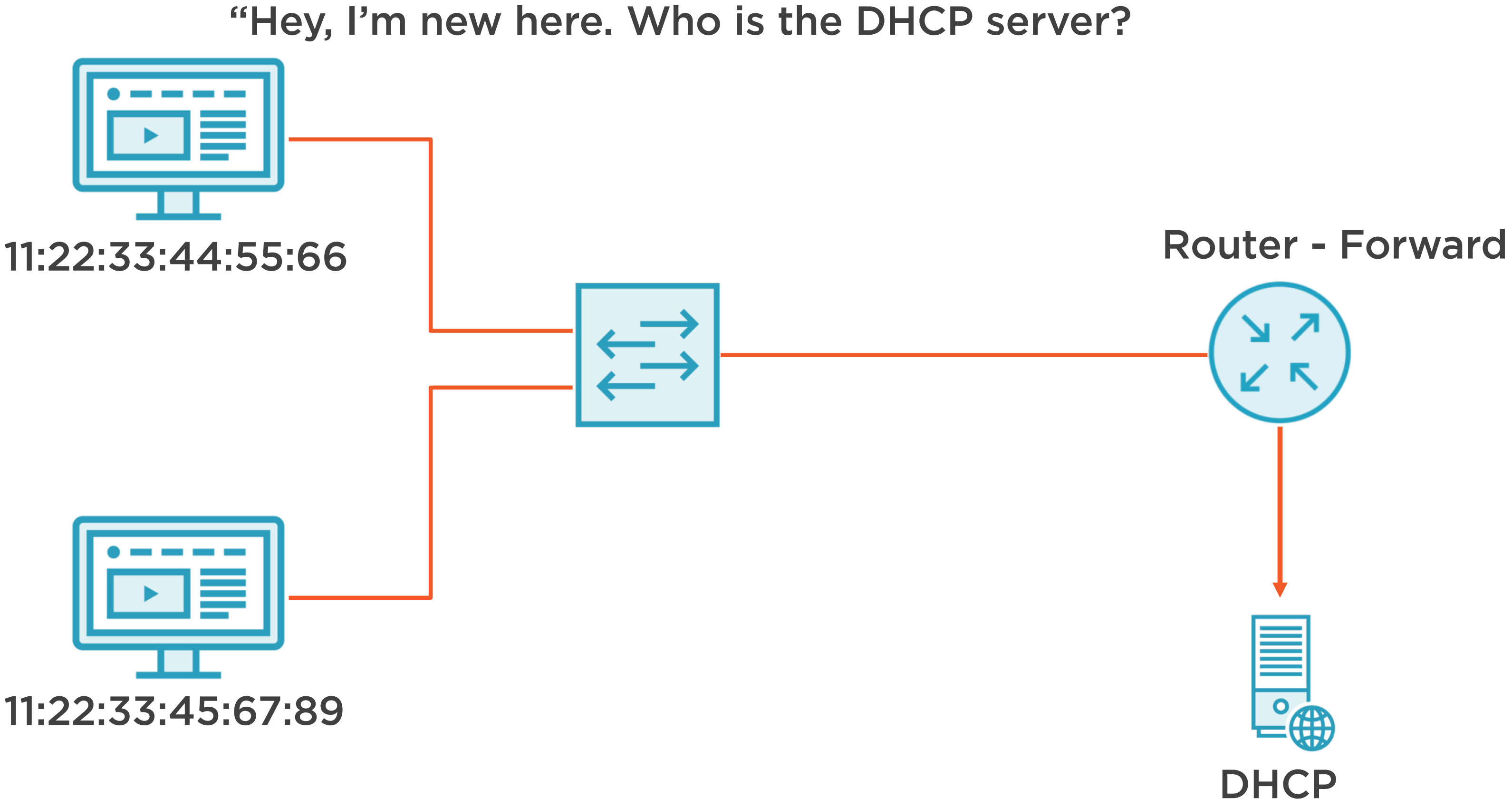
```
▶ Ethernet II, Src: Arcadyan_ae:e9:af (e0:51:63:ae:e9:af),
▶ Internet Protocol Version 4, Src: 192.168.10.151, Dst: 19
▼ User Datagram Protocol, Src Port: 45352 (45352), Dst Port
     Source Port: 45352 (45352)
     Destination Port: 55391 (55391)
     Length: 343
     Checksum: 0x99d0 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 3]
  ▶  [Timestamps]
```

Demo

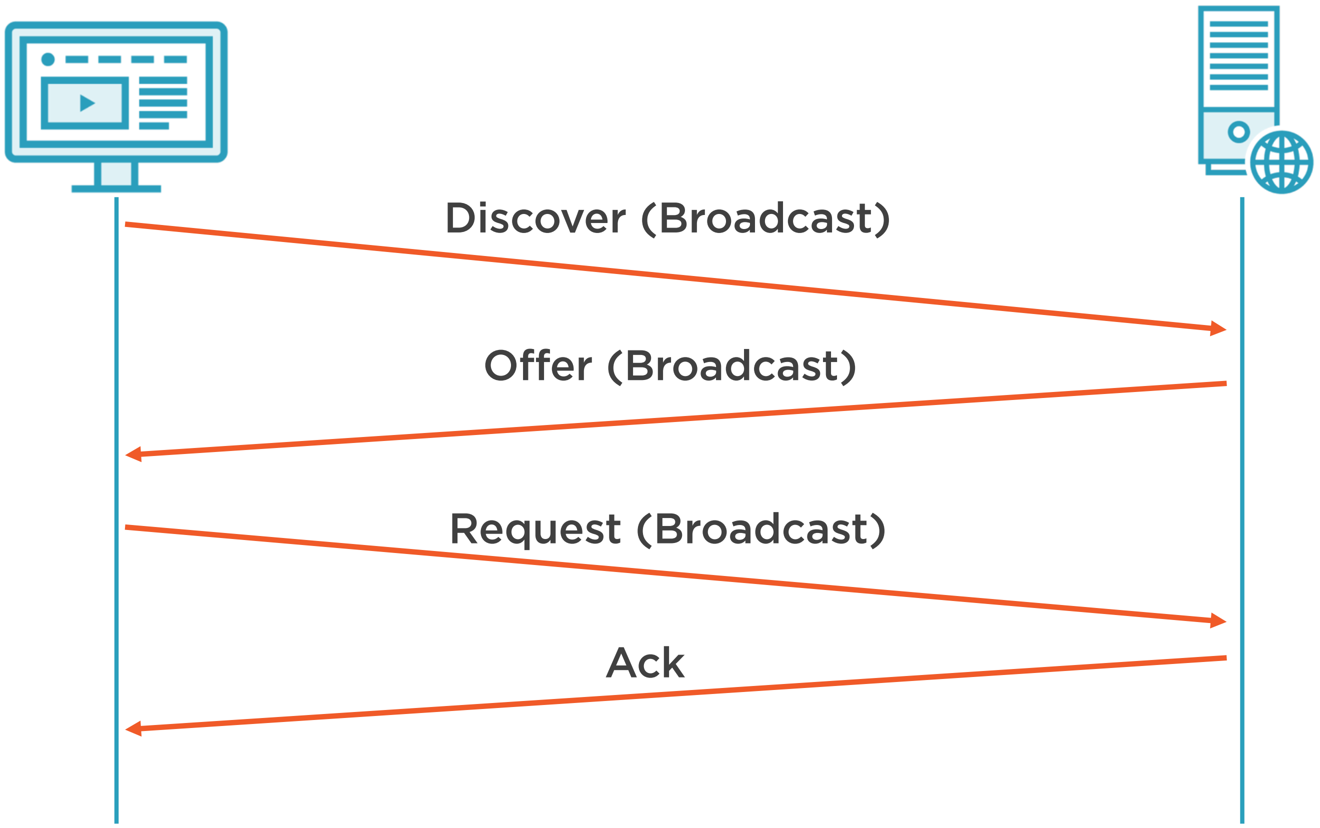
Analyzing UDP with Wireshark

The DHCP Protocol

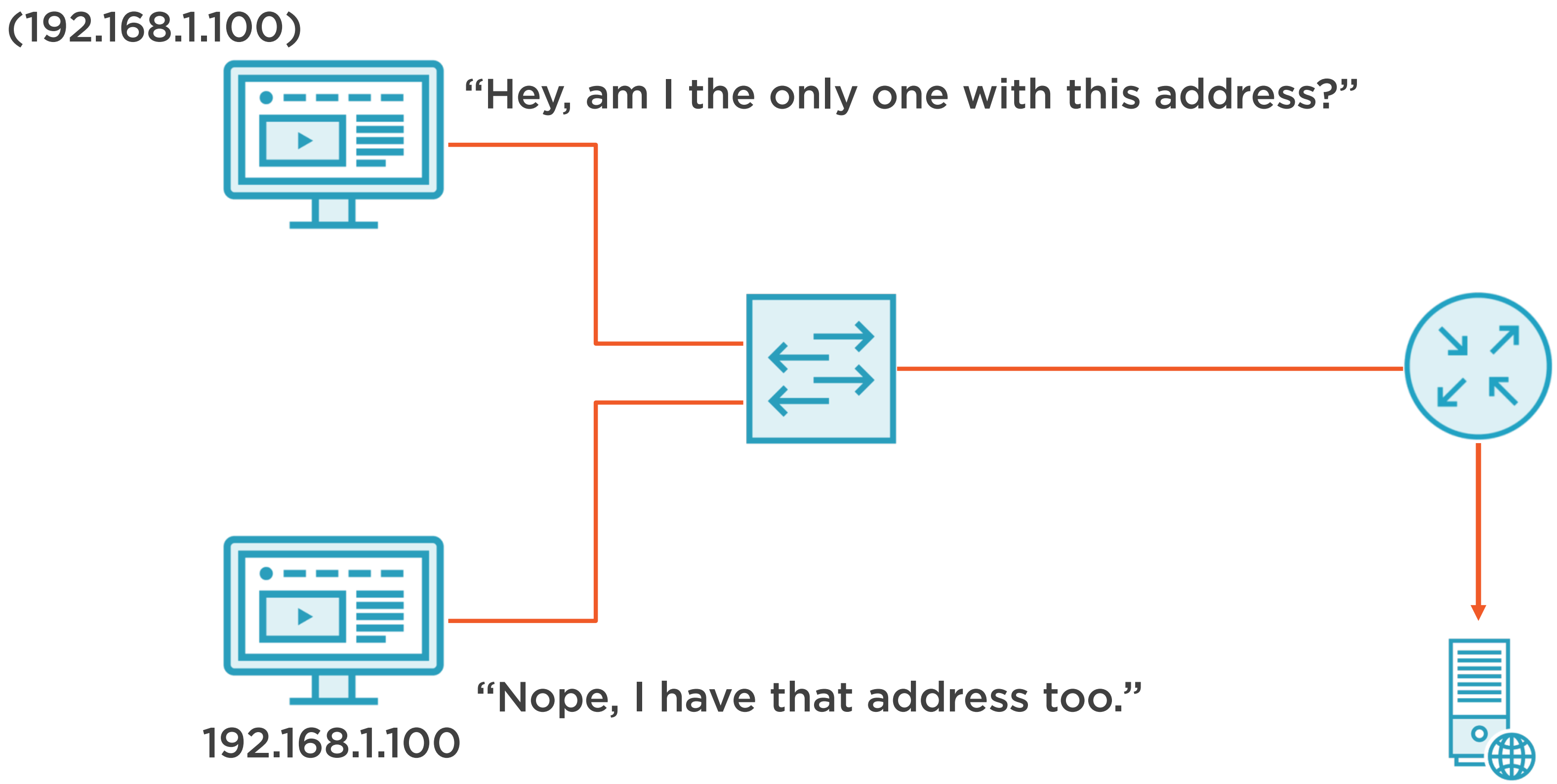
Dynamic Host Configuration Protocol



Dynamic Host Configuration Protocol



Dynamic Host Configuration Protocol



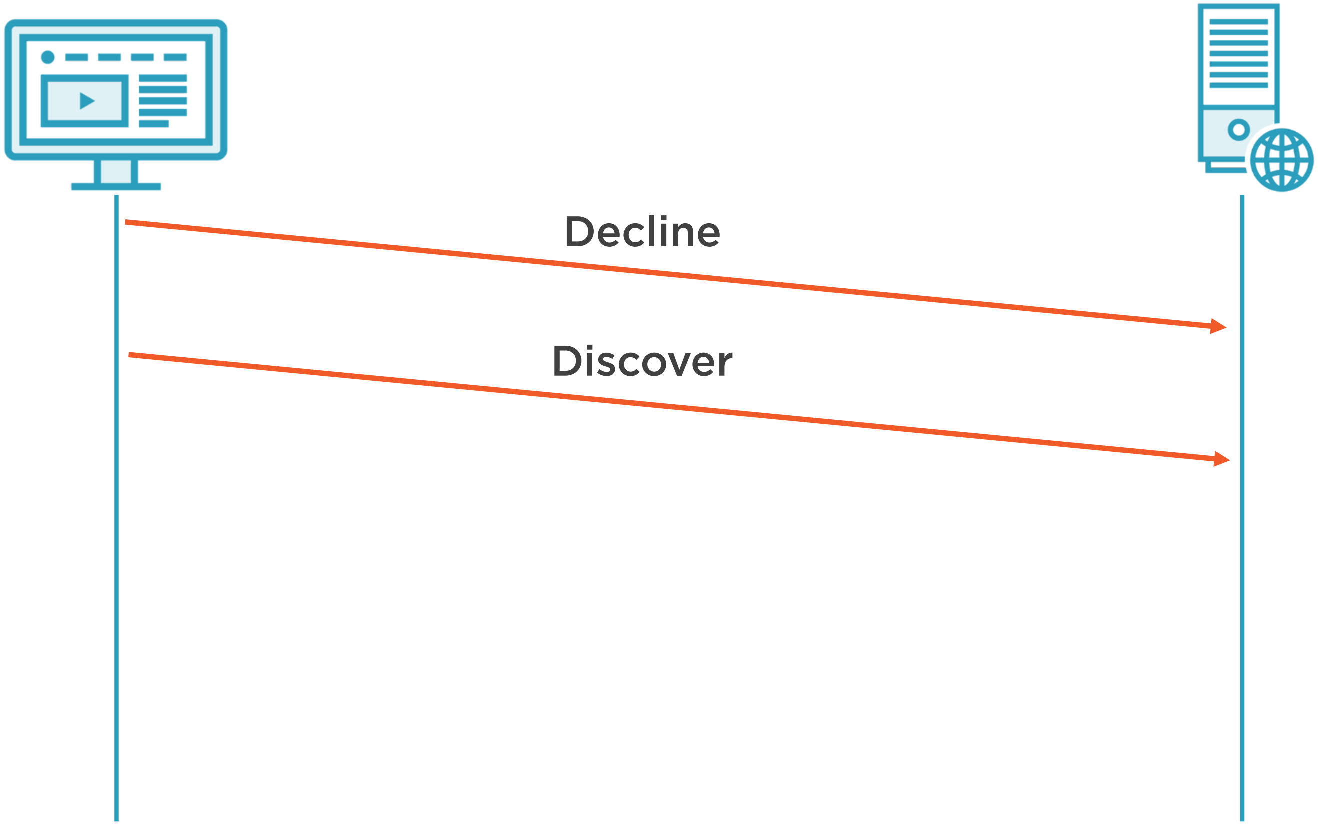
(192.168.1.100)

“Hey, am I the only one with this address?”

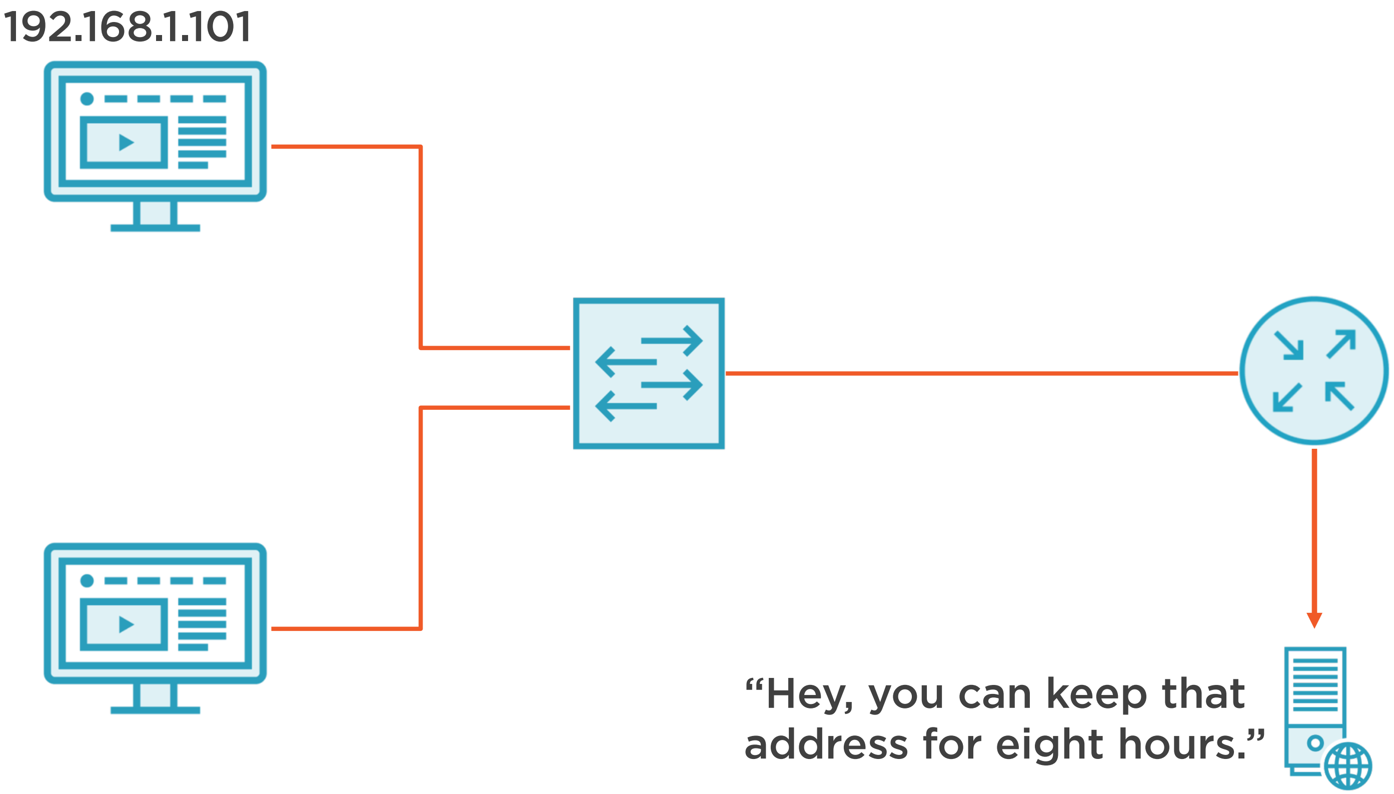
“Nope, I have that address too.”

192.168.1.100

Dynamic Host Configuration Protocol



DHCP Lease



"Hey, you can keep that address for eight hours."

Demo

Analyzing DHCP with Wireshark

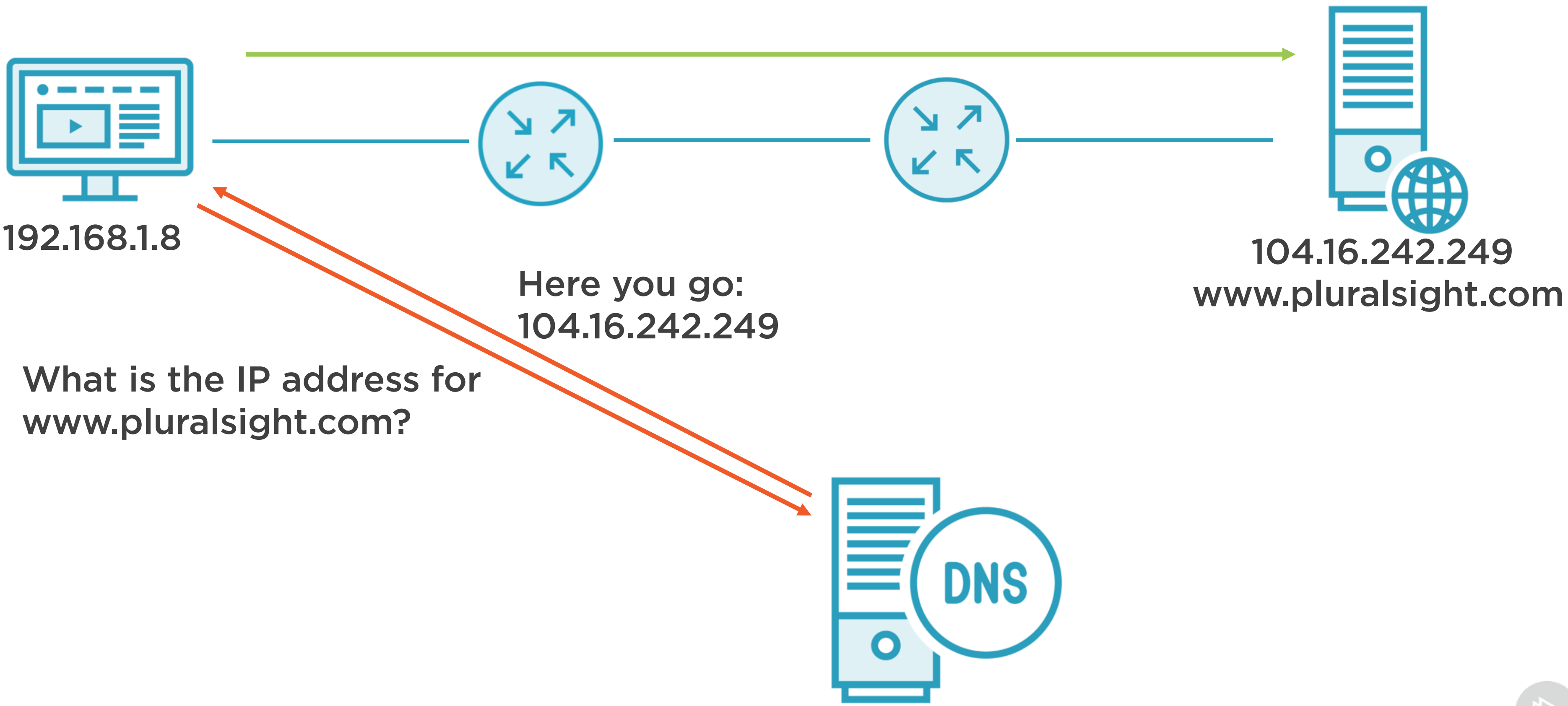
The questions for lab 8 are located in the file comments section of the trace file

Domain Name System

DNS – The Phonebook of the Internet

104.16.242.34

DNS



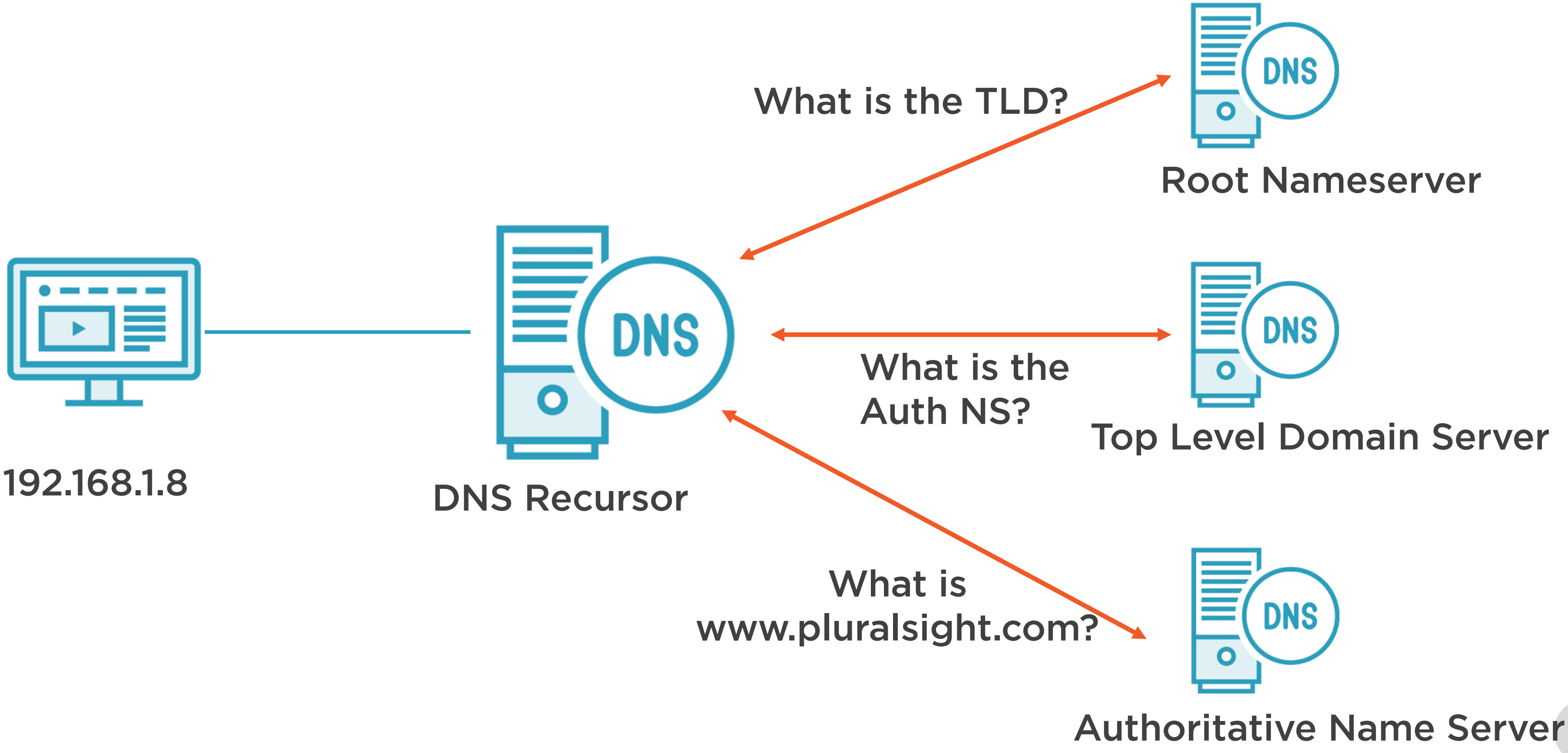
192.168.1.8

Here you go:
104.16.242.249

What is the IP address for
www.pluralsight.com?

104.16.242.249
www.pluralsight.com

DNS on the Back End



Demo

Analyzing DNS with Wireshark