

# Trace File Analysis

Identifying Wire Latency, Client Latency,  
Server Latency

**Laura Chappell**

Founder | Wireshark University

**SHARKFEST '08**

Foothill College

March 31 - April 2, 2008

# *TurboCap*

**Full  
Speed**

**Traffic TAP**

**1 Gb**

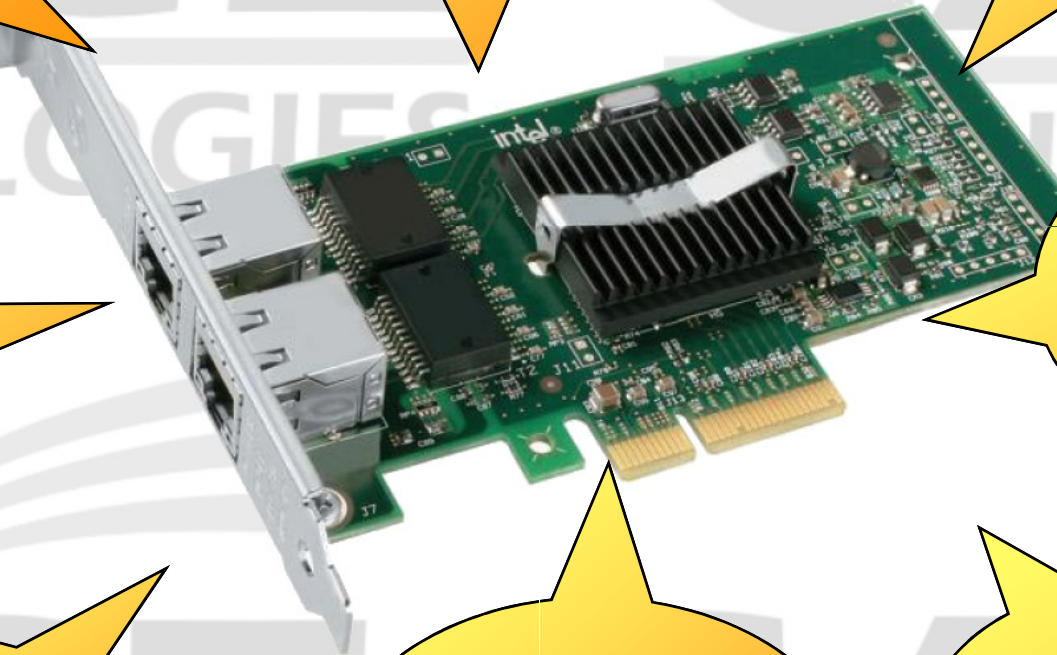
**2  
Copper  
ports**

**Capture  
and  
Injection**

**Wireshark**

**Aggregation**

**WinPcap**

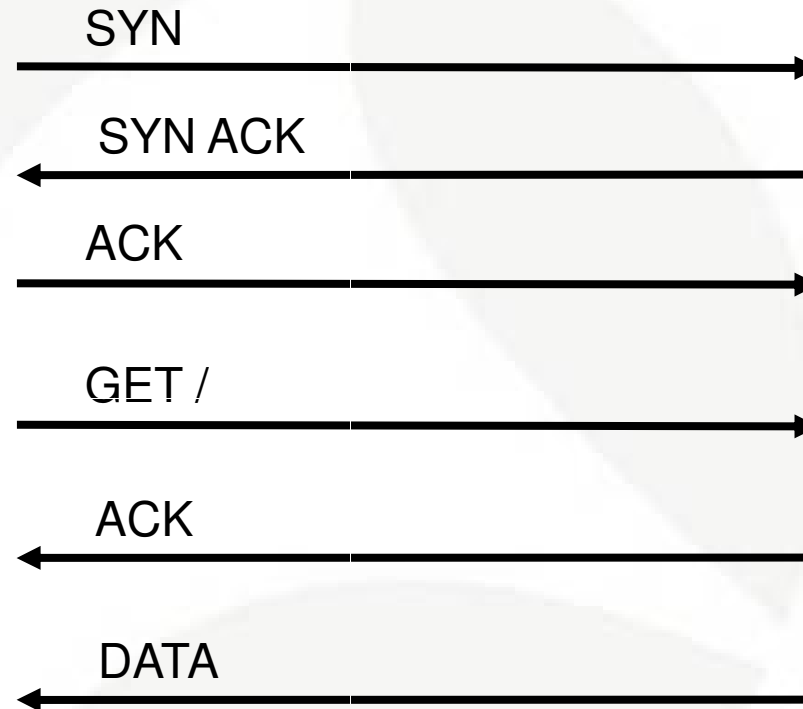


# Analyzing Network Performance Issues

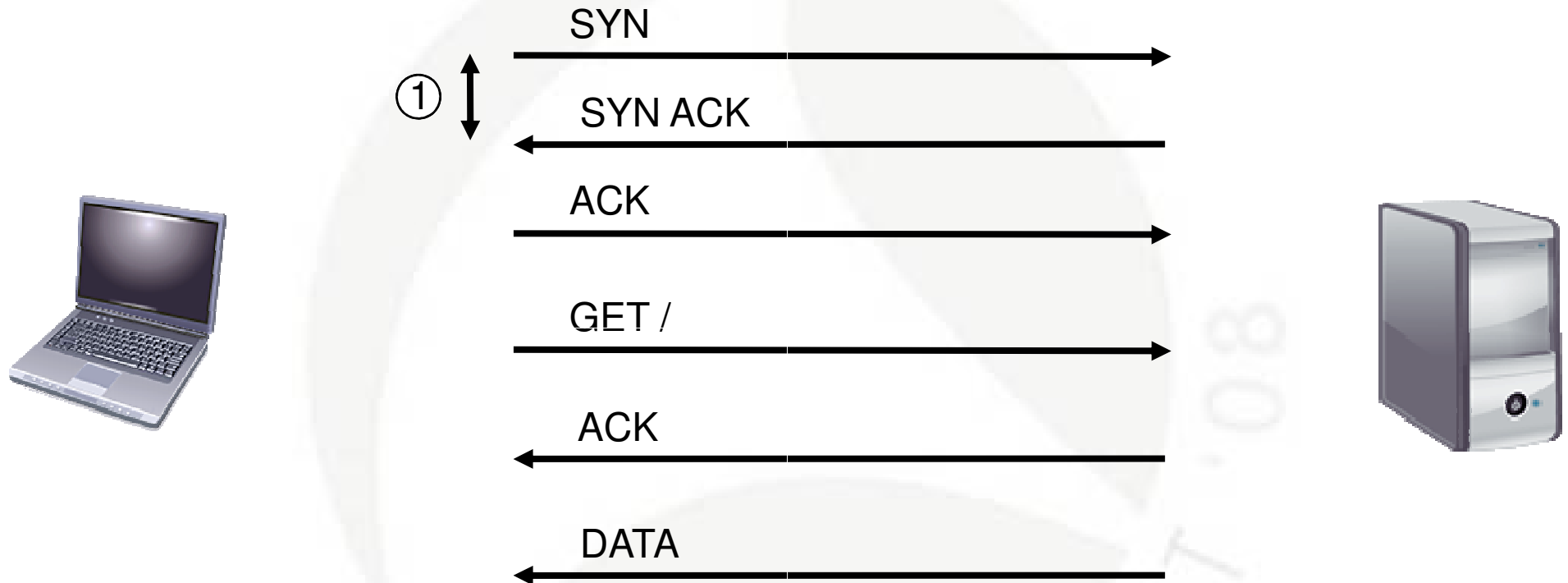
## Key Issues:

- High Latency (Client, Server, Link)
- Packet Loss (Upstream, Downstream)
- Congestion (Network, Receiver)
- Configuration Problems (Service Unavailable, Loops)
- Redirections (Routing, Service)
- Interdependencies (Third Parties)
- Low throughput (Itty-Bitty Stinkin' Packets)
- Negotiation Faults (Protocol or Application Layer)

# Wire Latency - Client Latency - Server Latency

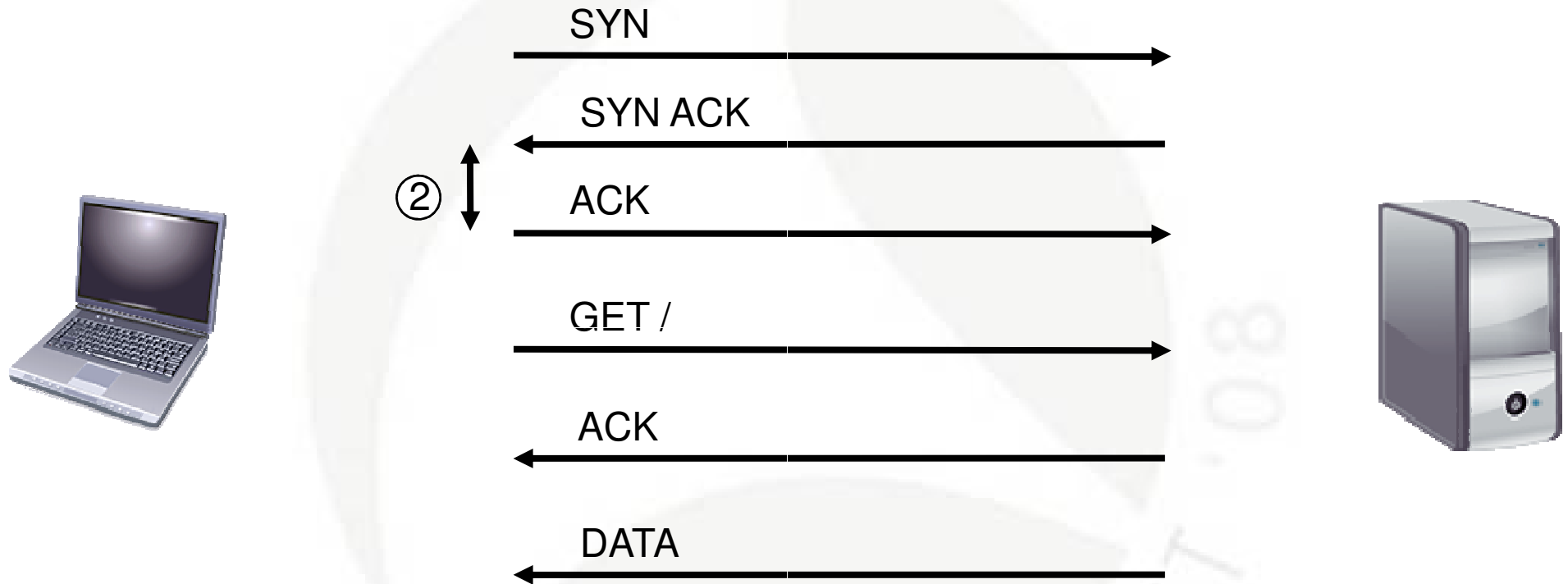


# Wire Latency - Client Latency - Server Latency



1 Time between the SYN and SYN ACK indicates the roundtrip wire latency time and processing through the TCP/IP stack to establish a connection. If this takes a long time on average, consider looking at links and devices along the network path that might be introducing latency.

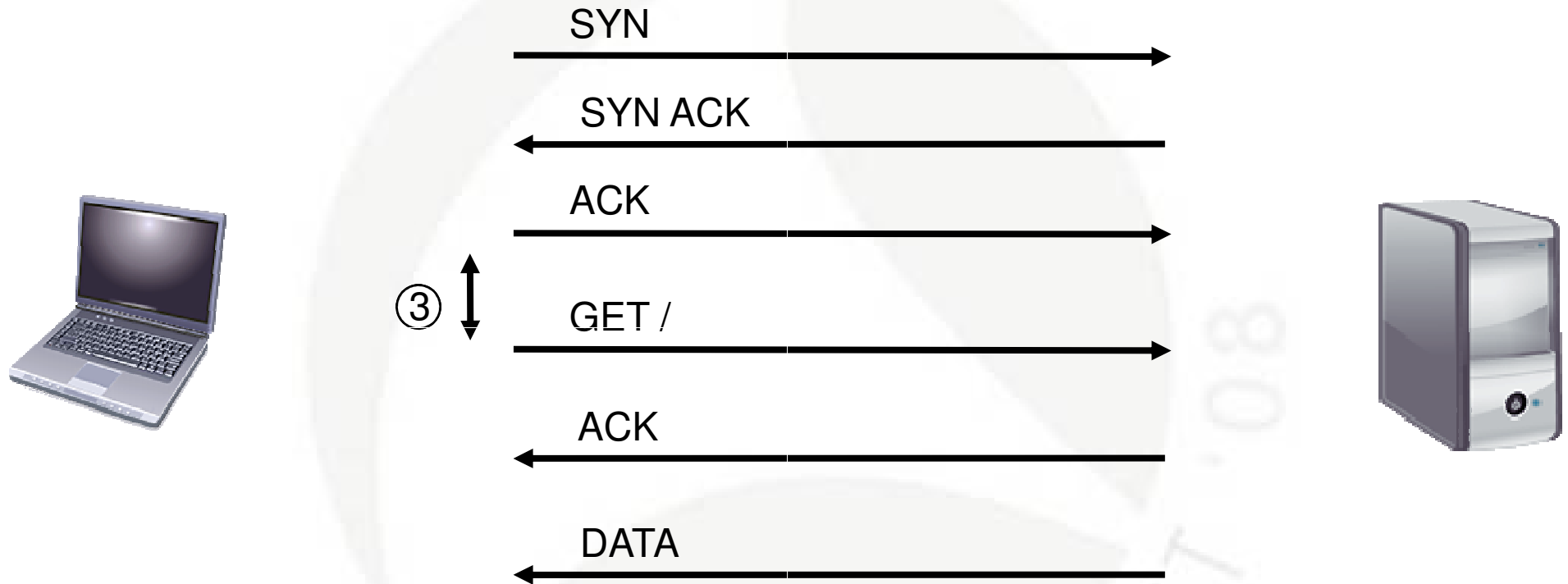
# Wire Latency - Client Latency - Server Latency



2

Time between the SYN ACK and the ACK indicates the speed of the client in responding – this only relates to the client's TCP/IP stack, not their ability to process applications.

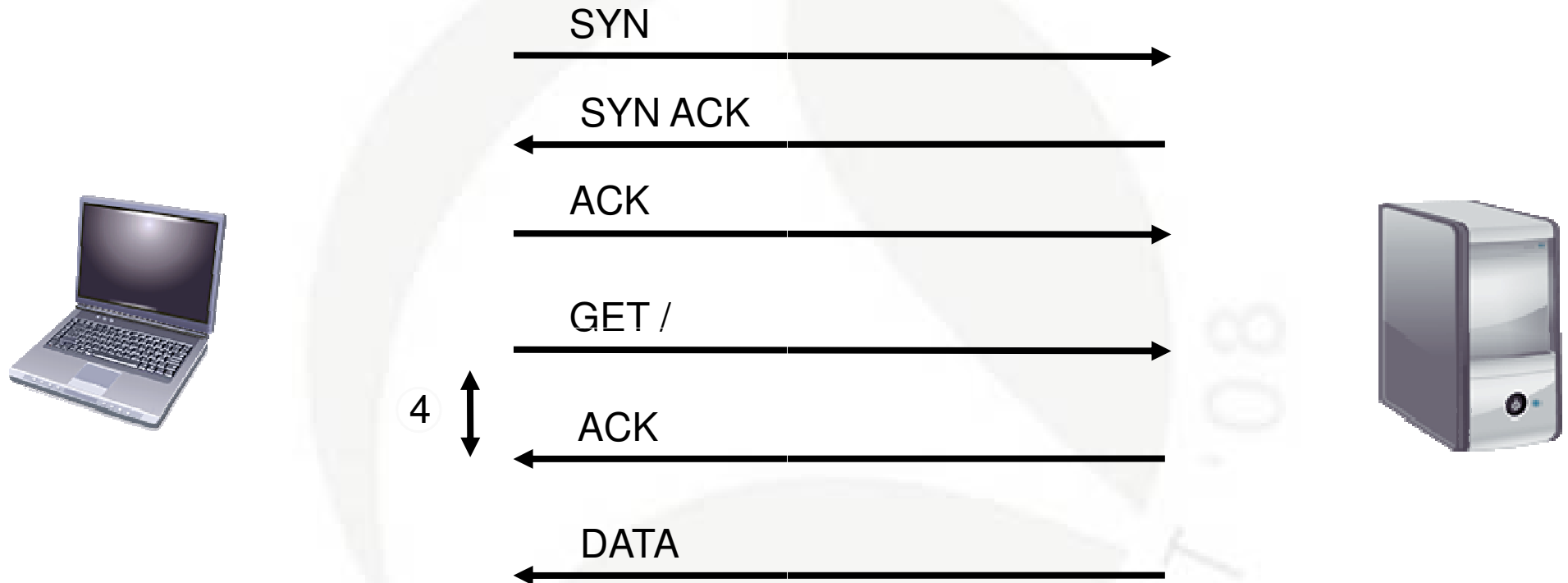
# Wire Latency - Client Latency - Server Latency



3

Time between the ACK and the GET command (or whatever command is sent next) indicates the speed of the client's application to make requests. Applications typically make an immediate request to the server upon completion of the TCP handshake process. (Exception – applications that wait for a server to send data first – FTP, for example – the client waits for the banner.)

# Wire Latency - Client Latency - Server Latency

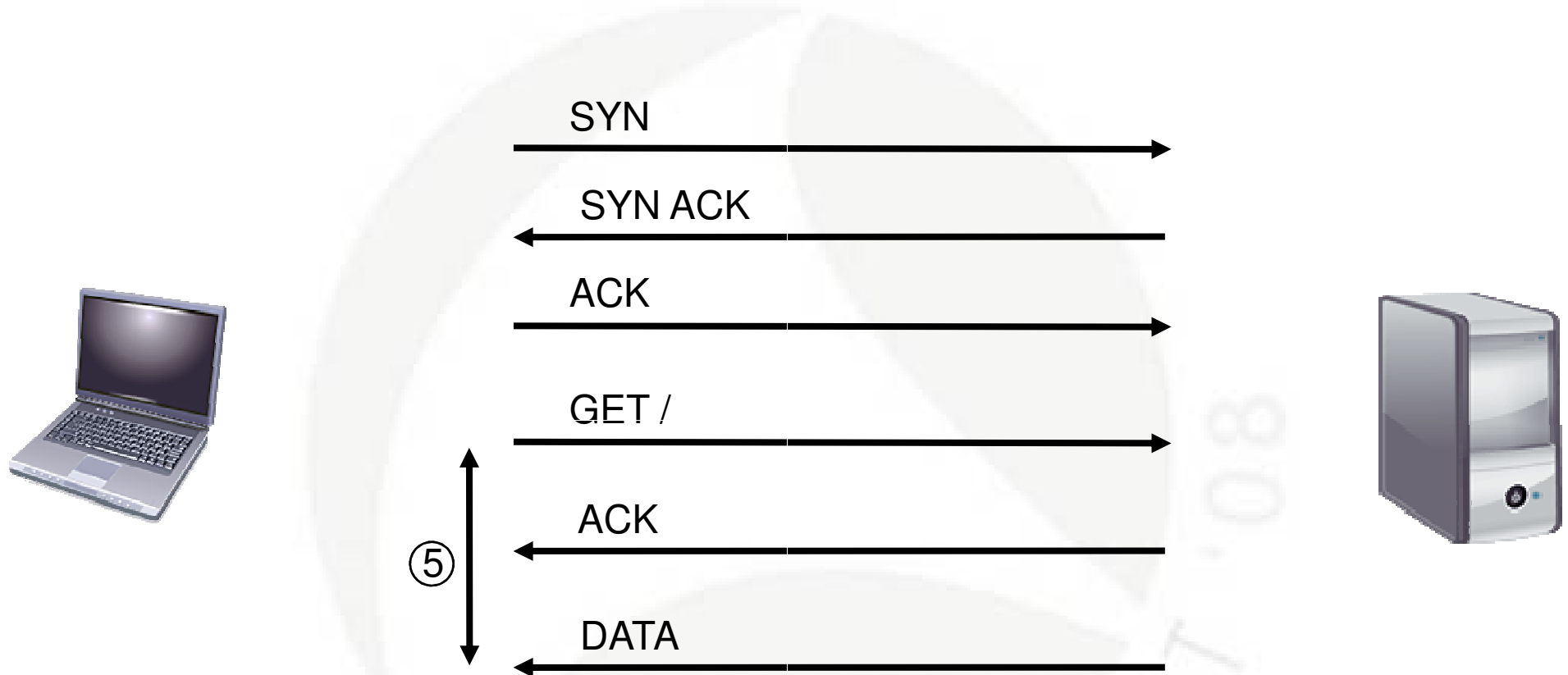


4

Time between the GET command and the ACK indicates wire latency again. If this takes a long time, then look at the network path again.



# Wire Latency - Client Latency - Server Latency



5

Time from the GET command to the actual return of data indicates the time required by the server to process the request and get the data back to the client. If this time value is high (but #4 is low), then we'd look at the server as the slow one in this connection.

# Lab: Latency

**Issue:** downloads take too long

**File:** download-bad.pcap

Review the handshake process and evaluate the time between:

- SYN and SYN ACK \_\_\_\_\_ ms
- SYN ACK and ACK \_\_\_\_\_ ms
- GET and related ACK \_\_\_\_\_ ms
- ACK and data requested \_\_\_\_\_ ms

At this point, where does the latency problem appear to be located? Server? Client? Wire?

# Lab: Latency

**Issue:** downloads take too long

**File:** anotherlousyhotelnetwork.pcap

Review the handshake process and evaluate the time between:

- DNS query \_\_\_\_\_ ms
- DNS response \_\_\_\_\_ ms
- SYN and SYN ACK \_\_\_\_\_ ms
- SYN ACK and ACK \_\_\_\_\_ ms
- GET and related ACK \_\_\_\_\_ ms
- ACK and data requested \_\_\_\_\_ ms

At this point, where does the latency problem appear to be located? Server? Client? Wire?

# What's Next?

Laura's Lab Kit v9

In show bags as well as...

ISO image: [www.novell.com/connectionmagazine/laurachappell.html](http://www.novell.com/connectionmagazine/laurachappell.html)

