

AP/ITEC 2210 3.0 A: System Administration Fall 2023

Instructor: Jamon Camisso

ITEC 2210 Chat: mattermost.itec2210.ca

Email: jamon@yorku.ca

Website: <https://eclass.yorku.ca/>

Date/Time: Wednesday, 19:00-22:00

Location: Zoom / ACE 003

Office hours: Via Mattermost any time

Lecture 1 - Effective Troubleshooting

- Readings:
 - SRE chapter 12 - Effective Troubleshooting
 - PSNA chapter 29 - Debugging
- Why start the course with troubleshooting?
- Provides a systematic approach to thinking about an unknown problem, system, application, etc.
- Essential skill in system administration, but applies everywhere. Framework for general problem solving

Lecture 1 - Effective Troubleshooting

- SRE provides a framework for troubleshooting
 - **Receive** problem report, detect problem, get paged...
 - **Triage** the issue
 - **Examine** components involved in the system(s)
 - **Diagnose** each step of a process
 - **Test** and treat until the issue is isolated
 - **Cure** (fix) the issue
- PSNA describes two specific methods: **elimination** and **successive refinement/addition**

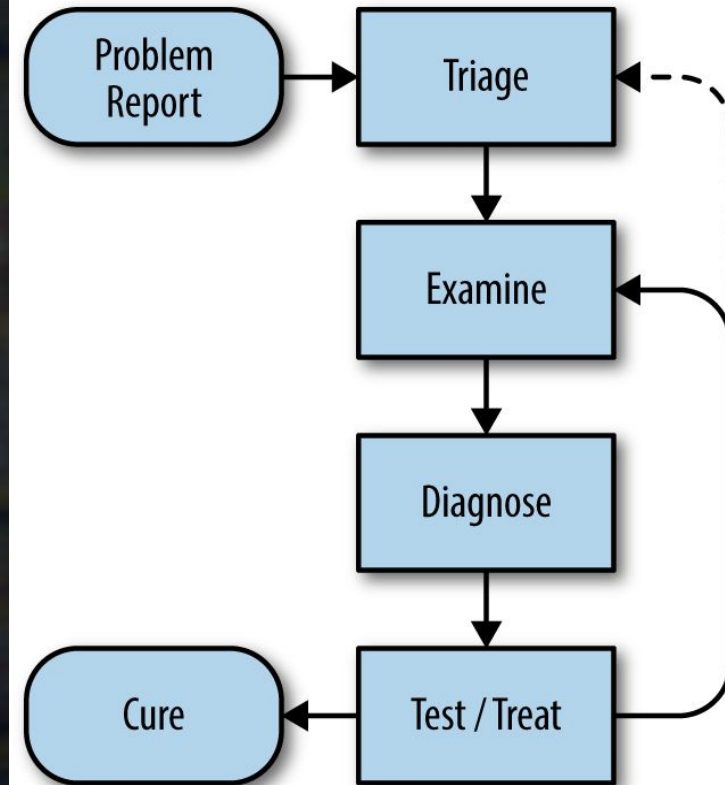
Lecture 1 - Effective Troubleshooting

- SRE notes a few common troubleshooting pitfalls:
- **Irrelevant** information, leads to wild goose chases
- **Incorrect** understanding of how to change a system, safely test, and isolate changes
- **Improbable** theories and recency bias
- Diving into a **falsely correlated** but contemporaneous issue that has arisen

Lecture 1 - Effective Troubleshooting

Problem report should contain:

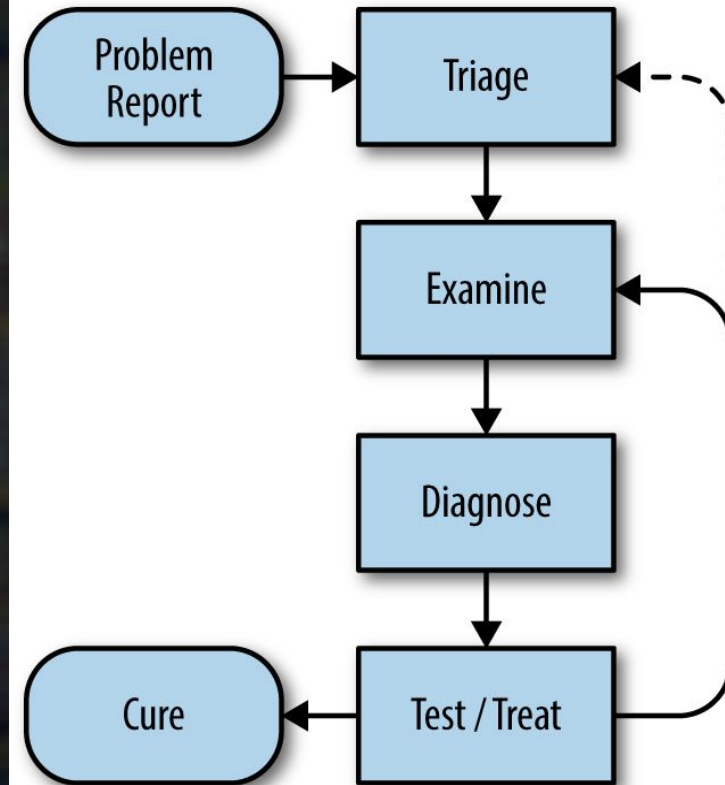
- **Expected** behaviour
- **Actual** behaviour
- **Reproduction** steps (EAR)
- Nice to have: any debugging that has already been performed*



Lecture 1 - Effective Troubleshooting

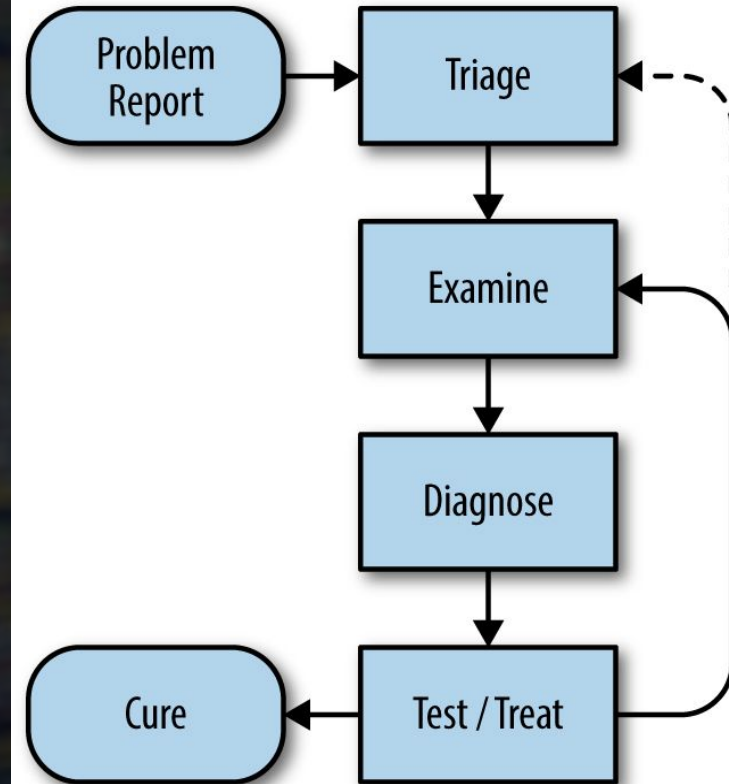
Problem report - as simple as:

- “I should be able to browse the corporate wiki”
- I get a 503 gateway error when browsing the site
- Visit `http://<foo>` in a browser, cURL etc



Lecture 1 - Effective Troubleshooting

- Effective triage
- Who is affected?
- What is affected?
- How widespread is the issue? Is it business critical?
- Save asking 'why' for last until the problem is fully understood



Lecture 1 - Effective Troubleshooting

- Effective **triage** continued
- SRE notes: *“Make the system work as well as it can under the circumstances”*
- Once things are as stable as they can be, move on to next step, **examining** the affected systems
- Make sure to record any steps taken so they can be reverted, automated, documented for later analysis or reuse

Lecture 1 - Effective Troubleshooting

- **Examining** the systems involved
- Look at log files, assume there's always a log *somewhere*
- Start at the beginning. For example, a cURL HTTP request:
 - Look at a full request to a front-end server
 - Find a corresponding request to a backend server
 - Trace a backend application request to a fileserver
 - Each system will/should/hopefully log the request

Lecture 1 - Effective Troubleshooting

- **Examining** the systems involved
- Some tools that will be useful (not exhaustive):
 - cURL/wget for debugging HTTP requests
 - netcat/nc to make and test TCP connections
 - lsof & strace to examine what a process is doing
 - netstat & tcpdump to gather network data and dumps
 - top, free, ps, vmstat to see what a server is doing
 - less/more/view to examine a file without editing it
 - vi, vim, nano, pico, emacs to edit a file (or view it)

Lecture 1 - Effective Troubleshooting

- **Diagnose** the issue
- Narrow things down using a combination of **elimination** and **successive refinement** (PSNA p532), or **bisection** (SRE p140)
- **Elimination**: remove different parts of the system until the problem disappears. The problem must have existed in the last portion removed
- Sometimes elimination is easy, for example toggle a setting somewhere. Sometimes it will require code changes.

Lecture 1 - Effective Troubleshooting

- **Diagnose** the issue
- **Successive refinement** can be as easy as connecting to systems one at a time in sequence until the problem system is reached
- Or it can involve hardware, firewalls, network settings, databases, file servers, authentication servers and so on
- Proceed one step at a time from a known good configuration until breakage occurs - the last change must be the culprit

Lecture 1 - Effective Troubleshooting

- **Diagnose** the issue
- **Bisection** is a way to subdivide components into groups and then eliminate or successively refine within a grouping
- Imagine you have a set of firewalls, TCP load balancers, routers and hardware switches, connected to a pool of HTTP servers and databases, and the issue is HTTP related
- Chances are you don't want to start with tcpdump, rather, you'd look at frontend HTTP servers and trace requests

Lecture 1 - Effective Troubleshooting

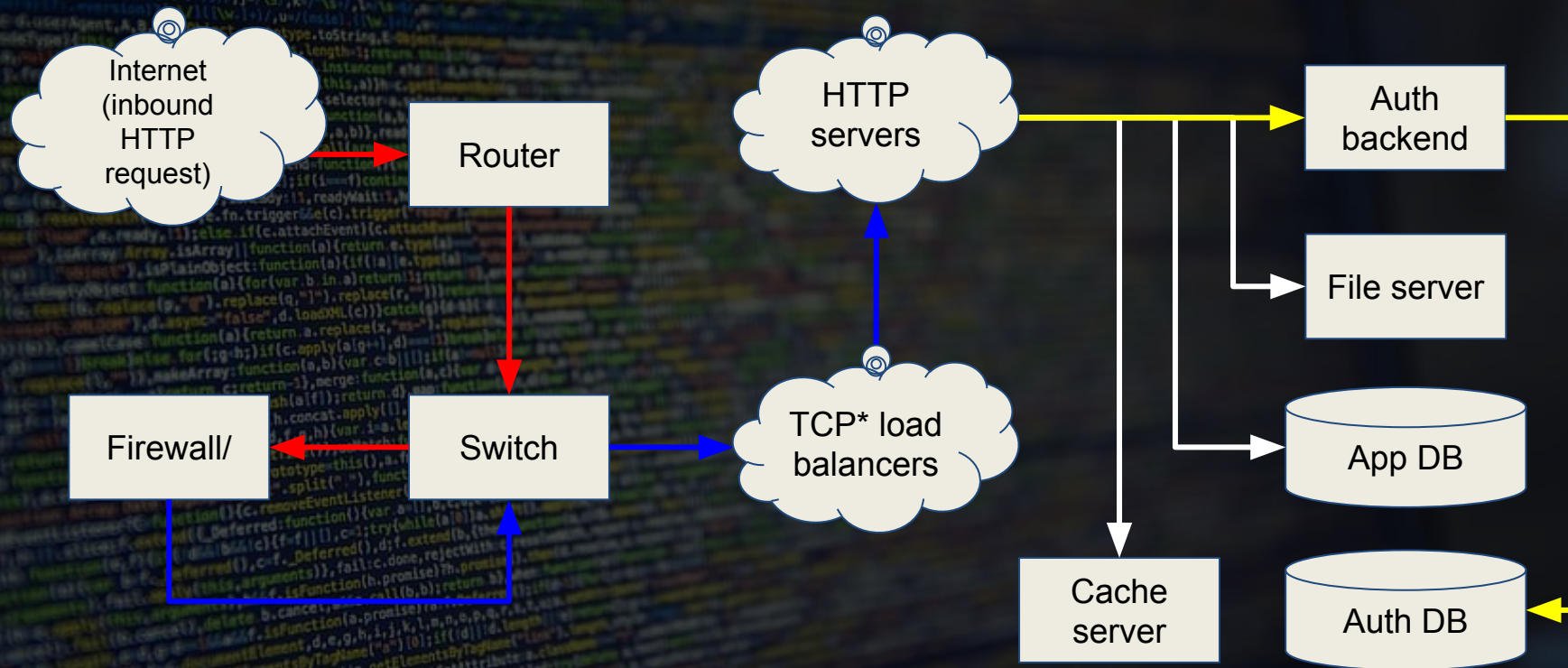
- **Test and Treat** the issue

- Try designing tests to rule out one set of hypotheses and rule in another. In the HTTP scenario, **bisect**, then **eliminate**:

- Test HTTP requests first to rule out TCP issues. In the router/switch/firewall components of the made up architecture, packets must be flowing to HTTP servers

- Now test TCP connections from HTTP servers to Auth, Cache then File server and see which isn't reachable

Lecture 1 - Effective Troubleshooting



Lecture 1 - Effective Troubleshooting

– Example

- **Problem report** could be as simple as a chat message from a developer: “I can’t access `http://10.0.0.1` here’s a screenshot from my browser.”
- Depending on the data in the screenshot you’d bisect infrastructure for troubleshooting appropriately
- Could be firewall level, client side, HTTP servers

Lecture 1 - Effective Troubleshooting

– TCP issue?

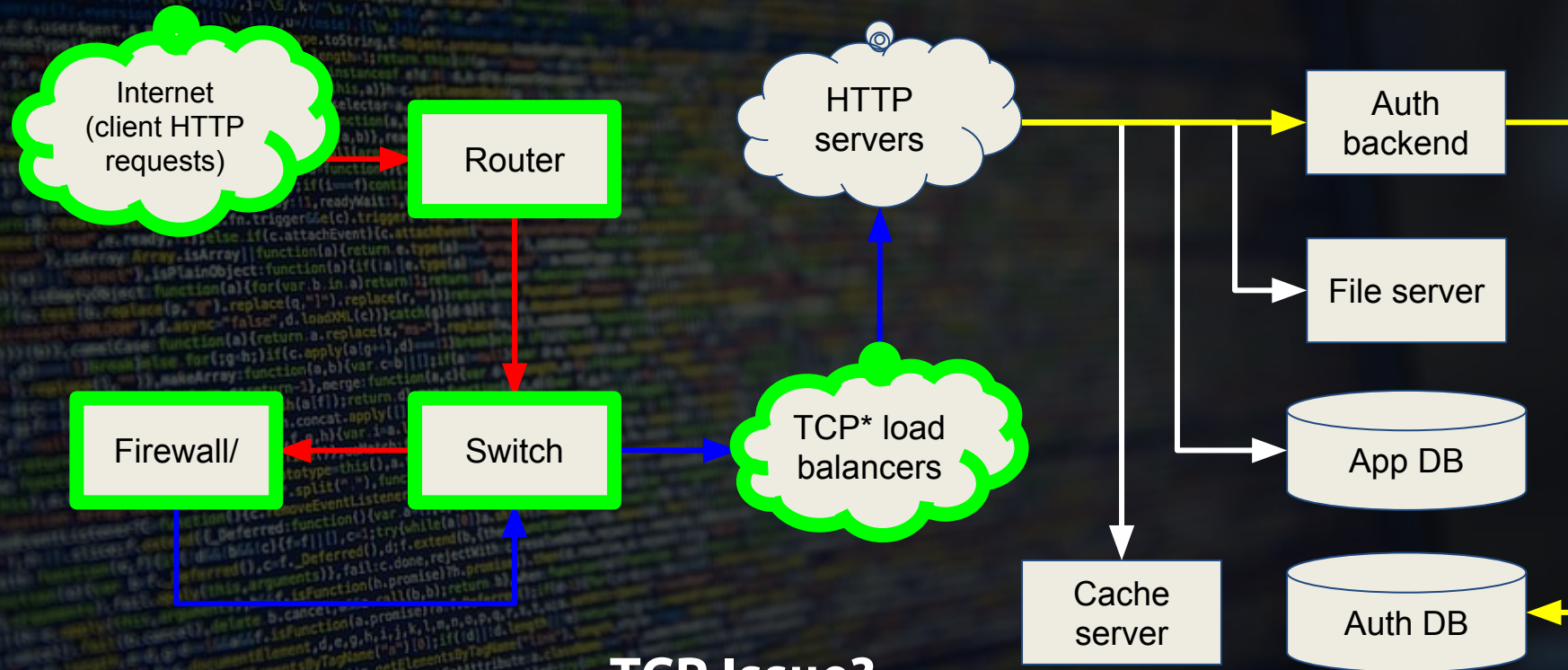
Unable to connect

Firefox can't establish a connection to the server at 10.0.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Nightly is permitted to access the Web.

Try Again

Lecture 1 - Effective Troubleshooting



TCP Issue?

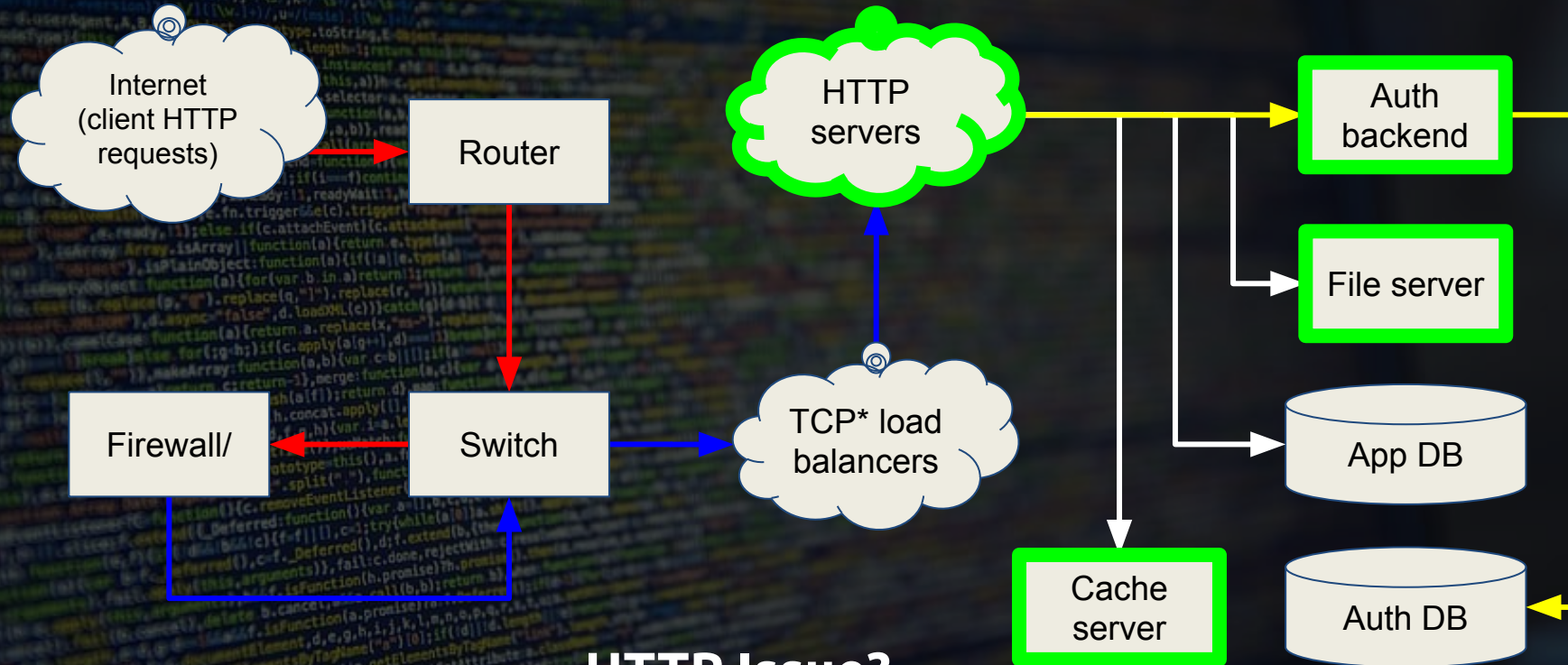
Lecture 1 - Effective Troubleshooting

– HTTP issue?

502 Bad Gateway

nginx/1.10.3 (Ubuntu)

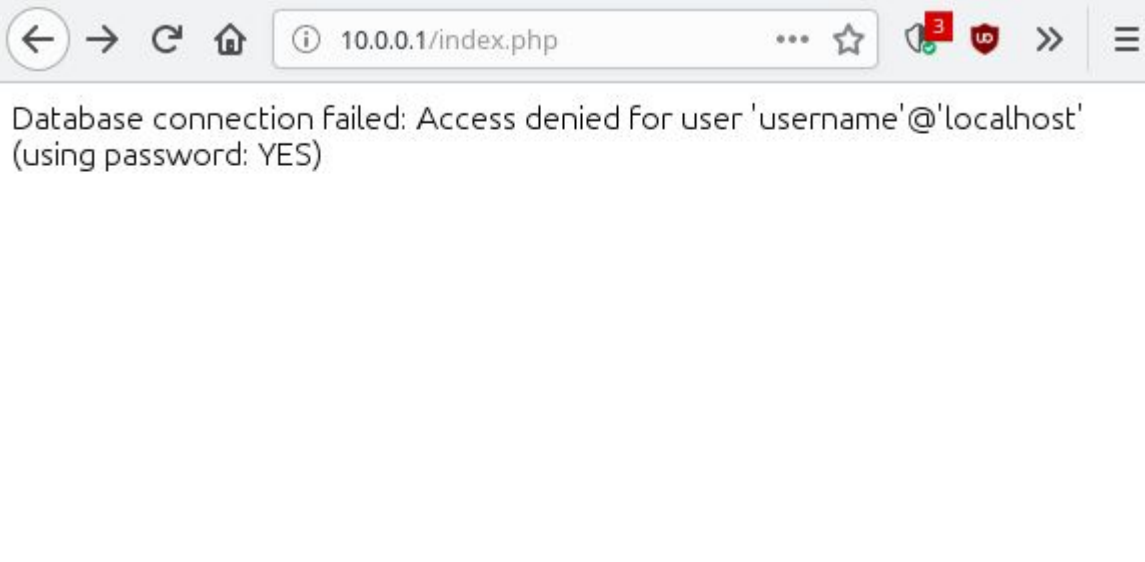
Lecture 1 - Effective Troubleshooting



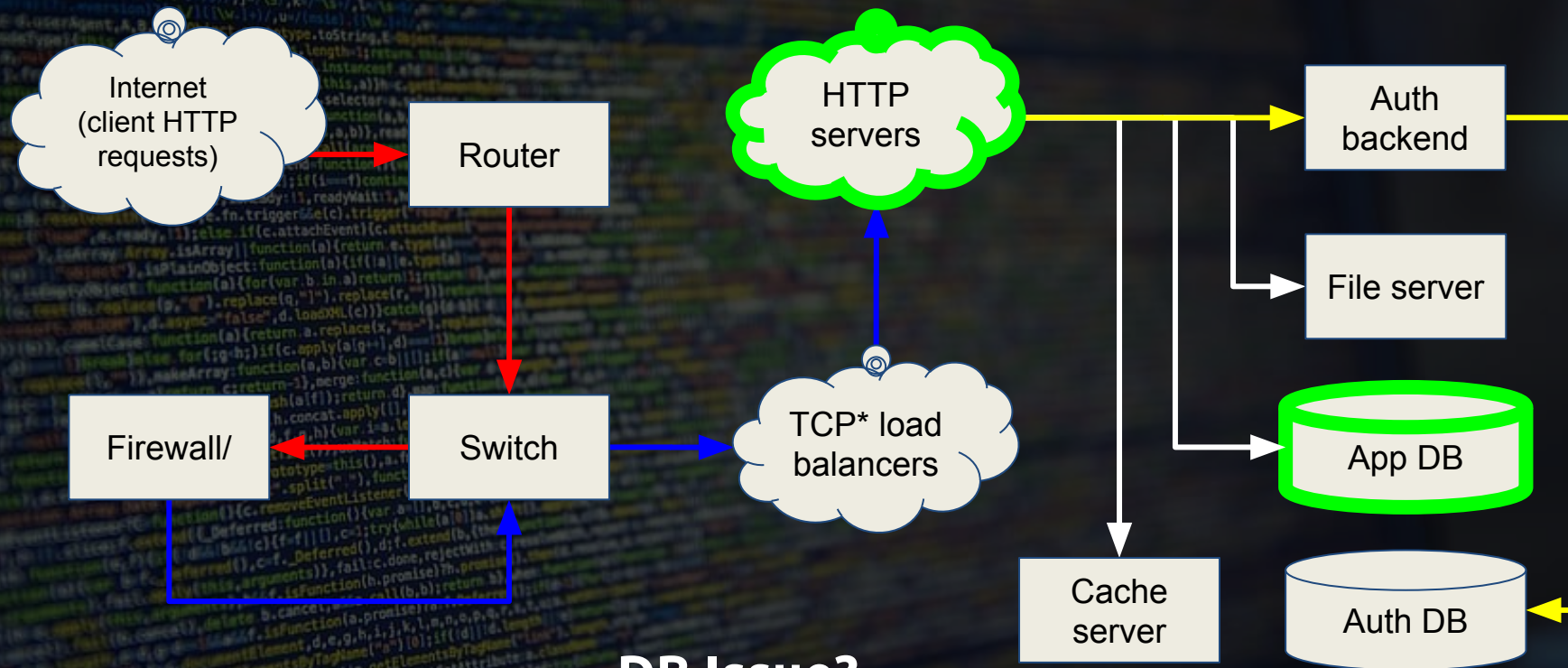
HTTP Issue?

Lecture 1 - Effective Troubleshooting

– DB issue?



Lecture 1 - Effective Troubleshooting



DB Issue?