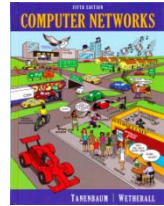


# CN5E Labs – Student README

---



Dear Student:

Welcome to the labs that accompany *Computer Networks*! These hands-on exercises are intended to deepen your understanding of the Internet protocols you are studying. You will examine real-world networks in action by recording packets as they are sent and received, and use a tool called a protocol analyzer to inspect the packets in detail. You can work through these labs either as part of a class-based offering, or on your own. Enjoy!

## Platforms and Tools

**The labs are suited for broad use and can be run on Windows, Mac OS, and Linux platforms.** They have been tested with Windows 7 (Service Pack 1), Mac OS 10.7 (Lion), and Linux Fedora Core 13. We do not recommend that you perform the labs on a virtual machine without testing; it is certainly possible with attention to the network configuration of the virtual machine, but we have not tested this setting.

**The labs target networks with IPv4 connectivity and work whether or not NAT is used to connect the computer to the network.** They have not been tested with connectivity via a VPN or IPv6, though you could readily adapt them to these and other network settings if needed.

**To work across platforms, the labs make use of tools that are widely-used and either installed as part of the operating system or freely-available as downloads.** Inevitably, there are differences between tools on different operating systems, e.g., the `wget` utility for Windows is replaced with the `curl` utility for Mac. We have noted the differences we know about, but you should expect some local variations and be willing to experiment with your tools.

**All of the labs use the Wireshark network protocol analyzer to inspect packet traces.** Different labs also use different tools depending on their purpose. Each lab begins by listing the tools that it uses, a small number of which you may need to install. The tools include: `wget/curl` and your web browser to fetch web pages; `ping` and `traceroute` to probe network paths; operating system utilities such as `ipconfig`, `ifconfig`, `arp`, `netstat` and `route` to check and manipulate the state of your computer's network interface; `telnet` to send and receive interactive traffic; and `dig` to examine the DNS.

## Your Network versus Supplied Traces

**We strongly encourage you to capture your own trace.** By doing so, you will learn about your own network, which is much more satisfying than learning about someone else's network. Each lab provides the instructions you need to capture an appropriate trace for common network scenarios. However, because there are a great many possible network settings it may not always be feasible for you to capture your own trace. Your instructor might also prefer you to use a previously captured trace in a class setting. Thus we also supply standard traces that you can use to complete the labs. Most of the labs can be done offline, with no connectivity, by using the supplied traces.

## Working through the Labs

Each lab covers a different Internet protocol. We suggest you do them in the following order:

1. Protocol Layers. Text §1.3 and §1.4. This is the introductory lab that comes first.
2. Ethernet. Text §4.3.
3. 802.11. Text §4.4.
4. IPv4. Text §5.6.1 to §5.6.3.
5. ICMP. Text §5.6.4.
6. ARP. Text §5.6.4.
7. DHCP. Text §5.6.4.
8. UDP. Text §6.4.
9. TCP. Text §6.5.
10. DNS. Text §7.1.
11. HTTP. Text §7.2.4.
12. SSL/TLS. Text §8.9.

However, the labs are relatively independent, and you may choose different orderings to suit your situation. Individual labs can be skipped, other than any dependencies noted above. They may also be taken “top down” instead of “bottom up” after the introductory lab.

Most labs can be completed in a single sitting, though they are rather long to read. To help the reader, we divide each lab into a series of steps that build on each other and use these formatting conventions:

- *Actions that must be taken are given in italics.* This is the absolute minimum an experienced lab taker must read.
- Examples of input and command-line programs are given in computer font. These are commands you will enter into a terminal window or text you will enter into a program’s user interface.
- Explanatory text that elaborates the instructions in more detail is given as normal text.
- Background material is given in grayed out type. This material includes descriptions of tools and how to use them that is not specific to the lab and may be repeated across labs. Skip it if you are already familiar.

## Solutions

No solutions are provided with the independent study version of the labs because taking them is mostly a self-explanatory experience. In a class setting, tailored solution handouts may be available.

## Feedback

**Please send us tips to streamline these labs for future students based on your experiences.** We welcome other feedback, whether corrections, constructive suggestions, or ideas for new labs. Send email to David Wetherall ([djw@uw.edu](mailto:djw@uw.edu)).

[END]