Protocols Lab

Tom Kelliher, CS 325

Feb. 9, 2011

1 Introduction

In this lab, you'll be interacting with Internet application servers directly through telnet, or indirectly through dig, jwhois, and traceroute. The purpose of the lab is for you to get a feel for yourself for the protocols that power some of the services available on the Internet.

Open an NX connection to merlin and login. (Don't change your password until you've completed the POP experiment.) Under the Applications menu, open the Accessories sub-menu and run an instance each of the Terminal and the Text Editor. Why a text editor? When communicating with a server, if you mis-type a character you generally can't use the Backspace key to correct it. What you can do if to type your commands in the text editor, and then use copy/paste to enter them into the running telnet session.

Hand in answers to each of the questions asked below.

2 SMTP

1. First off, using your Outlook account send an email message to your merlin account.
2. Now, do that again, but this time use telnet, connecting to merlin's SMTP port. Here's an example exchange from which you can construct your own exchange:

```
220 bluebird.goucher.edu ESMTP Sendmail 8.13.8/8.13.8;\
    Tue, 12 Feb 2008 11:11:49 -0500
>>> HELO bluebird.goucher.edu
250-bluebird.goucher.edu Hello bluebird.goucher.edu [127.0.0.1],\
    pleased to meet you
>>> MAIL From:<kelliher@bluebird.goucher.edu>
250 2.1.0 <kelliher@bluebird.goucher.edu>... Sender ok
>>> RCPT To:<kelliher@bluebird.goucher.edu>
>>> DATA
250 2.1.5 <kelliher@bluebird.goucher.edu>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 m1CGBnQi007121 Message accepted for delivery
kelliher... Sent (m1CGBnQi007121 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 bluebird.goucher.edu closing connection
```

3. Partner-up with someone else in the class and send a single email to each of you, using a single telnet session. (Hint: You can use the RCPT command multiple times.)

4. The MAIL and RCPT commands are used to fill-in the From and To fields in the email. What about the Subject, CC, etc. fields? Additional headers are given at the beginning of the data section. A blank line is used to separate these headers from the body of the email:

```
Subject: Zombies are cool
CC: sungar@merlin.goucher.edu

Hey!
```

   But, think about (and maybe try) this — Would the CC line above actually result in delivery of e-mail, or does something else have to be done? How about BCC recipients; how is that feature implemented?

5. What happens if you try to send email to a nonexistent user on the system? What happens if you specify a bogus FQDN and user in the MAIL command?

3 POP

1. Telnet to merlin's pop3 port. Below is another example exchange that you can use as a model to list all the email sent to your account, retrieve each individual message, delete them, and quit. Rather than delete all the messages, retrieve them all, delete all but one, finish the POP session, and start another POP session to determine whether the server actually deleted all but one of the messages. Finally, delete the one remaining message:

```
Connected to merlin.goucher.edu (10.67.1.43).
Escape character is '^]'.
+OK POP3 Ready <3128.1202855253@merlin.goucher.edu>
user kelliher
+OK
pass LinusTorvaldsForPresident
+OK opened mailbox for test
list
+OK
1 893
2 499
.
retr 1
+OK
Return-Path: <kelliher@goucher.edu>
...

This email is from post.
.
dele 1
+OK Message 1 marked
```

```
retr 2
+OK
Return-Path: <kelliher@merlin.goucher.edu>
...

This is a test from merlin.
.
dele 2
+OK Message 2 marked
quit
+OK
```

2. You'll notice that some responses from the pop3 server are terminated by a line consisting of a single period, and some aren't. Why?

4 HTTP

1. HTTP servers get really confused by backspace characters, and some of them close the connection if you don't get the request to them within a few seconds, so you'll really want to use that text editor to craft your requests and copy/paste them into the running telnet window.

   Obviously, most of the requests we'll be making will return lots of HTML that we don't really care about — we just want to see the response headers. Here's how to do that:

   ```
   telnet google.com http | head -20
   ```

2. Okay, here's the model client request:

   ```
   GET / HTTP/1.1
   Connection: close
   Host: google.com
   ```

   Remember: The client request is terminated by a blank line, so there are *two* carriage returns following the `Host` header.

   Ordinarily, the value of the `Host` header should be the same as the host to which you're connecting.

3. What happens if you make the request shown above to google.com? What response code and message did you get? Why?

   What happens if you make the same request, but set the `host` value to www.google.com? Why did that happen?

4. What happens if your request doesn't include the `host` line? If the `host` value doesn't match the FQDN of the host to which you're connecting?

5. Visit www.amazon.com How many cookies will be set?

6. Visit www.goucher.edu. Is content caching permitted? What web server does Goucher use? Repeat for phoenix.goucher.edu.
7. Visit www.yahoo.com. What is the P3P field?

5 DNS

For most of the following you'll be using dig. Here are a couple notes:

1. To lookup up a host's IP address use this:

   ```
   dig horned-screamer.cac.psu.edu
   ```

2. To lookup up an MX or NS record for a host or domain use:

   ```
   dig kta.org <type>
   ```

   replacing `<type>` with mx or ns.

3. To lookup the FQDN associated with an IP address use:

   ```
   dig -x 10.67.1.35
   ```

4. To direct your query to a specific name server, use the `@` option:

   ```
   dig @ns1.msft.net foo.bar.com
   ```

Try the following:

1. Find both the external and internal IP addresses associated with the hosts bluebird and merlin.
2. Find and interpret the MX record sets for the following domain names: goldfinch.goucher.edu, gmail.com, and psu.edu.
3. What FQDN has IP address 10.68.1.26? 171.64.7.115?
4. How many external NS records does goucher.edu have? Internal NS records?
5. How many name servers are there for the following domains: ., .edu, .com, .org? Which domain has the most name servers, and why?
6. Who are the administrative and technical contacts for the goucher.edu domain? (Hint: Use jwhois).

6 Traceroute

Traceroute is used to determine how many routers are between you and another host, and to determine where packets are encountering bottlenecks.

1. In your opinion, is there a router between merlin and phoenix? Find out. Surprised? Explain the result.
2. How many routers are between merlin and www.psu.edu? Do you see any evidence in the traceroute output of multiple routes between the two hosts?