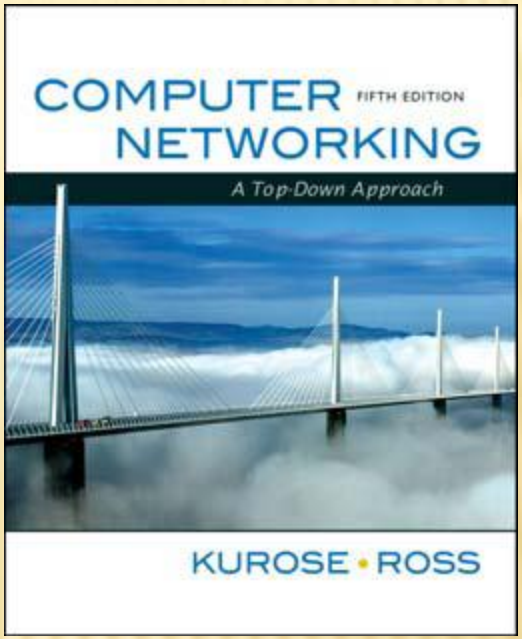

Computer Networking

LAB 2 – HTTP

OBJECTIVES

- The basic GET/response interaction
- HTTP message formats
- Retrieving large HTML files
- Retrieving HTML files with embedded objects
- HTTP authentication and security

1. THE BASIC HTTP GET/RESPONSE INTERACTION

1. Start up your web browser
2. Start up the Wireshark packet sniffer
3. Enter “http” in the filter window
4. Begin Wireshark packet capture
5. Enter the following to your browser
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
6. Stop Wireshark packet capture

RESULTS

- Two HTTP messages were captured:
  - the GET message from your browser
  - the response message from the server
- The packet-contents window shows details of the selected message:
  - the HTTP message was carried inside a TCP segment,
  - which was carried inside an IP datagram,
  - which was carried within an Ethernet frame

QUESTIONS

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What is the status code returned from the server to your browser?

QUESTIONS

5. When was the HTML file that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your browser?
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

2. THE HTTP CONDITIONAL GET/RESPONSE INTERACTION

- Most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object
- Make sure your browser's cache is empty
  - Firefox, select *Tools->Clear Recent History*
  - Internet Explorer, select *Tools->Internet Options->Delete*

STEPS

1. Start up your web browser
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
4. Select the refresh button on your browser
5. Stop Wireshark packet capture, and enter “http” in the filter window

QUESTIONS

1. Do you see an “IF-MODIFIED-SINCE” line in the first HTTP GET?
2. Did the server explicitly return the contents of the file? How can you tell?
3. Do you see an “IF-MODIFIED-SINCE:” line in the second HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
4. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?

3. RETRIEVING LONG DOCUMENTS

1. Start up your web browser
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
4. Stop Wireshark packet capture, and enter "http" in the filter window

QUESTIONS

1. How many HTTP GET request messages were sent by your browser?
2. How many data-containing TCP segments were needed to carry the single HTTP response?
3. What is the status code and phrase associated with the response to the HTTP GET request?

4. HTML DOCUMENTS WITH EMBEDDED OBJECTS

1. Start up your web browser
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
4. Stop Wireshark packet capture, and enter "http" in the filter window

QUESTIONS

1. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

5. HTTP AUTHENTICATION

1. Start up the Wireshark packet sniffer
2. Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html, username is “wireshark-students”, quotes), and the password is “network”
3. Stop Wireshark packet capture, and enter “http” in the filter window

QUESTIONS

1. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
2. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?