KAPLAN UNIVERSITY

Assignment Grading Rubric

Course: IT530 Unit: 3 Points: 90

Unit 3 Assignment

Outcomes addressed in this activity:

Unit Outcomes:

- Explain the purpose, functionality, and distinctions of the transport and network layer protocols.
- Compare the various implementations of multiplexing and demultiplexing.
- Explain technical considerations of NAT, fragmentation, ICMP, and IPv6.
- Analyze the relationship of transport and network layer protocols to other layers of the OSI model.
- Evaluate RIP, OSPF, and IS-IS with respect to performance, manageability, and security.
- Explain the various roles of connectionless and connection-oriented transport.

Course Outcomes:

IT530-3: Apply problem-solving and decision-making skills to address computer network issues.

Assignment Instructions:

This Assignment provides the "hands on" element to your studies. It gives you the opportunity to work with the protocols and see how they operate in real world environments. Read and perform the Unit 3 lab in the document entitled **"IT530 Assignment 3 Lab"** found in Doc Sharing.

Directions for Submitting Your Assignment:

Use the "What to hand in" section found at the back of the Unit 3 lab instructions as a guide for what to submit, and save it as a Word document, entitled Username-IT530 Assignment -Unit#.doc (Example: **TAllen- IT530 Assignment-Unit3.doc**). Submit your file by selecting the Unit 3: Assignment Dropbox by the end of Unit 3.

Assignment Requirements:

Answers contain sufficient information to adequately answer the questions and contain no spelling, grammar, or APA errors. Points deducted from grade for each writing, spelling, or grammar error are at your instructor's discretion.

For more information and examples of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

KAPLAN UNIVERSITY

Assignment Grading Rubric

Course: IT530 Unit: 3 Points: 90

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable assignments and discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity.

Unit 3 Assignment Grading Rubric = 90 points

Assignment Requirements	Points Possible	Points Earned
1. Document demonstrates that the student was able to correctly install and operate the Wireshark packet analyzer by providing a screenshot from their computer.	**0–18**	
2. Document demonstrates that the student was able to correctly list 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.	**0–18**	
3. Document demonstrates that the student was able to correctly determine the Internet address of the gaia.cs.umass.edu system.	**0–18**	

KAPLAN UNIVERSITY

Assignment Grading Rubric

Course: IT530 Unit: 3 Points: 90

4. Document demonstrates that the student was able to correctly determine the Internet address of their own system.	**0–18**	
5. Document demonstrates that the student was able to demonstrate understanding of packet traffic through written analysis.	**0–18**	
Total (Sum of all points)		
Less: Standard Requirements points deducted		
Assignment Total		

IT 530 Unit 3 Assignment Lab

Caution! Do not install or run the Wireshark packet capture and analyzer on any workplace system without written permission, signed by your supervisor! You are strongly encouraged to only use Wireshark on personally owned equipment.

1. Go to http://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html and carefully read the introductory tutorial.

2. Click <next> at the top or bottom of the introductory tutorial and read section 1.2, System Requirements. Check the system on which you will install Wireshark to make sure that it complies with Wireshark's system requirements. An easy way to do this is:
    a. Use Windows Explorer to navigate to "My Computer", right click "My Computer" and click on "Properties".

3. Click <next> and read section 1.3, Where to get Wireshark?

4. Click http://www.wireshark.org/download.html to download the latest copy of Wireshark for your particular system

5. Install Wireshark; using the Windows Installer is usually the easiest method and will also install the required "pcap" library for you.

6. Go to http://www.wireshark.org/docs/wsug_html_chunked/ChUseStartSection.html and study the use of the Wireshark interface.

7. Click <next> and note how each of the Wireshark menu items function. Pay special attention to the Capture and Analyze menu items.

8. Start Wireshark, and go to http://www.wireshark.org/docs/wsug_html_chunked/ChapterCapture.html
    a. Following the steps given by the Wireshark capture tutorial, start the capture. In a web browser, go to http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html You should see a brief congratulatory message on the web page.
    b. Stop the capture.

9. Now you're ready to analyze the packets in your capture. Go to http://www.wireshark.org/docs/wsug_html_chunked/ChapterWork.html#ChWorkViewPacketsSection
    a. Examine the top pane (the pane with colors for each packet) of the Wireshark interface, note down three different protocols that were in use during the capture.
    b. At the top of the Wireshark interface, there's a Filter box. In the box, type "http" without the quotes to filter the packets for http traffic.
    c. Find the HTTP GET packet that was sent from your computer to the web server shown in step 8a. Click once on the HTTP GET packet to select it.
    d. In the pane just below the top packet pane, you should see the full contents of the HTTP GET packet. Further information can be seen by clicking the small plus sign to the left of each line of information about the packet.
    e. Remember that the HTTP GET packet originated from your web browser; this means that the "source" IP for the HTTP GET packet is your computer.

f. The "destination" IP should be the system given in the link shown in step 8a.

Deliverables for this lab:

1. A screenshot of the Wireshark interface displaying the HTTP GET packet.
2. The three protocols that were noted down in step 9a.
3. The IP address of your computer, as determined from the "source" address in the HTTP GET packet.
4. The IP address of the destination web server, as determined from the "destination" address in the HTTP GET packet.
5. A brief (two or three paragraphs) analysis of the traffic behavior as shown in the capture.

KAPLAN UNIVERSITY

Assignment Grading Rubric

Course: IT530 Unit: 4 Points: 90

Unit 4 Assignment

Outcomes addressed in this activity:

Unit Outcomes:

- Evaluate link-layer services and their connection to the network layer.
- Evaluate network layer protocols and their applicability to overall network architecture.
- Recommend routing solutions appropriate for an organization's requirements.
- Characterize the application of Network Address Translation and its benefits for address management.
- Explain the significance of the different forms of wireless networking.
- Describe the significance of connection-oriented communication and connectionless communication techniques.

Course Outcomes:

IT530-4: Analyze scenarios involving data transfer, manipulation, and storage.

Assignment Instructions:

This Assignment provides the "hands on" element to your studies. It gives you the opportunity to work with the protocols and see how they operate in real world environments. Read and perform the Unit 4 lab in the document entitled "**IT530 Assignment 4 Lab**" found in Doc Sharing.

Directions for Submitting Your Assignment:

Use the "What to hand in" section found at the back of the Unit 4 lab instructions as a guide for what to submit, and save it as a Word document, entitled Username-IT530 Assignment -Unit#.doc (Example: **TAllen- IT530 Assignment-Unit4.doc**). Submit your file by selecting the Unit 4: Assignment Dropbox by the end of Unit 4.

Assignment Requirements:

Answers contain sufficient information to adequately answer the questions and contain no spelling, grammar, or APA errors. Points deducted from grade for each writing, spelling, or grammar error are at your instructor's discretion.

For more information and examples of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

KAPLAN UNIVERSITY

Assignment Grading Rubric

Course: IT530 Unit: 4 Points: 90

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable assignments and discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity.

Unit 4 Assignment Grading Rubric = 90 points

Assignment Requirements	Points Possible	Points Earned
1. Document demonstrates that the student was able to correctly discover source MAC addresses, destination MAC addresses from the Wireshark trace.	**0-18**	
2. Document demonstrates that the student was able to correctly determine the state of protection and the authentication algorithm used by the AUTHENTICATION packet.	**0-18**	
3. Document demonstrates that the student was able to correctly determine which	**0-18**	

KAPLAN UNIVERSITY

Assignment Grading Rubric

Course: IT530 Unit: 4 Points: 90

system sent the AUTHENTICATION packet.		
4. Document demonstrates that the student was able to correctly determine the cipher suites and authentication keys offered by the AUTHENTICATION packet.	**0-18**	
5. Document demonstrates that the student was able to correctly determine which system sent the ASSOCIATION packet.	**0-18**	
Total (Sum of all points)		
Less: Standard Requirements points deducted		
Assignment Total		

IT 530 Unit 4 Assignment Lab

Caution! Do not install or run the Wireshark packet capture and analyzer on any workplace system without written permission, signed by your supervisor! You are strongly encouraged to only use Wireshark on personally owned equipment.

Before beginning the lab, it is recommended that you read the 802.11 Tutorial document in Doc Sharing for a better understanding of 802.11 (wireless) packet behavior and packet types.

Because not all students will be able to capture wireless packets with their own computer system, a Wireshark "trace" file is provided in Doc Sharing for this lab; look for the Wireshark 802_11 file with the "pcap" file extension.

1. Download the Wireshark 802_11 trace file from Doc Sharing.

2. Start Wireshark. From the menu, select File, then Open and browse to where you have downloaded the trace file and select it to open it.

3. On page 12 of the 802.11 Tutorial (Doc Sharing), read the description of Beacon frames. Beacon frames are used by wireless access points to let other wireless nodes in the area know that the access point is available and is ready to synchronize with other nodes.

4. Study the Wireshark 802_11 trace file; in the "Info" column, you should be able to see the "Beacon frame" packets.

5. Click once on the No. 1 Beacon frame packet to select it.

6. In the "detail" panel just below the numbered packets panel, click on the small plus signs to expand the information contained within the packet.
    a. Note down the destination address (in hexadecimal) and the source address (also in hexadecimal).
    b. Note down the channel type.

7. In the top panel, scroll down to packet No. 1011.

8. Click once to select the packet.

9. In the "detail" panel just below the numbered packets panel, click on the small plus signs to expand the information contained within the packet.
    a. Note down the source IP address.
    b. Note down the destination IP address.
    c. Note down the source port.
    d. Note down the destination port.

10. In the top panel, scroll down to packet No. 1740.

11. Click once to select the packet.
    a. What type of packet is this? (Hint: look in the Info column).

12. In the "detail" panel just below the numbered packets panel, click on the small plus signs to expand the information contained within the packet.
    a. Note down whether or not the data in the packet is protected.
    b. Note down the Authentication Algorithm.
    c. Note down the source address (in hexadecimal).
    d. Note down the destination address (in hexadecimal).

13. In the top panel, scroll down to packet No. 1750.

14. Click once to select the packet.
    a. What type of packet is this?

15. In the "detail panel", click on the small plus signs to expand the information contained within the packet.
    a. Note down the source address (in hexadecimal).
    b. Note down the destination address (in hexadecimal).
    c. Note the types of cipher suite and authentication keys that the source can support.

Deliverables for this lab:

1. A screenshot of the Wireshark interface displaying the AUTHENTICATION packet.
2. The channel type for the BEACON frame.
3. The source and destination IP addresses for the TCP packet.
4. The source and destination port numbers for the TCP packet.
5. The state of protection for the AUTHENTICATION packet.
6. The Authentication Algorithm in use by the AUTHENTICATION packet.
7. Is the AUTHENTICATION packet being sent by a client system? Or the access point?
8. What types of cipher suite and authentication keys are available in the ASSOCIATION packet?
9. Is the ASSOCIATION packet being sent by a client system? Or the access point?
10. A brief (two or three paragraphs) analysis of the traffic behavior as shown in the capture.