

## **CW\_Specification\_CSI\_5\_PDN\_20/21**

Read this coursework specification carefully, it tells you how you are going to be assessed, how to submit your coursework on-time and how (and when) you'll receive your marks and feedback.

<b>Module Code</b>	CSI_5_PDN
<b>Module Title</b>	Principles of Data Networks
<b>Lecturer</b>	Dr. Muhammad Alam
<b>% of Module Mark</b>	60%
<b>Distributed</b>	[21/10/2024]
<b>Submission Method</b>	Submit online via this Module's Moodle site
<b>Submission Deadline</b>	[08/12/2022] 05:00 pm
<b>Release of Feedback &amp; Marks</b>	Feedback and provisional marks will be available in the Gradebook on Moodle.

### **Coursework Aim:**

**The aim of this coursework is to give opportunity to the students to obtain skills in the areas of data networking protocol analysis and networking application performance evaluation using both emulation and simulation tools.**

#### **Part A: Protocol Analysis using Wireshark**

The aim of this coursework is to understand the protocol analysis that must be carried out in a network by parsing information from different layers.

Coursework Specification Carry out the following tasks:

- Open the Wireshark program
- Start capturing the packets in the Wireshark
- Open the Web browser, clear the history (cache) of the Web browser.
- Surf the internet
- Stop capturing the packets in the Wireshark

Open the Wireshark screen and carry out the following actions.

### Questions:

1. In the context of Wireshark network analysis, what are the most commonly encountered TCP flags? Please provide a detailed explanation of each flag's significance and how it can be used to interpret the state of a TCP connection.

Additionally, illustrate your response with a visual representation of the TCP flag header and a screenshot of each TCP flag in Wireshark.

2. ICMP Ping is a widely used network diagnostic tool that leverages the Echo Request and Echo Reply messages of the ICMP protocol to determine network connectivity and measure response times.

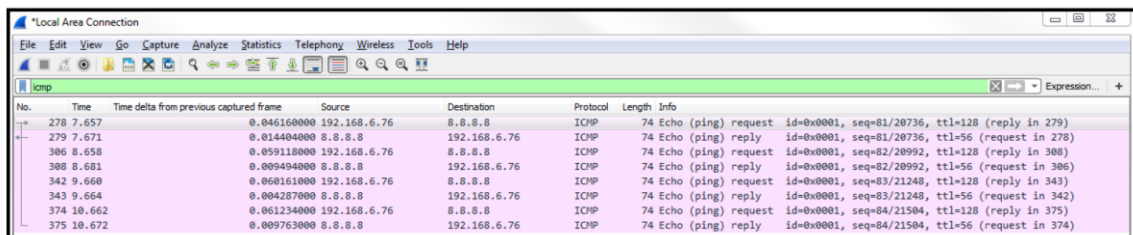
How ICMP Ping Works:

Echo Request: The ping command sends an ICMP Echo Request message to the target host.

Echo Reply: If the target host is reachable and operational, it responds with an ICMP Echo Reply message.

Response Time: The time it takes for the Echo Reply to return is measured and displayed as the ping latency.

In Wireshark, capture the data from the PING command and using ICMP in the filter area, display your results as shown in the following figure. Also, explain the ICMP packet details.



The screenshot shows the Wireshark interface with the filter 'icmp' applied. The packet list displays several ICMP Echo (ping) request and reply packets. The packet details pane shows the structure of an ICMP Echo (ping) request, including the type, code, checksum, and sequence number.

No.	Time	Time delta from previous captured frame	Source	Destination	Protocol	Length	Info
278	7.657	0.046160000	192.168.6.76	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=81/20736, ttl=128 (reply in 279)
279	7.671	0.014404000	8.8.8.8	192.168.6.76	ICMP	74	Echo (ping) reply id=0x0001, seq=81/20736, ttl=56 (request in 278)
306	8.658	0.059118000	192.168.6.76	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 308)
308	8.681	0.009494000	8.8.8.8	192.168.6.76	ICMP	74	Echo (ping) reply id=0x0001, seq=82/20992, ttl=56 (request in 306)
342	9.668	0.068161000	192.168.6.76	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=83/21248, ttl=128 (reply in 343)
343	9.664	0.004267000	8.8.8.8	192.168.6.76	ICMP	74	Echo (ping) reply id=0x0001, seq=83/21248, ttl=56 (request in 342)
374	10.662	0.061234000	192.168.6.76	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=84/21504, ttl=128 (reply in 375)
375	10.672	0.009763000	8.8.8.8	192.168.6.76	ICMP	74	Echo (ping) reply id=0x0001, seq=84/21504, ttl=56 (request in 374)

3. ICMP Traceroute is a network diagnostic tool that uses ICMP Time Exceeded messages to determine the route that packets take to reach a destination. By progressively increasing the Time To Live (TTL) field in the ICMP Echo Request messages, the traceroute can identify the routers along the path and measure the latency at each hop.

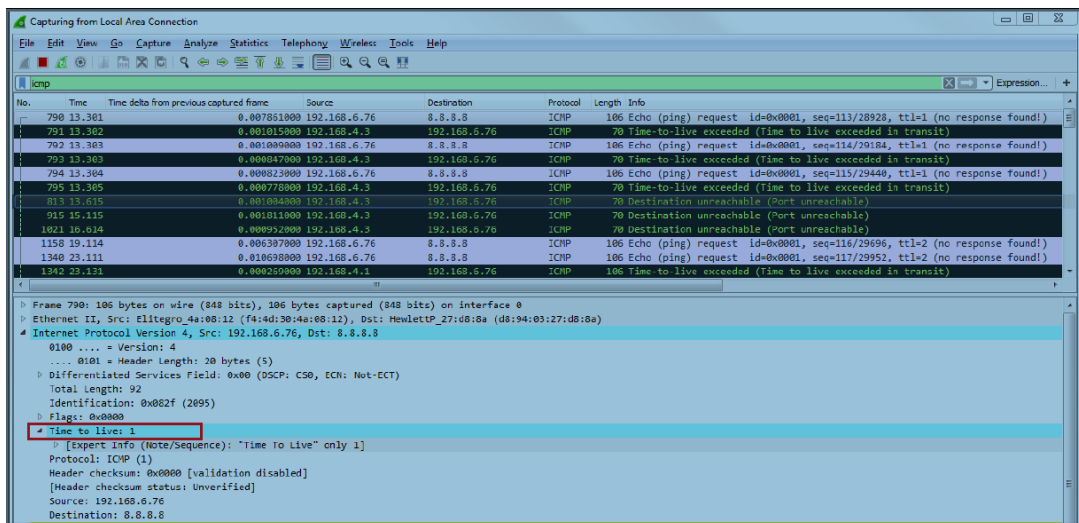
How ICMP Traceroute Works:

Initial TTL: The traceroute tool sends an ICMP Echo Request message with a TTL of 1.

Hop 1: The first router along the path decrements the TTL by 1 and, since it's now 0, sends an ICMP Time Exceeded message back to the source.

Hop 2: The traceroute tool then resends the Echo Request with a TTL of 2. This process continues until the destination is reached or the maximum hops are exceeded.

In Wireshark, capture the data from the traceroute command and using ICMP in the filter area, display the ICMP captured packets as shown in the following figure. Also, explain the Time to Live field and the overall working of the traceroute command in Wireshark.



- In Wireshark, capture data and provide a figure showing all the packets per second as shown in the following figure:



Provide a detailed explanation of the provided figure. There are various settings and display options of the graph, provide a detailed description of these settings.

- Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, enabling the communication between web browsers and web servers. It's a stateless protocol, meaning each request is treated independently, and the server doesn't maintain any session information.

Using Wireshark capture HTTP packets and display them as shown in the following figure. Provide a detailed analysis of how HTTP servers and clients interact. Please illustrate your response with a clear connection diagram.

No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
54	4.820	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
55	4.820	0.000042000	192.168.77.160	54		104.123.1.45	TCP	51216→80 [ACK] Seq=612 Ack=25481 Win=66780 Len=0
56	4.822	0.001952000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
57	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
58	4.822	0.000000000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
59	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
60	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
61	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
62	4.822	0.000000000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
63	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
64	4.822	0.000000000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
65	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
66	4.822	0.000042000	192.168.77.160	54		104.123.1.45	TCP	51216→80 [ACK] Seq=612 Ack=38881 Win=63000 Len=0
67	4.822	0.000010000	192.168.77.160	54		104.123.1.45	TCP	[TCP Window Update] 51216→80 [ACK] Seq=612 Ack=38881
68	4.822	0.000357000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
69	4.822	0.000001000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
70	4.822	0.000000000	104.123.1.45	1314		192.168.77.160	HTTP	Continuation
71	4.822	0.000013000	192.168.77.160	54		104.123.1.45	TCP	51216→80 [ACK] Seq=612 Ack=41861 Win=66780 Len=0

6. In a network captured using Wireshark, how do factors like packet size, transmission intervals, and network congestion influence the calculated throughput? Provide a detailed description of the process of using Wireshark's I/O graph or statistics features to track throughput over time, and discuss the significance of choosing appropriate time intervals for analysis when evaluating overall network performance.
7. How can basic and advanced filters be applied in Wireshark to isolate specific traffic types, protocols, or communication between particular devices within a network? Explain the difference between capture filters and display filters, providing examples of how complex filters can be created by combining multiple conditions (e.g., IP addresses, ports, protocols) to focus on specific traffic patterns or troubleshooting scenarios. Support your answer with a screenshot of each filter used.

## Part B: Understanding network components and simulating network scenarios.

8. Dynamic routing protocols are used in computer networks to automatically distribute routes between network devices when the network topology changes. They are used to:
  - Discover remote networks
  - Maintain up-to-date routing information
  - Choose the best path to destination networks
  - Find a new best path if the current path is no longer available

Examples are EGP, RIP, and OSPF.

Using Packet Tracer, build a small homogenous network using routers and switches, and provide a step-by-step configuration of the three routers using RIP protocol. Provide the ping command results with a screenshot.

9. A firewall is a security system that monitors and controls network traffic to prevent unauthorized access to a computer network. Using Packet Tracer, build a small network and configure a firewall that can accept and block traffic. Provide a step-by-step description of the configuration with screenshots.

10. How can Packet Tracer be effectively used to simulate and analyze the behavior of hubs in a network environment? Provide a detailed guide, including step-by-step instructions for configuring hubs, connecting devices, and examining network traffic. Discuss the limitations and drawbacks of using hubs compared to switches, and explore how Packet Tracer can be used to demonstrate these differences. Additionally, address the potential security implications of using hubs in a network and how Packet Tracer can be used to illustrate these risks.

### Coursework Submission Details:

<b>Type:</b>	Report
<b>Word Count:</b>	<p>As a guide, each student must aim for [2000-3000 words]. The maximum word limit is [4000 words].</p> <p>Footnotes and will not count towards word count totals but must only be used for referencing, not for the provision of additional text. The bibliography will not count towards the word total.</p> <p>No penalty will be applied if the total word limit is exceeded.</p>
<b>Standards:</b>	Properly addressing the report specification. Use of good English language and grammar. Logical structure to sections. Clear narrative voice in expression of arguments and information. Appropriate use of diagrams. Proper use of citations and presentation of references.
<b>Presentation:</b>	<ul style="list-style-type: none"><li>• Work must be referenced, and a bibliography provided</li><li>• Work must be submitted either as a Word document (.doc/docx) or a PDF</li><li>• Course work must be submitted using Arial font size 11 (or larger if you need to), with a minimum of 1.5 line spacing</li><li>• Your student number must appear at the front of the coursework. Your name must <b>not</b> be on your coursework.</li></ul>
<b>Referencing:</b>	Harvard Referencing should be used, see your <a href="#">Library Subject Guide</a> for guides and tips on referencing.
<b>Regulations:</b>	<p>Make sure you understand the <a href="#">University Regulations</a> on expected academic practice and academic misconduct. Note in particular:</p> <ul style="list-style-type: none"><li>▪ Your work must be your own. Markers will be attentive to both the plausibility of the sources provided as well as the consistency and approach</li></ul>

	<p>to writing of the work. Simply, if you do the research and reading, and then write it up on your own, giving the reference to sources, you will approach the work in the appropriate way and will cause not give markers reason to question the authenticity of the work.</p> <ul style="list-style-type: none"> <li>▪ All quotations must be credited and properly referenced. Paraphrasing is still regarded as plagiarism if you fail to acknowledge the source for the ideas being expressed.</li> </ul> <p><b>TURNITIN:</b> When you upload your work to the Moodle site it will be checked by anti-plagiarism software.</p>
--	--

## Learning Outcomes

This coursework will fully or partially assess the following learning outcomes for this module.

The following Learning Outcomes will be assessed:

- LO1 (Analyse network protocols, Explain the protocol functions on levels 2-4 of the TCP/IP stack): It will be assessed by using Wireshark to analyse and process the protocols used in different layers from data link up to the presentation layer using Wireshark.
- LO2 (Understanding the basics of networking): You will know how to design and develop simple networks.

## Assessment Criteria and Weighting

LSBU marking criteria have been developed to help tutors give you clear and helpful feedback on your work. They will be applied to your work to help you understand what you have accomplished, how any mark given was arrived at, and how you can improve your work in future.

	Criteria	Feedforward comments						
		100-80%	79-70%	69-60%	59-50%	49-40%	39-30%	29-0%
15%	<b>1. Research</b> Systematic identification and use of academic and relevant resources	Extensive independent relevant research evidenced by quality and quantity used. Ability to draw on own research and that of others.	Extensive independent relevant research evidenced by quality and quantity used. Some autonomous research.	Wide range of relevant sources identified and used. Very little guidance needed.	A range of sources identified and used. Limited guidance needed.	Limited research identified and used. Some guidance needed to complete research tasks.	Some evidence of research but insufficient amount. Needs support to develop research skills.	Little or no research presented. Needs significant support to develop research skills.
35%	<b>2. Critical Analysis of the Results</b> Analysis and interpretation of sources and results for both A and B <b>both Part A (1-7) and B (1-5).</b> Structuring of issues/debates.	Very high-quality analysis developed independently. Sustained evaluation and synthesis of results. Use of evidence-based arguments. Thoroughly identifies trends, inconsistency, congruence, and states the implications.	Sustained evaluation and synthesis of results. Use of evidence-based arguments. Thoroughly identifies trends, inconsistency, congruence, and states the implications.	Evaluation and synthesis of results. Use of evidence-based arguments. Identifies trends, inconsistency, congruence, and states the implications.	Evaluation and synthesis of results. Use of evidence-based arguments.	Some attempt at evaluation and synthesis of results. Some use of evidence-based arguments.	Limited evaluation of results. Limited use of evidence-based arguments	Little or no evaluation of results. Very little use of evidence-based arguments.
25%	<b>3. Testing and Problem-Solving Skills and Experimental Set-up</b> Design and implementation of the environment for <b>both Part A (1-7) and B (1-5).</b>	Autonomous creation and novel implementation. Adapts to unforeseen practical and theoretical challenges to achieve identified goals.	Almost entirely autonomous creation and implementation. Adapts to unforeseen practical and theoretical challenges to achieve identified goals.	Mainly autonomous creation and implementation. Adapts to unforeseen practical and theoretical challenges to achieve identified goals.	Some autonomy to create and implement. Some adaption made to unforeseen practical and theoretical challenges to achieve identified goals.	Exploration of possible solution(s). Use of established approaches to resolve practical and theoretical problems.	Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems.	Little or no exploration of solution(s). Question or problem unresolved.
10%	<b>4. Standards, Referencing and Academic Integrity<sup>1</sup></b> Acknowledges and gives credit to the work of others follows the conventions and practices of the discipline including appropriate use of referencing standards for discipline.	Consistent, error free application of relevant referencing conventions with great attention to detail.	Consistent, error free application of relevant referencing conventions.	Consistent application of relevant referencing conventions with few errors.	Application of relevant referencing conventions, with some errors and / or inconsistencies.	Generally correct application of relevant referencing conventions, with some errors and / or inconsistencies.	Limited application of referencing conventions and / or errors.	Very limited or no application of referencing conventions, and/or multiple errors.
15%	<b>5. Personal and Professional Development</b> Management of learning through self-direction, planning and reflection	Takes full responsibility for own learning and development through continuous cycles of well-articulated purposeful analysis and planning, supported by extensive evidence	Takes full responsibility for own learning and development through continuous cycles of well-articulated purposeful analysis and planning, supported by evidence.	Reflection and planning are self-directed, continuous, habitual and evidenced clearly. Strengths have been built on; weaknesses have been mitigated.	Evidence that a cycle of reflection and planning has been continuous and productive. Actively works to develop strengths and mitigate weaknesses.	Evidence that reflection and planning have led to increased disciplinary engagement and commitment. Developing an awareness of strengths and weaknesses.	Weak evidence of reflection and planning for learning but not followed through consistently. Incomplete awareness of personal strengths and weaknesses.	Insufficient evidence of reflection or planning for learning and no evidence of awareness of personal strengths and weaknesses.

<sup>1</sup> The application of this criterion is independent of the process outlined in the [Student Academic Misconduct Procedure](#)

## **How to get help**

We will discuss this Coursework Specification in class. However, if you have related questions, please contact me [name and email] as soon as possible.

## **Resources**

- How to use wireshark,  
[https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChapterIntroduction.html](https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html)