QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2021/2022**		**University Specialization**	**Cyber security**	
Course No.	**0125443**		**Course name**	**Networks Monitoring and documenting**	
Credit Hours	**3**		**Prerequisite Co-requisite**	**Secure Communication Protocols**	
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT ☐ Support course family requirements	☐ Mandatory requirements	☐ Elective requirements
Teaching style	☐ **Full online learning**		☐ **Blended learning**	✓ **Traditional learning**	
Teaching model	☐ **2Synchronous: 1asynchronous**		☐ **2 face to face : 1synchronous**	☐ **3 Traditional**	

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course covers standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs) and interconnecting T-1/E-1 and T-2/E-3 lines from a central site. The course emphasizes "learning by doing", and requires students to conduct a series of lab exercises. Through these labs, students can enhance their understanding of the principles, and be able to apply those principles to solve real problems.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	1-Charit Mishra, Mastering Wireshark,1st edition, 2016, Packt Publishing 2-Subramanian, Network Management: Principles and Practice, second edition,2010, Pearson.			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1-Ed Wilson, Network Monitoring and Analysis: A Protocol Approach to Troubleshooting,2000, Prentice-Hall. 2-Chris Chapman, Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools,2016, Elsevier. 3- Research paper and internet resources			
Supporting websites				
The physical environment for teaching	✓ Class room	✓ labs	☐ Virtual educational platform	☐ Others
Necessary equipment and software	**Network monitoring software: Wireshark , iNetMon.**			

Supporting people with special needs	
For technical support	

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Understanding the concept, needs and fundamental of network monitoring	
K2	Understand concepts and terminology associated with common metrics for measuring network performance	
K3	Understand and discuss the foundation of passive and active network monitoring tools	
K4	An ability to understand and explain RMON and SNMP	
	Skills	
S1	Ability to use Wireshark to capture and analyze network traffic	
S2	Applying Wireshark to filter, inspect, analyze and troubleshoot networks	
S3	Ability to evaluate the performance of networks based on their metrics and using the required tools	
S4		
	Competences	
C1	Using the results of monitoring process to solve networks problems and troubleshooting.	
C2	Efficient use of monitoring tools for evaluating the network performance.	
C3	Analyzing the critical metrics and generating a useful reports	
C4		

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	%20	0
Second / midterm exam	%30	**%30**	%20	30%
Participation / practical applications	0	**0**	10	30%
Asynchronous interactive	%30	**%30**	0	0

activities				
final exam	%40	**%40**	%50	40%

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	**Introduction to network monitoring** The goals of network monitoring Network indicators measurement	Lectures	**Internet resources**
2	**Passive and active monitoring** Common metrics of network performance	**Lectures**	**Research papers and internet resources**
3	**Simple network management protocol and its versions.** Management information base SNMP communication	**Lectures**	**Internet resources**
4	**Monitoring tools** Simple monitoring tools	**Lectures**	**Internet resources**
5	**Passive monitoring** Combinational monitoring	**Lectures**	**Research papers**
6	**Introduction to Wireshark** Introduction to packet analysis with Wireshark. Capturing methodologies	**Lectures**	**1-24, textbook(1)**
7	**Introduction to filter:** Capture filters Display filters **(First Exam)**	**Lab**	**27-41, textbook(1)**
8	**Searching for packets using the find dialog** Create new Wireshark profile	**Lab**	**42-52, textbook(1)**
9	**Mastering the advance features of Wireshark:** The statistics menu Conversations Endpoints Working with IO, Flow, and TCP stream graphs.	**Lab**	**53-73, textbook(1)**
10	**Inspecting application layer protocols.**	**Lab**	**91-126, textbook(1)**

	Domain name system File transfer protocol Hypertext transfer protocol Simple mail transfer protocol		
11	**Analyzing Transport Layer Protocols** The transmission control protocol The User Datagram Protocol	**Lab**	**127-152, textbook(1)**
12	**Troubleshooting** Recovery features **(second Exam)**	**Lab**	**231-262, textbook(1)**
13	**Remote network monitoring, RMON** RMON1 and RMON2	**Lab**	390-417**, textbook(2)**
14	**iNetMon portable** Network analyzer Network trace	**Lab**	**Internet resources**
15	**Network address book** The visualization engine Reporting toolkit	**Lab**	**Internet resources**
16	**Final Exam**		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			