

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

COURSE MODULE OF THE SUBJECT TAUGHT FOR THE SESSION 2026-27 - (ODD SEM)

Course Syllabus with CO's

Faculty Name: Ms. Sandhya G				Academic Year: 2026 - 2027			
Department: Computer Science & Engineering – Cyber Security							
Course Code	Course Title	Core / Elective	Prerequisite	Contact Hours			Total Hrs/
				L	T	P	Sessions
BCS502	COMPUTER NETWORKS	Core	Basic computer fundamentals, operating system and binary mathematics.	3	0	2	40T+20P
Course Objectives	1. Study the TCP/IP protocol suite, switching criteria and Medium Access Control protocols for reliable and noisy channels. 2. Learn network layer services and IP versions. 3. Discuss transport layer services and understand UDP and TCP protocols. 4. Demonstrate the working of different concepts of networking layers and protocols						
Topics Covered as per Syllabus							
Module -1							
Introduction: Data Communications, Networks, Network Types, Networks Models: Protocol Layering, TCP/IP Protocol suite, The OSI model, Introduction to Physical Layer: Transmission media, Guided Media, Unguided Media: Wireless. Switching: Packet Switching and its types.							
Module -2							
Data Link Layer: Error Detection and Correction: Introduction, Block Coding, Cyclic Codes. Data link control: DLC Services: Framing, Flow Control, Error Control, Connectionless and Connection Oriented, Data link layer protocols, High Level Data Link Control. Media Access Control: Random Access, Controlled Access. Check Sum and Point to Point Protocol							
Module -3							
Network Layer: Network layer Services, Packet Switching, IPv4 Address, IPv4 Datagram, IPv6 Datagram, Introduction to Routing Algorithms, Unicast Routing Protocols: DVR, LSR, PVR, Unicast Routing protocols: RIP, OSPF, BGP, Multicasting Routing-MOSPF							
Module -4							
Introduction to Transport Layer: Introduction, Transport-Layer Protocols: Introduction, User Datagram Protocol, Transmission Control Protocol: services, features, segments, TCP connections, flow control, Error control, Congestion control.							
Module -5							
Introduction to Application Layer: Introduction, Client-Server Programming, Standard Client Server Protocols: World Wide Web and HTTP, FTP, Electronic Mail, Domain Name System (DNS), TELNET, Secure Shell (SSH)							

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

Laboratory Component:

Sl.NO	Experiments
1	Implement three nodes point – to – point network with duplex links between them. Set the queue size, vary the bandwidth, and find the number of packets dropped.
2	Implement transmission of ping messages/trace route over a network topology consisting of 6 nodes and find the number of packets dropped due to congestion.
3	Implement an Ethernet LAN using n nodes and set multiple traffic nodes and plot congestion window for different source / destination.
4	Develop a program for error detecting code using CRC-CCITT (16- bits).
5	Develop a program to implement a sliding window protocol in the data link layer.
6	Develop a program to find the shortest path between vertices using the Bellman-Ford and path vector routing algorithm.
7	Using TCP/IP sockets, write a client – server program to make the client send the file name and to make the server send back the contents of the requested file if present.
8	Develop a program on a datagram socket for client/server to display the messages on client side, typed at the server side.
9	Develop a program for a simple RSA algorithm to encrypt and decrypt the data.
10	Develop a program for congestion control using a leaky bucket algorithm.

List of Textbooks

Text Books:

Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, Tata McGraw- Hill, 2013.

Reference Books

Larry L. Peterson and Bruce S. Davie: Computer Networks – A Systems Approach, 4th Edition, Elsevier, 2019.

Nader F. Mir: Computer and Communication Networks, 2nd Edition, Pearson Education, 2015.

William Stallings, Data and Computer Communication 10th Edition, Pearson Education, Inc., 2014.

List of URL's

<https://www.digimat.in/nptel/courses/video/106105183/L01.html>

<http://www.digimat.in/nptel/courses/video/106105081/L25.html>

<https://nptel.ac.in/courses/10610>

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

Course outcomes: The students should be able to:

- Explain the fundamentals of computer networks.
- Apply the concepts of computer networks to demonstrate the working of various layers and protocols in communication network.
- Analyze the principles of protocol layering in modern communication systems.
- Demonstrate various Routing protocols and their services using tools such as Cisco packet tracer.

Assessment Details (both CIE and SEE) The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE

CIE for the theory component of the IPCC (maximum marks 50)

- IPCC means practical portion integrated with the theory of the course.
- CIE marks for the theory component are 25 marks and that for the practical component is 25 marks.
- 25 marks for the theory component are split into 15 marks for two Internal Assessment Tests (Two Tests, each of 15 Marks with 01-hour duration, are to be conducted) and 10 marks for other assessment methods mentioned in 22OB4.2. The first test at the end of 40-50% coverage of the syllabus and the second test after covering 85-90% of the syllabus.
- Scaled-down marks of the sum of two tests and other assessment methods will be CIE marks for the theory component of IPCC (that is for 25 marks).
- The student has to secure 40% of 25 marks to qualify in the CIE of the theory component of IPCC. CIE for the practical component of the IPCC.

SEE for IPCC Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (duration 03 hours)

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), should have a mix of topics under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored by the student shall be proportionally scaled down to 50 Marks The theory portion of the IPCC shall be for both CIE and SEE, whereas the practical portion will have a CIE component only. Questions mentioned in the SEE paper may include questions from the practical component.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

Subject Code:	BCS502	TITLE: COMPUTER NETWORKS							Faculty Name:	Ms. Sandhya G			
List of Course Outcomes	Program Outcomes											Total	
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11		
CO-1	2	2	-	-		-	-	-	-	-	-	4	
CO-2	3	3	3	-		-	-	-	-	-	-	9	
CO-3	2	2	2	-	3	-	-	-	-	-	-	9	
CO-4	2	2	2	-	3	-	-	-	-	-	-	9	
Total	9	9	7	0	6	0	0	0	0	0	0	31	

Note: 3 = Strong Contribution, 2 = Average Contribution, 1 = Weak Contribution, - = No Contribution

The Correlation of Course Outcomes (CO's) and Program Specific Outcomes (PSO's)

Subject Code:	BCS502	TITLE: COMPUTER NETWORKS			Faculty Name:	Ms. Sandhya G
List of Course Outcomes	Program Specific Outcomes				Total	
	PSO-1	PSO-2	PSO-3			
CO-1	3	-	-	3		
CO-2	3	-	-	3		
CO-3	3	-	-	3		
CO-4	-	-	-	-		
Total	9	-	-	9		

Course Coordinator Signature

HOD Signature