




Al Musanna College of Technology

Department of Information Technology

Course Description Details

Advanced Diploma Level (Internet & E-Security)	
SL.No	Course Code/Name
	<p>Course Description</p> <p>Speech development strategies and delivery techniques- rhetorical sensitivity and critical thinking- feedback on developing speech forms - principles of public speaking - persuasive speech - Analyze audiences for the purpose of preparing speeches - visual aids for the purpose of speech - different methods of persuasion - introductory speech, a demonstration speech, an informative speech, a persuasive speech, and a special occasion speech - speaking styles to business, government, and industry functions</p> <p>ENTW3100-Public Speaking</p> 

Techniques to solve problems in probability ,counting and number theory - pigeonhole principle - counting methods - Generate functions - Recurrence relations - inclusion-exclusion formula - truth table, implications and equivalence, resolution and proof techniques - graph and set theory - characteristic of an algorithm - directed and undirected- Eulerian paths and cycles - Hamiltonian paths and cycles - Trees - h Sequential circuits - define-state machines - Deterministic and non- deterministic - finite automata - Groups and subgroups - Homomorphism and isomorphism of groups - Lagrange's theorem

MATH2200-Discrete
Structure



Course Name: Scaling Networks	Course Code: ITNT301
pre-requisite: ITNT201-Routing and Switching Essentials	Credit Hours: 3
Passing Grade: C	Level: Year3
No. Of Theory & Practical Hours (1 : 4)	
Goal: focuses on switching technologies and router operations that support small-to-medium business networks and includes wireless local area networks (WLANs) and security concepts. Students learn key switching and routing concepts. They can perform basic network configuration and troubleshooting, identify and mitigate LAN security threats, and configure and secure a basic WLAN.	
Objectives: By the end of this course, students will learn the following topics <ul style="list-style-type: none"> • L2 Security and WLANs • Routing Concepts and Configuration 	
Outcomes	Method
1. Explain how vulnerabilities compromise LAN security.	Theory & Practical
2. Implement switch security to mitigate LAN attacks.	Theory & Practical
3. Explain how WLANs enable network connectivity.	Theory & Practical
4. Implement a WLAN using a wireless router and a WLC.	Theory & Practical
5. Explain how routers use information in packets to make forwarding decisions.	Theory & Practical
6. Configure IPv4 and IPv6 static routes.	Theory & Practical
7. Troubleshoot static and default routes.	Theory & Practical



Course Name : Introduction to Cryptography	Course Code : ITSY301
Pre Requisite : MATH201	Credit Hours : 3
Passing Grade : C	Level: Advanced Diploma
No. of Theory Hrs: 2	No. of Practical Hrs : 2
Goal: This course aims to familiarize students with the fundamental concepts and applications of cryptography.	
Objectives: Upon completion of this course, the students should be able to:	
<ol style="list-style-type: none"> 1. Understand basic principles and concepts of modern cryptography. 2. Understand the functionality of various classical and modern cryptographic ciphers. 3. Appreciate the core techniques of cryptography and how they can be applied to meet various security goals. 4. Use various cryptographic tools/utilities. 	
Outcomes	Methodologies
Upon completion of this course, the students should be able to:	
1. Describe the terminology and fundamental concepts pertaining to the domains of cryptography and steganography.	Theory
2. Demonstrate the understanding of various classical substitution and transposition ciphers, and various types of classical substitution ciphers i.e. Simple, Homophonic, Polygram and Poly-alphabetic.	Theory
3. Compare and contrast symmetric, asymmetric and hybrid cryptosystems in terms of their functionality, types, strengths and weaknesses.	Theory
4. Describe the goals of data integrity, authentication and non-repudiation and how one-way hash functions, message authentication codes and digital signatures can be used to achieve these goals.	Theory
5. Discuss the operation and unique strengths of one-time pad, and how pseudo-random key streams limit the implementation of one-time pad in computers.	Practical
6. Describe the concepts of certification authority (CA) and digital certificates.	Theory
7. Demonstrate understanding of various modern symmetric-key and public-key ciphers, along with the modes of operation of symmetric-key ciphers.	Practical
8. Use cryptographic tools and utilities to comprehend the real-world application of symmetric, asymmetric and hybrid cryptosystems.	Practical
9. Discuss various legal issues related to information security.	Theory
Software & Hardware Tools: Any tool	



Course Name: Mobile Application Development (Updated)	Course Code: ITSE301
Pre-Requisite: 1) ITSE203-Object Oriented Programming AND 2) ITIS103-Web Technologies	Credit Hours: 3
Passing Grade: Depending on the Type of the course belongs to the Audit Degree.	Level: Year 3
No. Of Theory & Practical Hours : 0:4	
Goal: To equip students with technical and practical knowledge of Mobile Application Development.	
Objectives: The course should enable the student to: 1. Understand mobile operating systems. 2. Develop real time mobile applications. 3. Use database in mobile applications. 4. Use different types of views 5. Use service and fragments in applications	
Outcomes The students should be able to:	Method
1. Analyze mobile operating systems	Practical
2. Analyze different phases in mobile application development	Practical
3. Build mobile application.	Practical
4. Work with the various view layout controls including Listview	Practical
5. Use database to store and manage application data	Practical
6. Working with services and Fragments	Practical



Course Name : Network Security Assessment	Course Code : ITSY 302
Pre Requisite : Fundamentals of Computer Security	Credit Hours : 3
Passing Grade : C	Level : Advanced Diploma
No. of Theory Hrs : 2	No. of Practical Hrs : 2
Goal: The course aims to impart essential concepts and skills required to assess the security of computer networks, and extend students' knowledge in the domain of network security. The course also introduces fundamental concepts of security risk assessment.	
Objectives: Upon completion of this course, the students should be able to: 1. Understand fundamental concepts involved in assessing the security of a network. 2. Exhibit understanding of common threats, vulnerabilities and various types of attacks against network security, along with appropriate countermeasures. 3. Conduct vulnerability assessment in a network and generate adequate audit reports. 4. Understand the security risk assessment process.	
Outcomes	Methodologies
Upon completion of this course, the students should be able to:	
1. Describe relevant networking and information security concepts, in extension to their previous knowledge in this domain.	Theory
2. Explain various attacks launched by intruders to compromise the security of computer networks, along with appropriate countermeasures.	Theory
3. Describe the terminology, fundamental concepts, techniques and detailed process of conducting network security assessment.	Practical
4. Perform, both automated and manual, vulnerability assessment in an organizational network.	Practical
5. Generate appropriate audit reports, both manually and using automated assessment tools.	Practical
6. Describe the process of assessing security risks in an organizational network.	Theory
Software & Hardware Tools: Any tool	



Course Name : Web Application Security	Course Code : ITSY303
Pre Requisite : (ITDB201 OR ITSY201) AND ITSY301	Credit Hours : 3
Passing Grade : C	Level: Advanced Diploma
No. of Theory Hrs: 2	No. of Practical Hrs : 2
Goal: This course aims to prepare students to demonstrate the knowledge and skills needed to deal with common web application vulnerabilities.	
Objectives: Upon completion of this course, the students should be able to: 1. Understand fundamental concepts of Web Application Technology. 2. Exhibit understanding of common threats, vulnerabilities and various types of attacks against web application security, along with appropriate countermeasures.	
Outcomes	Methodologies
Upon completion of this course, the students should be able to:	
1. Describe the web application architecture and how HTTP protocol works.	Theory
2. Explain common vulnerabilities and threats to web applications.	Theory
3. Demonstrate various client-side and server-side attacks against web applications, including how authentication, session management, access controls and other client-side controls can be bypassed.	Practical
4. Explain the common best practices of securing web applications.	Theory
Software & Hardware Tools: Any tool	



Course Name: Probability and Statistics for Information Technology	Course Code: MATH311
Pre-Requisite: MATH1102 OR MATH1103	Credit Hours: 3
Passing Grade : Depending on the type of the course belongs to the Audit Degree	Level : Year 3
No. of Theory & Practical Hours 2 : 2	
Course Goal(s)	The student will demonstrate the ability to apply probability and statistical methods for representing and interpreting data and communicating results, using technology when needed.
Course Objectives	Course Learning Outcomes
<p>This course should enable the student to:</p> <p>1. Demonstrate the aptitude to apply fundamental concepts in exploratory data analysis, probability theory and random variables</p>	1. Identify different kinds of survey methods, types of data, examples of methods for organizing and summarizing data sets, including common graphical tools and summary statistics
	2. Find probabilities of single events, complementary events and the unions, intersections of collections of events, and other related probabilities using laws and counting rules
<p>2. Understand the definitions of discrete and continuous random variables including the of the moments of these random variables</p>	3. Contrast normal, binomial and Poisson random variables, their probability density and distribution functions, and general properties of the expectation
	4. Find probabilities for distributions over finite set based on normal distributions for which probabilities can be found without the use of calculus
<p>3. Demonstrate knowledge on statistical methods and probability theory in practical situations.</p>	5. Discriminate between a population and a sample; between a parameter and a statistic; and, between a confidence interval and a confidence level
	6. Identify the components of a traditional hypothesis test, including the parameter of interest, the null and alternative hypotheses and the test statistic and the p-value of a test statistic for one sample mean and difference of two sample means problems.
<p>4. Establish understanding of how to translate real-world problems into linear models</p>	7. Perform linear regression analysis for bivariate dataset
	8. Perform the F-test for situations where one-way ANOVA is appropriate
<p>5. Adapt a statistical package for data analysis</p>	9. Generate reports on exploratory data analysis, test of hypothesis, correlational analysis and one-way ANOVA using Microsoft R Open with RStudio as primary IDE



Course Name : Network Perimeter Security	Course Code : ITSY 304
Pre Requisite : Introduction to Cryptography (ITSY301)	Credit Hours : 3
Passing Grade : C	Level: Advanced Diploma
No. of Theory Hrs: 2	No. of Practical Hrs : 2
Goal: This course aims to acquaint students with the concepts and skills involved in securing network perimeter, by planning and implementing appropriate firewall.	
Objectives: Upon completion of this course, the students should be able to: 1. Understand fundamental concepts related to network security and firewalls. 2. Design appropriate firewall rule-set in accordance with security requirements of an organization 3. Secure organizational networks by configuring a suitable network-based firewall.	
Outcomes	Methodologies
Upon completion of this course, the students should be able to:	
1. Describe the terminology and fundamentals concepts related to firewalls and network perimeter defense.	Theory
2. Analyze the security concerns related to common protocols associated with different layers of TCP/IP model.	Theory
3. Categorize different type of firewalls in terms of their way of working and the layer of OSI and TCP/IP models at which they operate	Theory
4. Compare various DMZ architectures in terms of their strengths and limitations.	Theory
5. Comprehensively describe various features provided by network-based firewalls, including content filtering, virtual private network (including common VPN protocols such as PPTP, L2TP, IPSec and Socks), network address translation (NAT), load balancing and fault tolerance.	Theory
6. Configure suitable modern firewall products, in harmony with other security mechanisms employed in a network, and troubleshoot associated problems.	Practical
7. Design appropriate firewall rule-set in accordance with the requirements and network security policy of organization.	Practical
8. Describe other modern mechanisms used for network perimeter defense, including intrusion detection and prevention systems.	Theory
9. Explain various techniques commonly used to bypass firewalls, along with appropriate countermeasures.	Practical
Software & Hardware Tools: Any tool	



Course Name: Internet of Things Fundamentals	Course Code: ITNT309
Pre-Requisite: ITSE203 - Object Oriented Programming	Credit Hours: 3
Passing Grade: C	Level: Advanced Diploma – Year 3
No. Of Theory & Practical Hours : 2-2	
Goal: To explore things and their connection to the IoT	
Objectives: The course should enable the student to: <ul style="list-style-type: none"> 1. Explain the concepts of the things and connections that make up the IoT 2. To Build sensor / actuator systems using Arduino Microcontroller 3. Create Python Programs to provide functionality to Raspberri Pi. 4. Create an end-to-end IoT system 	
Outcomes At the end of this course, students should be able to:	Method
Understand the things and connections that make up the IoT.	Theory
Build sensor/actuator systems using the Arduino microcontroller	Practical/ Theory
Develop programs in Python that provide IoT functionality to the Raspberry Pi	Practical/ Theory
Explain the use of Cloud and Fog Technology in an IoT system.	Practical/ Theory
Understand the IoT systems that can solve global problems	Practical/ Theory
Design and Build an IoT prototype	Practical/ Theory



Course Name: LINUX System Administration-I	Course Code ITNT403
pre-requisite: ITSE102-Intr. To Operating System	Credit Hours: 3
Passing Grade: C	Level: B.Tech – Year4
No. Of Theory & Practical Hours (1:4)	
Goal: Be prepared to get LPIC-1: Junior Level Linux	
Objectives: The course should enable the student to : <ul style="list-style-type: none"> 1. Understand the architecture of a Linux system. 2. Install and maintain a Linux workstation, including X11 and setup it up as a network client. 3. Work at the Linux command line, including common GNU and UNIX commands. 4. Apply Shells, Shell Scripting, Data Management and X window system. 5. Handle files and access permissions as well as system security; and perform easy maintenance tasks: help users, add users to a larger system, backup and restore, shutdown and reboot. 	
Outcomes	Method
1. To understand the Linux OS, X Server installation, configuration and hardware architecture.	Theory / Practical
2. To understand the Linux Package Management concepts and their usability in various distributions	Theory / Practical
3. To demonstrate knowledge and understanding towards performing tasks using basic commands and shell.	Theory / Practical
4. To manage and control the Linux OS processes	Theory / Practical
5. To manage and control Partitions and file system attributes, permission, ownership, mounting, unmounting and quote management.	Theory / Practical
6. Demonstrate knowledge to control and manage the Linux OS run levels and other services.	Theory / Practical
7. Manage User and Group accounts using commands	Theory / Practical
8. Demonstrate Shell scripting knowledge to manage the automate services.	Theory / Practical
9. Manage and synchronize the system clock over NTP and understand the email server concept and Printing Service in Linux OS.	Theory / Practical
10. To understand and demonstrate network (Basic Configuration) and security management in Linux OS.	Theory / Practical
11. To understand and implement Troubleshooting, Data Encryption and DNS process in Linux OS.	Theory / Practical



Course Name : Ethical Hacking	Course Code : ITSY305
Pre Requisite : ITSY301 AND ITSY303	Credit Hours : 3
Passing Grade : C	Level: Advanced Diploma
No. of Theory Hrs: 2	No. of Practical Hrs : 2
Goal: The course aims to acquaint students' with the necessary ethics and various means to perform vulnerability assessments and penetration tests for the purpose of strengthening network defenses.	
Objectives: Upon completion of this course, the students should be able to:	
<ol style="list-style-type: none"> 1. Understand ethical and legal issues that must be taken into consideration before carrying out ethical hacking activities. 2. Conduct vulnerability assessments and penetration testing. 3. Conform to the guidelines, provisions and conditions specified in an ethical hacking agreement/plan. 	
Outcomes	Methodologies
Upon completion of this course, the students should be able to:	
1.Discuss ethical and legal issues surrounding hacking that differentiate ethical and malicious hacking activities.	Theory
2.Describe common techniques and methodologies, along with popular proprietary and open source tools, used in ethical hacking.	Theory
3.Develop a plan to perform various ethical hacking activities.	Practical
4.Perform comprehensive vulnerability assessments and penetration testing.	Practical
5.Prepare recommendations and suggestions to improve network security policies and mechanisms based on the findings of ethical hacking activities.	Theory
Software & Hardware Tools: Any tool	



Course Name: Mobile Application Development (Updated)	Course Code: ITSE301
Pre-Requisite: 1) ITSE203-Object Oriented Programming AND 2) ITIS103-Web Technologies	Credit Hours: 3
Passing Grade: Depending on the Type of the course belongs to the Audit Degree.	Level: Year 3
No. Of Theory & Practical Hours : 0:4	
Goal: To equip students with technical and practical knowledge of Mobile Application Development.	
Objectives: The course should enable the student to: <ul style="list-style-type: none"> 1. Understand mobile operating systems. 2. Develop real time mobile applications. 3. Use database in mobile applications. 4. Use different types of views 5. Use service and fragments in applications 	
Outcomes The students should be able to:	Method
1. Analyze mobile operating systems	Practical
2. Analyze different phases in mobile application development	Practical
3. Build mobile application.	Practical
4. Work with the various view layout controls including Listview	Practical
5. Use database to store and manage application data	Practical
6. Working with services and Fragments	Practical



Course Name: Computer Organization (Updated)	Course Code: ITSE305
Pre-Requisite: ITSE101-Programming I AND MATH2200-Discrete Structures	Credit Hours: 3
Passing Grade: Depending on the Type of the course belongs to the Audit Degree.	Level: Year 3
No. Of Theory & Practical Hours: 1 : 4	
Goal: To provide concepts of computer organization and to develop skills in assembly language programming.	
Objectives: The course should enable the student to : <ol style="list-style-type: none"> 1. Understand computer architecture. 2. Work with Boolean expressions. 3. Construct Sequential and Combinational logic circuits. 4. Discuss Micro programmed Control. 5. Discuss Input / Output and Memory Organization. 6. Explain pipelining and Vector Processing. 7. Construct assembly language programs. 8. Design logic circuits using appropriate tool. 	
Outcomes: At the end of this course, students should be able to:	Method
1. Discuss the organization of computers.	Theory
2. Use methods to simplify Boolean expressions.	Theory and Practical
3. Construct sequential and combinational logic circuits.	Theory and Practical
4. Discuss architecture of a processor including Addressing modes.	Theory
5. Discuss Micro-programmed Controller	Theory
6. Apply instruction set architecture including Data transfer, Arithmetic, Logic instructions, Machine control and interrupt instructions	Theory and Practical
7. Describe Pipelining and Vector Processing and Various interconnection structures.	Theory
8. Discuss different Memory Organizations and operations.	Theory
9. Describe Input-Output Organization.	Theory
10. Construct assembly language programs using appropriate tool.	Practical
11. Design sequential and combinational logic circuits using appropriate tool.	Practical



Course Name: Network Management	Course Code: ITNT302
pre-requisite: ITSY202- Network OS Administration & Security	Credit Hours: 3
Passing Grade: C	Level: Advnaced Diploma - Year3
No. Of Theory & Practical Hours (2:2)	
Course Goal: The course provides an overview of network management from both business and technical perspective	
<p>Course Objectives:</p> <ul style="list-style-type: none"> • Convey an informal understanding of the functions, tools, and activities that are associated with network management and how it operates by taking a glimpse at typical activities. • Discuss the basic components in network management and the roles they play. • Present the different aspects in network management that would help divide and conquer network management problems. • Provide an overview of management communication patterns and how management protocols are effectively applied in practice. 	
<p>Learning Outcomes:</p> <ol style="list-style-type: none"> 1. Explain the basic foundation and models that are needed to build various network management architectures and protocols. 2. Explain, demonstrate and apply different SNMP-based protocols with its specification that manage used over TCP/IP networks. 3. Illustrate and explain the Network Management using remote monitoring capabilities. 4. Illustrate and explain the architecture and features of some of the widely used Network Management systems and Tools 5. Explain and demonstrate the knowledge acquired on management and tools and systems, as well apply the practical applications in managing fault, configuration, performance, security, and accounting in Network Management 6. Explain the impact of emerging technologies in a Web based and object oriented management system 	



Course Name: Internet of Things Fundamentals	Course Code: ITNT309
Pre-Requisite: ITSE203 - Object Oriented Programming	Credit Hours: 3
Passing Grade: C	Level: Advanced Diploma – Year 3
No. Of Theory & Practical Hours : 2-2	
Goal: To explore things and their connection to the IoT	
Objectives: The course should enable the student to: <ol style="list-style-type: none"> 1. Explain the concepts of the things and connections that make up the IoT 2. To Build sensor / actuator systems using Arduino Microcontroller 3. Create Python Programs to provide functionality to Raspberri Pi. 4. Create an end-to-end IoT system 	
Outcomes At the end of this course, students should be able to:	Method
Understand the things and connections that make up the IoT.	Theory
Build sensor/actuator systems using the Arduino microcontroller	Practical/ Theory
Develop programs in Python that provide IoT functionality to the Raspberry Pi	Practical/ Theory
Explain the use of Cloud and Fog Technology in an IoT system.	Practical/ Theory
Understand the IoT systems that can solve global problems	Practical/ Theory
Design and Build an IoT prototype	Practical/ Theory



Course Name : Secure Application Development	Course Code : ITSY 306
Pre Requisite : Object Oriented Programming (ITSE203)	Credit Hours : 3
Passing Grade : C	Level : Advanced Diploma
No. of Theory Hrs : 2	No. of Practical Hrs : 2
Goal: This course aims to extend students' understanding of developing different types of secure applications.	
Objectives: Upon completion of this course, the students should be able to: <ol style="list-style-type: none"> 1. Understand the essential concepts pertaining to secure application development. 2. Apply their knowledge and skills to develop applications securely. 3. Assess the security of different applications. 	
Outcomes	Methodologies
Upon completion of this course, the students should be able to:	
1. Describe software security concepts and techniques pertaining to various phases of SDLC, and the requirements that motivate the need of software security.	Theory
2. Describe common application security vulnerabilities, including buffer overflows, cross-site scripting, and Injection flaws.	Theory
3. Use suitable tools for developing secure applications.	Practical
4. Demonstrate the use of cryptography, proper validation controls and secure database access methods in developing secure applications.	Theory
5. Perform code reviews for analyzing and evaluating the security of applications.	Practical
Software & Hardware Tools: Any tool	



Course Name: Mobile Application Development (Updated)	Course Code: ITSE301
Pre-Requisite: 1) ITSE203-Object Oriented Programming AND 2) ITIS103-Web Technologies	Credit Hours: 3
Passing Grade: Depending on the Type of the course belongs to the Audit Degree.	Level: Year 3
No. Of Theory & Practical Hours : 0:4	
Goal: To equip students with technical and practical knowledge of Mobile Application Development.	
Objectives: The course should enable the student to: <ol style="list-style-type: none"> 1. Understand mobile operating systems. 2. Develop real time mobile applications. 3. Use database in mobile applications. 4. Use different types of views 5. Use service and fragments in applications 	
Outcomes The students should be able to:	Method
1. Analyze mobile operating systems	Practical
2. Analyze different phases in mobile application development	Practical
3. Build mobile application.	Practical
4. Work with the various view layout controls including Listview	Practical
5. Use database to store and manage application data	Practical
6. Working with services and Fragments	Practical



Course Name: Computer Organization (Updated)	Course Code: ITSE305
Pre-Requisite: ITSE101-Programming I AND MATH2200-Discrete Structures	Credit Hours: 3
Passing Grade: Depending on the Type of the course belongs to the Audit Degree.	Level: Year 3
No. Of Theory & Practical Hours: 1 : 4	
Goal: To provide concepts of computer organization and to develop skills in assembly language programming.	
Objectives: The course should enable the student to : <ol style="list-style-type: none"> 1. Understand computer architecture. 2. Work with Boolean expressions. 3. Construct Sequential and Combinational logic circuits. 4. Discuss Micro programmed Control. 5. Discuss Input / Output and Memory Organization. 6. Explain pipelining and Vector Processing. 7. Construct assembly language programs. 8. Design logic circuits using appropriate tool. 	
Outcomes: At the end of this course, students should be able to:	Method
1. Discuss the organization of computers.	Theory
2. Use methods to simplify Boolean expressions.	Theory and Practical
3. Construct sequential and combinational logic circuits.	Theory and Practical
4. Discuss architecture of a processor including Addressing modes.	Theory
5. Discuss Micro-programmed Controller	Theory
6. Apply instruction set architecture including Data transfer, Arithmetic, Logic instructions, Machine control and interrupt instructions	Theory and Practical
7. Describe Pipelining and Vector Processing and Various interconnection structures.	Theory
8. Discuss different Memory Organizations and operations.	Theory
9. Describe Input-Output Organization.	Theory
10. Construct assembly language programs using appropriate tool.	Practical
11. Design sequential and combinational logic circuits using appropriate tool.	Practical



Course Name: Network Management	Course Code: ITNT302
pre-requisite: ITSY202- Network OS Administration & Security	Credit Hours: 3
Passing Grade: C	Level: Advnaced Diploma - Year3
No. Of Theory & Practical Hours (2:2)	
Course Goal: The course provides an overview of network management from both business and technical perspective	
Course Objectives: <ul style="list-style-type: none"> • Convey an informal understanding of the functions, tools, and activities that are associated with network management and how it operates by taking a glimpse at typical activities. • Discuss the basic components in network management and the roles they play. • Present the different aspects in network management that would help divide and conquer network management problems. • Provide an overview of management communication patterns and how management protocols are effectively applied in practice. 	
Learning Outcomes: <ol style="list-style-type: none"> 1. Explain the basic foundation and models that are needed to build various network management architectures and protocols. 2. Explain, demonstrate and apply different SNMP-based protocols with its specification that manage used over TCP/IP networks. 3. Illustrate and explain the Network Management using remote monitoring capabilities. 4. Illustrate and explain the architecture and features of some of the widely used Network Management systems and Tools 5. Explain and demonstrate the knowledge acquired on management and tools and systems, as well apply the practical applications in managing fault, configuration, performance, security, and accounting in Network Management 6. Explain the impact of emerging technologies in a Web based and object oriented management system 	



Course Name: Server Administration	Course Code: ITNT404
pre-requisite: ITSY202-Network OS Administration & Security	Credit Hours: 3
Passing Grade: C	Level: B.Tech - Year4
No. Of Theory & Practical Hours (1:4)	
Goal: Implement and administrate the core network services operating within a network environment.	
Objectives:	
<ul style="list-style-type: none"> • Learn how to configure and administrator common services deployed on servers. • Develop a conceptual understanding of each network services and learn how to plan, implement and administer each service. • Evaluate and monitor performance of the network services and infrastructure. 	
Outcomes	Method
1. Define the role of DNS server in network environment.	Theory
2. Define role of web server access and manage sites.	Theory / Practical
3. Describe and identify routing and remote access services and network policies.	Theory / Practical
4. Design and trouble shoot VPN (virtual private network)	Theory / Practical
5. Recognize how NAT (network address translation) works and how to configure.	Theory / Practical
6. Construct routing and remote access polices to permit and deny.	Theory / Practical
7. Describe the role of proxy server. Configure and trouble shoot proxy server for access web, remote access and mail access.	Theory / Practical
8. Discover required knowledge and skills to install configure, route and manage a mailing server.	Theory / Practical
9. Describe client access backup and restore database and manage recipient object such as mail boxes, distributed group and contacts.	Theory / Practical
10. Monitor and test traffic performance, troubleshoot connectivity and resolve service issues	Theory / Practical



Course Name: Internet of Things Fundamentals	Course Code: ITNT309
Pre-Requisite: ITSE203 - Object Oriented Programming	Credit Hours: 3
Passing Grade: C	Level: Advanced Diploma – Year 3
No. Of Theory & Practical Hours : 2-2	
Goal: To explore things and their connection to the IoT	
Objectives: The course should enable the student to: <ol style="list-style-type: none"> 1. Explain the concepts of the things and connections that make up the IoT 2. To Build sensor / actuator systems using Arduino Microcontroller 3. Create Python Programs to provide functionality to Raspberri Pi. 4. Create an end-to-end IoT system 	
Outcomes At the end of this course, students should be able to:	Method
Understand the things and connections that make up the IoT.	Theory
Build sensor/actuator systems using the Arduino microcontroller	Practical/ Theory
Develop programs in Python that provide IoT functionality to the Raspberry Pi	Practical/ Theory
Explain the use of Cloud and Fog Technology in an IoT system.	Practical/ Theory
Understand the IoT systems that can solve global problems	Practical/ Theory
Design and Build an IoT prototype	Practical/ Theory

