

# Information Technology (IT)

---

## Courses

### IT 120 CompTIA A+ Practical Applications (3 Hours)

Students will gain knowledge required to install, configure and maintain software for end users. This course will also cover the basics of networking as well as networking security/forensics. Students will apply troubleshooting skills to properly and safely diagnose, resolve and document common software issues. Students will also apply appropriate customer support and soft skills, understand the basics of virtualization and examine desktop imaging and deployment. 2 hrs. lecture/wk, 2 hrs. lab/wk, 1 hr. open lab/wk.

### IT 141 Introduction to Networks (3 Hours)

Introduction to Networks is the first of 3 courses in the Cisco Certified Network Associate (CCNA) curriculum. This course introduces the architecture, structure, functions, components, and models of the internet and other computer networks. The principles and structure of Internet Protocol (IP) addressing and the fundamentals of Ethernet concepts, media, and operations are introduced to provide a foundation for the curriculum. By the end of the course, students will be able to build simple local area networks (LANs), perform basic configurations for routers and switches, and implement IP addressing schemes. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

### IT 150 Switching, Routing, and Wireless Essentials\* (3 Hours)

**Prerequisites :** IT 140 or IT 141.

Switching, Routing and Wireless Essentials is the 2nd of 3 courses in the Cisco Certified Network Associate (CCNA) curriculum. This course 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 will learn how to perform basic network configuration and troubleshooting, identify and mitigate LAN security threats, and configure and secure a basic WLAN. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

### IT 155 Microsoft Administration Fundamentals\* (3 Hours)

**Prerequisites :** IT 120 or IT 205.

This course is designed to provide students with foundational knowledge of cloud concepts and services in Microsoft 365 and Microsoft Azure. Students will also learn about cloud security, privacy, compliance and trust in these environments. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

### IT 175 Cybersecurity Fundamentals\* (3 Hours)

**Prerequisites :** (IT 120 or IT 205) and (IT 140 or IT 141).

This course is designed to provide students with the knowledge and skills required to install and configure systems to secure applications, networks and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws and regulations. Students will perform these tasks to support the principles of confidentiality, integrity and availability. 2 hrs. lecture, 2 hrs. lab, 1 hr. open lab/wk.

### IT 202 IT Scripting\* (3 Hours)

**Prerequisites :** IT 231 .

The main objective of this course is to introduce students to writing scripts using Python. The course maps to the Python Institute PCAP (Python Certified Associate in Programming) certification exam with emphasis on networking programming. Topics covered in this course include lists, strings, dictionaries, functions, recursion, file processing, using modules, object-oriented programming and exception handling. 2 hrs. lecture, 2 hrs. open lab/wk.

### IT 204 Enterprise Networking, Security and Automation\* (3 Hours)

**Prerequisites :** IT 145 or IT 150.

Enterprise Networking, Security, and Automation is the 3rd of 3 courses in the Cisco Certified Network Associate (CCNA) curriculum. The course describes the architectures and considerations related to designing, securing, operating and troubleshooting enterprise networks. The course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access along with the introduction of software-defined networking, virtualization, and automation concepts that support the digitalization of networks. Students gain skills to configure and troubleshoot enterprise networks and learn to identify and protect against cybersecurity threats. They are introduced to network management tools and learn key concepts of software-defined networking, including controller-based architectures and how application programming interfaces (APIs) enable network automation. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

### IT 206 Network Security Fundamentals\* (3 Hours)

**Prerequisites :** IT 145 or IT 150.

This course is designed to provide an introduction to the core security concepts and skills needed for the installation, troubleshooting and monitoring of network devices to maintain the integrity, confidentiality and availability of data and devices. Topics covered include network threats, mitigation techniques, securing network devices, implementing firewall technologies, implementing intrusion prevention, securing local area networks (LANs), implementing virtual private networks (VPNs), and managing a secure network. Hands-on exercises will be used to reinforce the concepts. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

### IT 223 Azure Administration\* (3 Hours)

**Prerequisites :** IT 155 or IT 221.

This course teaches students the fundamentals of Azure Administration. Students will implement, manage and monitor identity, governance, storage, compute and virtual networks in a cloud environment. Students will provision, size, monitor and adjust resources as appropriate. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

**IT 224 Modern Desktop Administrator\* (3 Hours)**

**Prerequisites :** IT 155 or IT 221.

This course teaches students the fundamentals of Modern Desktop Administration. Students will deploy, configure, secure, manage and monitor devices and client applications in an enterprise environment. Students will manage identity, access, policies, updates and apps. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

**IT 230 Linux Fundamentals (3 Hours)**

This course is designed to provide students with a fundamental understanding of the Linux operating system environment. Students successfully completing this course will be able to perform Linux installation and package management; execute common Linux commands and utilities; and accomplish different system tasks such as navigating the filesystem and utilizing the resources of a basic Linux system.

**IT 231 Linux Administration\* (3 Hours)**

**Prerequisites :** IT 230.

This course is designed to provide students with the necessary knowledge and skills to perform competently as a Linux system administrator. Students successfully completing this course should be able to perform basic system administration tasks including configuring the graphical user interface, managing user accounts, managing system logging, configuring basic networking, writing shell scripts and maintaining system security.

**IT 238 Digital Forensics\* (3 Hours)**

**Prerequisites :** (IT 120 or IT 205) and IT 230.

This course will cover the fundamentals of computer and cyber forensics. Students will learn different aspects of digital evidence and methods to uncover illegal activities left on storage media. Various forensics tools, techniques and procedures will be used in a lab environment to perform forensic investigations. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

**IT 239 Ethical Hacking\* (3 Hours)**

**Prerequisites :** (IT 145 or IT 150) and IT 230.

This course introduces students to common computer vulnerabilities as well as exploits and techniques used by hackers. Students will develop countermeasures to mitigate attacks and strengthen system security. Topics covered include vulnerability scanning, social engineering, denial of service attacks, intrusion detection, buffer overflow and penetration testing. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

**IT 257 Cybersecurity Operations\* (3 Hours)**

**Prerequisites :** IT 175 and (IT 150 or IT 145) and IT 230.

Cybersecurity Operations is designed to map to the Cisco Certified CyberOps Associate certification. The course covers knowledge and skills needed to successfully handle the tasks, duties and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC). Topics covered include investigating endpoint vulnerabilities and attacks, evaluating network security alerts and applying incident response models to manage network security incidents. 2 hrs. lecture, 2 hrs. lab and 1 hr. open lab/wk.

**IT 271 Information Technology Internship I\* (3 Hours)**

**Prerequisites :** (IT 120 or IT 140 or IT 141 or IT 205 or IT 230) and Department approval.

This course affords the student the opportunity to apply classroom knowledge to a real-world environment. Students will gain advanced information technology experience working with local employers, under instructional oversight, which will promote the student's career goals. Student will work a total of 300 hours/semester at an approved job site.

**IT 272 Information Technology Internship II\* (3 Hours)**

**Prerequisites :** IT 271 and department approval.

This course is a continuation of IT 271, Internship I. It provides the student additional opportunity to apply classroom knowledge to an actual work environment. Students will work a total of 300 hours per semester at an approved job site.

**IT 292 Special Topics:\* (1-3 Hour)**

**Prerequisites :** Department approval.

This course periodically presents specialized topics in computer networking that are not available in the regularly offered curriculum. Special Topics may be repeated for credit, but only on different topics.