Maryland CTE Programs of Study

Networking I (2025)

GENERAL REQUIREMENTS. This course is recommended for students in Grades 9-12, and there are no prerequisites for this course. 1

1 GENERAL REQUIREMENTS. This course is recommended for students in Grades 9-12, and there are no prerequisites for this course. 1

INTRODUCTION 2

A Career and Technical Education (CTE) instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions. 2.A

B The Digital Technology Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services. 2.B

C The Networking Systems program of study emphasizes careers and educational pathways related to the design and implementation of computer and information networks, including local area networks (LAN), wide area networks (WAN), intranets, extranets, and other data communication systems. It covers the analysis of data processing challenges involved in developing and enhancing computer network systems. 2.C

D Networking I introduces students to the fundamentals of computer networks, covering LAN/WAN operation, IP addressing, switching, routing, and network security. The course emphasizes hands-on skills with modern technologies, including Ethernet, VLANs, IPv6, and cybersecurity practices. Students will also explore career pathways in IT, develop employability skills, and integrate academic concepts into practical networking scenarios, preparing for certifications like CompTIA A+. Additional modules will include foundational IT support skills in hardware, operating systems, and mobile device management to align with the full scope of the CompTIA A+ certification. 2.D

E Students will participate in at least two Career-Connected Education and Work-Based Learning experiences in this course, which might include informational interviews or job shadowing relevant to the program of study. 2.E

Skip to main content

Students are encouraged to participate in extended learning experiences through aligned Career and Technical Student Organizations (CTSOs). CTSOs are a

cocurricular requirement in the Carl D. Perkins Act, and alignment to CTSO activities is an expectation for CTE programs in the state of Maryland. 2.F

KNOWLEDGE AND SKILLS 3

A The student demonstrates the necessary skills for career development, maintenance of employability, and successful completion of course outcomes. The student is expected to: 3.A

1. Identify and demonstrate positive work behaviors that enhance employability and job advancement, such as regular attendance, promptness, proper attire, maintenance of a clean and safe work environment, and pride in work. 3.A.1
2. Demonstrate positive personal qualities such as flexibility, open-mindedness, initiative, active listening, and a willingness to learn. 3.A.2
3. Employ effective reading, writing, and technical documentation skills. 3.A.3
4. Solve problems using critical thinking techniques and structured troubleshooting methodologies. 3.A.4
5. Demonstrate leadership skills and collaborate effectively as a team member. 3.A.5
6. Implement safety procedures, including proper handling of hardware and following cybersecurity guidelines. 3.A.6
7. Exhibit an understanding of legal and ethical responsibilities in the IT field, following data privacy laws and best practices for security. 3.A.7
8. Demonstrate time-management skills and the ability to prioritize tasks in a technical setting. 3.A.8

B The student identifies various career pathways in the information technology field. The student is expected to: 3.B

1. Develop a career plan that includes the necessary education, certifications, job skills, and experience for specific roles in IT networking. 3.B.1
2. Create a professional resume and portfolio that reflect skills, projects, certifications, and recommendations. 3.B.2
3. Demonstrate effective interview skills for roles in IT and networking. 3.B.3

C The student develops technology and digital literacy skills. The student is expected to: 3.C

1. Use technology as a tool for research, organization, communication, and problem-solving. 3.C.1
2. Use digital tools, including computers, mobile devices, collaboration platforms, and cloud services, to access, manage, and create information. 3.C.2
3. Demonstrate proficiency in using emerging and industry-standard technologies, including virtualization tools, network management software, and cybersecurity applications. 3.C.3
4. Understand ethical and legal considerations for technology use, including the principles of data protection, copyright, and responsible technology use. 3.C.4

Skip to main content

5 Install and configure client operating systems such as Windows, Linux, and macOS, including user account setup and system recovery tools. 3.C.5

6 Use mobile devices (iOS and Android) for synchronization, configuration, and basic troubleshooting. 3.C.6

7 Explain cloud computing concepts (e.g., SaaS, IaaS, PaaS) and use cloud storage and virtualization environments 3.C.7

D The student integrates core academic skills into networking practices. The student is expected to: 3.D

1 Demonstrate the use of clear communication techniques, both written and verbal, that are consistent with industry standards. 3.D.1

2 Apply mathematical concepts such as binary conversion, subnetting, and data rate calculations in network configuration and troubleshooting. 3.D.2

3 Use scientific principles, such as signal properties and electromagnetic interference, in network design and troubleshooting. 3.D.3

4 Use basic scripting and command-line tools for troubleshooting (e.g., ipconfig, netstat, sfc, chkdsk). 3.D.4

E The student understands and operates data networks. The student is expected to: 3.E

1 Describe the functions and characteristics of various network devices, including routers, switches, firewalls, access points, and network interface cards (NICs). 3.E.1

2 Identify components required for modern network and Internet communication, including cables, connectors, and transceivers for both wired and wireless networks. 3.E.2

3 Select the correct network components based on performance requirements, scalability, and cost considerations. 3.E.3

4 Explain the operation of the OSI and TCP/IP models and associated protocols, including HTTP/HTTPS, DNS, DHCP, and SNMP, as well as the real-world relevance of these models during packet flow diagnostics. 3.E.4

5 Discuss the impact of evolving networking applications, such as cloud computing, Voice over IP (VoIP), streaming services, and Internet of Things (IoT), on network infrastructure. 3.E.5

6 Interpret network diagrams and documentation to understand network layout and connectivity. 3.E.6

7 Analyze the routing path between hosts and identify potential network issues using tools like traceroute and packet sniffers. 3.E.7

8 Differentiate between Local Area Networks (LANs), Wide Area Networks (WANs), Metropolitan Area Networks (MANs), and Software-Defined Networks (SDNs). 3.E.8

F The student configures, verifies, and troubleshoots network switching. The tudent is expected to: 3.F

Skip to main content

1 Select appropriate cabling and connectors for different network scenarios, including fiber optics, twisted pair (Cat 5e, Cat 6, Cat 6a), and coaxial cables. 3.F.1

2 Explain Ethernet standards, network topologies, and switching concepts such as VLANs, spanning tree protocol (STP), and MAC address table. 3.F.2

3 Configure switches to segment networks, manage traffic, and ensure redundancy. 3.F.3

4 Perform switch configuration tasks, including setting up Virtual Local Area Networks (VLANs), trunking, and port security. 3.F.4

5 Use network monitoring tools to verify switch operation and status, troubleshoot connectivity, and diagnose faults. 3.F.5

6 Identify security measures on switches, such as access control lists (ACLs), port-based security, and 802.1X authentication. 3.F.6

7 Examine best practices for MAC address filtering and switchport security to introduce layered defense methods. 3.F.7

8 Diagnose and resolve switch-related issues such as incorrect VLAN assignments, misconfigured trunk links, and spanning tree problems. 3.F.8

G The student implements Internet Protocol (IP) addressing schemes and services for networks. The student is expected to: 3.G

1 Explain the purpose and structure of IP addressing, including IPv4, IPv6, and subnetting. 3.G.1

2 Compare IPv4 and IPv6, including differences in address structure, configuration, and migration considerations. 3.G.2

3 Design and apply IP addressing schemes that include subnetting, variable-length subnet masks (VLSM), and address allocation. 3.G.3

4 Configure and verify IP addresses for hosts, servers, and networking devices in both IPv4 and IPv6 environments. 3.G.4

5 Explain the functions of Network Address Translation (NAT), Port Address Translation (PAT), and IPsec. 3.G.5

6 Identify IPv6 transition methods (e.g., dual stack, tunneling), as they are prevalent in today's enterprise environments. 3.G.6

7 Configure Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) for dynamic IP management. 3.G.7

8 Explain public and private IP address usage, and describe strategies for IPv4 address exhaustion mitigation, such as IPv6 transition. 3.G.8

9 Troubleshoot IP addressing issues using tools like ipconfig, ping, and Wireshark. 3.G.9

10 Configure IP settings in operating systems during system setup and troubleshooting. 3.G.10

Skip to main content

The student configures, verifies, and troubleshoots routing. The student is expected to: 3.H

1. Describe routing principles, including static and dynamic routing, distance-vector, and link- state protocols. 3.H.1
2. Explain the role of routing protocols such as OSPF, EIGRP, RIP, and BGP in network communication. 3.H.2
3. Examine the use of routers for inter-VLAN routing, network segmentation, and remote access. 3.H.3
4. Verify network configuration using command-line tools (ping, traceroute, SSH) and network diagnostic software. 3.H.4
5. Implement secure router configurations, including firewall rules, VPNs, and encryption. 3.H.5
6. Manage router firmware and configuration files, including updates, backups, and restores. 3.H.6
7. Implement routing security features such as route filtering, authentication, and access lists. 3.H.7
8. Troubleshoot routing issues related to network misconfiguration, hardware failures, and incorrect access controls. 3.H.8

I The student understands and implements network security measures. The student is expected to: 3.I

1. Apply network security principles, including firewalls, intrusion prevention systems (IPS), and encryption. 3.I.1
2. Configure wireless network security protocols, such as WPA3, and implement secure wireless settings. 3.I.2
3. Identify and mitigate common security threats, including malware, phishing, DDoS attacks, and social engineering. 3.I.3
4. Conduct vulnerability assessments and implement appropriate security measures. 3.I.4
5. Understand compliance standards such as GDPR, HIPAA, and PCI-DSS, and their impact on network security. 3.I.5
6. Identify logging and monitoring tools to detect and respond to security incidents. 3.I.6
7. Implement data loss prevention (DLP) strategies to protect sensitive information. 3.I.7
8. Identify and explain core security frameworks such as the CIA triad and Authentication, Authorization, and Accounting (AAA). 3.I.8
9. Explain and implement workstation security practices such as antivirus software, local firewall settings, and password policies. 3.I.9
10. Identify social engineering tactics (e.g., phishing, impersonation) and apply prevention methods. 3.I.10
11. Understand physical security controls (e.g., badge access, cable locks, surveillance). 3.I.11

Skip to main content

J **The student understands how to configure, maintain, and troubleshoot personal computer hardware and software. The student is expected to:** 3.J

1. Identify components of a computer system, including CPUs, RAM, storage devices (HDD, SSD), motherboards, and power supplies. 3.J.1
2. Compare and install peripheral devices such as printers, monitors, input devices, and external storage. 3.J.2
3. Configure system BIOS/UEFI settings and understand firmware roles. 3.J.3
4. Diagnose and repair common hardware issues, including boot failures and overheating. 3.J.4
5. Replace and upgrade hardware components following proper procedures. 3.J.5
6. Identify appropriate tools for hardware maintenance and antistatic handling. 3.J.6
7. Interpret hardware specifications and compatibility requirements. 3.J.7
8. Use diagnostic software and troubleshooting flowcharts to resolve hardware problems. 3.J.8