



Spring 2025 Training Catalog

last updated on 1/10/24

Cisco Certified Support Technician (CCST) Networking

Date	01/24/25 - 3/21/25	Time	11:00 a.m. - 12:00 p.m. on Fridays
Location	Virtual		
Registration	https://forms.office.com/g/5PuZgf7chX		
Presenter Name	Ray Girdler, Chris Nestrud, and Lucas Evans		
Session Title	Networking Basics (Part of Cisco Certified Support Technician - CCST Networking Path)		
Session Description	<p>Networking Basics is the first of four courses in the path toward the Cisco Certified Support Technician (CCST) Networking certification. In this course, you will be enrolled in a learning cohort and complete a series of self-paced modules designed to build a solid understanding of fundamental networking concepts. Cohort participants will meet every Friday to review learned material, discuss key concepts, and engage with a content expert to deepen their understanding.</p> <p>This course requires approximately 25 hours of self-paced study outside of the weekly Friday meetings. Whether you're preparing for a career in networking, refreshing your knowledge for an industry-recognized certification, or simply exploring the world of networking, this course is an excellent starting point.</p> <p>What You'll Learn:</p> <ul style="list-style-type: none"> • Networking Fundamentals: Grasp the foundational concepts of networking, including the role of network devices, media, and protocols. • Network Traffic Observation: Learn how data flows through a network and how to configure devices to connect and communicate. • Networking Applications & Protocols: Explore the various applications and protocols used to manage and accomplish networking tasks. <p>This course is designed for individuals who want to build a strong foundation in networking and is perfect for those aiming to pursue higher-level certifications or advance in their technical careers.</p>		
Min. Requirements	No minimum skills required.		
Targeted Audience	IT Staff	Num. of Participants	25
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework <ul style="list-style-type: none"> • K0674: Knowledge of computer networking protocols • K0712 Knowledge of Local Area Networks (LAN) • K0713 Knowledge of Wide Area Networks (WAN) • K0718 Knowledge of network communications principles and practices • K0861 Knowledge of network port capabilities and applications • K0915 Knowledge of network architecture principles and practices • K0983 Knowledge of computer networking principles and practices • K0998 Knowledge of Wireless Local Area Network (WLAN) tools and techniques • K1011 Knowledge of network addressing principles and practices • K1065 Knowledge of network operations principles and practices • K1174 Knowledge of network components • K1175 Knowledge of network monitoring tools and techniques 		

ISACA Certified in Risk and Information Systems Control

Date	02/03/24 - 02/06/24 (4 days)	Time	9:30 a.m. - 4:30 p.m.
Location	501 Woodlane Street, 5th Floor, TSS Delta Conference Room, Little Rock, AR 72201		
Registration	email raymond.girdler@arkansas.gov		
Presenter Name	ISACA		
Session Title	ISACA Certified in Risk and Information Systems Control (CRISC) Training		
Session Description	<p>The ISACA Certified in Risk and Information Systems Control (CRISC) course is a comprehensive training program designed to equip professionals with the skills needed to manage enterprise IT risks and implement effective information systems controls. Participants will learn to identify, assess, and evaluate IT risks, as well as design and monitor control systems to mitigate potential threats. The course covers essential topics such as risk identification, assessment, response, and monitoring, making it ideal for IT professionals, risk managers, and control professionals looking to strengthen their organization's IT resilience and compliance. Attendees will also receive a one-year ISACA membership and a test voucher to support their certification journey.</p>		
Min. Requirements	Responsible for identifying risks and managing risk response to ensure organizational resilience.		
Targeted Audience	IT Staff, Senior Leadership	Num. of Participants	18
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework <ul style="list-style-type: none"> • K0721: Knowledge of risk management principles and practices • S0453: Skill in creating a risk management strategy • T1343: Provide cybersecurity guidance to organizational risk governance processes 		

(ISC)² Certified in Cybersecurity

Date	04/04/24 - 05/16/24	Time	11:00 a.m. - 12:00 p.m. on Fridays
Location	Virtual		
Registration	https://forms.office.com/g/EHTE9xiWPX		
Presenter Name	Ray Girdler, Alan Floyd, and Chad Johnson		
Session Title	(ISC) ² Certified in Cybersecurity (CC) Training		
Session Description	<p>This course provides the foundational knowledge, skills, and abilities necessary for entry- or junior-level cybersecurity roles. It establishes a baseline understanding of fundamental security best practices, policies, and procedures. Participants will meet every Friday to review material, discuss key concepts, and engage with a content expert to deepen their understanding.</p> <p>The course covers five key domains:</p> <ul style="list-style-type: none"> • Security Principles • Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts • Access Controls Concepts • Network Security • Security Operations 		
Min. Requirements	There are no specific prerequisites. It is recommended that candidates have basic information technology (IT) knowledge.		
Targeted Audience	IT Staff	Num. of Participants	25
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework <ul style="list-style-type: none"> • K0680: Knowledge of cybersecurity principles and practices • K0709: Knowledge of business continuity and disaster recovery (BCDR) policies and procedures • K1014: Knowledge of network security principles and practices 		

For questions about the program or course information, contact:

DIS State Cybersecurity Office (SCSO)

Ray Girdler

State IT Security Specialist

Raymond.Girdler@arkansas.gov

Visit the SCSO webpage for more information:

<https://transform.ar.gov/information-systems/cybersecurity/>