



# Network Security Engineer Program

## Overview:

The Network Security Engineer program prepares students for various industry certifications as well as prepares them for a career as a Network Security Engineer. On average a Network Security Engineer makes \$79,000 annually. During the program students will get a full understanding of what it takes to become a Network Security Engineer learning both theory and technical skills needed for the position. Students will learn about networks, routing, ethical hacking and forensics and how it related to network design and protection protocols and more. The core program covers the following industry certifications Cisco CCNA, CISCO CCNP (ENARSI), CISCO CCNP (ENCOR), Certified Professional Ethical Hacker (CPEH), and Certified Digital Forensics Examiner (CDFE).

**Program Duration:** 200 Flex Classroom Hours

## Program Courses:

Cisco CCNA Implementing and Administering Cisco Solutions  
Cisco CCNP Enterprise Network Core Tech (ENCOR)  
Cisco CCNP Enterprise Advanced Routing & Services (ENARSI)  
Certified Professional Ethical Hacker (CPEH)  
Certified Digital Forensics Examiner (CDFE)

## Program Features:

Our students are able to enjoy the benefits of round-the-clock on-demand lectures and hands on live labs in combination with scheduled live instructor led online classes where they are able to learn and interact with a live instructor. This provides the ultimate learning environment where students are able to learn, comprehend, experience, engage and ultimately master the subject matter in ways never before achieved in traditional classroom or online training.

- Live Virtual Classroom
- Elite Online Instructors
- Total Flexibility
- Hands-on Labs
- Certification Preparation
- Satisfaction Guarantee
- Career Development:
  - Career Counseling
  - Resume Building Assistance
  - Job Market Outlook
  - Job Placement Assistance



# Network Security Engineer Program

## *Cisco CCNA Implementing and Administering Cisco Solutions*

### Course Overview

This course will prepare students to take the CCNA 200-301 exam. Topics covered include networking fundamentals, basic ethernet LAN implementation, designing ethernet LANs, understanding IPv4, implementing IPv4, IPv4 design and troubleshooting, IPv4 services, configuring IPv4 routing protocols, implementing IPv6, and wireless LANs

### Course Outline

Chapter 01 – Networking Fundamentals

Chapter 02 – Basic Ethernet LAN Implementation

Chapter 03 – Designing Ethernet LANs

Chapter 04 – Understanding IPv4

Chapter 05 – Implementing IPv4

Chapter 06 – Ipv4 Design and Troubleshooting

Chapter 07 – Ipv4 Services

Chapter 08 – Configuring IPv4 Routing Protocols

Chapter 09 – Implementing IPv6

Chapter 10 – Wireless LANs



# Network Security Engineer Program

## *Cisco CCNP Enterprise Network Core Tech (ENCOR)*

### Course Overview

This course will prepare students to take the CCNP 350-401 ENCOR Implementing and Operating Cisco Enterprise Network Core Technologies exam. Topics covered include examining Cisco enterprise network architecture, implementing campus LAN connectivity, understanding and implementing EIRGP and OSPF, understanding virtual private networks and wireless principles, implanting secure access control, understanding enterprise security network architecture, network programmability protocols and more.

### Course Outline

Chapter 01 – Examining Cisco Enterprise Network Architecture

Chapter 02 – Understanding Cisco Switching Paths

Chapter 03 – Implementing Campus LAN Connectivity

Chapter 04 – Building Redundant Switched Topology

Chapter 05 – Implementing Layer 2 Port Aggregation

Chapter 06 – Understanding EIGRP

Chapter 07 – Implementing OSPF

Chapter 08 – Optimizing OSPF

Chapter 09 – Exploring EBGp

Chapter 10 – Implementing Network Redundancy

Chapter 11 – Implementing NAT

Chapter 12 – Introducing Virtualization Protocols and Techniques

Chapter 13 – Understanding Virtual Private Networks and Interfaces

Chapter 14 – Understanding Wireless Principles

Chapter 15 – Examining Wireless Deployment Options

Chapter 16 – Understanding Wireless Roaming and Location Services

Chapter 17 – Examining Wireless AP Operation

Chapter 18 – Understanding Wireless Client Authentication

Chapter 19 – Troubleshooting Wireless Client Connectivity

Chapter 20 – Introducing Multicast Protocols

Chapter 21 – Introducing QoS

Chapter 22 – Implementing Network Services

Chapter 23 – Using Network Analysis Tools



# Network Security Engineer Program

Chapter 24 – Implementing Infrastructure Security

Chapter 25 – Implementing Secure Access Control

Chapter 26 – Understanding Enterprise Network Security Architecture

Chapter 27 – Exploring Automation and Assurance Using Cisco DNA Center

Chapter 28 – Examining the Cisco SD-Access Solution

Chapter 29 – Understanding the Working Principles of the Cisco SD-WAN Solution

Chapter 30 – Understanding the Basics of Python Programming

Chapter 31 – Introducing Network Programmability Protocols

Chapter 32 – Introducing APIs in Cisco DNA Center and vManage



# Network Security Engineer Program

## *Cisco CCNP Enterprise Advanced Routing & Services (ENARSI)*

### Course Overview

This course will prepare students to take the CCNP 300-410 ENARSI Implementing Cisco Enterprise Advanced Routing and Services exam. Topics covered include EIRGRP implementation, optimization and troubleshooting, OSPF implementation and optimization, understanding IBGP, MPLS L3 VPN architecture and routing, DMVPN, DHCP, IPv6 first hop security, securing Cisco routers, DNA center assurance troubleshooting and more.

### Course Outline

Chapter 01 – EIGRP Implementation

Chapter 02 – EIGRP Optimization

Chapter 03 – EIGRP Troubleshooting

Chapter 04 – OSPF Implementation

Chapter 05 – OSPF Optimization

Chapter 06 – Troubleshooting OSPF

Chapter 07 – Redistribution Configuration

Chapter 08 – Troubleshooting Redistribution

Chapter 09 – Path Control

Chapter 10 – IBGP

Chapter 11 – Optimizing BGP

Chapter 12 – MP-BGP

Chapter 13 – Troubleshooting BGP

Chapter 14 – MPLS

Chapter 15 – MPLS L3 VPN Architecture

Chapter 16 – MPLS L3 VPN Routing

Chapter 17 – VRF-Lite Configuration

Chapter 18 – DMVPN

Chapter 19 – DHCP

Chapter 20 – IPv6 First Hop Security

Chapter 21 – Securing Cisco Routers

Chapter 22 – Troubleshooting Infrastructure Security and Services

Chapter 23 – DNA Center Assurance Troubleshooting



# Network Security Engineer Program

## *Certified Professional Ethical Hacker (CPEH)*

### Course Overview

The Certified Professional Ethical Hacker (CPEH) course will provide students with the knowledge to become an ethical hacker. Students will gain knowledge geared towards understanding cryptography, password cracking, malware, social engineering, network attacks, hacking wireless networks, and more.

Chapter 01 - Introduction to Ethical Hacking

Chapter 02 - Linux Fundamentals

Chapter 03 - Protocols

Chapter 04 - Cryptography

Chapter 05 - Password Cracking

Chapter 06 - Malware

Chapter 07 - Security Devices

Chapter 08 - Information Gathering - Reconnaissance-Passive (External Only)

Chapter 09 - Social Engineering

Chapter 10 - Reconnaissance-Active Scanning-Enumeration

Chapter 11 - Vulnerability Assessment

Chapter 12 - Network Attacks

Chapter 13 - Hacking Servers

Chapter 14 - Assessing and Hacking Web Technologies

Chapter 15 - Hacking Wireless Networks

Chapter 16 - Maintaining Access and Covering Tracks



# Network Security Engineer Program

## *Certified Digital Forensics Examiner (CDFE)*

### Course Overview

The Certified Digital Forensics Examiner (CDFE) training course will provide students with a comprehensive understanding of digital forensics. Students will gain knowledge on computer forensics, handling various incidents and the investigative process, types of digital evidence, protocols and techniques related to digital forensics and more.

Chapter 01 – Computer Forensics Incidents

Chapter 02 – Incident Handling

Chapter 03 – Computer Forensics Investigative Theory

Chapter 04 – Investigative Process

Chapter 05 – Digital Acquisition & Analysis Tools

Chapter 06 – Disks and Storages

Chapter 07 – Forensic Examination Protocols

Chapter 08 – Digital Evidence Protocols

Chapter 09 – Digital Evidence Presentation

Chapter 10 – Computer Forensic Laboratory Protocols

Chapter 11 – Computer Forensic Processing Techniques

Chapter 12 – Specialized Artifact Recovery

Chapter 13 – Electronic Discovery and Electronically Stored Information

Chapter 14 – Mobile Forensics

Chapter 15 – Digital Forensics Reporting