

NETWORK ENGINEER PROGRAM- CYBERSECURITY ACCELERATOR

HANDS-ON LABS

ND PROJECTS





LIVE WEEKLY COACHING AND STUDY GROUPS

Weekly Live Coaching

Every block of study comes equipped with dedicated live instruction via weekly study groups. The live instructed study groups provide students with the opportunity to engage with an NGT Academy Technical Instructor or Career Coach in a live online classroom environment every week. During these live study groups students can ask questions to gain clarification on topics, participate in live lab demonstrations, live instructed lessons, certification exam preparation, career success exercises, and general coaching, mentoring, and guidance for program success!



CERTIFICATIONS

Tools You'll Use



Full Stack Network Engineer - Cisco IOS Command Line, Cisco Packet Tracer, terminal emulators, port scanners, command line tools, cabling tools, cable tester, routing tables, mac-address tables, ping, traceroute, routing protocols, security protocols, basic and advanced routing and switching technologies, looking glass sites, password managers, text editors & text comparators, screen cap tools, TFTP and FTP server/client and syslog servers.



Cybersecurity Accelerator - Linux command line, Kali Linux, virtualization, network scanners, packet sniffers, password crackers, WiFi crackers, system hacking, vulnerability scanners, NMAP, telnet, nc, Wireshark, Metasploit, Aircrack, Hashcat, Python web server, process explorer, strings, msfvenom, Ettercap, Openvas Greenbone, Shodan, Sublist3r, theHarvester, Google dorks, HxD, Scalpel, Github, and MRC.

Career Success Services

Our mission is to help students achieve career success, so we offer free access to:

Live Career Coaching: Your dedicated Career Coaches provide career success workshops, and live coaching office hours every week!

Employer Network: Access to the exclusive NGT Academy employer network and new job opportunities posted weekly!

Asset Reviews: Each student will be able to submit their LinkedIn profile, resume, and cover letter for review by one of our career success coaches.

Digital Content Library: Our digital library includes industry-proven templates for resumes and cover letters, as well as digitized sessions and how-to guides on LinkedIn optimization, writing effective resumes and cover letters, job search strategies, and interview preparation.

Digital Community

Our digital community provides a 24/7 platform where students can share information, exchange ideas, and learn from their peers, NGT alumni, and other members of the community, including NGT staff.







\$97,430 (\$53K-\$116K) AVERAGE SALARY **VIEW SOURCE**





CAREER PATHS



FULL STACK NETWORK ENGINEER PROGRAM

Full Stack Network Associate

Plan out your path in Network Engineering, and learn the skills needed to become job-ready! To begin, you will dissect the IT Industry, learn the available career options and build your career plan. You will then be guided through the most important foundational concepts and technical skills necessary to get started with full-stack networking. Get ready to skyrocket through the IT Industry and become a rockstar engineer!



GETTING STARTED IN YOUR IT CAREER

You will begin with gaining insights into becoming a Network Engineer and understanding your career path options, and then you will move into understanding the overarching IT architectures that every engineer needs to know!

IT & NETWORK ESSENTIALS

You will dive into the most fundamental and foundational technical concepts to understand information technology and networking systems. We will cover networking basics, The OSI Model, Ethernet and VLANs, TCP & UDP, Topologies, cabling systems, network devices, IP addressing, subnetting, and routing and switching!

IP ADDRESSING & SUBNETTING

Here we will deconstruct the worlds of IP Addressing and subnetting providing you with the easiest method for subnetting both Class C and Class B default networks. After fully understanding IPv4 we will also introduce you to the world of IPv6!

ETHERNET, LANS, & SWITCHING

You will learn all about switching and making sure you understand core switching knoweldge with Ethernet, Spanning-Tree, VLANs, cabling, and power. In this module you will also learn how to make your own cables for Ethernet!

IP ROUTING IN LANS & WANS

In this module we will break down routing in greater detail and begin to understand exactly how routers route. We will cover topics and labs related to static routing, dynamic routing, routing protocols, and core routing concepts.

FULL STACK NETWORKING CONCEPTS

Building upon everything learned thus far, now you will dive into network security, wireless networking, voice over IP and virtualization to give a perspective on the knowledge of a Full Stack Network Engineer!

FULL STACK NETWORK ASSOCIATE

Build labs and practice your configuration skills with Full Stack Networking. Build out common networking designs and deploy fundamental topologies using Cisco IOS. Gain all the practice on real-world skills that you need before performing your Skills Qualification Check and obtaining your Full Stack Network Associate Certification!

FSNA CERTIFICATION: LEVEL UP!

To obtain your Full Stack Network Associate (FSNA) certification you will complete your final lab build-out including routing, switching, voice over IP, wireless network access, and network security. Your knowledge and skills will both be assessed to prove your abilities and obtain your FSNA certification!

FSNA Advanced Skills Training

FSNA ADVANCED SKILLS

A 100% skills-based block of study which prepares students for their upcoming projects and Full Stack Network Professional certification. In this training block, students will work to upgrade their existing FSNA network which they have already built to achieve FSNA certification. The new technologies being implemented are a router upgrade, NAT/PAT, IOS Firewall, and ACLs configuration, core switch upgrade, new VLANs, adding port-aggregation between switches, adding fiber optics for WAN connectivity, dual-router remote server network with EIGRP and HSRP, and lastly add another remote site with BGP connectivity across the private WAN. By the end of the FSNA Advanced Skills block student will be ready and eager to tackle the projects and all technical implementations that will be performed in FSNE Advanced Training!

Full Stack Network Professional

To earn the Full Stack Network Professional (FSNP) certification, students must first learn how to plan, design, implement and close out IT projects. Students will dive into real-world skills training and project-based learning with over 100+ hours of project build-out time. After building out these real-world projects students will also learn how to troubleshoot networks with common troubleshooting scenarios that are found in the field. To finally garner the FSNP certification students must pass their Skills Qualification Check (SCQ) proving they have the understanding needed to be an effective network engineer.



Full Stack Networking Project

The Full Stack Networking Project is designed to provide an understanding of a complete HQ/Branch network and the project build-out process. Students will learn how to plan, design, and implement their own Full Stack Network with a headquarters location and two branch offices. This project is performed locally on the student's computer and all configurations are completed using the Cisco Packet Tracer network simulation software. Cisco Packet Tracer is available for free from the Cisco Networking Academy.

HQ B2 | INET

PLANNING PHASE

In the Planning Phase we will perform all the necessary work to plan out our project. We'll start by gathering infromation and learning the requriements of the project. Then, we will produce a super professional diagram that details our solution. After we have the diagram, we will work on a Bill of Materials and Statement of Work that details the entire project plan. To wrap up the Planning Phase we will present our solution to the customer or business unit and once the project is approved we can get started with the **Execution Phase!**

EXECUTION PHASE

In the Execution Phase we will implement all the equipment and technologies defined in our Statement of Work. We'll start with setting up the Headquarters core network and then add internet, WAN routing, voice, and wireless services. After the Headquarters network build out is complete we'll begin work on Branch 1 and then Branch 2. By the end of this phase you will have deployed an entire 3 facility Full Stack Network!

CONTROLLING PHASE

CLOSING PHASE

Network Professional!

course.

In the Controlling Phase we will perform all of our final testing and make sure all deliverables in the Statement of Work have been met. We'll also tackle some support requests and make sure the customer is well taken care of before we move on to closing out the project.

You have arrived at the Closing Phase - It's been quite a journey! In

implemented Full Stack Network to the customer! To close things

out gracefully we will wrap up the project with a formal close-out

This phase wraps up the entire project and at this point you have

completed the great feat of deploying a complete HQ/branch

process and make sure we obtain feedback on the project delivery.

network environment with routing, switching, voice over IP, wireless

networking, and network security! Having compeleted this robust

project you now have an understanding of what it takes to roll out

services! After deploying this real-world project you are ready to

start preparing for your next two project deployments and your

Skills Qualification Check to become certified as a Full Stack

Troubleshooting Cisco IOS Networks

super valuable asset as you work to become skilled in

an IT project from start to finish and deploy the full stack of network

The Troubleshooting Cisco IOS Networks course is designed to give

troubleshooting. The labs in this course are performed on Cisco IOS

you real-world troubleshooting experience with reality-based

based routers and switches, using a wholistic approach, and

troubleshooting layers 1 through 4 as we progress through the

scenarios and solutions. This hands-on approach to training is a

the Closing Phase we get to have the pleasure of delivering the fully

Cisco ASA SSL VPN Project

This project is based on a very common deployment: installation of a new dedicated firewall in the network. In this case, we need a more advanced internet edge device to provide better site to site VPN capabilities and also telecommuter support with Remote Access VPN.



Colo Data Center Project

Another common extension of the network is to add a hot-site for disaster recovery and redundant network services. A Co-located Data Center will provide us redundancy in our infrastrutcture as well as our storage and server environments in the case of a disaster.



FSNP SQC Preparation Labs

Before performing the live Skills Qualification Check (SQC) to become certified as a Full Stack Network Professional, candidates will be provided with preparation labs and lab guides that will assist with reinforcement of all the concepts and skills that are checked during the live SQC.

FSNP Skills Qualification Check

During the final week students are scheduled to perform their live SQC to verify skills. The time allotted for the SQC itself is 4 hours. Students must perform their SQC in the NGT Academy online labs platform, achieve an 80% or better in lab completion, and solve troubleshooting tickets to complete the skills check as this part of the training is skills-based only. Upon successful completion the candidate will be awarded the Full Stack Network Professional (FSNP) certification.

FSNP

Cisco Certified Network Associate

The Cisco Certified Network Associate (CCNA) certification is one of the strongest associate level IT certifications in the world and proves your ability to install, configure, operate and troubleshoot enterprise networks and Cisco IOS. CCNA certified professionals understand the most core and fundamental technologies related to network engineering, and are versed in the configuration and installation of Cisco routers and switches in a broad range of IT environments. In this course students are presented with a series of premium instructional videos and hands-on labs that teach all the knowledge and skills needed to pass the 200-301 CCNA exam, obtain your CCNA certification, and get on your path to becoming a rockstar engineer!



NETWORK FUNDAMENTALS RELATED TO CISCO NETWORKING

You will learn all of the foundational network concepts found on the CCNA exam. In this section we will review network components such as routers, switches, firewalls, access-points, endpoints, servers and controllers. We will also cover topologies here as well as physical cabling and important protocols such as TCP and UDP. To wrap up and complete the network fundamentals module we will discuss operating systems and also the fundamentails of virtualization!

NETWORK ADDRESSING & MODELS

In this section we will thoroughly break down layer 2 and layer 3 addressing with MAC, IPv4 (addressing & subnetting), and IPv6. We will also look at addressing from the aspect of the Transport layer, how all of this network communication fits into a standard reference model and where we get these terms called layers.

NETWORK ACCESS

In this section we begin our dive into Cisco IOS configurations with LAN technologies such as VLANs, Trunking, layer 2 discovery protocols, port aggregation with EtherChannel/LACP, and Spanning-Tree Protocol. We will also look at Cisco Wireless Architectures, WLAN infrastructure, Wireless LAN Controllers, and WLAN setup and configuration to wrap up the LAN technologies that provide our clients with access to the network!

FULL

IP CONNECTIVITY

In this module we will move into configuring our routers and learn all about the core routing related concepts such as routing tables, static routing and routing protocols. We will configure routers to route dynamically within the autonomous system with Open Shortest Path First version 2 (OPSFv2) and learn how we an create routing redundancy in the LAN with first hop redundancy.

IP SERVICES

Here we will break down network services such as Network Timing Protocol (NTP), Dynamic Host Configuration Protocol (DHCP) and Quality of Service. We will break down and understand the Domain Name System (DNS), and learn how to manage our networks with SNMP and Syslog. We will also break down remote network access protocols and services such as Telnet and SSH, and understand how we can control and standardize network access for specific applicaitons and protocols with Quality of Service (QoS).

SECURITY FUNDAMENTALS

With the exponential growth of networked devices and internet connectivity, security has become an essential part of all IT infrastructures as all modern computer systems are networked and connected. Any connected system can be hacked, so all network engineers must understand key security concepts and industry standard security implementations. In this module you will learn all about these topics and also how to create secure networked connectivity with site to site VPNs and enhance security on the LAN with technologies such as DHCP snooping, ARP inspection, and port security.

AUTOMATION AND PROGRAMMABILITY

In this module you will learn about automated networking and device management using controller-based systems such as Cisco DNA center. In addition, we will dive into the internal network device architectures that can be conrolled with controller-based and software-defined networking. We will also discuss REST-based API (CRUD, HTTP vers, and data encoding) as it pertains to network automation and programmability as well as configuration management mechanisms such as Puppet, Chef, and Asible.

EXAM PREPARATION

You will learn how to prepare for the CCNA certification exam. We will supply testing information to help you focus on your studies, a practice exam, and information on how to get your exam scheduled. It's time to knock out that exam and become CCNA certified.

OPTIONAL CompTIA Network+

The Network+ certification course is designed to help students prepare for and obtain the CompTIA Network+ certification. This is a comprehensive certification course that covers the five domains of study as presented in the Network+ exam: Networking Concepts, Infrastructure, Network Operations, Network Security, and Network Troubleshooting and Tools. Students are presented with a series of lessons, labs, guizzes and practice tests that provide a complete learning experience and help the student prepare for the Network+ certification exam.



NGT Live! BONUS

Experience NGT LIVE! Dive into your first live IT conference with this premium experience. NGT Live was a live two-day virtual conference & career forum that brought together the IT community to share ideas and solutions to leveling up IT skills. The goal is to host an ecosystem-wide conference that was best in class, providing a platform where current and future industry leaders could network, educate, and learn from one another. And, to ensure we added the best possible value, we hosted a conference-wide career fair connecting hundreds of students with employers and jobs!



Server Virtualization & VMWare Course BONUS

This course is designed to help you understand how virtualization works at the fundamental level and how organizations of different sizes can take advantage of the capability. After covering the concepts and design, we focus on how you could build a VMware lab and access VMware products. Being able to play with the software and deploy it to learn the capabilities is essential. The deployment module walks you step by step through the process of deploying VMware ESXi and managing the virtual environment with VMware vSphere.







CYBER SECURITY ACCELERATOR

This robust training program provides students with a foundational understanding of the most important concepts and skills to prepare for a career in cybersecurity. In addition to learning through high quality instruction, students will also perform real-world labs and attack scenarios all throughout the program. The program begins with the NGT Cyber Security Associate course where students will prove their basic knowledge and skills to obtain their NCSA certification. After achieving NCSA, students will work toward their CompTIA Security+ and EC-Council specialization certifications. Dive into the worlds of ethical hacking, forensics, and attack & defense, and learn the crucial skills needed to work in cybersecurity at enterprise organizations - Your career in cybersecurity starts here!

1 FSNA is required before beginning the Cybersecurity Accelerator

NGT Cyber Security Associate

This course provides students with a foundational understanding of the most important cyber security topics, concepts, and skills. In addition to learning your foundational cybersecurity knowledge, we will build out a personal cybersecurity lab environment that you will be able to use throughout the course and for future labs and attack scenarios. After completing this course students will perform a written exam and skills qualification check to obtain their NGT Cyber Security Associate (NCSA) certification.



α

LABS

MODULES

We get started right away with building out a personal cybersecurity attack & defense lab environment! In this lab you will learn over 100+ skills related to network attacks, vulnerability analysis, forensics, incident response, reconnaissance, network security, packet analysis, and cryptography.



Cybersecurity Lab Environment

You will learn how to build your own lab environments that will enable you to vet your cybersecurity and hacking skills from now and into the future. We'll start with basic Linux and then build out various types of attacks where we'll dive into real-world hacking scenarios, demo real-world exploits, launch our own sandboxed-contained attacks, and explore system vulnerabilities and cybersecurity defense!

With Linux being the primary operating system for cybersecurity tools, you will learn how to use Linux command line and launch and run various tools that are used in the field. Some of the tools we use in our cybersecurity labs are: Linux command line, Kali Linux, Oracle virtualbox, NMAP, telnet, nc, Wireshark, Metasploit, Aircrack, Hashcat, Python web server, process explorer, strings, msfvenom, Ettercap, Openvas Greenbone, Shodan, Sublist3r, theHarvester, Google dorks, HxD, Scalpel, Github, and MRC.





Network Defense

IDENTIFY & ANALYZE THREATS

To begin, you will be introduced to a high level overview of the cybersecurity ecosystem. You will understand the threat actors and the different types of attacks you see in this domain. We will also take a look into the various toolkits and how they fit into common cyber security frameworks.

CRYPTOGRAPHY

This module will cover the fundamentals of cryptography along with practical use cases in today's world. It is an important aspect of security and forms the basis to many protocols that keep us safe. This module will help you understand what happens behind the scenes with these algorithms and how they are useful.

NETWORK SECURITY

Network security is the basis of cyber security operations. In this module we will look at the common security implementations in place and what the common weaknesses are. We will learn about low hanging fruit which are typically overlooked and provide a great way to raise threat awareness.

SECURE PROTOCOLS

This module is meant to help understand basic protocols and the best practices needed to create a security focused organization. The best offense is a defense and we will learn about the different tactics needed to raise the bar.

SYMPTOMS OF COMPROMISE

By recognizing the symptoms of an attack, analysts can help stop them much sooner. Here we will cover what to expect in different scenarios so that you can diagnose the problem in an efficient manner. This analysis is key to understanding what went wrong and how to prevent it from happening again in the future.

DEVICES & TOOLS

Cyber toolkits! A successful analyst has a wide arsenal of tools and knows how to effectively use them. In this module we will teach you which tools are available and how to apply them for all the various security solutions and strategies.

TESTING THE INFRASTRUCTURE

In this module we will take a look at all the practical applications of attacking your own infrastructure to help defend it. We will teach you how to identify your organizations own weaknesses such that you can help mitigate weaknesses and help define what changes need to be made.



INCIDENT RESPONSE

Incident response is a crucial approach on what to do in the event of a security breach. An organization needs the security team to have a playbook ready in times of crisis and how to react to certain events. We will take a look at planning on what is needed to be done.

NCSA CERTIFICATION: LEVEL UP!

To obtain your NexGenT Cyber Security Associate (NCSA) certification you will complete your NCSA Written Exam and NCSA Skills Qualification Check (SQC) Lab to prove your knowledge and skills to obtain your NCSA certification!



CompTIA Security+

The Security+ is the global standard foundational IT security certification. It is a strong vendor-agnostic IT & cybersecurity certification that helps to establish your core security-based knowledge and security best practices in Information Technology and networking systems.



The Security+ certification course is designed to help students prepare for and obtain the CompTIA Security+ certification. This is a comprehensive course that covers the five domains of study as presented in the Security+ certification blueprint: Attacks, Threats and Vulnerabilities, Architecture and Design, Implementation, Operations and Incident Response, and Governance, Risk and Compliance. Students are presented with a series of lessons, quizzes, and practice tests that provide a complete learning experience and make them ready to tackle the Security+ certification exam!

INTRODUCTION

In this module we will break down the CompTIA Security+ certification and ensure students understand how the exam objectives are laid out. We'll also look at an overview of this course and what you can expect from each module. It's time to begin your journey to become Security+ certified!

THREATS, ATTACKS & VULNERABILITIES

In this module we will dive right into security concepts and get started with learning about the most common types of network attacks. We will also explore the different types of systems and how they can be vulnerable to various types of cyber attacks. We will wrap up the module with an overview of performing penetration testing and security assessments.

ARCHITECTURE & DESIGN

Here we will expand upon general security related concepts and dive into different architectures such as cloud technologies, secure applications, physical security, cryptography, and embedded systems to understand their design and systems security implications.

IMPLEMENTATION

In this module we will learn how to implement security solutions across multiple different systems including application security, network design, wireless security, mobile security, cloud security, IAM, PKI, and Authentication and Authorization

OPERATIONS & INCIDENT RESPONSE

In this module we will expand into security tools, and how to properly investigate and respond to security related network and systems events. We will wrap up this module learning about endpoint security and also digital forensics!

EXAM PREPARATION

This module is all about preparing for the Security+ certification exam. Here, you'll find practice exams and information to help you focus on your study and preparations. Good luck on your exam - knock it out of the park!

EC-COUNCIL ESSENTIAL SERIES

Network Defense Essentials

Network Defense Essentials is a first-of-its-kind MOOC certification that provides foundational knowledge and skills in network security with add-on labs for handson experience. The course includes 12 modules and optional upgrades to lab ranges covering fundamental network security concepts, including IoT, cryptography, and PKI.

Ethical Hacking Essentials

Ethical Hacking Essentials is a first-of-its-kind MOOC certification that provides foundational knowledge and skills in ethical hacking with add-on labs for hands-on experience. The course contains 12 modules and add-on labs covering fundamental ethical hacking concepts, including emerging technologies like IoT and OT, cloud computing, etc.

Digital Forensics Essentials

Digital Forensics Essentials is a first-of-its-kind MOOC certification that offers foundational knowledge and skills on digital forensics with add-on labs for hands-on experience. Twelve modules cover the fundamental concepts of digital forensics, such as dark web forensics, investigating web application attacks, and more.



Network

Ethical

Defense Essentials

Hacking Essentials

NGT Live! BONUS

Experience NGT LIVE! Dive into your first live IT conference with this premium experience. NGT Live was a live two-day virtual conference & career forum that brought together the IT community to share ideas and solutions to leveling up IT skills. The goal is to host an ecosystem-wide conference that was best in class, providing a platform where current and future industry leaders could network, educate, and learn from one another. And, to ensure we added the best possible value, we hosted a conference-wide career fair connecting hundreds of students with employers and jobs!

