



AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE (AFRALTI)



CCNA Security Course

Course Introduction

The Cisco CCNA Security curriculum provides a next step for individuals who want to enhance their CCNA-level skill set and help meet the growing demand for network security professionals. The curriculum provides 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. CCNA Security helps prepare students for entry-level security career opportunities and the globally recognized Cisco CCNA Security certification.

This course is a hands-on, career-oriented e-learning solution with an emphasis on practical experience to help students develop specialized security skills, along with critical thinking and complex problem solving skills. CCNA Security is a blended curriculum with both online and classroom learning. Students who enroll in CCNA Security are expected to have CCNA-level networking concepts knowledge and skills, along with basic PC and Internet navigation skills.

While there are no required course prerequisites, students are encouraged to complete the CCNA Discovery or CCNA Exploration curricula to acquire the fundamental CCNA-level routing and switching skills needed for success in this course. CCNA Security provides a next step for CCNA Discovery or CCNA Exploration students who want to expand their CCNA-level skill set to prepare for a career in network security.

Opportunity

The Internet is changing life as we know it – bringing new economic and social opportunities to communities throughout the world, and increasing the global demand for information and communication technology (ICT) skills. Security and risk management skills are among the most highly sought after skills in networking, and demand continues to grow. Organizations around the world are experiencing a shortage of qualified ICT candidates with the specialized knowledge and skills needed to administer devices and applications in a secure infrastructure, recognize network vulnerabilities, and mitigate security threats.

Careers

CCNA Security supports students who plan to start a career, build a career, or switch focus in an IT networking career to security technologies. The curriculum emphasizes practical experience to help



students develop the skills needed for job roles such as network security specialists, security administrators, and network security support engineers. The CCNA Security curriculum is designed to meet the needs of today's IT professionals.

Assessments

Innovative formative and summative assessments are integrated into the CCNA Security curriculum and supported by an advanced online delivery system. Immediate, rich feedback supports instructor and student evaluation of acquired knowledge and skills. Assessments can be as simple as a multiple choice question or as complex as troubleshooting a simulated network.

Who Should Enroll

- University-level students seeking career-oriented, entry-level security specialist skills
- IT professionals wishing to broaden or add specialized skills to their technology expertise
- Current CCNA certification holders who wish to build on their CCNA knowledge base

Pre-Requisites

- CCNA-level networking concepts and skills
- Basic PC and Internet navigation skills

Note: Students can acquire the CCNA-level routing and switching skills needed for success in this course by completing CCNA programme offered at AFRALTI.

Duration – Six Weeks

Evening session: 5.30 - 7.30 pm

Afternoon Session: 2.00pm – 5.00 pm

Course Intakes: 08 Feb – 19 Mar 2009 , 05 Apr – 16 May 2009

Tuition Fees: KSh.40,000

Course Description

CCNA Security aims to develop an in-depth understanding of network security principles as well as the tools and configurations available. The course covers the following concepts:

- Protocol sniffers/analyzers
- TCP/IP and common desktop utilities
- Cisco IOS® Software
- Cisco VPN client
- Packet Tracer
- Web-based resources

Various types of hands-on labs provide practical experience, including procedural and troubleshooting labs, skills integration challenges, and model building. The curriculum also includes



Packet Tracer-based skills integration challenges that build throughout the course and lead to an “exam-like” culminating activity in the last chapter.

Course Outline

Chapter

Goals

- | | |
|---|---|
| 1. Modern Network Security Threats | Explain network threats, mitigation techniques, and the basics of securing a network |
| 2. Securing Network Devices | Secure administrative access on Cisco routers |
| 3. Authentication, Authorization and Accounting | Secure administrative access with AAA |
| 4. Implementing Firewall Technologies | Implement firewall technologies to secure the network perimeter |
| 5. Implementing Intrusion Prevention | Configure IPS to mitigate attacks on the network |
| 6. Securing the Local Area Network | Describe LAN security considerations and implement endpoint and Layer 2 security features |
| 7. Cryptography | Describe methods for implementing data confidentiality and integrity |
| 8. Implementing Virtual Private Networks | Implement secure virtual private networks |
| 9. Securing the Network | Given the security needs of an enterprise, create and implement a comprehensive security policy |

For more Information & enquiries, please contact:

Cisco Academy Training Center for Eastern Africa (CATC-EA)
P O Box 58902-00200, Nairobi, Kenya
Tel: +254 (0)20 444 0633 / 444 0625
Fax: +254 (0)20 444 44 83
Cell: +254 0710-207061/0733-444421
Net: <http://www.afralti.org>
Email: info@afralti.org

[Register Now!!](#)

