



# Institute of Continuing Education (IEC) American International University–Bangladesh

☎ 01630665666 ✉ Email: [ice@aiub.edu](mailto:ice@aiub.edu) 🌐 Web: <http://ice.aiub.edu/>

## CCNA v7 (200-301) Course Outline

### CCNA 1 – Introduction to Networks

Introduction to Networks (ITN) covers the architecture, structure, functions and components of the Internet and other computer networks. Students achieve a basic understanding of how networks operate and how to build simple local area networks (LAN), perform basic configurations for routers and switches, and implement Internet Protocol (IP).

Chapter	Topic
1	Networking Today
2	Basic Switch and End Device Configuration
3	Protocols and Models
4	Physical Layer
5	Number Systems
6	Data Link Layer
7	Ethernet Switching
8	Network Layer
9	Address Resolution
10	Basic Router Configuration
11	IPv4 Addressing
12	IPv6 Addressing
13	ICMP
14	Transport Layer
15	Application Layer
16	Network Security Fundamentals
17	Build a Small Network

Students who complete Introduction to Networks will be able to perform the following functions:

- Configure switches and end devices to provide access to local and remote network resources.
- Explain how physical and data link layer protocols support the operation of Ethernet in a switched network.
- Configure routers to enable end-to-end connectivity between remote devices.
- Create IPv4 and IPv6 addressing schemes and verify network connectivity between devices.
- Explain how the upper layers of the OSI model support network applications.
- Configure a small network with security best practices.
- Troubleshoot connectivity in a small network.



## Institute of Continuing Education (IEC) American International University–Bangladesh

☎ 01630665666 ✉ Email: [ice@aiub.edu](mailto:ice@aiub.edu) 🌐 Web: <http://ice.aiub.edu/>

### CCNA 2 – Switching, Routing and Wireless Essentials

Switching, Routing and Wireless Essentials (SRWE) covers the architecture, components and operations of routers and switches in small networks and introduces wireless local area networks (WLAN) and security concepts. Students learn how to configure and troubleshoot routers and switches for advanced functionality using security best practices and resolve common issues with protocols in both IPv4 and IPv6 networks.

Chapter	Topic
1	Basic Device Configuration
2	Switching Concepts
3	VLANs
4	Inter-VLAN Routing
5	STP Concepts
6	EtherChannel
7	DHCPv4
8	SLAAC and DHCPv6
9	FHRP Concepts
10	LAN Security Concepts
11	Switch Security Configuration
12	WLAN Concepts
13	WLAN Configuration
14	Routing Concepts
15	IP Static Routing
16	Troubleshoot Static and Default Routes

Students who complete the Routing and Switching Essentials course will be able to perform the following functions:

- Configure VLANs and Inter-VLAN routing applying security best practices.
- Troubleshoot inter-VLAN routing on Layer 3 devices.
- Configure redundancy on a switched network using STP and EtherChannel.
- Troubleshoot EtherChannel on switched networks.
- Explain how to support available and reliable networks using dynamic addressing and first-hop redundancy protocols.
- Configure dynamic address allocation in IPv6 networks.
- Configure WLANs using a WLC and L2 security best practices.
- Configure switch security to mitigate LAN attacks.
- Configure IPv4 and IPv6 static routing on routers.



## Institute of Continuing Education (IEC) American International University–Bangladesh

☎ 01630665666 ✉ Email: [ice@aiub.edu](mailto:ice@aiub.edu) 🌐 Web: <http://ice.aiub.edu/>

### CCNA 3 – Enterprise Networking, Security and Automation

Enterprise Networking, Security and Automation (ENSA) describes the architecture, components, operations and security to scale for large, complex networks, including wide area network (WAN) technologies. The course emphasizes network security concepts and introduces network virtualization and automation. Students learn how to configure, troubleshoot, and secure enterprise network devices and understand how application programming interfaces (API) and configuration management tools enable network automation.

Chapter	Topic
1	Single-Area OSPFv2 Concepts
2	Single-Area OSPFv3 Configuration
3	Network Security Concepts
4	ACL Concepts
5	ACLs for IPv4 Configuration
6	NAT for IPv4
7	WAN Concepts
8	VPN and IPsec Concepts
9	QoS Concepts
10	Network Management
11	Network Design
12	Network Troubleshooting
13	Network Virtualization
14	Network Automation

Students who complete the Scaling Networks course will be able to perform the following functions:

- Configure single-area OSPFv2 in both point-to-point and multiaccess networks.
- Explain how to mitigate threats and enhance network security using access control lists and security best practices.
- Implement standard IPv4 ACLs to filter traffic and secure administrative access.
- Configure NAT services on the edge router to provide IPv4 address scalability.
- Explain techniques to provide address scalability and secure remote access for WANs.
- Explain how to optimize, monitor, and troubleshoot scalable network architectures.
- Explain how networking devices implement QoS.
- Implement protocols to manage the network.
- Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks.