

VERSION

PROFESSIONAL

23

SR. CODE

EAPL/PROF/2024/PRTC17

COURSE CODE

EAPNP

SUB CATEGORY

INFRASTRUCTURE

 TOTAL DURATION 90 HOURS	 THEORY TAKEN 36 HOURS	 PRACTICAL TAKEN 54 HOURS
---	---	--

ELYSIUM
ACADEMY
CCNP
ENTERPRISE
(350-401
ENCOR)
**ELYSIUM
ACADEMY
CCNP
ENTERPRISE
(350-401
ENCOR)**
ELYSIUM
ACADEMY
CCNP
ENTERPRISE

COURSE DESCRIPTION



The CCNP Enterprise (350-401 ENCOR) course is designed to provide comprehensive training in advanced networking concepts, technologies, and best practices. This course covers topics such as network design, security, automation, virtualization, and troubleshooting.

COURSE GOALS



The CCNP Enterprise (350-401 ENCOR) course aims to provide in-depth knowledge and The goals of the course include preparing candidates for the CCNP Enterprise certification exam, enhancing their ability to design, implement, and troubleshoot enterprise networks, and equipping them with the expertise needed to keep pace with evolving technologies in the networking field.

FUTURE SCOPE



The CCNP Enterprise (350-401 ENCOR) certification course offers a wide range of career opportunities and growth potential in the field of networking and IT. By obtaining this certification, you demonstrate proficiency in designing, implementing, operating, and troubleshooting enterprise networks.

01

CHAPTER

ARCHITECTURE

1. Explain the different design principles used in an enterprise network

1. High-level enterprise network design such as 2-tier, 3-tier, fabric, and cloud
2. High availability techniques such as redundancy, FHRP, and SSO

2. Describe wireless network design principles

1. Wireless deployment models (centralized, distributed, controller-less, controller-based, cloud, remote branch)
2. Location services in a WLAN design
3. Client density

3. Explain the working principles of the Cisco SD-WAN solution

1. SD-WAN control and data planes elements
2. Benefits and limitations of SD-WAN solutions

4. Explain the working principles of the Cisco SD-Access solution

1. SD-Access control and data planes elements
2. Traditional campus interoperating with SD-Access

5. Interpret wired and wireless QoS configurations

1. QoS components
2. QoS policy



06
HRS



08
HRS

6. Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, & adjacency tables

02

CHAPTER

VIRTUALIZATION

1. Describe device virtualization technologies

1. Hypervisor type 1 and 2
2. Virtual machine
3. Virtual switching

2. Configure and verify data path virtualization technologies

1. VRF
2. GRE and IPsec tunneling

3. Describe network virtualization concepts

1. LISP
2. VXLAN


04
HRS


07
HRS

03

CHAPTER

INFRASTRUCTURE

1. Layer 2

1. Troubleshoot static and dynamic 802.1q trunking protocols
2. Troubleshoot static and dynamic Ether Channels


09
HRS


12
HRS

2. Layer 3

1. Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, metrics, and area types)
2. Configure simple OSPFv2/v3 environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point, and broadcast network types, & passive-interface)
3. Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)
4. Describe policy-based routing

3. Wireless

1. Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference, noise, bands, channels, and wireless client devices capabilities
2. Describe AP modes and antenna types
3. Describe access point discovery and join process (discovery algorithms, WLC selection process)
4. Describe the main principles and use cases for Layer 2 and Layer 3 roaming
5. Troubleshoot WLAN configuration and wireless client connectivity issues using GUI only
6. Describe wireless segmentation with groups, profiles, and tags

4. IP Services

1. Hypervisor type 1 and 2
2. Virtual machine
3. Virtual switching

04

CHAPTER

NETWORK ASSURANCE

1. Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog
2. Configure and verify Flexible NetFlow
3. Configure SPAN/RSPAN/ERSPAN
4. Configure and verify IPSLA
5. Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
6. 4.6 Configure and verify NETCONF and RESTCONF


04
HRS


07
HRS

05

CHAPTER

SECURITY

1. Configure and verify device access control

1. Lines and local user authentication
2. Authentication and authorization using AAA

2. Configure and verify infrastructure security features

1. ACLs
2. CoPP

3. Describe REST API security

4. Configure and verify wireless security features

1. 802.1X
2. WebAuth
3. PSK
4. (4-way handshake)

5. Describe the components of network security design

1. Threat defense
2. Endpoint security
3. Next-generation firewall
4. TrustSec and MACsec
5. Network access control with 802.1X, MAB, & WebAuth


08
HRS


11
HRS

06

CHAPTER

AUTOMATION

- 1. Interpret basic Python components and scripts**
- 2. Construct valid JSON-encoded files**
- 3. Describe the high-level principles and benefits of a data modeling language, such as YANG**
- 4. Describe APIs for Cisco DNA Center and vManage**
- 5. Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF**
- 6. Construct an EEM applet to automate configuration, troubleshooting, or data collection**
- 7. Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack**



05
HRS



09
HRS

Placement Assistance

100%

135+ Professional Courses

Practical Sessions

90%

67+ Global Pacts

Corporate Placements

65%

170+ IT Companies Tie-Up

ELYSIUM
GROUP OF
COMPANIES

**ELYSIUM
ACADEMY**

**PRIVATE
LIMITED**

AUTHORIZED INTERNATIONAL

Partners

