



סילבוס קורס הנדסת תקשורת DevNet&AI

תוכנית "לוחמים להייטק" בשיתוף האגף והקרן לחיילים משוחררים במשרד הביטחון, צה"ל, עמותת עתידים, מפעל הפיס ומכללת IITC גאים להציג: **קורס הנדסת תקשורת DevNet & AI ייעודי ללוחמות ולוחמים משוחררים** הצטרפו לתוכנית ההכשרה המקיפה ביותר בעולמות התקשורת, האוטומציה והבינה המלאכותית. הקורס כולל תהליך מיון, **710 שעות לימוד אקדמיות** ומתפרס על פני **5-6 חודשי לימוד** במודל "בוטקאמפ" אינטנסיבי. התוכנית שמה דגש חזק על למידה פרקטית, יישום ותרגול Hands-On של כלים עדכניים מהתעשייה, המדמים סביבות Production אמיתיות, כדי להבטיח כשירות תעסוקתית גבוהה כבר מהיום הראשון.

יתרונות הקורס

- **למידה מהבסיס:** הכשרה טכנולוגית מעמיקה בעולמות התקשורת וה-DevNet בשילוב כלי AI.
- **ניסיון מעשי:** פרויקטים מסכמים המדמים עבודה בצוותים טכנולוגיים בתעשייה.
- **ליווי לקריירה:** הכנה מלאה לעולם התעסוקה, סדנאות כתיבת קו"ח, הכנה לראיונות עבודה והשמה.
- **מעטפת אישית:** מלגת קיום חודשית מטעם עמותת עתידים וליווי אישי לאורך כל הדרך.

תנאי קבלה וזכאות

- **קהל יעד:** מסיימי ומסיימות שירות צבאי בתפקיד לחימה - עד 5 שנים מסיום השירות הסדיר. משרתי ומשרתות מילואים פעילים, וגם חיילות וחיילים בוזזים ששירתו בתפקיד לחימה - זכאים עד 10 שנים מסיום השירות הסדיר.
- **בגרות מלאה:** נדרשת בגרות מלאה עם לפחות 3 יח' מתמטיקה ו-3 יח' אנגלית.
- **מימון:** הקורס במימון כמעט מלא של האגף והקרן לחיילים משוחררים, צה"ל ועמותת עתידים.
- **השתתפות עצמית:** 1,000 ש"ח בלבד (ניתן למימוש מהפיקדון האישי).

פרטים לוגיסטיים

- **תאריך פתיחה:** 20/07/2026.
- **מתכונת הלימודים:** ימים א'-ה', בין השעות 09:00-16:30.
- **מיקום:** מכללת IITC, רמת גן (מרחק הליכה מתחנת רכבת תל אביב סביזור מרכז).



CCNA - 160 H

1. Network Fundamentals

1.1 Explain the role and function of network components

- Routers
- Layer 2 and Layer 3 switches
- Next-generation firewalls and IPS
- Access points
- Controllers
- Endpoints
- Servers
- PoE

1.2 Describe characteristics of network topology architectures

- Two-tier
- Three-tier
- Spine-leaf
- WAN
- Small office/home office (SOHO)
- On-premises and cloud

1.3 Compare physical interface and cabling types

Single-mode fiber, multimode fiber, copper Connections (Ethernet shared media and point-to-point)

1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

1.5 Compare TCP to UDP

1.6 Configure and verify IPv4 addressing and subnetting

1.7 Describe private IPv4 addressing

1.8 Configure and verify IPv6 addressing and prefix

1.9 Describe IPv6 address types

- Unicast (global, unique local, and link local)
- Anycast
- Multicast
- Modified EUI 64

1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)

1.11 Describe wireless principles

- Nonoverlapping Wi-Fi channels
- SSID
- RF
- Encryption

1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)

1.13 Describe switching concepts

- MAC learning and aging
- Frame switching
- Frame flooding
- MAC address table

CCNA - 160 H

2. Network Access

2.1 Configure and verify VLANs (normal range) spanning multiple switches

- Access ports (data and voice)
- Default VLAN
- InterVLAN connectivity

2.2 Configure and verify interswitch connectivity

- Trunk ports
- 802.1Q
- Native VLAN

2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol

- Root port, root bridge (primary/secondary), and other port names
- Port states and roles
- PortFast
- Root guard, loop guard, BPDU filter, and BPDU guard

2.6 Describe Cisco Wireless Architectures and AP modes

2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)

2.8 Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)

2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings

CCNA - 160 H

3. IP Connectivity

3.1 Interpret the components of routing table

- Routing protocol code
- Prefix
- Network mask
- Next hop
- Administrative distance
- Metric
- Gateway of last resort

3.2 Determine how a router makes a forwarding decision by default

- Longest prefix match
- Administrative distance
- Routing protocol metric

3.3 Configure and verify IPv4 and IPv6 static routing

- Default route
- Network route
- Host route
- Floating static

3.4 Configure and verify single area OSPFv2

- Neighbor adjacencies
- Point-to-point
- Broadcast (DR/BDR selection)
- Router ID

3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols

4. IP Services

4.1 Configure and verify inside source NAT using static and pools

4.2 Configure and verify NTP operating in a client and server mode

4.3 Explain the role of DHCP and DNS within the network

4.4 Explain the function of SNMP in network operations

4.5 Describe the use of syslog features, including facilities and severity levels

4.6 Configure and verify DHCP client and relay

4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, and shaping

4.8 Configure network devices for remote access using SSH

4.9 Describe the capabilities and functions of TFTP/FTP in the network

CCNA - 160 H

5. Security Fundamentals

5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

5.2 Describe security program elements (user awareness, training, and physical access control)

5.3 Configure and verify device access control using local passwords

5.4 Describe security password policy elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

5.5 Describe IPsec remote access and site-to-site VPNs

5.6 Configure and verify access control lists

5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

5.8 Compare authentication, authorization, and accounting concepts

5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

5.10 Configure and verify WLAN within the GUI using WPA2 PSK

6. Automation and Programmability

6.1 Explain how automation impacts network management

6.2 Compare traditional networks with controller-based networking

6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)

6.3.a Separation of control plane and data plane

6.3.b Northbound and Southbound APIs

6.4 Explain AI (generative and predictive) and machine learning in network operations

6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)

6.6 Recognize the capabilities of configuration management mechanisms such as Ansible and Terraform

6.7 Recognize components of JSON-encoded data

ENARSI - 250 H

The **Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)** training gives you the knowledge and skills needed to install, configure, operate, and troubleshoot a dual stack enterprise network. This training covers advanced routing and infrastructure technologies, expanding on the topics covered in the Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) training.

This training prepares you for the 300-410 ENARSI v1.1 exam. If passed, you earn the Cisco Certified Specialist – Enterprise Advanced Infrastructure Implementation certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Enterprise certification.

How You'll Benefit

This training will help you:

- Gain the knowledge you need to install, configure, operate, and troubleshoot a dual stack enterprise network
- Qualify for professional-level job roles in advance routing and services
- Prepare for the 300-410 ENARSI 1.0 exam

This exam tests your knowledge of implementing and troubleshooting for advanced routing technologies and services, including:

- Layer 3
- VPN services
- Infrastructure security
- Infrastructure services

Course Objectives

- Configure, optimize, and troubleshoot enhanced interior gateway routing protocol (EIGRP)
- Configure, optimize, and troubleshoot open shortest path first (OSPF)v2 and OSPFv3
- Implement and troubleshoot route redistribution using filtering mechanisms
- Implement path control using policy-based routing (PBR) and IP service level agreement (SLA)
- Configure, optimize, and troubleshoot border gateway protocol (BGP)
- Implement multiprotocol BGP (MP-BGP)
- Describe the features of multiprotocol label switching (MPLS)
- Describe the major architectural components of an MPLS virtual private network (VPN)
- Identify the routing and packet forwarding functionalities for MPLS VPNs
- Explain how packets are forwarded in an MPLS VPN environment
- Implement Cisco internetwork operating system (IOS®) dynamic multipoint VPNs (DMVPNs)
- Implement and troubleshoot dynamic host configuration protocol (DHCP)
- Describe the tools available to secure the IPV6 first hop
- Troubleshoot Cisco router security features
- Troubleshoot infrastructure security and services
- Troubleshoot network issues with Cisco DNA Center Assurance

ENARSI - 250 H

Course Outline

1. Implementing EIGRP
2. Optimizing EIGRP
3. Troubleshooting EIGRP
4. Implementing OSPF
5. Optimizing OSPF
6. Troubleshooting OSPF
7. Configuring Redistribution
8. Troubleshooting Redistribution
9. Implementing Path Control
10. Implementing IBGP
11. Optimizing BGP
12. Implementing MP-BGP
13. Troubleshooting BGP
14. Exploring MPLS
15. Introducing MPLS L3 VPN Architecture
16. Introducing MPLS L3 VPN Routing
17. Configuring VRF-Lite
18. Implementing DMVPN
19. Implementing DHCP
20. Introducing IPv6 First Hop Security
21. Securing Cisco Routers
22. Troubleshooting Infrastructure Security and Services
23. Troubleshooting with DNA Center Assurance

Lab Outline

1. Configure EIGRP Using Classic Mode and Named Mode for IPv4 and IPv6
2. Verify the EIGRP Topology Table
3. Configure EIGRP Stub Routing, Summarization, and Default Routing
4. Configure EIGRP Load Balancing and Authentication
5. Troubleshoot EIGRP Issues
6. Configure OSPFv3 for IPv4 and IPv6
7. Verify the Link-State Database
8. Configure OSPF Stub Areas and Summarization
9. Configure OSPF Authentication
10. Troubleshoot OSPF Issues
11. Implement Routing Protocol Redistribution
12. Manipulate Redistribution
13. Manipulate Redistribution Using Route Maps
14. Troubleshoot Redistribution Issues
15. Implement PBR
16. Configure IBGP and EBGP
17. Implement BGP Path Selection
18. Configure BGP Advanced Features
19. Configure BGP Route Reflectors
20. Configure MP-BGP for IPv4 and IPv6
21. Troubleshoot BGP Issues
22. Configure Routing with VRF-Lite
23. Implement Cisco IOS DMVPN
24. Obtain IPv6 Addresses Dynamically
25. Troubleshoot DHCPv4 and DHCPv6 Issues
26. Troubleshoot IPv4 and IPv6 ACL Issues
27. Configure and Verify uRPF
28. Troubleshoot Network Management Protocol Issues: Lab 1
29. Troubleshoot Network Management Protocol Issues: Lab 2

AUTOMATION - 200 H

Software Development and Design

1. Compare data formats (XML, JSON, and YAML)
2. Describe parsing of common data format (XML, JSON, and YAML) to Python data

structures

1. Describe the concepts of test-driven development
2. Compare software development methods (agile, lean, and waterfall)
3. Explain the benefits of organizing code into methods / functions, classes, and modules
4. Explain the advantages of common design patterns (MVC and Observer)
5. Explain the advantages of version control
6. Utilize common version control operations with Git
7. Clone
8. Add/remove
9. Commit
10. Push / pull
11. Branch
12. Merge and handling conflicts
13. diff

Understanding and Using APIs

1. Construct a REST API request to accomplish a task given API documentation
2. Describe common usage patterns related to webhooks
3. Describe the constraints when consuming APIs
4. Explain common HTTP response codes associated with REST APIs
5. Troubleshoot a problem given the HTTP response code, request and API documentation
6. Interpret the parts of an HTTP response (response code, headers, body)

7. Utilize common API authentication mechanisms: basic, custom token, and API keys
8. Compare common API styles (REST, RPC, synchronous, and asynchronous)
9. Construct a Python script that calls a REST API using the requests library

Application Deployment and Security

1. Describe the benefits of edge computing
2. Describe the attributes of different application deployment models (private cloud, public cloud, hybrid cloud, and edge)
3. Describe the attributes of these application deployment types
4. Virtual machines
5. Bare metal
6. Containers
7. Describe components for a CI/CD pipeline in application deployments
8. Construct a Python unit test
9. Interpret contents of a Dockerfile
10. Utilize Docker images in local developer environment
11. Describe application security issues related to secret protection, encryption (storage and transport), and data handling
12. Explain how firewall, DNS, load balancers, and reverse proxy in application deployment
13. Describe top OWASP threats (such as XSS, SQL injections, and CSRF)
14. Utilize Bash commands (file management, directory navigation, and environmental variables)
15. Describe the principles of DevOps practices

AUTOMATION - 200 H

Infrastructure and Automation

1. Describe the value of model driven programmability for infrastructure automation
2. Compare controller-level to device-level management 2025Cisco Systems, Inc. This document is Cisco Public. Page 3
3. Describe the use and roles of network simulation and test tools (such as Cisco Modeling Labs and pyATS)
4. Describe the components and benefits of CI/CD pipeline in infrastructure automation
5. Describe the principles of infrastructure as code
6. Describe the capabilities of automation tools such as Ansible, Terraform, and Cisco NSO
7. Identify the workflow being automated by a Python script that uses Cisco APIs including ACI, Meraki, Cisco Catalyst Center, and RESTCONF
8. Interpret the workflow being automated by an Ansible playbook (management packages, user management related to services, basic service configuration, and start/stop)
9. Interpret the workflow being automated by a bash script (such as file management, app install, user management, directory navigation)
10. Interpret the results of a RESTCONF or NETCONF query
11. Interpret basic YANG models
12. Interpret a unified diff
13. Describe the principles and benefits of a code review process
14. Interpret a sequence diagram that includes API calls

AI MODULE - 100 H

AI Fundamentals & Use Cases

1. Basics of AI, Machine Learning, and Generative AI
2. Common enterprise AI use cases
3. How AI workloads differ from traditional applications

AI Workloads & Models

1. Training vs. inference workloads
2. AI/ML models and compute clusters
3. Data pipelines and processing requirements
4. Tools used in AI environments

AI Infrastructure (Compute & Storage)

1. CPUs vs GPUs vs accelerators
2. High-performance compute requirements
3. Storage performance (throughput, latency, scale)
4. Virtualization and resource allocation

Networking for AI

1. High-bandwidth, low-latency networking
2. East-west traffic patterns in AI clusters
3. Lossless Ethernet concepts (critical for AI)
4. Network design for distributed workloads

AI Architecture & Design

1. Designing AI-ready data centers
2. On-prem vs hybrid vs cloud AI deployments
3. Scalability and interoperability

Security & Governance

1. Securing AI data and pipelines
2. Privacy and compliance considerations
3. Risk management

Deployment & Operations

1. Deploying AI workloads on infrastructure
2. Migration strategies
3. Monitoring and maintaining AI environments

Performance & Optimization

1. Bottleneck analysis
2. GPU and workload optimization
3. Scaling clusters efficiently