

AFRICA | **NIL**



CISCO Course Catalogue

Empower your IT career with globally recognised Cisco certifications.

Our Cisco training programmes are designed to build practical networking expertise, validate industry-relevant skills, and prepare professionals for a connected digital world.



AFRICA

NIL

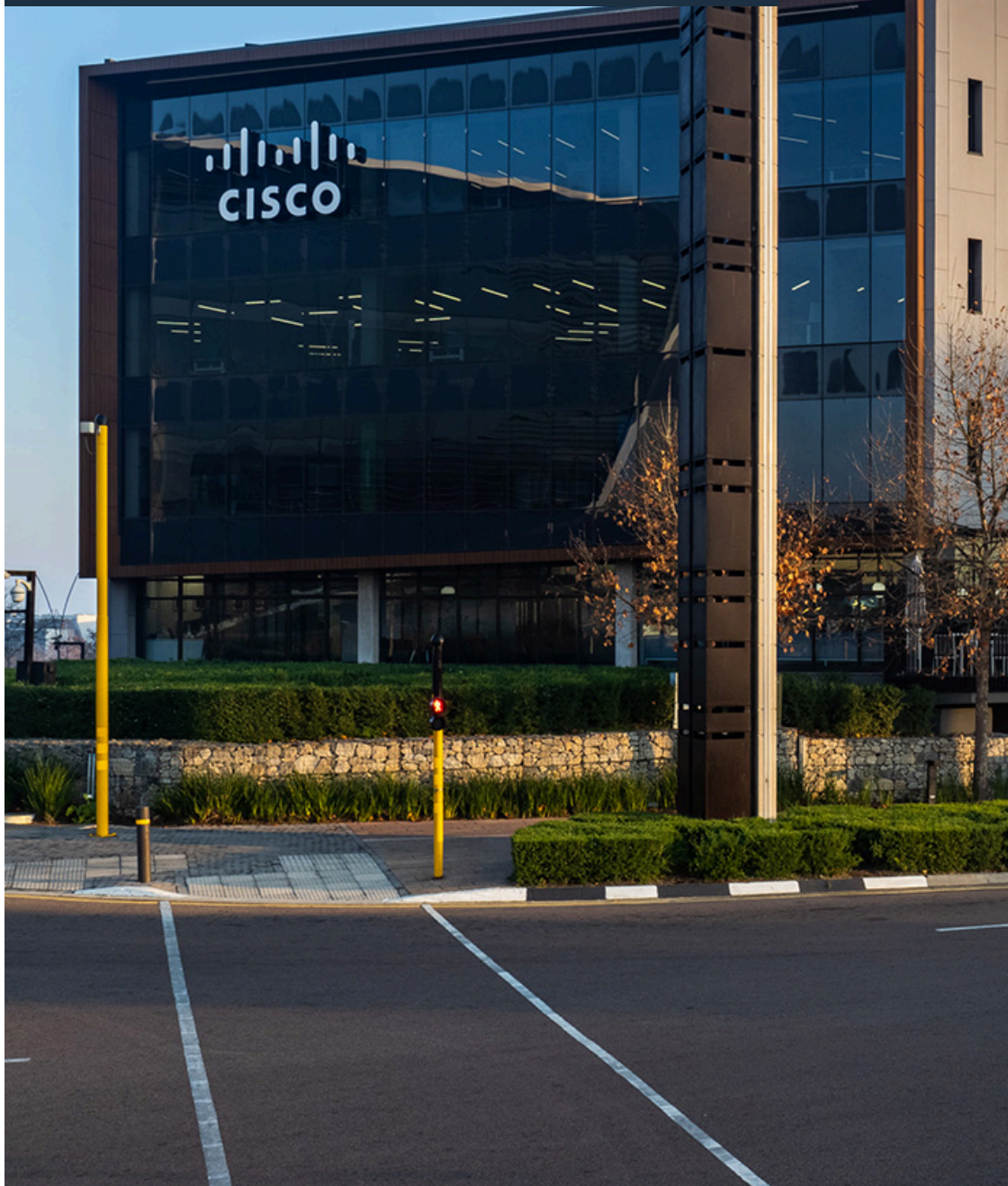


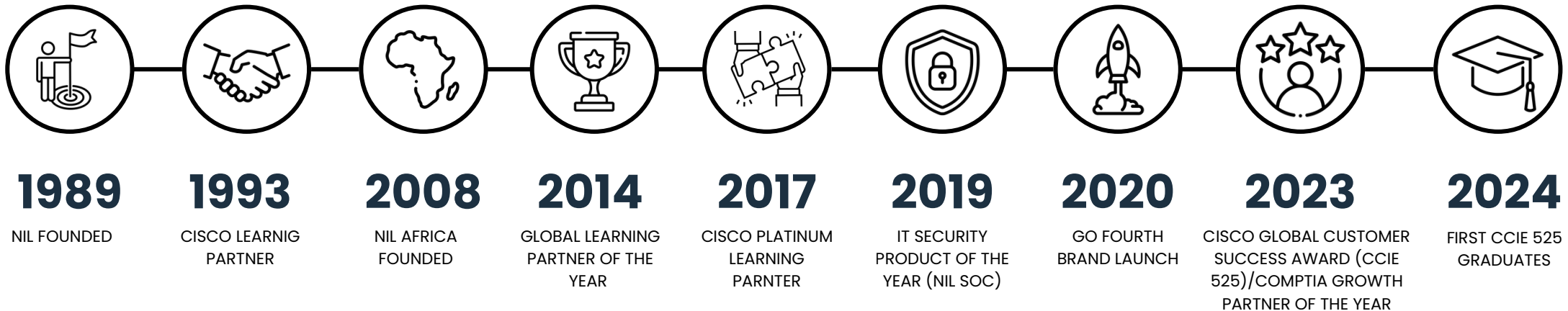
Table Of Content

Explore Our Learning Collections

1.Our timeline	Pg.3
2.Cisco Certified Associate Courses	Pg.4
3.Cisco Certified Professional Courses	Pg.7
4.CCNP Enterprise Infrastructure Elective Courses	Pg.8
5.CCNP Collaboration	Pg.11
6.CCNP Collaboration Elective Courses	Pg.12
7.CCNP Security Elective Courses	Pg.14
8.CCNP Service Provider Elective Courses	Pg.16
9.CCNP Data Centre Elective Courses	Pg.20
10.Cisco Cybersecurity Professional	Pg.23
11.Intelligent Networking	Pg.27
12.Smart Service Provider Networks	Pg.32
13.Cybersecurity	Pg.38
14.Cloud & Hybrid Infrastructure	Pg.40
15.Workforce Mobility	Pg.45
16.Intelligent Automation	Pg.49



Our Timeline



Cisco Certified Associate Courses

Build foundational networking skills aligned with Cisco industry standards.



Build a Strong Foundation for Your IT Career

Cisco Associate-level certifications are designed for professionals looking to establish or strengthen their skills in networking, cybersecurity, collaboration, and enterprise technologies.

These globally recognised credentials validate your ability to manage, configure, and troubleshoot Cisco solutions, giving you a competitive edge in today's IT job market.

Associate Certifications at a Glance

Cisco Certified Network Associate

The foundational networking certification. Gain essential knowledge in networking, security, automation, and IP connectivity.

Cisco Certified Cybersecurity Associate

Develop the skills to monitor, detect, and respond to cybersecurity threats within a Security Operations Centre (SOC).

Cisco Certified Automation Associate

Combine software development with networking. Learn to use APIs, automation, and programmability to optimise Cisco solutions.

Benefits of Certification with a Cisco Learning Partner

Take the first step in building your Cisco career pathway. Whether you're starting in networking, exploring cybersecurity, or bridging into automation, Cisco Associate certifications provide the foundation for professional success.

- Official Cisco-authorized training materials.
- Hands-on labs and real-world scenarios.
- Expert instructors with direct Cisco experience.
- Exam preparation guidance and practice resources.

Cisco Certified Associate Courses

Implementing and Administering Cisco Solutions (CCNA)	Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)	Automating Networks Using Cisco Platforms (CCNAUTO)
Duration 5 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 42	CLCs 43	CLCs 45
CE Credits 30	CE Credits 30	CE Credits 48
Exam 200-301	Exam 200-201	Exam 200-901
Course Outline: This training teaches you how to install, operate, configure, and verify a basic IPv4 and IPv6 network, configure network components, such as switches, routers, and wireless local area network (LAN) controllers (WLANs), manage network devices, and identify basic security threats. This training also covers the introduction of AI and machine learning (ML) in network operations. Learning Objectives: • Explain Network fundamentals • Configure & manage Cisco devices • Implement network architectures and services • Apply security principles • Describe the role of AI/ML in network operations Who Should Enroll: • Entry-level Network Engineers • Entry-level Network Administrators • Entry-level Network Support Technicians • Entry-level Help Desk Technicians Pre-requisites: • Basic computer literacy • Basic PC operating system navigation skills • Basic internet usage skills • Basic IP address knowledge	Course Outline: This training provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. This prepares you the job role of a cybersecurity analyst in a SOC. Learning Objectives: • Explain core security concepts • Apply security monitoring techniques • Perform host-based analysis • Conduct network intrusion analysis • Implement security policies and procedures Who Should Enroll: This training is designed for associate-level cybersecurity analysts who are working in security operation centres. Pre-requisites: • Basic computer literacy • Basic PC operating system navigation skills • Basic internet usage skills • Basic IP address knowledge	Course Outline: This training teaches you how to implement basic network applications using Cisco platforms, and how to implement automation workflows across network, security, collaboration, and computing infrastructure. The training gives you experience solving real-world problems using Cisco Application Programming Interfaces (APIs) and modern development tools. Learning Objectives: • Apply software development practices • Demonstrate core networking knowledge • Integrate network-based APIs using HTTP and REST • Explore Cisco platforms and programmability • Automate infrastructure and operational tasks • Explain application deployment and security fundamentals Who Should Enroll: • Network automation engineers • Software developer • System integration programmers • Infrastructure architects • Network designers Pre-requisites: • Basic computer literacy • Basic PC operating system navigation skills • Basic internet usage skills • Experience with a programming language (specifically Python)

Cisco Meraki Solutions Specialist

Engineering Cisco Meraki Solutions (ECMS)

Duration	4 Days
Delivery	ILT / VILT / Self-paced
CLCs	38
CE Credits	24
Exam	500-220

Course Outline:

This training gives you the knowledge and skills needed to deploy, plan, design, implement, and operate complex Cisco Meraki solutions. This training helps prepare you for roles focused on implementing, securing, and managing Cisco® Meraki™ based networks from a centralised dashboard.

Learning Objectives:

- Illustrate hierarchical network design and architectures
- Compare, configure, and optimise switching and routing protocols
- Implement network redundancy, NAT, and enterprise connectivity
- Configure and manage wireless networks and centralised controllers
- Troubleshoot Layer 2/3 connectivity and enterprise network issues
- Secure and administer Cisco devices following best practices
- Explain enterprise network security architectures and solutions
- Apply network programmability, APIs, Python scripting, QoS, and multicast concepts

Who Should Enroll:

- Network engineers
- Network administrators
- Network managers
- Systems engineers

Pre-requisites:

- Experience designing, deploying, scaling, and managing enterprise networks
- Strong understanding of dynamic routing protocols and secure connectivity technologies
- Foundational knowledge of RF fundamentals
- Foundational knowledge of network security controls, threat modelling, and wireless security
- Familiarity with modern network monitoring/management practices

Cisco Certified Professional Courses

Advance Your Skills. Lead in IT.

Cisco Professional-level certifications demonstrate advanced technical knowledge, practical skills, and the ability to design, implement, and troubleshoot sophisticated Cisco solutions.

To achieve CCNP status you will need to pass two exams in the technology of your choice:

- Core Exam
- Specialisation Exam

Professional Certifications at a Glance

Security: Prepare to secure enterprise networks, detect threats, and respond to security incidents.

Collaboration: Master Cisco collaboration technologies, including voice, video, and messaging solutions.

Automation: Advance your network automation and programmability skills, leveraging APIs and software development in complex IT environments.

Data Centre: Design, implement, and manage scalable data centre technologies and services.

Service Provider: Gain expertise in designing, deploying, and managing scalable service provider networks.

Cybersecurity: Develop advanced skills to defend, detect, and respond to evolving cyber threats across complex networks. Elevate your IT career. Cisco Professional-level certifications empower you to lead network design, security, and automation projects while proving your expertise to employers worldwide.

Enterprise Infrastructure: Validates advanced skills in implementing, operating, securing, and automating enterprise networks.

Wireless: Demonstrate your advanced knowledge and practical skills in designing, implementing, and managing modern wireless networks.

Cisco Certified Professional Courses

At-A-Glance: CCNP Enterprise Infrastructure Electives

ENARSI: Focuses on advanced routing and services, including Layer 3 IP, VPNs, EIGRP, OSPF, BGP, and infrastructure security, preparing learners for complex enterprise network environments.

ENSDWI: Covers designing, deploying, and operating enterprise networks, emphasizing WAN technologies, network services, QoS, and integrating automation and programmability for scalable and resilient infrastructures.

ENCC: Explores Cisco core networking technologies, including routing, switching, security, and services, preparing learners to implement, troubleshoot, and manage enterprise campus networks effectively.

ENNA: Focuses on network analysis, monitoring, and troubleshooting techniques using tools, telemetry, and Cisco solutions to ensure performance, reliability, and proactive network issue resolution.

ENSLD: Introduces enterprise network design principles, hierarchical models, campus and WAN architectures, and best practices to plan, design, and implement effective, scalable networks.

ENAUTO: Introduces network automation, programmability, and model-driven architecture using Python, APIs, SDN concepts, and Cisco automation tools to simplify and streamline enterprise network management.

Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	43
CE Credits	64
Exam	350-401

Course Outline:

This training gives you the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. You'll also learn to implement security principles, implement automation and programmability within an enterprise network, and how to overlay network design by using SD-Access and SD-WAN solutions.

Learning Objectives:

- Illustrate hierarchical network design and architectures
- Compare, configure, and optimize switching and routing protocols
- Implement network redundancy, NAT, and enterprise connectivity
- Configure and manage wireless networks and centralized controllers
- Troubleshoot Layer 2/3 connectivity and enterprise network issues
- Secure and administer Cisco devices following best practices
- Explain enterprise network security architectures and solutions
- Apply network programmability, APIs, Python scripting, QoS, and multicast concepts

Who Should Enroll:

- Mid-level network engineers
- Network administrators
- Network support technicians
- Help desk technicians

Pre-requisites:

- Understanding of how to implement enterprise LAN networks
- Basic understanding of enterprise routing and wireless connectivity
- Basic understanding of Python scripting

CCNP Enterprise Infrastructure Elective Courses

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)	Implementing Cisco SD-WAN Solutions (ENSDWI)	Designing and Implementing Cloud Connectivity (ENCC)
Duration 5 Days	Duration 5 Days	Duration 4 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 43	CLCs 43	CLCs 33
CE Credits 40	CE Credits 32	CE Credits 32
Exam 300-410	Exam 300-415	Exam 300-440
Course Outline: This 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. Learning Objectives: • Configure, optimize, and troubleshoot EIGRP, OSPF, and BGP protocols • Implement route redistribution, policy-based routing (PBR), and IP SLA for path control • Describe and implement MPLS VPN architectures and packet forwarding • Implement and troubleshoot DMVPN, DHCP, and IPv6 first-hop security features • Troubleshoot infrastructure security, services, and network issues using Cisco Catalyst Center Assurance Who Should Enroll: • Entry-Level Network Engineers • Network Administrators • Network Support Technicians • Help Desk Technicians Pre-requisites: • Understand network fundamentals and LAN implementation • Apply basic network device management and security practices • Explain interior gateway protocols (EIGRP, OSPF) and BGP • Implement core infrastructure services and security features (ACLs, SNMP, DHCP, IP SLA, Syslog, AAA, CoPP) • Demonstrate basic network automation concepts	Course Outline: This course teaches learners to design, deploy, configure, and manage Cisco SD-WAN in large networks. Topics include legacy WAN migration, routing protocols, advanced control and data policies, WAN Edge deployment, Direct Internet Access (DIA), AppQoE traffic optimisation, multicast and QoS, and implementing Cisco SD-WAN security solutions. Learning Objectives: • Explain Cisco SD-WAN concepts, deployment options, and fabric architecture • Deploy and configure WAN Edge devices using ZTP, PnP, and templates • Implement dynamic routing and advanced control/data policies including QoS and application-aware routing • Configure Direct Internet Access (DIA) and Cloud OnRamp for optimised connectivity • Apply SD-WAN security features and integrate them into network designs • Manage, monitor, and optimise the SD-WAN fabric including multicast and AppQoE capabilities Who Should Enroll: • Pre- and post-sales network engineers involved in the installation, support, and troubleshooting of a Cisco SD-WAN overlay network Pre-requisites: • Knowledge of SDN concepts as applied to large scale live networks • Strong understanding of enterprise WAN design • Strong understanding of routing protocol operations • Familiarity with TLS and IPSec	Course Outline: This training develops skills to design and implement enterprise cloud connectivity using private and public internet links. Learners explore AWS, Azure, and GCP integration, SaaS, DIA, and Cisco Umbrella. Topics include IPsec and SD-WAN connectivity, overlay routing with OSPF and BGP, policy implementation, and troubleshooting cloud connectivity, security, and application performance. Learning Objectives: • Explain core cloud computing concepts • Configure secure cloud connectivity options • Implement SaaS access and resilient architectures • Apply Cisco SD-WAN capabilities and security • Deploy overlay routing with OSPF and BGP • Troubleshoot connectivity and routing in cloud networks Who Should Enroll: This training is suitable for cloud professionals in roles such as architects, administrators, engineers, network and automation specialists, security managers, consultants, application developers, systems engineers, and technical solutions architects. Pre-requisites: • Basic computer literacy • Basic PC operating system navigation skills • Basic internet usage skills • Experience with a programming language (specifically Python)

CCNP Enterprise Infrastructure Elective Courses

Designing and Implementing Enterprise Network Assurance (ENNA)	Designing Cisco Enterprise Networks (ENSLD)	Automating and Programming Cisco Enterprise Solutions (ENAUTO)
Duration 4 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 36	CLCs 41	CLCs 44
CE Credits 32	CE Credits 40	CE Credits 34
Exam 300–445	Exam 300–420	Exam 300–435
Course Outline: This training expands your expertise in enterprise network assurance and management. You will explore Cisco assurance solutions, including ThousandEyes and Meraki Insight, and gain skills to deploy, configure, and manage them. It covers setup, optimisation, and daily operations, to monitor performance, troubleshoot issues, and ensure seamless, resilient, and continuous assurance across enterprise environments. Learning Objectives: • Explain core cloud computing concepts • Configure secure cloud connectivity options • Implement SaaS access and resilient architectures • Apply Cisco SD-WAN capabilities and security • Deploy overlay routing with OSPF and BGP • Troubleshoot connectivity and routing in cloud networks Who Should Enroll: • Network Administrators • System Engineers • Network Analysts • NOC Operators Pre-requisites: • Basic understanding of network fundamentals, including Cisco Catalyst SD-WAN, Cisco Catalyst Center, and Cisco Meraki • Basic understanding of Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Hypertext Transfer Protocol Secure (HTTPS), Secure Sockets Layer (SSL), and Domain Name System (DNS) protocol	Course Outline: This training strengthens your expertise in designing modern enterprise networks. It covers essential design principles, protocols, and technologies for wired and wireless environments, including SD-Access, VPN, QoS, IPv6, WAN, security services, and network programmability. Gain the advanced skills, practical experience, and best practices needed to create scalable, efficient, and secure enterprise networks. Learning Objectives: • Design enterprise routing and campus network architectures with Cisco SD-Access • Design resilient WAN and SD-WAN solutions • Integrate secure VPN technologies • Apply QoS and multicast design principles • Plan IPv6 and enable network automation Who Should Enroll: • Network Design Engineers • Network Engineers • System Administrators Pre-requisites: • Understanding network fundamentals • Implementing LANs • Implementing LAN connectivity	Course Outline: This course highlights the tools and the benefits of leveraging programmability and automation in the Cisco-powered Enterprise Campus and WAN. You will also examine platforms including IOS XE, Cisco Catalyst Center, Cisco SD-WAN, and Cisco Meraki. The current ecosystem of APIs, SDKs, and relevant workflows are studied together with open industry standards, tools, and APIs. Learning Objectives: • Explain model-driven network automation concepts • Automate network configuration and operations • Implement configuration management and compliance automation • Operate and automate Cisco platforms and controllers • Monitor, validate, and troubleshoot automated networks • Apply secure and AI-enabled automation practices Who Should Enroll: • Network Engineers • Systems Engineers • Technical Solutions Architects • Network Administrators and Managers Pre-requisites: • Basic programming language concepts • Basic understanding of virtualisation • Ability to use Linux and CLI tools; Secure Shell (SSH) and bash • CCNP level core networking knowledge • Foundational understanding of Cisco Catalyst Center, Meraki, and Cisco Catalyst SD-WAN

Cisco Certified Professional Courses

At-A-Glance: CCNP Enterprise Wireless Electives

ENWLSD: Focuses on designing enterprise wireless networks, including RF fundamentals, wireless LAN architectures, controller deployment, security, and optimisation for high-performance and reliable wireless connectivity.

ENWLSI: Builds on wireless implementation, guiding configuration, troubleshooting, and integration of enterprise WLANs, mobility, location services, and wireless security using Cisco controllers and access points.

Implementing and Operating Cisco Wireless Core Technologies (WLCOR)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	TBC
CE Credits	TBC
Exam	350-101

Course Outline:

This training gives you the knowledge and skills needed to implement core wireless technologies, including radio frequency and 802.11 technology fundamentals, client connectivity, wireless monitoring and management, and automation and AI.

Learning Objectives:

- Design, deploy, and configure Cisco enterprise wireless networks, including Catalyst 9800 Series WLCs and Meraki platforms
- Implement secure client connectivity and advanced features, such as roaming and guest access
- Monitor and manage wireless networks using Cisco Catalyst Center and automated tools
- Troubleshoot complex wireless issues using systematic methodologies and diagnostic tools
- Apply wireless networking theory, including radio frequency (RF) principles, protocols, and channel planning, to optimise enterprise networks

Who Should Enroll:

- Wireless network engineers
- Wireless network architects
- Network engineers
- Network architects

Pre-requisites:

- Understanding of how to implement enterprise LAN networks
- Basic understanding of enterprise routing and wireless connectivity
- Basic understanding of Python scripting

CCNP Enterprise Infrastructure Elective Courses

Implementing Cisco Enterprise Wireless Networks (ENWLSI)	Automating and Programming Cisco Enterprise Solutions (ENWLSD)
Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 43	CLCs 43
CE Credits 40	CE Credits 40
Exam 300-120	Exam 300-110
Course Outline: This training equips you to implement network settings to provide a secure wireless network infrastructure and troubleshoot any related issues. This training will prepare you to use Cisco ISE, Cisco PI, Cisco DNA Center, Cisco Spaces, and Cisco CMX to monitor and troubleshoot network issues. Learning Objectives: - Secure and administer wireless infrastructure - Implement and troubleshoot wireless access and authentication - Monitor, manage, and troubleshoot wireless operations - Analyse and optimise wireless client performance, including coverage, capacity, and throughput troubleshooting. - Deploy advanced wireless services and wireless service optimisation features. - Implement and operate location-based and analytics services, including presence analytics, and location accuracy validation and troubleshooting Who Should Enroll: - Wireless Network Administrators - Wireless Network Engineers - Network Support Engineers - Network Security Engineers Pre-requisites: - General knowledge of networks - General knowledge of wireless networks - General knowledge of monitoring and troubleshooting	Course Outline: This course introduces you to concepts you need to know when planning advanced designs of Cisco wireless products. The training covers design specifics from scenario design concepts, through the installation phase, and into post-deployment validation. Learning Objectives: - Apply Cisco structured wireless design methodologies to plan wireless networks. - Explain wireless standards and technologies - Design and implement advanced Cisco wireless features - Develop wireless designs for specific applications, vertical environments, and bridge or mesh deployments - Conduct wireless planning and validation activities, including site surveys and network performance verification - Execute end-to-end wireless design projects, including location-based services such as Cisco CMX and Cisco Spaces. Who Should Enroll: - Network and Wireless Engineers - Systems and Consulting Engineers - Technical Solutions Architects - Network Administrators and Managers Pre-requisites: - General knowledge of networks - General knowledge of wireless networks - Routing and switching knowledge



CCNP Collaboration

Implementing and Operating Cisco Collaboration Core Technologies On-Premises (CLCOR-OP)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	44
CE Credits	38
Exam	350-801

Course Outline:

This training is designed to provide you with a deep, working knowledge of on-premises Cisco collaboration infrastructure and competence in configuring and troubleshooting Cisco Unified Communications Manager, managing user identity via LDAP, designing complex dial plans, implementing edge services including Cisco Expressway and Cisco Unified Border Element, and integrating unified messaging systems like Cisco Unity Connection.

This is the first of two trainings which will prepare you for the 350-801 CLCOR exam.

Learning Objectives:

- Explain Cisco collaboration architecture and deployment models
- Implement layered security across collaboration environments
- Configure Cisco Unified Communications Manager (CUCM) for user and device provisioning
- Design and implement call routing and dial plans
- Deploy and manage collaboration edge and interconnect solutions
- Apply troubleshooting tools and methodologies
- Design and implement media resources
- Leverage APIs and automation in collaboration environments

Who Should Enroll:

- Network administrators
- Collaboration engineers

Pre-requisites:

- Basic understanding of networking technologies
- Basic understanding of voice and video
- Basic understanding of on-premises, cloud, and hybrid collaboration deployment models

Implementing and Operating Cisco Collaboration Core Technologies Hosted Cloud (CLCOR-HC)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	44
CE Credits	38
Exam	350-801

Course Outline:

This is designed to give you a working knowledge of hybrid and cloud Cisco collaboration core technologies. After completing this training, you will have a basic understanding of the Cisco collaboration solutions architecture. You will have proven competence in deploying cloud and hybrid services, cloud and hybrid calling, as well as Quality of Service (QoS).

This is the second of two trainings which will prepare you for the 350-801 CLCOR exam.

Learning Objectives:

- Explain Cisco collaboration architecture high-availability design
- Implement layered security across collaboration environments
- Deploy and manage Webex collaboration solutions, and migration from on-premises environments
- Design and implement Webex Calling
- Leverage Webex APIs and Cloud Connected UC
- Design and apply QoS for collaboration traffic

Who Should Enroll:

- Network administrators
- Collaboration engineers

Pre-requisites:

- Basic understanding of networking technologies
- Basic understanding of voice and video
- Basic understanding of on-premises, cloud, and hybrid collaboration deployment models

CCNP Collaboration Elective Courses

Implementing Cisco Advanced Call Control and Mobility Services (CLACCM)	Implementing Cisco Collaboration Applications (CLICA)	Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI)
Duration 4 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 43	CLCs 43	CLCs 43
CE Credits 40	CE Credits 40	CE Credits 40
Exam 300-815	Exam 300-810	Exam 300-820
Course Outline: This training develops expertise in advanced call control and mobility using Cisco Unified Communications Manager. It covers globalised call routing, dial plan replication, mobility services, SIP URI routing, call admission control, SRST, CUBE deployments, signalling and media protocols, and advanced routing features. Learning Objectives: - Analyse and troubleshoot SIP signalling and media. - Implement call features, including recording, time-of-day routing, and call coverage. - Configure Extension Mobility and Unified Mobility. - Deploy Cisco Unified Communications Manager Express for SIP endpoints. - Implement globalised call routing across clusters. - Configure and troubleshoot SRST on IOS gateways. - Implement CAC, AAR, URI calling, and ILS with GDPR. - Configure and troubleshoot Cisco Unified Border Element (CUBE). Who Should Enroll: - Collaboration Administrators - Collaboration Engineers Pre-requisites: - Foundational IT and networking knowledge - Fundamental knowledge of voice and collaboration concepts - Introductory Cisco Collaboration experience	Course Outline: This training teaches you the knowledge and skills to configure and troubleshoot Single Sign-On (SSO), Cisco Unity Connection and Cisco Unity Express, and Application clients. Topics covered include streamlining communication procedures, strengthening compliance measures, and enhancing communication systems and devices. Learning Objectives: - Configure and integrate Cisco Unity Connection. - Configure and troubleshoot Cisco Unity Connection call handlers. - Configure and troubleshoot Cisco Unity Express. - Explain Single Sign-On (SSO) for Cisco Unified Communications applications. - Integrate Cisco Jabber and IM and Presence with Cisco and third-party applications. - Customise and troubleshoot Cisco Jabber and IM and Presence services. - Configure and troubleshoot chat rooms and message archiving. - Integrate Unified Attendant Console Advanced and configure call recording and monitoring. Who Should Enroll: - Collaboration Administrators - Collaboration Engineers Pre-requisites: - Basic understanding of networking technologies - Basic understanding of voice and video - Cisco Unified Communications Manager (CUCM) experience including single site dial plan, single Public Switched Telephone Network (PSTN) gateway, and Session Initiation Protocol (SIP) trunks	Course Outline: This training provides you with an understanding of Cisco Expressway Series solutions, such as B2B calls, Cisco Mobile and Remote Access for remote workers, authentication options, and additional Cisco Expressway Series features. Topics covered also include details about the Webex solutions, and the benefits of hybrid integrations between Cisco on-premises solutions and Webex Meetings in the cloud. Learning Objectives: - Describe Cisco Expressway Core features, functionality, and additional capabilities. - Configure and troubleshoot integration between Cisco Unified Communications Manager and Expressway. - Configure and secure Business-to-Business (B2B) collaboration using Expressway. - Explain Mobile and Remote Access (MRA) features and security options. - Integrate Expressway with Unity Connection and IM & Presence. - Describe Cisco Webex cloud deployment models and administration via Control Hub. - Explain Webex Hybrid Services and their integration with on-premises systems. - Manage users, sites, and administrative tasks within Cisco Webex. Who Should Enroll: - Collaboration Administrators - Collaboration Engineers Pre-requisites: - Understanding of networking technologies - Understanding voice and video - Knowledge of Cisco collaboration core technologies

CCNP Security

Implementing and Operating Cisco Security Core Technologies

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	43
CE Credits	64
Exam	350-701

Course Outline:

This training equips you with the skills and knowledge to implement core Cisco security solutions effectively. You will learn to protect networks, devices, and data against advanced cybersecurity threats, gain hands-on experience with threat detection and mitigation technologies, and prepare for senior-level security roles in complex enterprise environments.

Learning Objectives:

- Explain security concepts, network threats, and attack techniques.
- Implement access control and security policies on Cisco ASA.
- Deploy and configure Cisco Secure Email Gateway and Web Security.
- Manage Cisco Umbrella, Secure Endpoint, and network access.
- Implement site-to-site and remote VPNs using ASA, Threat Defense, and IOS VTI.
- Configure data plane and control plane protections on IOS and ASA.
- Deploy network telemetry, Secure Network Analytics, and cloud security solutions.
- Understand software-defined networking, network programmability, and cloud security.

Who Should Enroll:

- Network engineers
- Solutions architects
- Network administrators
- Network designers

Pre-requisites:

- Familiarity with basics of networking security concepts
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

At-A-Glance: CCNP Security Electives

SNCF: Focuses on advanced routing and services, including Layer 3 IP, VPNs, EIGRP, OSPF, BGP, and infrastructure security, preparing learners for complex enterprise network environments.

SISE: Covers designing, deploying, and operating enterprise networks, emphasizing WAN technologies, network services, QoS, and integrating automation and programmability for scalable and resilient infrastructures.

SESA: Explores Cisco core networking technologies, including routing, switching, security, and services, preparing learners to implement, troubleshoot, and manage enterprise campus networks effectively.

SWSA: Focuses on network analysis, monitoring, and troubleshooting techniques using tools, telemetry, and Cisco solutions to ensure performance, reliability, and proactive network issue resolution.

SVPN: Introduces enterprise network design principles, hierarchical models, campus and WAN architectures, and best practices to plan, design, and implement effective, scalable networks.

SCAZT: Focuses on designing enterprise wireless networks, including RF fundamentals, wireless LAN architectures, controller deployment, security, and optimisation for high-performance and reliable wireless connectivity.

SDSI: Builds on wireless implementation, guiding configuration, troubleshooting, and integration of enterprise WLANs, mobility, location services, and wireless security using Cisco controllers and access points.



CCNP Security Elective Courses

Securing Networks with Cisco Firewall (SNCF) 300-710

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)

Duration	4 Days
Delivery	ILT / VILT / Self-paced
CLCs	40
CE Credits	40

Course Outline:

This training shows you how to implement and configure Cisco Secure Firewall Threat Defense for deployment as a next generation firewall at the internet edge. You'll gain an understanding of Cisco Secure Firewall architecture and deployment, base configuration, packet processing and advanced options, and conducting Secure Firewall administration troubleshooting.

Learning Objectives:

- Describe Cisco Secure Firewall Threat Defense features, deployment, and management.
- Configure initial settings, high availability, and basic NAT.
- Configure discovery, prefilter, tunnel, access control, and security intelligence policies.
- Configure file and intrusion policies.
- Perform threat analysis via Cisco Secure Firewall Management Center.
- Conduct system administration tasks.
- Troubleshoot traffic flow.
- Manage devices with Cisco Secure Firewall Threat Defense Manager.

Who Should Enroll:

- Network security engineers
- Network Administrators

Pre-requisites:

- Knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP)
- Basic knowledge of routing protocols
- Familiarity with the content explained in the Securing Internet Edge with Cisco Secure Firewall Threat Defense training

Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)

Duration	4 Days
Delivery	ILT / VILT / Self-paced
CLCs	40
CE Credits	40

Course Outline:

This training teaches deployment and configuration of Cisco Secure Firewall Threat Defense as a data center or Internet Edge firewall. You will learn identity-based policies, SSL decryption, site-to-site and remote VPNs, advanced IPS, event management, integrations, troubleshooting, automation with APIs, and migration from Cisco ASA systems.

Learning Objectives:

- Explain Cisco Secure Firewall Threat Defense features, deployment, and management.
- Configure initial settings, high availability, and NAT.
- Implement discovery, prefilter, tunnel, and access control policies.
- Configure security intelligence, file, and intrusion policies.
- Perform threat analysis using Management Center.
- Conduct system administration tasks.
- Troubleshoot traffic flow.
- Manage devices with Threat Defense Manager.

Who Should Enroll:

- Network security engineers
- Network Administrators

Pre-requisites:

- Knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP)
- Basic knowledge of routing protocols
- Familiarity with the content explained in the Securing Internet Edge with Cisco Secure Firewall Threat Defense training

CCNP Security Elective Courses

Implementing and Configuring Cisco Identity Services Engine (SISE)	Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)	Designing Cisco Security Infrastructure (SDSI)
Duration 5 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 43	CLCs 44	CLCs 44
CE Credits 40	CE Credits 40	CE Credits 41
Exam 300-715	Exam 300-740	Exam 300-745
Course Outline: This training teaches deployment and use of Cisco Identity Services Engine (ISE) v3.x for secure access across wired, wireless, and VPN networks. You will gain hands-on experience with Zero Trust use cases, including policy enforcement, BYOD, endpoint compliance, TACACS+ administration, web authentication, guest access, and network visibility. Learning Objectives: - Describe Cisco ISE features, deployment options, and TrustSec configurations. - Explain policy enforcement components and configure policies. - Troubleshoot policies and third-party Network Access Device (NAD) support. - Configure guest access, hotspots, and guest portals. - Describe and configure profiler services and reporting best practices. - Implement BYOD solutions and endpoint compliance. - Configure client posture services. - Configure device administration with Cisco ISE. Who Should Enroll: - Network security engineers - Network security architects - ISE administrators Pre-requisites: - Familiarity with the Cisco IOS® Software Command-Line Interface - Familiarity with Cisco AnyConnect® Secure Mobility Client - Familiarity with Microsoft Windows operating systems - Familiarity with 802.1X	Course Outline: This training teaches you the skills for designing and implementing cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and assurance, and responding to cloud threats. Learning Objectives: - Compare NIST, CISA, and DISA frameworks and their impact on cybersecurity posture. - Describe Cisco Security Reference and SAFE architectures. - Implement certificate-based authentication, Duo MFA, endpoint compliance, and SSO. - Explain Cisco SD-WAN security services and Cloud OnRamp. - Describe Cisco Umbrella SIG features, cloud access, and reverse proxy protections. - Understand Cisco Secure Firewall, web application firewalls, and Secure Workload deployment. - Apply cloud security, attack mitigation, multicloud policy, and visibility tools. - Use APIs and automation for cloud threat detection, troubleshooting, and response. Who Should Enroll: - Network engineers - Network security engineers - Network architects Pre-requisites: - Basic understanding of enterprise routing - Basic understanding of WAN and Cisco SD-WAN - Basic understanding of Public Cloud services	Course Outline: This training provides comprehensive knowledge of security architecture design, covering secure infrastructure and applications, risk management, and event handling. It explores the integration of artificial intelligence (AI) and automation to enhance security operations, while addressing compliance requirements and best practices in implementing DevSecOps principles for secure, efficient, and resilient systems. Learning Objectives: - Explain core security architecture concepts, design principles, and frameworks. - Identify security layers, technologies, and compliance enforcement methods. - Implement secure network access, including 802.1X, MAB, and web authentication. - Compare traditional and next-gen firewalls, WAFs, IDS/IPS, and WAN security. - Protect endpoints, cloud services, microservices, and containers. - Secure application data in transit and at rest. - Integrate DevSecOps, AI, and automation for security and incident response. - Use tools and frameworks to detect, respond to, and mitigate security incidents. Who Should Enroll: - Systems architects - Security architects Pre-requisites: - Knowledge of Cisco security core technologies

CCNP Security

Securing Email with Cisco Email Security Appliance (SESA)	Securing the Web with Cisco Web Security Appliance (WSA)	Implementing Secure Solutions with Virtual Private Networks (VPN)
Duration 4 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 36	CLCs 20	CLCs 43
CE Credits 24	CE Credits 16	CE Credits 40
Exam 300-720	Exam 300-725	Exam 300-730
Course Outline: This training teaches deployment and administration of Cisco Secure Email Gateway to protect email systems from phishing, ransomware, and business email compromise. You will gain hands-on experience implementing, troubleshooting, and managing key capabilities, including malware protection, spam and virus filtering, outbreak filtering, encryption, quarantines, and data loss prevention. Learning Objectives: - Describe and administer Cisco Secure Email Gateway. - Control sender/recipient domains and spam using Talos SenderBase. - Apply anti-virus, outbreak, mail, content, and message filters. - Implement data loss prevention and email encryption. - Authenticate SMTP sessions and email. - Perform LDAP queries. - Use system quarantines, delivery methods, and centralized cluster management. - Test and troubleshoot email security configurations. Who Should Enroll: - Security engineers - Security administrators - Security architects Pre-requisites: - Foundational IT and networking knowledge - Fundamental knowledge of security concepts - Experience with IP routing	Course Outline: This training teaches implementation, use, and administration of Cisco Web Security Appliance (WSA) to protect against web and email threats. You will gain hands-on experience deploying proxy services, authentication, HTTPS and access policies, user controls, anti-malware, data security, and data loss prevention, ensuring effective web threat management. Learning Objectives: - Describe Cisco WSA - Deploy proxy services - Utilise authentication - Describe decryption policies to control HTTPS traffic - Understand differentiated traffic access policies and identification profiles - Enforce acceptable use control settings - Defend against malware - Describe data security and data loss prevention - Perform administration and troubleshooting Who Should Enroll: - Security engineers - Security administrators - Security architects Pre-requisites: - Foundational IT and networking knowledge - Fundamental knowledge of security concepts - Experience with IP routing	Course Outline: This training teaches implementation, configuration, monitoring, and support of enterprise VPN solutions. You will gain hands-on experience deploying and troubleshooting IPsec, DMVPN, FlexVPN, and remote access VPNs, enabling secure, encrypted data transmission, remote accessibility, and enhanced privacy for enterprise networks. Learning Objectives: - Introduce site-to-site VPN options available on Cisco router and firewalls - Introduce remote access VPN options available on Cisco router and firewalls - Review site-to-site and remote access VPN design options - Review troubleshooting processes for various VPN options available on Cisco router and firewalls Who Should Enroll: - Security engineers - Security administrators - Security architects Pre-requisites: - Familiarity with the various Cisco router and firewall command modes - Experience navigating and managing Cisco routers and firewalls - Clear understanding of the benefits of site-to-site and remote access VPN options

CCNP Service Provider

Implementing and Operating Cisco Service Provider Core Technologies (SPCOR)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	43
CE Credits	64
Exam	350–501

Course Outline:

This training expands your knowledge and skills of service provider core networks. You will learn how to implement and operate service provider networks using technologies such as core architecture, services, networking, automation, quality of service (QoS), security, and network assurance.

Learning Objectives:

- Describe service provider network architectures, transport technologies, and Cisco IOS/XR software models.
- Implement core routing protocols in service provider networks, including OSPF, IS-IS, and BGP.
- Apply routing policies using route maps and routing policy language.
- Implement high availability, traffic engineering, and segment routing concepts.
- Deploy VPN services, including MPLS L2VPN, MPLS L3VPN, and multicast.
- Design and implement QoS architectures for service provider environments.
- Secure control, management, and data planes on Cisco devices.
- Apply automation, YANG modeling, virtualization, and orchestration using Cisco NSO.

Who Should Enroll:

- Network administrators
- Network engineers
- Systems engineers

Pre-requisites:

- Familiarity with Cisco IOS, IOS XE and IOS XR software configuration
- Knowledge of IPv4 and IPv6
- Understanding of MPLS technologies and VPN technologies

At-A-Glance: CCNP Service Provider Electives

SPRI: The training teaches you theories and practices to integrate advanced routing technologies, expanding your knowledge and skills in service provider core networks.

SPVI: The training prepares you to deploy, configure, monitor, operate, and troubleshoot end customer VPN environments built over a common Service Provider MPLS backbone.

SPCNI: Gain the knowledge to design, implement, and manage virtualisation cloud infrastructures for optimisation in a service provider network using programmability and orchestration.



CCNP Service Provider Elective Courses

Implementing Cisco Service Provider Advanced Routing Solutions (SPRI)	Implementing Cisco Service Provider VPN Services (SPVI)	Designing and Implementing Cisco Service Provider Cloud Network Infrastructure (SPCNI)
Duration 5 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 44	CLCs 43	CLCs 44
CE Credits 37	CE Credits 40	CE Credits 40
Exam 300-510	Exam 300-515	Exam 300-540
Course Outline: This training teaches you theories and practices to integrate advanced routing technologies including routing protocols, multicast routing, policy language, Multiprotocol Label Switching (MPLS), and segment routing, increasing your knowledge and skills of implementing Service Provider core advanced technologies through hands-on application and practical instruction Learning Objectives: • Configure and optimise multiarea OSPF and special area types. • Implement and optimise IS-IS multilevel networks. • Configure BGP for route selection, security, convergence, and scalability. • Apply routing policy and route redistribution. • Troubleshoot service provider routing protocols. • Implement MPLS, segment routing, SRv6, and traffic engineering. • Implement IPv6 tunneling mechanisms. • Deploy and troubleshoot IP multicast services. Who Should Enroll: • Network Administrators • System Engineers • Network Designers Pre-requisites: • Intermediate to advanced knowledge of Cisco IOS, IOS XE and Cisco IOS XR Software configuration • Knowledge of IPv4 and IPv6 TCP/IP networking • Intermediate knowledge of BGP, OSPF, and ISIS routing protocols • Understanding of MPLS and multicast technologies • Familiarity with segment routing	Course Outline: This training prepares you to implement and support VPN solutions on top of an MPLS network infrastructure. It includes hands-on labs covering MPLS VPN fundamentals, operations, and architectures that prepare you to deploy, monitor, operate, and troubleshoot customer VPN environments built on a service provider MPLS backbone. Learning Objectives: • Describe VPN concepts and operations at a service provider • Implement Layer 3 MPLS VPN operations at a service provider • Implement Layer 3 Inter-domain MPLS VPN services traversing multiple service providers • Implement Layer 3 Multicast MPLS VPN operations at a service provider • Troubleshoot typical issues in Layer 3 MPLS VPN environments • Implement and troubleshoot Layer 2 VPN operations in a service provider environment • Implement and troubleshoot MPLS VPN solutions for IPv6 environments Who Should Enroll: • Network engineers • Network administrators • Network architects Pre-requisites: • Solid IP and routing fundamentals • Foundational understanding of MPLS and L2 and L3 VPNs. • Hands-on familiarity with Cisco IOS/IOS XR and service provider network architectures.	Course Outline: This training teaches you to design and implement virtualisation cloud infrastructures in service provider networks. You will learn virtualised network functions, programmability, and orchestration, cloud computing fundamentals, cloud and data centre interconnect solutions, and methods to monitor, secure, optimise, and ensure high availability across virtualised cloud environments. Learning Objectives: • Describe Cisco NFVI, VIM, NSO, and infrastructure management. • Explain OpenStack networking, operations, and NFVI security. • Describe application hosting on IOS XR, containers, and Kubernetes. • Explain cloud computing models, services, and carrier-neutral facilities. • Implement MPLS, Segment Routing, SRv6, and SR-TE. • Secure control and data planes using BGP, IGP, MACsec, uRPF, and black-holing. • Deploy high availability, multihoming, QoS, and traffic optimisation. • Use telemetry, ThousandEyes, and Cisco Crosswork for visibility and assurance. Who Should Enroll: • Network engineers • Cloud engineers • Cloud and network architects Pre-requisites: • Experience with BGP, IS-IS, and OSPF • Knowledge of Layer 2 IEEE switching and related protocols, MPLS configuration and troubleshooting in a large network environment

CCNP Data Centre

Implementing and Operating Cisco Data Centre Core Technologies (DCCOR)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	46
CE Credits	64
Exam	350–601

Course Outline:

This training teaches you to implement data centre LANs and SANs and compute using Cisco Nexus Switches, Cisco MDS Switches, Cisco Unified Computing System (UCS) B-Series Blade Servers, and Cisco UCS C-Series Rack Servers. You will also learn the essentials of automation and security in data centres. It provides hands-on experience with deploying, securing, operating, and maintaining Cisco data centres.

Learning Objectives:

- Implement Layer 2/3 protocols, STP, port channels, HSRP/VRRP/GLBP, OSPF, BGP, multicast, and VXLAN.
- Apply network and UCS infrastructure security features.
- Understand high-performance Ethernet fabrics and Cisco ACI architecture and traffic flows.
- Configure ACI building blocks, VMM integration, and fabric setup.
- Manage network configuration, updates, monitoring, and telemetry-based assurance.
- Deploy Fibre Channel, FCoE, SAN services, and storage security.
- Implement UCS servers, Fabric Interconnects, unified computing, and SAN integration.
- Use automation and orchestration tools including Ansible, Puppet, and Python.

Who Should Enroll:

- Network engineers / administrators / designers
- Data centre engineers / administrators / designers
- Server engineers / administrators / designers
- Storage engineers / administrators / designers

Pre-requisites:

- Familiarity with Ethernet and TCP/IP networking, SANs and Fibre Channel protocol
- Understanding of Cisco Data Centre architecture
- Understanding of server system design and architecture
- Familiarity with hypervisor technologies

At-A-Glance: CCNP Data Centre Electives

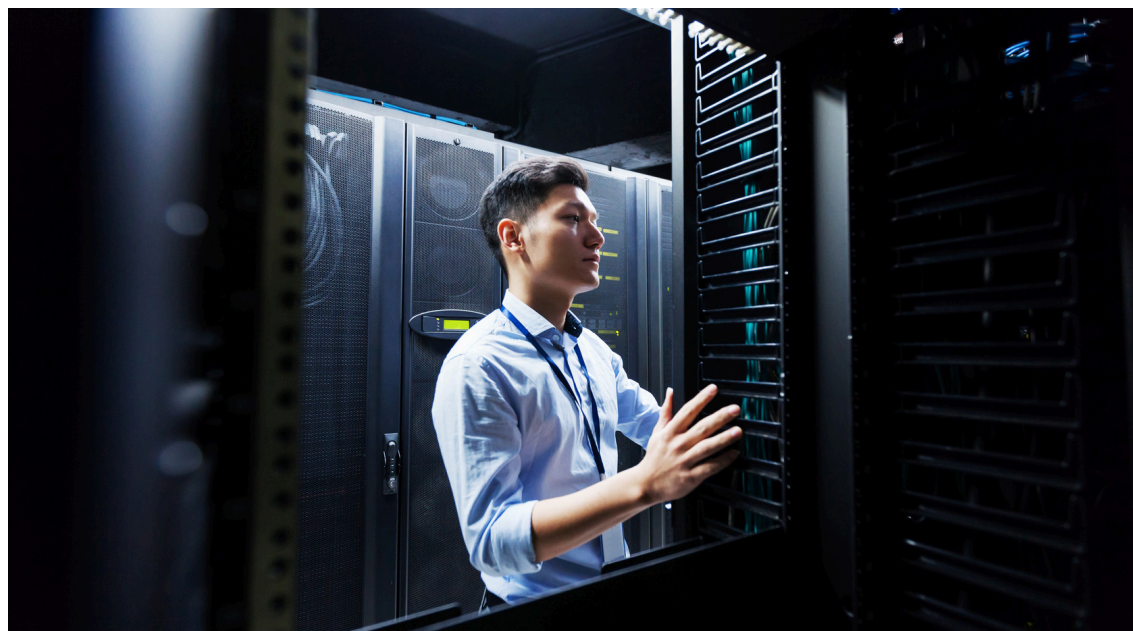
DCID: Provides knowledge and skills focused on data centre design based on Cisco solutions and technologies, including theoretical case studies and design-oriented activities.

DCIT: Shows you how to troubleshoot LAN, SAN, Cisco® Data Centre Unified Fabric, Cisco UCS®, and Cisco ACI®.

DCACI: Introduces you to the Cisco Nexus 9000 Series Switches in Cisco Application Centric Infrastructure (ACI) mode.

DCNAUTO: shows you how to implement Cisco Data Centre automated solutions, including programming concepts, orchestration, and automation tools.

DCAI: Focuses on the critical skills needed to build, deploy, and operate the robust, scalable infrastructure that underpins AI solutions.



CCNP Data Centre Elective Courses

Designing Cisco Data Centre Infrastructure (DCID)	Troubleshooting Cisco Data Centre Infrastructure (DCIT)	Implementing Cisco Application Centric Infrastructure (DCACI)
Duration 5 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 41	CLCs 46	CLCs 46
CE Credits 40	CE Credits 50	CE Credits 40
Exam 300-610	Exam 300-615	Exam 300-620
Course Outline: This training teaches data centre design using Cisco solutions. You will learn network virtualisation, Layer 2/3 technologies, routing protocols, and data centre interconnects, along with Cisco UCS design for B- and C-Series servers, Unified Fabric, and management using UCS Manager, DCNM, and UCS Director. Learning Objectives: - Explain Layer 2/3 forwarding, VXLAN, and data centre traffic patterns. - Describe rack designs, access/aggregation/core layers, and hardware redundancy. - Virtualise network, compute, and storage functions. - Apply data centre security and advanced best practices. - Describe storage, RAID, Fibre Channel, FCoE, and storage security. - Explain Cisco UCS servers, connectivity, hyperconverged solutions, and domain setup. - Configure UCS service profiles, pools, policies, interfaces, and templates. - Use device management, orchestration, and automation tools. Who Should Enroll: - Network engineers / administrators / designers - Data centre engineers / administrators / designers - Solutions Architects Pre-requisites: - Understand LAN/SAN and data centre storage - Understand Cisco Nexus and MDS families. - Knowledge of server virtualisation and Cisco UCS	Course Outline: This training shows you how to troubleshoot LAN, SAN, Cisco Data Centre Unified Fabric, Cisco UCS, and Cisco ACI. You will learn methodologies and tools to identify issues that may occur in data centre network architecture, and practice troubleshooting installation, configuration, and interconnectivity issues on Cisco MDS switches, Cisco Nexus switches, Cisco Fabric Extenders (FEXs), Cisco UCS, and Cisco ACI. Learning Objectives: - Troubleshoot data centre networks using CLI tools and methodologies. - Identify and resolve VLAN, PVLAN, port channel, and VXLAN issues. - Troubleshoot routing, high-availability, and LAN security protocols. - Troubleshoot single devices, Fibre Channel interfaces, and NX-OS switching (including NPV mode). - Troubleshoot Cisco UCS architecture, configuration, B- and C-Series server LAN/SAN/Fibre Channel operations. - Use Cisco UCS IMC tools, Intersight, and Nexus Dashboard for monitoring and troubleshooting. - Troubleshoot Cisco ACI, automation, and programmability tools. - Apply Python, Ansible, and NX-API for configuration verification and operational improvements. Who Should Enroll: - Network engineers / administrators / designers - Data centre engineers / administrators / designers - Solutions Architects Pre-requisites: - Configure, secure, and maintain Cisco UCS, Cisco ACI and LAN and SAN based on Cisco Nexus and MDS switches	Course Outline: The 5-day lab-intensive training covers the key components and procedures you need to know to understand, configure, and manage Cisco Nexus 9000 Series Switches in ACI mode, how to connect the Cisco ACI fabric to external networks and services, and fundamentals of Virtual Machine Manager (VMM) integration. Learning Objectives: - Describe Cisco ACI Fabric Infrastructure and basic Cisco ACI concepts - Describe Cisco ACI policy model logical constructs - Describe Cisco ACI basic packet forwarding - Describe external network connectivity - Describe VMM Integration - Describe Layer 4 to Layer 7 integrations - Explain Cisco ACI management features Who Should Enroll: - Network engineers / administrators / designers - Data centre engineers / administrators / designers - Solutions Architects Pre-requisites: - Understanding of networking protocols, routing, and switching - Familiarity with Cisco Ethernet switching products - Understanding of Cisco data centre architecture - Familiarity of virtualisation fundamentals

CCNP Data Centre Elective Courses

Automating Cisco Data Centre Networking Solutions (DCNAUTO)		Implementing Cisco Data Centre AI Infrastructure (DCAI)	
Duration	5 Days	Duration	5 Days
Delivery	ILT / VILT / Self-paced	Delivery	ILT / VILT / Self-paced
CLCs	44	CLCs	44
CE Credits	24	CE Credits	38
Exam	300-510	Exam	300-640
Course Outline: This training teaches you how to implement and optimize automation in Cisco data center environments. You will gain hands-on experience with Cisco Nexus platforms, programmability features, and modern automation tools used to streamline operations across switching, compute, and fabric controllers.		Course Outline: This training equips professionals with the skills to support, secure, and optimise AI workloads within modern data centre environments. This comprehensive program delves into the unique characteristics of AI/ML applications, their influence on infrastructure design, and best practices for automated provisioning.	
Learning Objectives: - Review Cisco ACI fundamentals, GUI workflows, and automation benefits. - Use ACI REST API and Postman for basic interactions. - Apply Python libraries to configure and verify ACI fabric. - Build Ansible playbooks for tenant configuration and health reporting. - Integrate Kubernetes via ACI Apps Center. - Automate Nexus operations using NX-API, ZTP, POAP, and iPX. - Leverage UCS and NDFC APIs with Python and Ansible. - Implement automation with Intersight and Terraform for ACI deployments.		Learning Objectives: - Define core AI and generative AI concepts, use cases, and trends - Explain AI/ML cluster architecture, model lifecycles, and data prep - Apply Python, JupyterLab, and GenAI to automate NetOps - Design secure, compliant, and sustainable AI infrastructure optimised for cost and performance - Align AI/ML workload requirements with effective placement and interoperability strategies - Design AI-ready data centre networks, including L2/L3 protocols - Implement high-performance, lossless Ethernet using RDMA/RoCE, QoS, ECN, and PFC - Monitor and optimise AI workloads using Cisco Nexus Dashboard Insights, NDFC, and AI-specific compute, storage, and RAG-enabled models	
Who Should Enroll: - Network engineers / administrators / designers - Data centre engineers / administrators / designers		Who Should Enroll: - Network engineers / administrators / designers - Data centre engineers / administrators / designers	
Pre-requisites: - Basic knowledge of programming language concepts - Basic understanding of virtualisation and VMware - Ability to use Linux and CLI tools, such as SSH and bash - Foundational understanding of Cisco ACI		Pre-requisites: - Cisco UCS compute architecture and operations - Cisco Nexus switch portfolio and features - Data Centre core technologies	



Cisco Automation Professional

Designing, Deploying and Managing Network Automation Systems (AUTOCOR)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	44
CE Credits	32
Exam	350-901

Course Outline:

This course equips learners to design, implement, and operate modern network automation solutions, covering Python, Ansible, and Terraform alongside integrated CI/CD pipelines. It introduces AI-driven automation using LLM-powered network agents and MCP integration, while addressing secure coding, logging, containerisation, and model-driven telemetry, with a strong practical focus to enable the development of scalable, secure, and efficient automated network environments.

Learning Objectives:

- Evaluate network automation tools, architectures, and model-driven approaches
- Develop Python-based automation solutions
- Implement model-driven automation to configure and manage network devices
- Apply Infrastructure as Code (IaC) practices to manage network state
- Design and implement CI/CD pipelines
- Validate and monitor automated networks
- Secure automation environments and code
- Leverage AI in network automation, including generative AI, LLM integration, and AI agents

Who Should Enroll:

- Network engineers / administrators / designers
- Software developers
- Infrastructure architects

Pre-requisites:

- Foundational proficiency in Python programming
- Working knowledge of networking concepts and configurations
- Basic understanding of APIs, including REST, NETCONF, and RESTCONF
- Familiarity with version control systems (Git) and platforms such as GitLab or GitHub
- Knowledge of the Linux command line, including SSH, file management, and virtual environments.
- Exposure to containerisation (Docker) and a basic awareness of AI and LLM concepts.



At the Cisco DevNet Professional level, candidates can specialise by selecting one of two automation-focused elective exams: ENAUTO or DCNAUTO.

The ENAUTO elective emphasises enterprise network automation, programmability, and software-driven operations across routing, switching, wireless, and security domains.

The DCNAUTO elective focuses on data centre automation, covering Cisco ACI, Nexus, UCS, and model-driven programmability.

Both electives validate advanced skills in APIs, Python, automation frameworks, and infrastructure as code, enabling professionals to design, implement, and operate programmable Cisco environments.

Cisco Cybersecurity Professional

Performing Cybersecurity Using Cisco Security Technologies (CBRCOR)	Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)	Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)
Duration 5 Days	Duration 5 Days	Duration 12 Hours
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery Self-paced
CLCs 40	CLCs 44	CLCs 6
CE Credits 40	CE Credits 40	CE Credits 48
Exam 350-201	Exam 300-220	Exam 200-901
Course Outline: This training teaches how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analysing threats, and making appropriate recommendations to improve cybersecurity through leveraging playbooks in formulating an Incident Response in real-world scenarios. Learning Objectives: • Define SOC service models, coverage, and operational roles • Compare cloud security operations considerations • Describe SOC platform design, automation, and orchestration • Apply asset protection using segmentation and Zero Trust • Investigate incidents using SIEM and SOAR • Operate core security monitoring and response tools • Analyse threats using IOCs, IOAs, UEBA, and network traffic analysis • Perform proactive threat hunting following best practices Who Should Enroll: • Cybersecurity Engineers / Investigators • Incident Managers / Responders • Network Engineers • Cybersecurity / SOC engineers / analysts Pre-requisites: • Familiarity with UNIX/Linux shells (bash, csh) and shell commands • Familiarity with the Splunk search and navigation functions • Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar	Course Outline: This training provides an understanding of proactive security investigation skills across networks, endpoints, and data sources. You will learn core threat-hunting concepts, methodologies, and workflows, practice attack simulation, and build hands-on expertise using Cisco and third-party security platforms to identify activity that evades traditional detection tools. Learning Objectives: • Define threat hunting and its core investigative concepts • Apply threat-hunting frameworks, models, and processes • Execute structured threat-hunting methodologies and procedures • Conduct network-based threat-hunting investigations • Perform endpoint and memory-based threat hunting • Use Cisco tools to detect and analyse advanced threats • Execute end-to-end practical threat-hunting workflows • Produce clear, actionable threat-hunting reports Who Should Enroll: • Threat Hunters • Cyber Threat Analysts • Threat Managers • Risk Managers Pre-requisites: • General knowledge of networks and network security	Course Outline: This training prepares you to identify and respond to cybersecurity threats, vulnerabilities, and incidents. Additionally, you will be introduced to digital forensics, including the collection and examination of digital evidence on electronic devices and learn to build the subsequent response threats and attacks. You will also learn how to proactively conduct audits to prevent future attacks. Learning Objectives: • Analyse and structure effective root cause analysis reports • Apply YARA and MITRE ATT&CK techniques for malware and adversary identification • Use scripting to parse, search, and correlate logs across multiple data sources • Correlate host-based and network-based data by incident type • Evaluate alerts from firewalls, IPS, and security analytics platforms • Leverage Cisco security tools to investigate incidents and recommend mitigations • Assess incident response playbooks and ThreatGrid report components • Analyse threat intelligence in standard formats such as STIX and TAXII Who Should Enroll: • Cybersecurity Engineers / Investigators • Incident Managers / Responders Pre-requisites: • Foundational knowledge of incident response and threat types • Understanding of networking fundamentals, and traffic analysis • Basic experience with security tools, log review, and SIEM concepts

PROJECT 525



The Cisco Certified Internetwork Expert (CCIE) is the highest level of certification in networking, security, service provider technologies, and data centre management. Achieving this prestigious certification demonstrates your ability to design, implement, and troubleshoot complex networks, positioning you as a highly sought-after IT professional.

Project 525 is a structured 12-month mentoring programme, developed in collaboration with Cisco, designed to prepare IT professionals for the CCIE exam. It provides a comprehensive and structured approach to learning, combining guided study, hands-on practice, and expert mentorship to ensure success.

- Well-Structured Program – A 12-month guided plan to help you stay on track toward CCIE certification.
- Flexible Self-Study – Learn at your own pace while managing work and other commitments.
- Expert Mentorship – Get weekly, collaborative group coaching from CCIE-certified mentors.
- Hands-On Technical Labs – Develop real-world networking skills through practical experience.
- Intensive Bootcamps – Strengthen your expertise with high-impact, immersive training sessions.
- Global Recognition – Join an elite community of CCIE-certified professionals worldwide.
- Career Advancement – Open doors to top-tier job opportunities and higher earning potential.
- Comprehensive Study Resources – Gain access to exclusive training materials and practice exams.



Product and Solution Training

Our training equips professionals with the knowledge and skills to effectively deploy, manage, and optimise technology products and solutions. Participants gain hands-on experience with industry-standard tools, learn best practices for implementation, and understand how solutions drive business value. Designed for IT professionals, technical specialists, and decision-makers, this training bridges the gap between technical proficiency and practical application, enabling teams to deliver measurable results and innovation.

Our Solution Areas are

Intelligent
Networking

Smart Telco
Networks

Cyber Security

Cloud & Hybrid
Infrastructure

Workforce
Mobility

Software,
Development &
Intelligent
Automation

Data,
Analytics & AI

Intelligent IT
Operations &
Services



Intelligent Networking

Networking is at the heart of every modern enterprise, connecting people, systems, and data to drive business outcomes. Learn how intelligent networking enhances operational efficiency, strengthens performance, and delivers tangible business value.

These training resources help professionals discover and master Cisco technologies and solutions. Through hands-on learning, participants develop skills in network management, observability, software-defined networking, and automation to optimise operations and deliver measurable results.

Intelligent Networking

	Managing Cisco Network Operating Systems (CNIOS)	Transforming to a Cisco Intent-Based Network (IBNTRN)
Duration 3 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 27	CLCs 42	CLCs 46
CE Credits 12	CE Credits 32	CE Credits 40
	Course Outline: This training introduces the fundamental concepts of Cisco networking operating systems, including IOS XE, NX-OS, and IOS XR. This training is designed for individuals who are new to Cisco or networking professionals who want to deepen their understanding of Cisco operating systems used across various network devices. Upon completion of this training, you will be able to navigate the command-line interface (CLI), configure basic settings as well as advanced protocols, and understand the unique features and architectures of Cisco network operating systems. Learning Objectives: • Navigate the CLIs of IOS XE, NX-OS, and IOSXR • Perform initial setup, upgrades, and troubleshooting on various Cisco platforms • Configure essential network features, such as vPCs, Fibre Channel, VXLAN, and router clustering • Explore automation options and learn how to interact with Cisco TAC • Gain proficiency in navigating Cisco documentation and securing network environments Who Should Enroll: • Junior Network Engineers • NOC Engineers • IT Operations Engineers • Network Administrators Pre-requisites: • Basic understanding of core networking concepts • Fundamental knowledge of Cisco network devices • Basic understanding of network security concepts	Course Outline: This course teaches you how the functionality of Cisco SD-Access fits into Cisco Digital Network Architecture (DNA). Through a combination of lessons and hands-on learning, you will learn about operating, managing, and integrating Cisco Catalyst Center, programmable network infrastructure, and Cisco SD-Access fundamentals. Learning Objectives: • Explain Cisco DNA vision, strategy, and core components • Design and operate campus networks with Cisco Catalyst Center and Cisco ISE integration • Discover, inventory, and validate device readiness for SD-Access • Automate operations using templates, image lifecycle management, and Plug and Play onboarding • Use Cisco Catalyst Center workflows to design, onboard, and manage campus networks • Describe Cisco SD-Access architecture • Deploy and operate SD-Access fabrics, devices and endpoints • Automate, monitor, and migrate wired, wireless, and IoT networks Who Should Enroll: • Network administrators and engineers • System engineers • Technical architects • Technical support personnel Pre-requisites: • CCNP Enterprise-level knowledge of routing and switching • Experience with Cisco Unified Wireless networks • Familiarity with Cisco ISE, 802.1X, and Cisco TrustSec • Understanding of segmentation using VLANs and VRFs • Basic knowledge of overlay technologies, including VXLAN and LISP

Intelligent Networking

Implementing Cisco Catalyst 9000 Switches (ENC9K)	Implementing and Troubleshooting Networks Using Cisco ThousandEyes (ENTEIT)	Cisco Catalyst Center Foundations (CCFND)
Duration 3 Days	Duration 3 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 30	CLCs 28	CLCs 44
CE Credits 18	CE Credits 24	CE Credits 44
Course Outline: This course provides you with insight into Cisco Catalyst 9000 Series Switches and their solution components, architecture, capabilities, positioning, and implementation. You will also learn to manage the switches using CLI, Cisco DNA Center, and the IOS-XE GUI. Learning Objectives: - Position Catalyst 9K switches within the SD-Access architecture - Map legacy Catalyst platforms to Catalyst 9K models for migration - Explain the role of Cisco Silicon One core features - Describe management, maintenance, and high-availability capabilities across the portfolio - Summarise integrated security, QoS, IoT convergence, and BGP EVPN support - Explain automation, APIs, and Infrastructure as Code capabilities - Describe deployment models and Day 0 onboarding with Catalyst Center - Differentiate Catalyst 9200, 9300, 9400, 9500, and 9600 use cases Who Should Enroll: - Network designers - Network managers - System engineers Pre-requisites: - Cisco CCNP+ certification or equivalent experience - Knowledge of configuring LAN routing and switching with Cisco Catalyst switches - Familiarity with the Cisco IOS XE operating system - Familiarity with using network management software - Familiarity with Cisco Intent-based networking and policy-based management automation technologies	Course Outline: The focus of this training is the implementation and configuration of the Cisco ThousandEyes solution, it provides hands-on experience with installing and configuring Cisco ThousandEyes agents with different test types. This solution is also used to perform root cause analysis when troubleshooting. Learning Objectives: - Describe different Enterprise Agent deployment options, requirements, and procedures for agent deployment - Describe different ThousandEyes test types - Compare ThousandEyes web layer tests - Describe, deploy, and configure an Endpoint Agent - Describe how to perform system administration - Utilise ThousandEyes when performing the root cause analysis - Describe Internet Insights - Explain alerts and dashboards configuration in the monitoring solutions Who Should Enroll: - Network Administrators - Network Engineers - Network Managers - System Engineers Pre-requisites: - Basic understanding of network fundamentals - Basic understanding of Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), HTTP, SSL, and DNS protocol	Course Outline: This training is designed to expand your knowledge of Cisco Catalyst Center, including its basics, deployment and scalability options, initial configurations, best practices, and integration with Cisco Identity Services Engine (ISE). The training will focus on network automation, network assurance, network security, and network programmability using Cisco Catalyst Center. Learning Objectives: - Explain Cisco Catalyst Center architecture, intent-based networking, and key enterprise use cases - Apply automation, assurance (AIOps), and DevOps integrations to NetOps and SecOps - Deploy Catalyst Center, including pre-deployment requirements and initial setup - Design for high availability, scalability, and disaster recovery - Configure system settings, automation workflows, and compliance auditing - Onboard and manage devices, integrating with Cisco ISE - Monitor and troubleshoot network, device, and client health - Implement SD-Access fabric networking with policy-based segmentation Who Should Enroll: - Network engineers / analysts - Security engineers Pre-requisites: - Basic understanding of network fundamentals - Basic familiarity with Cisco ISE - Basic familiarity with network automation and programmability

Intelligent Networking

Implementing Cisco Multicast (MCAST)	Implementing Cisco Quality of Service (QoS)	Cisco SDWAN Fundamentals (SDWFND)
Duration 5 Days	Duration 5 Days	Duration 2 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 43	CLCs 43	CLCs 20
CE Credits 40	CE Credits 40	CE Credits 14
Course Outline: This course teaches you the fundamentals of IP multicasting, including multicast applications, sources, receivers, group management, and IP multicast routing protocols such as Protocol Independent Multicast (PIM) used within a single administrative domain. Learning Objectives: - Describe IP multicast services - Identify IP multicast issues on a data link layer - Explain why PIM-SM is the most current scalable multicast protocol - Describe Rendezvous Point (RP) distribution solutions - Recognise the drawbacks of the PIM-SM and describe two extensions to provide possible solutions - Explain basic concepts of Multiprotocol BGP (MP-BGP) and its use in the IP multicast environment - Configure and deploy Multicast Source Discovery Protocol (MSDP) in the interdomain environment - Describe solutions to mitigate security issues in the IP multicast network - Describe the process of monitoring and maintaining multicast high-availability operations - Design multicast-related application and network solutions in customer and service provider networks Who Should Enroll: - Network engineers - System engineers Pre-requisites: - Work experience and configuration skills for Cisco routers and LAN switches	Course Outline: This training builds in-depth expertise in Quality of Service (QoS), covering core models such as Best Effort, IntServ, and DiffServ, along with QoS theory, design considerations, and implementation on Cisco platforms. You will learn to design, configure, and apply advanced QoS features to deliver efficient, reliable multiservice, wireless, and software-defined networks. Learning Objectives: - Explain the need for QoS, core principles, and QoS models. - Implement QoS using Modular QoS CLI (MQC) and AutoQoS. - Apply QoS policies in converged networks and monitor performance. - Use Cisco queuing mechanisms to manage congestion. - Apply congestion avoidance techniques to minimise packet loss and delay. - Improve bandwidth efficiency with link efficiency mechanisms. - Design and implement wireless QoS for time-sensitive and high-bandwidth applications. - Deploy end-to-end QoS in SDN and enterprise-service provider environments using best practices. Who Should Enroll: - Network Designers / Engineers - Network Managers - System Engineers Pre-requisites: - Knowledge equivalent to a CCNA certification	Course Outline: In this course You will learn how to deploy, manage, and operate a secure, programmable, and scalable SD-WAN fabric using Cisco SD-WAN products, it also covers how to configure, operate, and monitor overlay routing across the SD-WAN network. You will also learn about data and control policies, and how to deploy QoS and Direct Internet Access (DIA) in the SD-WAN overlay network. Learning Objectives: - Identify the various network elements of the Cisco SD-WAN solution. - Deploy WAN Edge routers. - Create templates to aid in the deployment and operation of the Cisco SD-WAN network. - Configure and verify Cisco SD-WAN overlay routing. - Create simple policies to control traffic flow through the Cisco SD-WAN fabric. Who Should Enroll: - Network administrators and engineers - System engineers - Technical architects Pre-requisites: - Strong understanding of enterprise WAN design - Strong understanding of routing protocol operations - Familiarity with Transport Layer Security (TLS) and IP Security (IPsec)

Intelligent Networking

Understanding Cisco Wireless Foundations (WLFNDU)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
CLCs	43
CE Credits	30

Course Outline:

This training teaches you the knowledge and skills you need to configure, manage, and troubleshoot a Cisco wireless LAN (WLAN) network. Topics include understanding critical aspects of RF technology, industry standards for Wi-Fi and security, how to design, install, and configure a WLAN network of any size, and using Cisco Catalyst Center.

Learning Objectives:

- Implement foundational wireless theory, RF math, and antenna principles.
- Understand wireless operations, including Wi-Fi 6 capabilities.
- Design and secure wireless client access and authentication.
- Implement 802.1X, EAP, and secure guest access.
- Describe Cisco wireless architectures, components, and deployment models.
- Understand CAPWAP, Cisco WLCs, and access point portfolios.
- Deploy and operate centralised WLANs using Cisco 9800 Series WLCs.
- Manage, monitor, and troubleshoot wireless networks with Cisco Catalyst Center.

Who Should Enroll:

- Network and wireless engineers
- System engineers
- Solution architects and network designers

Pre-requisites:

- General knowledge of networks and wireless networks





Smart Service Provider Networks

Telecommunications networks are the backbone of every connected society, enabling services, devices, and data to flow seamlessly. Learn how smart telco networks enhance operational efficiency, improve service quality, and drive business and customer value.

These training resources help professionals explore and master telco technologies and solutions. Through hands-on learning, participants build skills in network management, observability, software-defined networking, and automation to optimise performance, streamline operations, and deliver measurable results.

Smart Service Provider Networks

Cisco Aggregation Services Router 9000 Series Essentials (ASR9KE)	Configuring BGP on Cisco Routers (BGP)	Cisco IOS XR Software Essentials (IOSXRE)
Duration 4 Days	Duration 5 Days	Duration 4 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 36	CLCs 43	CLCs 36
CE Credits 32	CE Credits 40	CE Credits 24
Course Outline: This course introduces the Cisco® ASR 9000 Series platforms, covering hardware, Layer 2/3 services, routing protocols including Segment Routing, multicast, QoS, and network virtualisation. You'll explore Cisco IOS XR 64-bit Linux-based features, learn to install IOS XR software packages, and reinforce concepts through hands-on labs and practical exercises. Learning Objectives: - Describe Cisco ASR 9000 Series router features and benefits - Explain Cisco 64-bit IOS XR operating system features and benefits - Understand data flow and configuration management on the ASR 9000 - Install and maintain IOS XR 64-bit software and updates - Configure multicast routing and Layer 3 VPN services - Implement Ethernet link bundles and L2VPNs (E-Line, E-LAN, EoMPLS, VPLS) - Configure service-based CFM and Layer 2 multicast features - Implement basic QoS and network virtualisation (nV) on the ASR 9000 Who Should Enroll: - Network engineers - System engineers Pre-requisites: - Basic IOS XR 64-bit configuration and router installation experience - Routing protocol knowledge: BGP, OSPF, IS-IS - Layer 2 switching, MPLS, or multicast configuration experience - Experience troubleshooting Cisco routers in large networks	Course Outline: This training provides knowledge of BGP, the routing protocol and foundation for the Internet and new-world technologies such as Multiprotocol Label Switching (MPLS). It prepares you to design and implement efficient, optimal BGP networks covering the theory and configuration of BGP on Cisco IOS routers, detailed troubleshooting, and hands-on exercises. Learning Objectives: - Configure, monitor, and troubleshoot basic BGP for interdomain routing across multiple domains - Use BGP attributes and policy controls to influence route selection with multiple ISP connections - Connect customer networks to the Internet with multiple BGP links - Configure service provider networks as transit AS and enable route reflection to scale BGP - Optimise BGP scalability using available tools and features Who Should Enroll: - Network Engineers / Administrators / Managers - System Engineers Pre-requisites: - Intermediate to advanced knowledge of Cisco IOS Software configuration - Configuring and troubleshooting RIP, EIGRP, OSPF and IS-IS	Course Outline: This training introduces Cisco IOS XR Software, covering architecture, installation, upgrades, CLI usage, and automatic provisioning. You'll learn essential services—security, logging, timing, AAA, and modular QoS—plus basic MPLS routing and forwarding. Hands-on labs also cover programmability and monitoring features, including SNMP, telemetry, process monitoring, and IOS XR automation. Learning Objectives: - Describe Cisco IOS XR Software architecture and package installation - Perform initial device configuration and zero-touch provisioning - Implement and manage system security and AAA services - Configure and troubleshoot QoS, routing protocols, and MPLS in service provider networks - Monitor device performance using CLI, logging, and process monitoring - Configure SNMP and deploy model-driven telemetry for network visibility - Understand timing, synchronisation, and forwarding mechanisms - Deploy third-party applications and utilise programmable features on Cisco IOS XR Who Should Enroll: - Network Engineers / Administrators / Managers - System Engineers - Solutions Architects and designers Pre-requisites: - Experience working with CLI-based network devices - Knowledge of general routing concepts

Smart Service Provider Networks

IPv6 Fundamentals, Design, and Deployment (IP6FD)	Implementing Cisco MPLS (MPLS)	Implementing the Cisco NCS540 Series Routers (NCS540HWE)
Duration 5 Days	Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 43	CLCs 43	CLCs 44
CE Credits 40	CE Credits 40	CE Credits 40
Course Outline: This training provides you with the knowledge and skills needed to implement and configure the IP version 6 (IPv6) features of Cisco IOS software. It also provides an overview of IPv6 technologies; covers IPv6 design and implementation, operations, addressing, routing, services, and transition; and the deployment of IPv6 in both enterprise and service provider networks. The training includes case studies that are useful for deployment scenarios and remote labs. Learning Objectives: • Explain IPv4 limitations, IPv6 rationale, benefits, address architecture, and header changes • Configure and troubleshoot IPv6 including ICMP, neighbour discovery, DHCPv6, and DNS • Describe IPv6 routing protocols: OSPFv3, EIGRP, MP-BGP, and FHRP for redundancy • Explain dual-stack deployment, and IPv4-to-IPv6 transitions • Describe IPv6 multicast addressing, MAC mappings, and scoping • Apply IPv6 security and best practices • Plan and implement IPv6 in enterprise, branch, MPLS, broadband, and cloud environments • Analyse IPv6 market drivers and strategies for large-scale adoption Who Should Enroll: • Network engineers Pre-requisites: • Understanding of networking and routing to CCNP level • Working knowledge of the Microsoft Windows operating system	Course Outline: This course provides hands-on training in implementing high-performance Multiprotocol Label Switching (MPLS) for efficient packet forwarding. You'll learn to configure edge routers and switches to label and forward packets with minimal lookup overhead, integrate Layer 2 traffic management with Layer 3 routing, and leverage MPLS with standard technologies to enable advanced, value-added services in service provider networks. Learning Objectives: • Describe the features of MPLS • Describe how MPLS labels are assigned and distributed • Identify the Cisco IOS tasks and command syntax necessary to implement MPLS on frame-mode Cisco IOS platforms • Describe the routing and packet forwarding model in the MPLS peer-to-peer architecture • Identify the Cisco IOS command syntax required to successfully configure, monitor, and troubleshoot VPN operations • Identify how the MPLS VPN model can be used to implement managed services and internet access • Describe the various internet access implementations that are available and the benefits and drawbacks of each model • Provide an overview of MPLS Traffic Engineering Who Should Enroll: • Network Engineers / Administrators / Managers • System Engineers Pre-requisites: • Intermediate to advanced knowledge of Cisco IOS Software configuration • Configuring and troubleshooting EIGRP, OSPF, IS-IS and BGP	Course Outline: This training teaches you how to deploy Cisco Network Convergence System (NCS) 540 Series routers in a network environment. You will be introduced to the features and functions of the Cisco NCS 540 series platforms, system architecture, services implementation, quality of service (QoS), system security, model-driven telemetry, and programmability. Learning Objectives: • Classify Cisco NCS 540 hardware variants, form factors, features, and use cases • Describe NCS 540 hardware architecture and packet flow • Explain traffic queuing, scheduling, and forwarding, including modular QoS on NCS 540 • Describe Cisco IOS XR architecture, programmable features, software installation, and security • Explain timing and synchronisation methods on IOS XR platforms • Describe and implement segment routing, including SR IPv6 • Implement L2 / L3 VPNs, EVPN configuration and troubleshooting • Implement model-driven telemetry for enhanced network visibility and management Who Should Enroll: • Network Engineers / Administrators • System Engineers • Field Engineers Pre-requisites: • Knowledge of core networking technologies, concepts and protocols • Routing protocol configuration experience with border gateway protocol (BGP), IS-IS, and OSPF

Smart Service Provider Networks

Cisco NCS 2000 Deploying 96-Channel Flex Spectrum (OPT201)		Implementing Segment Routing on Cisco IOS XR (SEGRTE201)		Cisco 8000 Series Routers Essentials (SP8KE)	
Duration 3 Days		Duration 4 Days		Duration 5 Days	
Delivery ILT / VILT / Self-paced		Delivery ILT / VILT / Self-paced		Delivery ILT / VILT / Self-paced	
CLCs 30		CLCs 40		CLCs 42	
CE Credits 24		CE Credits 32		CE Credits 40	
Course Outline: This course teaches you to plan, configure, and control optical networks using the Cisco® Network Convergence System 2000 series Flex Spectrum platform. You'll also learn to design Flex Spectrum networks with multi-degree Reconfigurable Optical Add-Drop Multiplexer (ROADM) multi-shelf nodes using Cisco Transport Planner (CTP) software. Learning Objectives: • Install the Cisco NCS 2000 series hardware • Configure an optical network and circuits using the Cisco Transport Controller (CTC) software • Learn which components and configurations take advantage of and/or are required for the Flex Spectrum 96-channel feature • Configure optical networks with multidegree ROADM multishelf nodes • Configure optical networks with colorless, contentionless, omnidirectional, and MPO cross-connect advanced features • Describe and configure the NCS 2000 400-Gbps Xponder line card Who Should Enroll: • Network engineers / designers • NOC personnel • Systems engineers Pre-requisites: • Working knowledge of optical fibre networking, single and multimode fibres, and small form-factor pluggables (SFPs)		Course Outline: This course covers fundamental segment routing (SR) concepts, configuring and verifying SR within IGP, and interworking with LDP. Learn to implement TI-LFA, instantiate and verify SR traffic engineering (SR-TE) policies, and deploy segment routing within BGP for scalable, resilient, and efficient network routing. Learning Objectives: • Describe the key concepts of segment routing • Implement and verify IGP segment routing • Migrate an existing Multiprotocol Label Switching (MPLS) LDP-based network to segment routing • Implement and verify TI-LFA segment routing • Instantiate segment routing policies • Instantiate multidomain segment routing policies • Configure and verify BGP prefix segments and SR-based services Who Should Enroll: • Network Engineers • Field engineers • System Engineers Pre-requisites: • Familiarity with Cisco Internetwork Operating System (IOS®) XR software • Knowledge of general networking concepts		Course Outline: This training introduces you to the features and functions of the Cisco® 8000 Series router platforms. Through a combination of lectures and labs, you will gain an understanding of all major aspects of the platform, including hardware, software, Layer 2 and Layer 3 services, Quality of Service (QoS) features, network virtualisation, and programmability. Learning Objectives: • Describe Cisco 8000 Series hardware, architecture, and packet flows with CLI verification • Explain QoS, VOQ, congestion management, and priority flow control • Outline SONiC and IOS XR architectures, install software, and provision via ZTP • Configure MPLS, Layer 3 VPNs, and EVPN (Native and VPWS) • Implement segment routing, SRGB, and IS-IS/OSPF SR • Deploy TI-LFA, SR-TE, and SRv6 • Implement model-driven telemetry for visibility and monitoring • Use IOS XR programmability and deploy third-party applications Who Should Enroll: • Network Engineers • Systems Engineers • Field Engineers Pre-requisites: • Experience with router installation, Layer 2 switching, and MPLS configuration • Proficiency configuring routing protocols: BGP, IS-IS, and OSPF • Hands-on experience troubleshooting Cisco routers in large network environments	

Smart Service Provider Networks

Understanding Cisco Service Provider Network Foundations (SPFNDU)	Cisco Service Provider 5G Technologies Foundations (SPMBL100)	Implementing Cisco Converged SDN Transport Solution (SPSDNTXP)
Duration 5 Days	Duration 4 Days	Duration 4 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 45	CLCs 38	CLCs 32
CE Credits 30	CE Credits 24	CE Credits 40
Course Outline: This training is designed to provide you with the foundational knowledge for the suite of Cisco CCNP Service Provider trainings. The training expands what you learned from the Cisco CCNA training with a focus on theoretical and practical knowledge needed for the service provider environment. You will learn about architectures, protocols, software and hardware platforms, and solutions within the service provider realm. Learning Objectives: - Describe service provider network architectures, devices, and software - Explain roles of internet governance organisations and tools for information verification - Configure Cisco IOS, IOS XE, and IOS XR routers, including initial setup and daily tasks - Describe service provider access, core, and switching technologies - Explain overlay technologies and configure VXLAN - Describe major routing protocols and configure Layer 3 services - Explain MPLS components, protocols, and usage in SP networks - Introduce Linux networking, BASH scripting, and their application in Cisco IOS XR Who Should Enroll: - Network Administrators / Engineers / Managers / Designers - Systems Engineers Pre-requisites: - Knowledge of IPv4 and IPv6 TCP/IP networking - Familiarity with a typical service provider environment - Basic knowledge about networking devices and their roles	Course Outline: This course introduces mobile network components, basic 5G concepts, and features of 5G technology used to improve user experience. Additionally, you'll examine the mobile packet core solutions, 5G transport architecture, and Cisco automation and orchestration tools used in 5G networks. Learning Objectives: - Describe mobile network architecture basics - List enabling technologies for 5G and describe 5G key use cases - Perform basic operations on a Cisco 5G NSA mobile packet core - Describe the Cisco 5G Converged SDN Transport Architecture - Describe Cisco NFVI and perform basic operations using Cisco ESC and Cisco Virtualised Infrastructure Manager (VIM) - Describe Cisco service provider automation and orchestration solutions to deploy and manage 5G network functions - Describe the Cisco Ultra Cloud Core architecture and deploy the Cisco SMI - Explain the 5G ready distributed Telco DC with Cisco ACI solution - Describe the Cisco 5G security architecture Who Should Enroll: - Network Administrators / Engineers / Managers / Designers - Systems Engineers Pre-requisites: - Knowledge of general networking concepts - Experience working with CLI-based network devices - Basic understanding of MPLS - Familiarity with service provider architectures	Course Outline: This training introduces you to Software-Defined Networking (SDN)-ready architecture. You will examine service provider design principles including Unified Multiprotocol Label Switching, Evolved Programmable Networks, and the Cisco® Compass Metro Fabric. You'll also explore individual components of the design including segment routing and its supporting features. Learning Objectives: - Explain the fundamentals of converged SDN transport and its role in modern networks. - Describe segment routing concepts and implement segment routing - Configure and verify Topology-Independent Loop-Free Alternate (TI-LFA) and segment routing traffic engineering (SR-TE). - Implement and validate multidomain SR-TE for scalable traffic engineering across network domains. - Describe VPN services and configure basic EVPN Layer 2 functions - Configure and verify Layer 3 VPN services in a service provider environment. - Explain Cisco Network Services Orchestrator (NSO) architecture and its role in network orchestration. - Use Cisco WAE and automation tools to simplify network operations and implement programmability workflows. Who Should Enroll: - Network Engineers / Architects - Support Engineers Pre-requisites: - Knowledge of general networking concepts - Experience working with CLI-based network devices

Smart Service Provider Networks

Leveraging Cisco IOS XR VPN Services (XRVPNs)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
CLCs	27
CE Credits	24

Course Outline:

This course teaches you to implement and troubleshoot Layer 2 and Layer 3 VPN services on Cisco IOS XR, the core OS for service provider networks. You will configure MPLS- or Segment Routing-based VPNs, IPv4/IPv6 Layer 3 VPNs, Multicast VPNs, and Ethernet VPN (EVPN) services—including EVPN-IRB, EVPN-SR fabrics, and advanced EVPN features.

Learning Objectives:

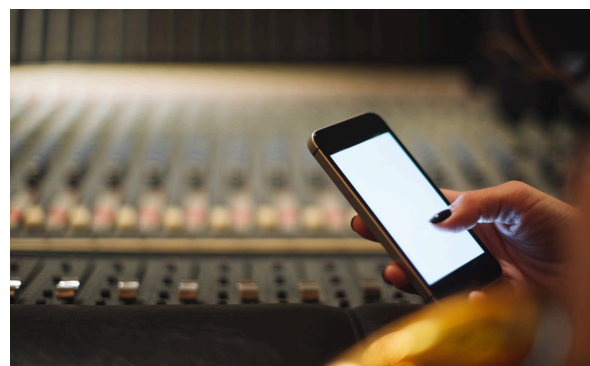
- Implement and configure MPLS, including label propagation and Layer 3 MPLS VPNs in Cisco IOS XR.
- Configure and verify Segment Routing, including IS-IS/OSPF integration and Segment Routing Global Block (SRGB).
- Implement and configure Segment Routing over IPv6 (SRv6) and MPLS VPN solutions for IPv6 networks.
- Troubleshoot Layer 3 MPLS VPNs, including PE-PE and PE-CE connectivity and Multicast LDP (MLDP) issues.
- Implement Layer 2 VPN services in service provider environments.
- Configure and troubleshoot Ethernet VPN (EVPN), addressing limitations of traditional L2 VPNs.
- Implement and troubleshoot EVPN IRB solutions.
- Configure EVPN-SR data centre fabrics and leverage advanced EVPN features for complex network deployments.

Who Should Enroll:

- Network Administrators / Engineers / Managers / Designers
- Systems Engineers

Pre-requisites:

- Familiarity with service provider network operation
- Familiarity with Cisco IOS XR software configuration and operation
- Ability to implement and troubleshoot routing protocol including OSPF, IS-IS, and BGP in a service provider network





Cybersecurity

Security is critical to every enterprise, protecting data, systems, and networks while enabling business continuity. Learn how Cisco security solutions safeguard organisations, detect and respond to threats, and ensure compliance with industry standards.

These training resources help professionals explore and master Cisco security technologies and solutions. Through hands-on learning, participants build skills in threat detection, incident response, secure network architecture, endpoint protection, and automation, empowering them to strengthen defences, manage risk, and deliver measurable business value.

Cybersecurity

Introduction to 802.1X Operations for Cisco Security Professionals (802.1X)		Enhancing Cisco Security Solutions with Splunk (ECSS)		Implementing Cisco SD-WAN Security and Cloud Solutions (SDWSCS)	
Duration 3 Days		Duration 5 Days		Duration 3 Days	
Delivery ILT / VILT / Self-paced		Delivery ILT / VILT / Self-paced		Delivery ILT / VILT / Self-paced	
CLCs 27		CLCs 44		CLCs 29	
CE Credits 32		CE Credits 32		CE Credits 24	
Course Outline: This training shows you how to configure and prepare to deploy Cisco Identity-Based Networking Services (IBNS) solutions based on Cisco Catalyst switches, Cisco 9800 LAN Controllers, and Cisco Meraki deployments. You will learn the fundamentals of the 802.1X protocol and configuration, Cisco IBNS, configuring access for non-suppliant devices, architectural components, and considerations with 802.1X. Learning Objectives: - Identify Cisco IBNS operation and how 802.1X functions as part of the IBNS solution - Compare the different types of EAP authentication to select the best method for a solution deployment - Configure Cisco Catalyst switches for 802.1X access - Configure Cisco Wireless LAN Controllers for 802.1X access - Configure Meraki devices for 802.1X access - Apply MAB and guest services to integrate devices without direct 802.1X support to the network - Explain network design considerations and troubleshooting for Cisco IBNS Who Should Enroll: - Security Administrators - Network Administrators - System Engineers - Technical Support Personnel Pre-requisites: - Basic routing and switching knowledge		Course Outline: This training covers intermediate-level knowledge of Splunk, including its fundamentals, key components, and architecture so you can detect, investigate, and respond to security threats effectively. You'll learn to use various Splunk components, including Splunk Enterprise, Splunk SIEM, and Splunk SOAR. You'll also discover how to use and troubleshoot the Cisco Security Cloud App, Cisco Legacy Apps, and technology add-ons (TAs) for integrating Cisco security solutions with Splunk. Learning Objectives: - Explain the Splunk Enterprise/Cloud fundamentals - Explain the use of SIEM, SOAR to enhance the SOC's ability to detect, investigate, and respond to security threats effectively - Implement Cisco Security Solutions to Splunk Integration using the Cisco Security Cloud App - Implement Cisco Security Solutions to Splunk Integration using Cisco Legacy Apps and TAs - Illustrate the value of integrating Cisco security solutions with Splunk using real-world use cases - Troubleshoot the Cisco Security Cloud App and the Cisco Apps and TAs Who Should Enroll: - System Engineers - SOC Engineers - Network Architects Pre-requisites: - Cisco CCNP Security or equivalent knowledge		Course Outline: This training provides advanced knowledge and hands-on skills for Cisco SD-WAN security and cloud services. You will learn to deploy on-box security features, such as application-aware firewall, intrusion prevention, URL filtering, malware protection, and TLS/SSL decryption, and integrate SD-WAN with multiple cloud service providers. It also covers configuring local and cloud-based security services using Cisco Umbrella, and automating SD-WAN fabric integration with cloud providers via Cisco vManage workflows. Learning Objectives: - Describe Cisco SD-WAN security functions, deployment options, and on-premises threat prevention - Implement content filtering and secure Direct Internet Access (DIA) - Explain and configure service chaining and SASE use cases - Describe and deploy Cisco Umbrella SIG with DNS policies - Explore and implement Cloud Access Security Broker (CASB) solutions, including Microsoft 365 - Use Cisco ThousandEyes to monitor cloud services and Microsoft 365 applications - Deploy Cisco SD-WAN Cloud OnRamp for SaaS and multi-cloud optimisation - Monitor and manage SD-WAN networks using Cisco vManage and vAnalytics Who Should Enroll: - Network Engineers / Architects - Network Security Engineers Pre-requisites: - Basic understanding of enterprise routing - Basic understanding of WAN networking / Cisco SD-WAN - Basic understanding of public cloud services	

Cybersecurity

Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRULES)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
CLCs	28
CE Credits	24

Course Outline:

This training provides the knowledge and skills to create, test, and optimise custom rules, including standard and advanced rule-writing techniques, integrating OpenAppID, filtering rules, tuning for performance, and other best practices for effective rule management when using SNORT.

Learning Objectives:

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules

Who Should Enroll:

- Security Administrators
- Network Administrators
- System Engineers
- Technical Support Personnel

Pre-requisites:

- Basic knowledge of networking protocols and security concepts
- Basic Linux command-line skills and familiarity with text editors
- Basic knowledge of Snort-based IDS/IPS systems

Securing Cisco Networks with Open Source Snort (SSFSNORT)

Duration	4 Days
Delivery	ILT / VILT / Self-paced
CLCs	36
CE Credits	20

Course Outline:

This training shows you how to deploy a network intrusion detection system based on Snort, you will learn how to install, configure, operate, and manage a Snort system. You will also explore rules writing with an overview of basic options, advanced rules writing, how to configure PulledPork, and how to use OpenAppID to provide protection of your network from malware. You will learn techniques of tuning and performance monitoring, traffic flow through Snort rules.

Learning Objectives:

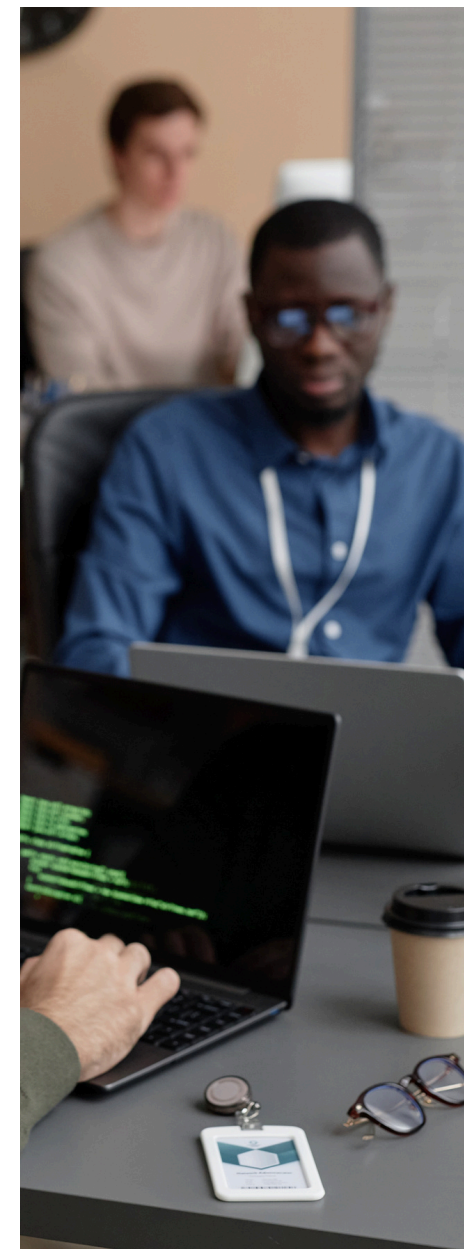
- Explain the Splunk Enterprise/Cloud fundamentals
- Explain the use of SIEM, SOAR to enhance the SOC's ability to detect, investigate, and respond to security threats effectively
- Implement Cisco Security Solutions to Splunk Integration using the Cisco Security Cloud App
- Implement Cisco Security Solutions to Splunk Integration using Cisco Legacy Apps and TAs
- Illustrate the value of integrating Cisco security solutions with Splunk using real-world use cases
- Troubleshoot the Cisco Security Cloud App and the Cisco Apps and TAs

Who Should Enroll:

- Security Administrators
- Network Administrators
- System Engineers
- Technical Support Personnel

Pre-requisites:

- Technical understanding of TCP/IP networking and network architecture
- Proficiency with Linux and UNIX text editing tools



Cybersecurity

Splunk AppDynamics for Hybrid Application Monitoring (SAHA)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
CLCs	36
CE Credits	32

Course Outline:

This training explores application performance monitoring (APM) and business analytics for hybrid applications using Cisco AppDynamics. You will also learn about customer digital experience and application dependency monitoring, leveraging network insights through Cisco ThousandEyes and integrating them with real user monitoring in AppDynamics. Finally, you will learn about application security with Cisco Application Security.

Learning Objectives:

- Understand the core principles and architecture of Cisco FSO
- Deploy, configure, and manage Cisco AppDynamics
- Troubleshoot issues affecting business transactions
- Understand the foundations of Cisco ThousandEyes and AppDynamics
- Deploy and configure Cisco ThousandEyes
- Learn app dependency monitoring with AppDynamics and ThousandEyes
- Explore hybrid application security and business risk observability

Who Should Enroll:

- Security Administrators
- Network Administrators
- System Engineers
- Technical Support Personnel

Pre-requisites:

- Basic understanding of application architectures and deployment models
- Fundamental knowledge of APM
- Basic understanding of networking concepts
- Foundational knowledge of application security practice



Cloud & Hybrid Infrastructure

Cloud and hybrid infrastructure is central to every modern enterprise, enabling scalable, flexible, and resilient IT services that support business growth. Learn how Cisco solutions empower organisations to deploy, manage, and optimise hybrid environments while ensuring performance, security, and reliability.

These training resources help professionals explore and master Cisco cloud and hybrid technologies. Through hands-on learning, participants build skills in cloud architecture, virtualisation, automation, and hybrid operations to streamline IT management, enhance operational efficiency, and deliver measurable business value.

Cloud & Hybrid Infrastructure

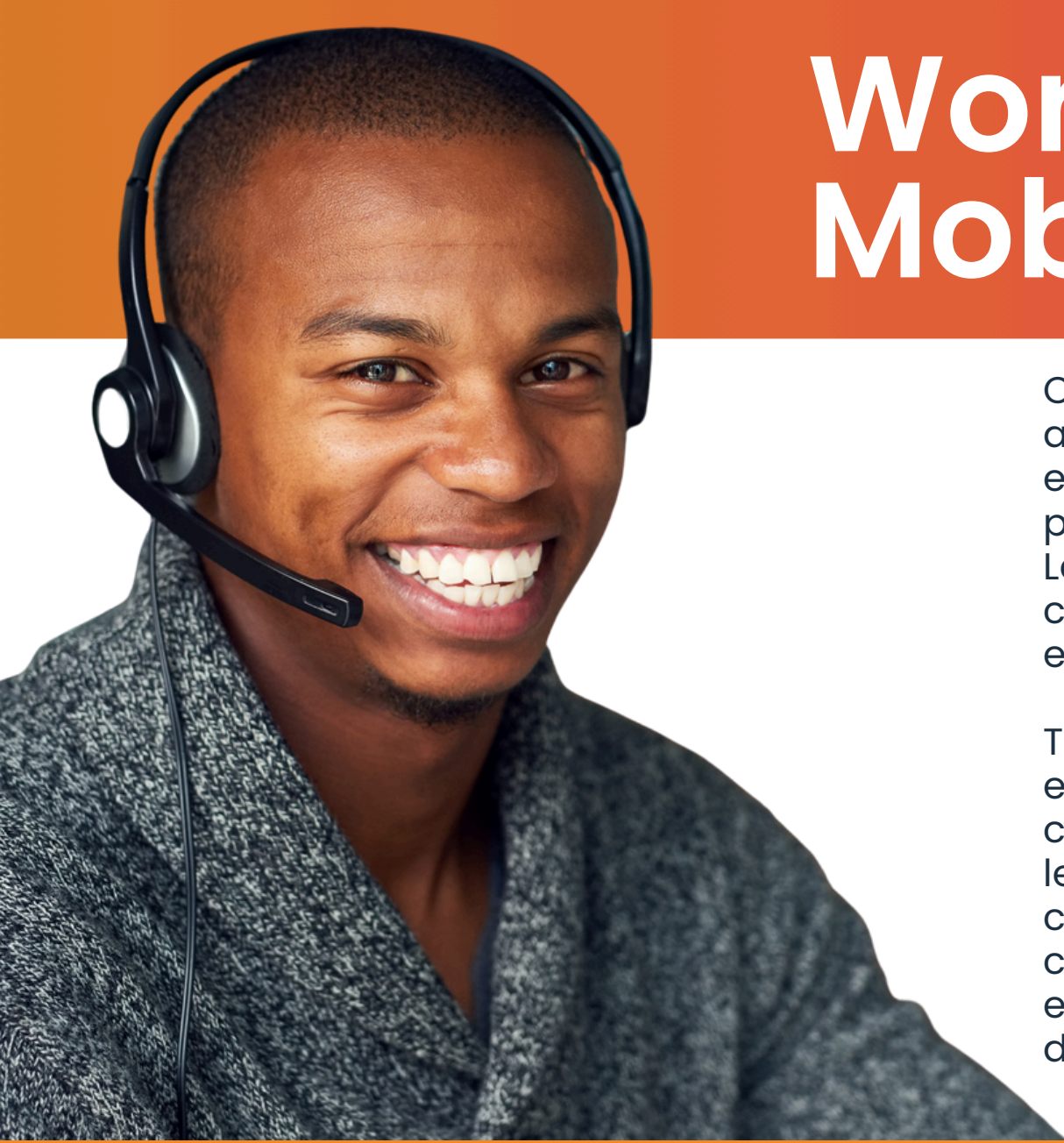
Understanding Cisco Data Centre Foundations (DCFNDU)	Cisco Data Centre Nexus Dashboard Essentials (DCNDE)	Cisco Nexus Dashboard Advanced (DCNDA)
Duration 5 Days	Duration 5 Days	Duration 3 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 44	CLCs 44	CLCs 27
CE Credits 25	CE Credits 26	CE Credits 24
Course Outline: This training, will teach you the foundational knowledge and skills you need to configure Cisco data centre technologies, including networking, virtualisation, storage area networking, and unified computing. You will get an introduction to Cisco Application Centric Infrastructure (ACI), automation and cloud computing. You will get hands-on experience with configuring features on Cisco Nexus Operating System (NX-OS) and Cisco Unified Computing System. Learning Objectives: - Identify and describe core data centre networking concepts. - Recognise Cisco Nexus products, NX-OS features, and tools. - Configure and explain Layer 3 redundancy, port channels, and vPCs. - Demonstrate switch, server, and network virtualisation concepts. - Compare and implement Fibre Channel, NPV/NPIV, and FCoE - Apply Ethernet enhancements to create lossless data centre fabrics. - Use Cisco UCS Manager, ACI, and Nexus Dashboard for management. - Explain cloud computing basics and leverage APIs for automation. Who Should Enroll: - Data Centre Designers / Administrators / Engineers - Systems Engineers - Technical Solutions Architects - Network Architects / Managers - Server / Storage Administrators Pre-requisites: - Good foundation of networking protocols - Basic knowledge of computer virtualisation	Course Outline: This training provides foundational knowledge of the Cisco Nexus Dashboard platform, covering architecture, components, and deployment planning. You will learn installation requirements, licensing, connectivity, clustering, and software stacks, navigate the GUI, manage sites, monitor and troubleshoot operations, and administer authentication, including administrator authorisation and day-to-day platform management. Learning Objectives: - Explore the Cisco Nexus Dashboard platform and core capabilities - Explain licensing, clustering, connectivity, GUI, software stack, roles, and application installation - Perform Cisco Nexus Dashboard maintenance tasks - Configure and manage local and remote authentication - Monitor platform health, resources, and operational status - Describe Cisco Nexus Dashboard Fabric Controller (NDFC) features and dashboards - Explore data centre fabrics using NDFC, including topology, VXLAN EVPN, APIs, and lifecycle management - Describe and apply enhanced role-based access control (RBAC) for fabric objects Who Should Enroll: - Systems Engineer - Data Centre Engineer / Administrator / Manager Pre-requisites: - Understanding of data centre architecture and concepts, data centre infrastructure operations and Cisco data centre switches	Course Outline: This training focuses on how to deploy and use Cisco Nexus Dashboard Insights (NDI) and Cisco Nexus Dashboard Orchestrator (NDO) to successfully monitor data centre networks, and to provision a Cisco Application Centric Infrastructure (ACI)-based multisite network. Learning Objectives: - Apply troubleshooting methodology to Cisco ACI networks - Troubleshoot logical and physical constructs of the Cisco ACI policy - Understand Cisco APIC and its troubleshooting aspects - Troubleshoot endpoint learning in Cisco ACI - Troubleshoot Layer 2 traffic bridging and Layer 3 routing in the Cisco ACI network - Troubleshoot hypervisor integration in Cisco ACI - Troubleshoot Layer 4 to Layer 7 service insertion - Troubleshoot contracts and route leaking in Cisco ACI Who Should Enroll: - Data Centre Network Administrators / Operators - Data Centre Architects / Engineers / Managers Pre-requisites: - Understanding of Cisco routing and switching in a data center - Fundamentals of network management and network operation - Understanding of Cisco ACI

Cloud & Hybrid Infrastructure

Implementing Cisco Application Centric Infrastructure – Advanced (DCACIA)	Cisco Application Centric Infrastructure Operations and Troubleshooting (DCACIO)	Troubleshooting Cisco Application Centric Infrastructure (DCACIT)
Duration 5 Days	Duration 3 Days	Duration 2 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 45	CLCs 35	CLCs 21
CE Credits 40	CE Credits 32	CE Credits 24
Course Outline: This training teaches you to deploy and manage Cisco Nexus 9000 Series Switches in Cisco ACI mode. You'll learn to configure the fabric, implement policy-driven management, and integrate software and hardware. It covers advanced ACI features, including Multi-Pod/Multi-Site deployments, Rogue Endpoint detection, VRF route leaking, contracts, zoning rules, and service-node redirection. Learning Objectives: • After completing the course, you should be able to: • Describe Cisco ACI Fabric Infrastructure and basic Cisco ACI concepts • Describe Cisco ACI policy model logical constructs • Describe Cisco ACI basic packet forwarding • Describe external network connectivity • Describe VMM Integration • Describe Layer 4 to Layer 7 integrations • Explain Cisco ACI management features Who Should Enroll: • Network Designers / Administrators / Engineers / Managers • Systems Engineers • Data Centre Engineers / Architects • Field Engineers • Server / Storage Administrators Pre-requisites: • Understanding of networking protocols, routing, and switching • Familiarity with Cisco Ethernet switching products • Understanding of Cisco data centre architecture • Familiarity with virtualisation fundamentals	Course Outline: This course shows you how to manage, monitor, and troubleshoot Cisco® Nexus® 9000 Series Switches in ACI mode. You will learn about operational tools, best practices, caveats, and practice troubleshooting common issues on a live fabric. Based on lessons learned in a wide range of production deployments, this course gives you the real-world knowledge and skills to boost operational efficiencies in your own deployment. Learning Objectives: • Describe the ACI built-in tools for operating and monitoring the fabric. • Describe the complex challenges related to monitoring and Cisco tools that address them: Cisco Nexus Dashboard and Cisco Nexus Dashboard Insights. • Describe fabric installation upgrade, backup, restore, and best practices for Cisco NX-OS-to-ACI migration and Cisco ACI management access. • Describe best practices for Cisco ACI naming conventions, Day-0 configuration, VMM integration, and Cisco ACI migrations. Who Should Enroll: • Network Engineer / Manager • Systems Engineer • Data Centre Engineer • Field Engineer • Server Administrator Pre-requisites: • Understanding of ACI architecture and concepts, data centre infrastructure operations and Cisco data centre switches	Course Outline: This training teaches you the key components and procedures needed to manage, monitor, and troubleshoot Cisco® Nexus® 9000 Series Switches in Application Centric Infrastructure (ACI) mode, a solution to simplify, optimise, and accelerate infrastructure deployment and governance. Learning Objectives: • Apply troubleshooting methodology to Cisco ACI networks • Troubleshoot logical and physical constructs of the Cisco ACI policy • Understand Cisco APIC and its troubleshooting aspects • Troubleshoot endpoint learning in Cisco ACI • Troubleshoot Layer 2 traffic bridging and Layer 3 routing in the Cisco ACI network • Troubleshoot hypervisor integration in Cisco ACI • Troubleshoot Layer 4 to Layer 7 service insertion • Troubleshoot contracts and route leaking in Cisco ACI Who Should Enroll: • Network Engineer / Manager • Systems Engineer • Data Centre Engineer • Field Engineer • Server Administrator Pre-requisites: • Understanding of Data centre infrastructure operations • Familiarity with Cisco data centre switch management • Basic programming and network troubleshooting knowledge • Experience in Linux or Windows system/network administration

Cloud & Hybrid Infrastructure

Implementing Cisco NX-OS Switches and Fabrics in the Data Centre (DCNX)	AI Solutions on Cisco Infrastructure Essentials (DCAIE)	Cisco Intersight Essentials (DCEIS)
Duration 5 Days	Duration 4 Days	Duration 3 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 46	CLCs 35	CLCs 28
CE Credits 40	CE Credits 34	CE Credits 18
Course Outline: This training teaches you how to install, configure, and manage Cisco Nexus switch platforms in a scalable, highly available environment. You will learn how to describe various aspects of the Cisco Nexus product families and platforms, including implementation, management, security, programmability and storage. You will also learn how to configure device aliases and zoning, Fibre Channel over Ethernet (FCoE), and N-Port Identifier Virtualisation (NPIV), and N-Port Virtualisation (NPV) mode. Learning Objectives: - Describe the Cisco Nexus platforms and their roles in data centres - Explain Cisco Nexus platform architectures, implementations, and management models - Configure port channels, virtual port channels (vPCs), and first-hop redundancy protocols - Describe and apply security features on Cisco Nexus devices - Explain routing, forwarding, and QoS on Cisco Nexus switches - Describe VXLAN fundamentals and use cases on Nexus platforms - Explain system monitoring, management processes, and NX-OS programmability - Configure storage networking features, including FCoE, NPIV/NPV, device aliases, and zoning Who Should Enroll: - Data Centre Engineers / Architects - Field Engineers Pre-requisites: - Be familiar with Cisco data centre technologies - Understand networking protocols, routing, and switching	Course Outline: This course covers the essentials of deploying, migrating, and operating AI solutions on Cisco data centre infrastructure. You'll be introduced to key AI workloads and elements, as well as foundational architecture, design, and security practices critical to successful AI solutions. Learning Objectives: - Explain core AI, ML, and generative AI concepts, applications, and trends - Describe how AI enables intelligent network operations and security - Describe AI/ML cluster architectures, model lifecycles, and management fundamentals - Use JupyterLab, Python, and generative AI to automate NetOps - Describe AI infrastructure design, including compute, storage, cost, and sustainability - Explain AI/ML networking requirements and data centre connectivity models - Describe high-performance, lossless networking for AI workloads - Configure and monitor AI-optimised fabrics using Nexus Dashboard Insights and NDFC Who Should Enroll: - Network Designer / Engineer / Administrator / Manager - Systems Engineer - Data Centre Engineer - Field Engineer - Server / Storage Administrator Pre-requisites: - Understanding of Cisco UCS compute architecture and operations - Knowledge of the Nexus switch portfolio and features	Course Outline: This training introduces Cisco UCS hardware, connectivity, and management, with a focus on Cisco Intersight. You will learn Intersight features, licensing, server profile deployment, and OS installation prerequisites, and gain hands-on experience managing compute, network, and storage resources, including automation using the Cisco Intersight API with HashiCorp Terraform. Learning Objectives: - Describe Cisco UCS platforms, including hardware, connectivity, management, and converged infrastructure - Explain Cisco Intersight fundamentals, licensing, key features, deployment models, and Managed Mode - Implement server profiles and OS deployment using Cisco Intersight - Manage Cisco UCS firmware lifecycles with Intersight - Deploy and manage Cisco HyperFlex using Cisco Intersight - Use Intersight Virtualisation Services and ecosystem integrations - Apply Intersight Workload Optimiser and Cloud Orchestrator for workload optimisation and automation - Automate and integrate Intersight using APIs, Terraform, and the IMM Transition Tool Who Should Enroll: - Network Engineer / Administrator / Manager - Systems Engineer - Server / Storage Administrator Pre-requisites: - General knowledge of Cisco UCS servers - Server virtualisation knowledge



Workforce Mobility

Collaboration and contact centre solutions are essential to every enterprise, connecting employees, customers, and partners to drive productivity and deliver seamless experiences. Learn how Cisco technologies enable effective communication, streamlined workflows, and enhanced customer engagement.

These training resources help professionals explore and master Cisco collaboration and contact centre solutions. Through hands-on learning, participants develop skills in unified communications, team collaboration, contact centre operations, and automation to improve efficiency, strengthen engagement, and deliver measurable business value.

Workforce Mobility

The Essentials of Webex Calling (CLWXCALL)		Understanding Cisco Contact Center Enterprise Foundations (CCEF)	Administering Cisco Contact Center Enterprise (CCEA)
Duration	3 Days	Duration	1 Day
Delivery	ILT / VILT / Self-paced	Delivery	ILT / VILT / Self-paced
CLCs	27	CLCs	10
CE Credits	18	CE Credits	6
Course Outline: This training is designed to guide you through a complete Webex Calling setup, from the initial installation of Webex Control Hub to configuring Webex Calling features through the Cisco Unified Communications Manager (CUCM) and Cisco Unified Border Element (CUBE) public switch telephone network (PSTN) setup.		Course Outline: This course gives you an overview of the Cisco® Packaged Contact Center Enterprise (PCCE) and Unified Contact Center Enterprise (UCCE) solutions. You will gain an understanding of contact centre basics and describe the available Cisco contact centre solutions and intended target customers. You will also focus on the CCE family of products and explore key features and functionality of the solution including architecture, major system components, and tools used for administration and reporting.	
Learning Objectives: - Describe Webex solution components: Meetings, Messaging, and Calling - Navigate Webex Control Hub for management, services, analytics, and reporting - Add and manage users, devices, and calling features in Control Hub - Provision Cisco IP Phones and configure user and organisation calling settings - Explain PSTN connectivity options for Webex Calling - Design and deploy premises-based PSTN using local gateways and supported routers - Configure high availability and failover with CUBE and local gateways - Configure and troubleshoot Webex Calling and media issues in PSTN deployments		Learning Objectives: - Navigate Cisco CCE configuration, scripting, and administration tools - Configure dialled numbers, call types, media routing domains, and business hours - Build and test basic ICM routing scripts and VXML applications - Configure agents, skill groups, teams, supervisors, and roles - Implement IVR functionality, attributes, precision queues, and RONA handling - Enhance agent efficiency using Cisco Finesse features - Configure reporting components and run CUIC reports - Validate end-to-end call flows and routing behaviour	
Who Should Enroll: - Collaboration Engineers - Collaboration Administrators		Who Should Enroll: - Contact Center Enterprise (CCE) administrators - Deployment engineers	
Pre-requisites: - A basic understanding of unified communications - A basic understanding of cloud-based unified communications		Pre-requisites: - Solid understanding of IP networking fundamentals - Working knowledge of Unified Communications Manager and voice gateways - Basic understanding of Cisco UCCE architecture and operation	

Workforce Mobility

Administering Advanced Cisco Contact Centre Enterprise (CCEAA)	Reporting Cisco Contact Center Enterprise (CCER)	Implementing Cisco Contact Centre Enterprise (CCEI)
Duration 3 Days	Duration 2 Days	Duration 3 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 28	CLCs 18	CLCs 27
CE Credits 18	CE Credits 12	CE Credits 24
Course Outline: This course teaches you how to perform advanced administration tasks for the Cisco Contact Center Enterprise (CCE) solution through an in-depth examination of its technical and operational requirements, as well as the tools used to configure, operate, and maintain the solution. You will learn how to optimise CCE management for proactive contact centre operations and how to manage scalability and component interaction to support centralised application management. Learning Objectives: • Explain PCCE components, protocols, and call flows using the Discovery platform • Build a baseline CCE configuration using the Bulk Import utility • Develop advanced VXML applications with database lookup and digit collection • Integrate VXML and CCE scripting to present caller data to the agent desktop • Provision CCE for CUCM-originated contact center and non-contact center calls • Deploy and manage custom Finesse desktop gadgets • Configure and deploy Mobile Agent functionality • Implement and validate Post Call Survey in a CCE environment Who Should Enroll: • Deployment Engineers Pre-requisites: • Solid understanding of IP networking fundamentals • Working knowledge of Unified Communications Manager and voice gateways • Basic understanding of Cisco UCCE architecture and operation	Course Outline: This course delivers a comprehensive architectural overview of the Cisco Contact Center Enterprise (CCE) solution, covering core and optional components, deployment models, and their interrelationships. It examines end-to-end reporting capabilities and data integration across multiple sources, and builds Tier 2/Day 2 operational expertise in analysis, troubleshooting, and support. The course also positions CCE as a business platform for delivering connected, contextual, and continuous customer journeys across channels and time. Learning Objectives: • Explain the Cisco Unified Intelligence Center (UIC) including the benefits and features of the system and describe the high-level architecture of Cisco UIC in the UCCE environment • Understand the UIC administration console to perform administrative, maintenance and provisioning functions • Discuss the functional attributes of the Cisco UIC • Customise Cisco UIC Reports and Views • Consolidate disparate data into manageable, comprehensive reports • Understand the business application of the CCE solution and how it provides a framework of correlation between core and optional components Who Should Enroll: • Deployment engineers • Administrators • Managers overseeing CCE deployments Pre-requisites: • Solid understanding of IP networking fundamentals • Strong knowledge of Cisco PCCE functionality • Experience administering Cisco PCCE environments	Course Outline: This course teaches you how to build and implement a Cisco Packaged Contact Center Enterprise (PCCE) solution, including advanced integration of external data, Single Sign-On (SSO), and process detail for the CCE solution with examples of the various deployment models. This integration process enables businesses and organisations to deliver a connected digital experience of continuous and capability-rich journeys for your customers, across time and channels. This course teaches you to install the CCE solution and provide Tier 2–3 solution support. The focus is on Day 1 support for a new CCE deployment Learning Objectives: • Design and size a PCCE deployment by examining components, protocols, and variables. • Develop system design specifications and deployment plans. • Install CCE software and manage CA-signed certificates. • Configure Remote Site functionality. • Build advanced VXML applications with Call Studio and CCE Scripting. • Configure end-to-end Dial Plans with CUBE, CUSP, VVBs, and VXML gateways. • Integrate reporting with CUIC, LiveData, and Finesse. • Create routing scripts and configure Single Sign-On. Who Should Enroll: • Deployment Engineers Pre-requisites: • Solid understanding of IP networking fundamentals • Strong understanding of Cisco PCCE functionality • Advanced experience administering of Cisco PCCE • Knowledge of UCM and Voice Gateways

Workforce Mobility

Reporting Cisco Contact Centre Enterprise (CCECE)		Troubleshooting Cisco Contact Centre Enterprise (CCET)	
Duration	2 Days	Duration	2 Days
Delivery	ILT / VILT / Self-paced	Delivery	ILT / VILT / Self-paced
CLCs	36	CLCs	18
CE Credits	12	CE Credits	24
Course Outline: This course teaches how to deploy Cisco Enterprise Chat and Email (ECE) within an existing Enterprise Contact Center. You will learn to prepare and configure PCCE and ECE for integration, perform initial deployment, and manage ongoing administration tasks, including SSO, object imports, queue and workflow setup, scripting, reporting, logging, and agent-enhancing features.		Course Outline: This course is focused on Day 2 support of a Packaged Contact Center Enterprise (PCCE) deployment by Tier 3 support personnel. Cisco® PCCE provides an enterprise-class contact center in a prepackaged deployment model that offers simplified deployment, operation, and maintenance. You will learn to identify the processes and tools used to diagnose common deployment issues so that support personnel can select optimal methods to resolve those issues.	
Learning Objectives: - Describe the Cisco ECE solution and its deployment with CCE - Identify ECE components and available enterprise deployment models - Navigate and differentiate partitions, processes, and instances in the Classic ECE interface - Configure PCCE and ECE integration requirements, including email services and Single Pane of Glass - Add and configure the ECE Agent gadget on Cisco Finesse Desktop - Configure and verify chat functionality, queues, entry points, and template sets - Implement and verify callback, delayed callback, and customized chat experiences - Configure and enable Agent Single Sign-On in the ECE/CCE environment		Learning Objectives: - Describe CCE flows and processes required to support and troubleshoot the PCCE deployment - Introduce the many diagnostic tools available to the engineer responsible for troubleshooting a PCCE environment - Learn the troubleshooting techniques to maximise the benefits the prepackaged deployment model - Anticipate and rectify possible deployment issues by learning the tools and processes that provide solutions for deployment issues - Apply troubleshooting tools and techniques to address issues with CCE Certificates, Cisco Finesse, and PCCE Deployment	
Who Should Enroll: - Deployment engineers - Administrators - Managers overseeing CCE deployments		Who Should Enroll: - Deployment engineers - Managers overseeing CCE deployments	
Pre-requisites: - Solid understanding of IP networking fundamentals - Advanced experience administering Cisco PCCE - Experience deploying Cisco PCCE		Pre-requisites: - Strong understanding of IP networks - Advanced experience administering of Cisco PCCE - Experience deploying Cisco PCCE - Experience administering and troubleshooting Cisco Unified Communications Manager and Voice Gateways	



Workforce Mobility

Understanding Cisco Collaboration Foundations (CLFNDU)	Implementing Cisco Collaboration Conferencing (CLCNF)
Duration 5 Days	Duration 5 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 44	CLCs 43
CE Credits 21	CE Credits 24
Course Outline: This training gives you the skills and knowledge needed to administer and support a simple, single-site Cisco® Unified Communications Manager (UCM) solution with Session Initiation Protocol (SIP) gateway. The training covers initial parameters, management of devices, management of users, and management of media resources. Learning Objectives: - Understand Cisco collaboration solutions across on-premises, cloud, and hybrid environments - Explain Cisco Unified Communications Manager design, clustering, redundancy, deployment models, and operational administration - Analyse codecs, SIP call flows, session setup/teardown, and key media resources such as MTPs, transcoders, conferencing, and MOH - Design CUCM call routing using digit manipulation, translation patterns, route logic, and class of service configuration - Identify Cisco IP phones and Webex endpoints, registration methods, software compatibility, and lifecycle management - Evaluate Cisco Jabber, IM & Presence, and Unity Connection architecture, integration, and user communication workflows - Analyse Expressway and CUBE for secure voice/video traversal, encryption, toll-fraud prevention, and external network connectivity - Configure Webex Control Hub, Webex Calling, reporting, and hybrid services including Video Mesh, Edge Audio, and cloud-connected UC Who Should Enroll: - Network Administrators - Network Engineers - Systems Engineers Pre-requisites: - Internet web browser usability knowledge and general computer usage - Knowledge of Cisco Internetwork Operating System (Cisco IOS®) command line	Course Outline: In this course you will gain knowledge and skills to design and implement common conferencing deployment scenarios of Cisco Meeting Server, its integration with call control features such as Cisco Unified Communications Manager and Cisco Expressway, and other Cisco conferencing devices. Learning Objectives: - Understand Cisco conferencing across on-premises, hybrid, and cloud models - Describe and compare CMS physical and virtual deployment options - Configure Cisco Meeting Server for WebRTC and SIP connectivity - Design and configure resilient multi-server CMS deployments to support enterprise-scale conferencing - Use Cisco Meeting Server APIs to configure profiles and manage conferencing services - Configure Rendezvous, scheduled, and ad-hoc conferencing by integrating Cisco Meeting Server with Cisco Unified Communications Manager - Implement recording, streaming, and scheduled conferencing using Cisco Meeting Server, Cisco TMS, and Cisco Meeting Management - Integrate CMS with Microsoft Teams and Cisco UC tools Who Should Enroll: - Deployment engineers - Network engineers Pre-requisites: - SIP signalling fundamentals - Knowledge of Cisco Unified CM and Cisco Expressway - Familiarity with APIs - Video endpoint operation and configuration





Intelligent Automation

This technology area focuses on building modern software solutions and automating business processes across cloud, network, and application platforms. It emphasises developer-centric practices, API-driven integration, and low-code and pro-code approaches to accelerate application delivery and operational efficiency.

Training equips professionals to design, build, and integrate applications that connect systems, data, and workflows. Learners develop skills in automation, extensibility, and lifecycle management, enabling faster innovation, improved scalability, and more resilient digital services across enterprise environments.

Intelligent Automation

Programming for Network Engineers (PRNE)	Intermediate Python for Network Engineers (IPYNE)	Introducing Automation for Cisco Solutions (CSAU)
Duration 4 Days	Duration 5 Days	Duration 3 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 36	CLCs 16	CLCs 29
CE Credits 24	CE Credits 29	CE Credits 16
Course Outline: This training is designed to equip you with fundamental skills in Python programming, you will learn to use Python basics to create useful and practical scripts with Netmiko to retrieve data and configure network devices. Upon completion of this course, you should have a basic understanding of Python, including the knowledge to create, apply, and troubleshoot simple network automation scripts. Learning Objectives: • Create and run Python scripts • Describe Python data types and strings and their use cases • Explain loops, conditionals, and operators in Python • Describe classes, methods, functions, namespaces, and scopes • Use Python for data manipulation and storage • Explain Python modules and packages and their benefits • Manipulate user input and manage errors/exceptions • Debug Python code effectively Who Should Enroll: • Network administrators • Network engineers • Network managers • Systems engineers Pre-requisites: • Familiarity with Cisco IOS--XE software or other Cisco network device configuration and operation skills • Basic network management knowledge • Cisco CCNA certification or equivalent knowledge	Course Outline: This training will teach you to use Python for network automation and programmability. Develop scripts for device management, inventory, configuration backup, testing, and monitoring. Automate interactions with REST APIs (e.g., Cisco Meraki, ThousandEyes) and apply best practices in debugging, logging, unit testing, and CI/CD integration for scalable, reliable network operations. Learning Objectives: • Apply Python for network automation, programmability, and scaling from traditional to modern networks. • Develop scripts using core Python, libraries (e.g., Netmiko), and functions for device management and inventory automation. • Parse, analyze, validate, and back up device configurations using CLI tools, PyATS, and Git. • Automate network testing, monitoring, and REST API interactions with platforms like Cisco Meraki and ThousandEyes. • Implement best practices: debugging, logging, unit testing, and CI/CD integration for reliable automation workflows. Who Should Enroll: • Network administrators • Network engineers • Network managers • Systems engineers Pre-requisites: • Familiarity with Cisco IOS--XE software or other Cisco network device configuration and operation skills • Basic network management knowledge • Cisco CCNA certification or equivalent knowledge	Course Outline: This training gives you a broad overview of network automation skills, you will learn the fundamentals of automation such as model-driven programmability solutions with representational state transfer configuration (RESTCONF) and network configuration (NETCONF) protocols. It also covers data formats and types, including Extensible Markup Language (XML), JavaScript Object Notation (JSON), Yaml Ain't Markup Language (YAML), and Yet Another Next Generation (YANG), and their value in network automation. Learning Objectives: • Explain the role of automation and programmability in network operations • Compare waterfall and agile methodologies for network automation • Interpret and troubleshoot Python scripts for common network automation use cases • Apply DevOps principles, tools, and pipelines to network operations • Use automation development and virtual environments • Build and consume HTTP-based APIs using Python, including requests, XML, JSON, and YAML • Explain YANG models and the use of NETCONF and RESTCONF • Automate network devices using playbooks and templates Who Should Enroll: • Network Engineers and Automators • Network Architects and Designers • Reliability Engineers • Application Developers Pre-requisites: • General knowledge of networks, including OSPF, BGP & SNMP • Fundamentals of Python • Basic Linux commands

Intelligent Automation

NSO Essentials for Programmers and Network Architects (NSO201)	NSO Advanced for Python Programmers (NSO300)	Cisco NSO Administration and DevOps (NSO303)
Duration 4 Days	Duration 5 Days	Duration 4 Days
Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced	Delivery ILT / VILT / Self-paced
CLCs 36	CLCs 36	CLCs 36
CE Credits 40	CE Credits 50	CE Credits 50
Course Outline: This training introduces Cisco Network Services Orchestrator (NSO), covering installation, device management, and service creation using YANG templates with XPath. You'll learn NSO fundamentals, NETCONF, service and device templates, service package creation, network element drivers, API integration, system configuration and troubleshooting, alarms and reporting, and scalability and performance optimisation. Learning Objectives: - Align NSO service activation with business requirements and device communication. - Apply NETCONF, YANG models, and device commit capabilities. - Design and deploy real-world services with parameter-to-device mapping. - Troubleshoot NSO deployments and verify device connectivity. - Utilize config-templates, Reactive FASTMAP, and feature packs. - Integrate NSO with APIs to extend automation workflows. - Manage alarms and monitor network operations effectively. - Understand ETSI MANO principles and NSO 5.3 enhancements. Who Should Enroll: - System engineers / Integrators / Programmers / Administrators - Network administrators - Solutions designers Pre-requisites: - Solid understanding of IP networking fundamentals - Foundational knowledge of CLI, UNIX, programming, YANG, NETCONF, XML, and basic network device management.	Course Outline: This course builds on NSO201, focusing on advanced Cisco NSO capabilities. You will learn to customise templates with Python, deploy services using Docker and Nano services, and create advanced Layer 3 MPLS VPN services. The training emphasises efficient service scaling, enhanced security, and optimised physical space through virtualised network functions, leveraging NFV orchestration and Cisco Elastic Services Controller for automated, dynamic network management. Learning Objectives: - Describe the NSO application framework and service lifecycle integration - Deploy NSO in Docker and implement Python- and template-based services - Implement Nano services and stacked services - Deploy Layer 3 MPLS VPN services for new and existing deployments - Describe managed services and scale service orchestration - Explain ETSI MANO framework and NFV principles - Manage VNF lifecycle using Cisco Elastic Services Controller (ESC) Who Should Enroll: - System engineers / Integrators / Programmers / Administrators - Network administrators - Solutions designers Pre-requisites: - Solid understanding of IP networking fundamentals - Knowledge of CLI, UNIX, programming, YANG, NETCONF, XML, and network device management.	Course Outline: This training advances your Cisco NSO expertise by focusing on system administration and DevOps integration for network automation and orchestration. You will learn to set up, configure, deploy, and maintain production-ready NSO instances, including Docker deployment, access control, Git, and CI/CD workflows. Practical exercises cover NETCONF NEDs, CDM migration, alarm management, and real-world operational scenarios. Learning Objectives: - Explain network and IT convergence and NSO architecture - Deploy, configure, and secure NSO with high availability - Integrate NSO and manage change and service issues - Manage services, devices, and perform NED upgrades - Monitor services, ensure compliance, and track inventory - Apply Git and version control for NSO workflows - Implement CI/CD and scalable system management - Follow software development methodologies and service maintenance best practices Who Should Enroll: - Network engineers / architects - Software engineers / architects - Systems Administrators - DevOps / Integration engineers Pre-requisites: - Basic knowledge of Cisco and UNIX-like CLIs, YANG data modelling, and Python development



OUR CONTACT INFO

-  +27 (0)87 086 3550
-  www.nil.co.za
-  salesadmin@nil.co.za
-  NIL Data, Ground Floor, Building 2, The Ingress,
23 Magwa Crescent, Waterfall City, Midrand

