IPRULERS

CCNP ENTERPRISE CERTIFICATION AND TRAINING

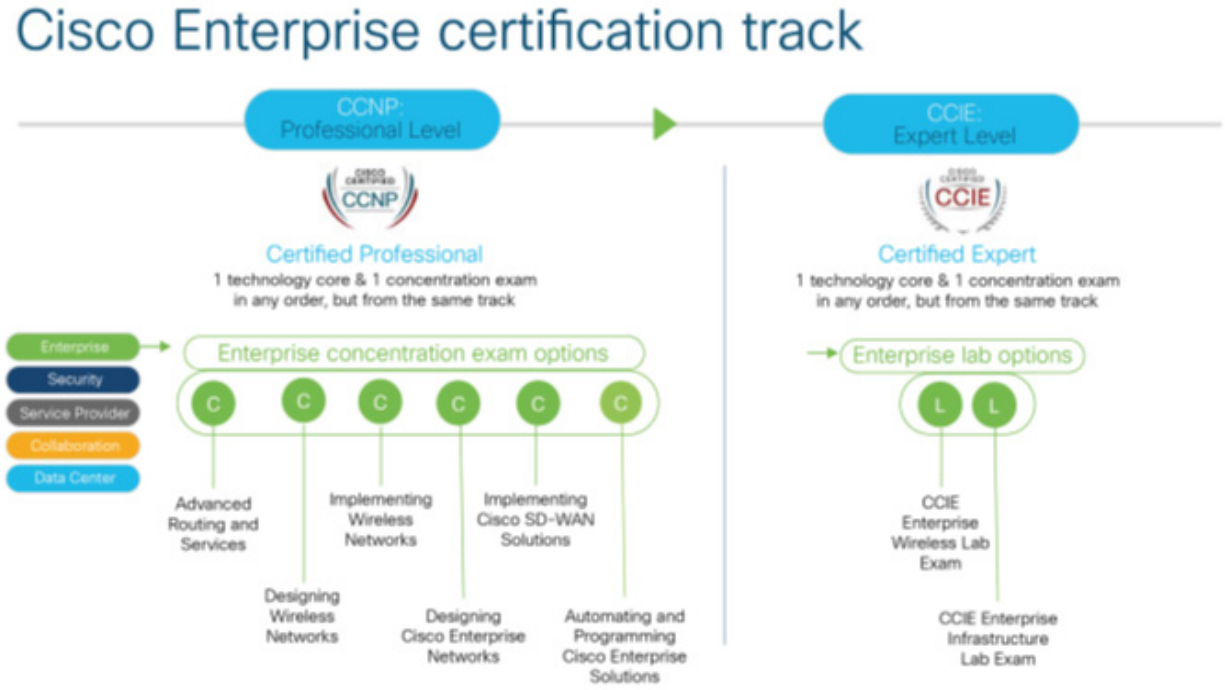
www.iprulers.com training@iprulers.com

IPRulers is the new face of **CCNP Enterprise Certification and Training** in Dubai, UAE, which provides both online and class-room-based training in the latest cutting-edge technologies in the IT infrastructure and networking portfolio. With grouped as well as one-to-one classes and online tutorials that could be scheduled for weekdays or weekends in accordance to the students' choice, IPRulers is fast becoming a leading name in Dubai in providing a highly valued Cisco Certificate, with a 100% pass rate on the first attempt. Students can choose between different concentration topics to go with the core topic to customize their certification and keep in touch with the dynamic technologies in the field, all with the help of IPRulers.

The IPRulers CCNP Enterprise Certification Program is a testimony to a candidate's networking skills. It provides in-depth technology classes in a few additional subjects along with the former CCNP Routing and Switching, CCNP Wireless and CCDP course, led by an expert team of trainers who have multiple CCIEs with experience in the industry and hands-on training. Clearing two assessments, one in the core subject, and one in the concentration subject, accrues the Certification, hence enabling focus and customization in any one technical area according to the candidate's selection.

COURSE DETAILS

The CCNP Enterprise Certification comprises of clearing two exams – one in a core subject, and another in a concentration subject. This gives a CCNP Enterprise Badge.



Clearing only the core subject gives a Core Specialist Badge, which is also the qualification for CCIE Enterprise Infrastructure and CCIE Enterprise Wireless Certifications. This exam focuses on Enterprise Infrastructure including dual-stack (IPv4 and IPv6) architecture, virtualization, infrastructure, network assurance, security, and automation.

Achieving only the concentration subject gives a Concentration Specialist Badge. This exam focuses on new, industry-specific topics such as advanced routing and services, Cisco Viptela SD-WAN solution, designing Cisco enterprise.

CCNP ENTERPRISE CORE EXAM

350-401 ENCOR – Implementing and Operating Cisco Enterprise Core Technologies ENCOR v1.1

CCNP ENTERPRISE CONCENTRATION EXAM

- 300-410 ENARSI v1.1 – Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- 300-415 ENSDWI v1.2 – Implementing Cisco SD-WAN Solutions (SDWAN300)
- 300-420 ENSLD v1.1 – Designing Cisco Enterprise Networks (ENSLD)
- 300-425 ENWLSD v1.1 – Designing Cisco Enterprise Wireless Networks (ENWLSD)
- 300-430 ENWLSI v1.1 – Implementing Cisco Enterprise Wireless Networks (ENWLSI)
- 300-435 ENAUTO v1.1 – Implementing Automation for Cisco Enterprise Solutions (ENAUI)
- 300-440 ENCC v1.0 - Designing and Implementing Cloud Connectivity

PREREQUISITES

- The CCNP Enterprise does not require any qualification for attendance of the course. However, comprehensive knowledge of the subjects is necessary for attending the examinations.
- A CCNA certificate is not necessary. Students can appear for CCNP Enterprise examinations if they have the equivalent theoretical and practical knowledge.
- Experience in networking field will be an advantage to attempt the CCNP examination.

COURSE OUTLINE

CORE EXAM

350-401 v1.1- Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

1.0 Architecture

1.1 Explain the different design principle used in an enterprise network

1.2 Describe wireless network design principles

1.3 Explain the working principles of the Cisco SD-WAN solution

1.4 Explain the working principles of the Cisco SD-Access solution

1.5 Interpret wired and wireless QoS configurations

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

2.0 Virtualization

2.1 Describe device virtualization tech nologies

2.2 Configure and verify data path virtualization technologies

2.3 Describe network virtualization con-cepts

3.0 Infrastructure

3.1 Layer 2

3.2 Layer 3

3.3 Wireless

3.4 IP Services

4.0 Network Assurance

4.1 Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog

4.2 Configure and verify Flexible Net Flow

4.3 Configure SPAN/RSPAN/ERSPAN

4.4 Configure and verify IPSLA

4.5 Describe Cisco DNA Center work flows to apply network configura tion, monitoring, and management

4.6 Configure and verify NETCONF and RESTCONF

5.0 Security

5.1 Configure and verify device access control

5.2 Configure and verify infrastructure security features

5.3 Describe REST API security

5.4 Configure and verify wireless securi ty features

5.5 Describe the components of net work security design

6.0 Automation

6.1 Interpret basic Python components & scripts

6.2 Construct valid JSON-encoded files

6.3 Describe the high-level principles benefits of a data modeling language, such as YANG

6.4 Describe APIs for Cisco DNA Center & vManage

6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF

6.6 Construct an EEM applet to automate configuration, troubleshooting, or data collection

6.7 Compare agent vs. agentless orches tration tools, such as Chef, Puppet, Ansible, and SaltStack

1.0 Layer 3 Technologies

1.1 Troubleshoot administrative distance (all routing protocols)

1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)

1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)

1.4 Troubleshoot redistribution between any routing protocols or routing sources

1.5 Troubleshoot manual and auto-summarization with any routing protocol

1.6 Configure and verify policy-based routing

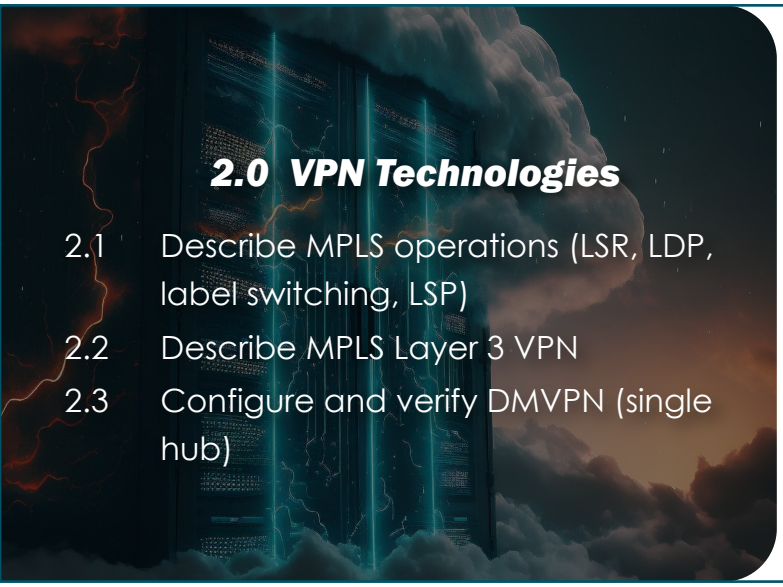
1.7 Configure and verify VRF-Lite

1.8 Describe Bidirectional Forwarding Detection

1.9 Troubleshoot EIGRP (classic and named mode; VRF and global)

1.10 Troubleshoot OSPF (v2/v3)

1.11 Troubleshoot BGP (Internal and External, unicast, and VRF-Lite)



2.0 VPN Technologies

2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)

2.2 Describe MPLS Layer 3 VPN

2.3 Configure and verify DMVPN (single hub)

3.0 Infrastructure Security

3.1 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)

3.2 Troubleshoot router security features

3.3 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)

3.4 Describe IPv6 First Hop security fea tures (RA guard, DHCP guard, bind ing table, ND inspection/snooping, source guard)

4.0 Infrastructure Services

4.1 Troubleshoot device management

4.2 Troubleshoot SNMP (v2c, v3)

4.3 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)

4.4 Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)

4.5 Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)

4.6 Troubleshoot NetFlow (v5, v9, flexible NetFlow)

4.7 Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)

300-415 - Implementing Cisco SD-WAN Solutions (SDWAN300)

1.0 Architecture

1.1 Describe Cisco SD-WAN architecture and components
1.2 Describe Cisco SD-WAN Edge platforms and capabilities
1.3 Describe Cisco SD-WAN Cloud OnRamp

2.0 Controller deployment

2.1 Describe controller cloud deployment
2.2 Describe controller on-premises deployment
2.3 Configure certificates and device lists
2.4 Troubleshoot control plane connectivity

3.0 Router Deployment

3.1 Describe WAN Edge deployment
3.2 Configure Cisco SD-WAN data plane
3.3 Configure OMP
3.4 Configure TLOCs
3.5 Configure CLI and vManage feature configuration templates
3.6 Describe multicast support in Cisco SD-WAN
3.7 Describe configuration groups, feature profiles, and workflows

4.0 Policies

4.1 Configure control policies
4.2 Configure data policies
4.3 Configure end-to-end segmentation
4.4 Configure Cisco SD-WAN application-aware routing
4.5 Configure direct Internet access

5.0 Security and Quality of Service

5.1 Configure service insertion
5.2 Describe Cisco SD-WAN security features
5.3 Describe Cloud security integration
5.4 Configure QoS treatment on WAN Edge routers
5.5 Describe Application Quality of Experience (App-QoE)

6.0 Management and Operations

6.1 Describe authentication, monitoring, and reporting from vManage
6.2 Configure authentication, monitoring, and reporting
6.3 Describe REST API monitoring
6.4 Describe software image management from vManage

1.0 Architecture

1.1 Describe Cisco SD-WAN architecture and components

1.2 Describe Cisco SD-WAN Edge platforms and capabilities

1.3 Describe Cisco SD-WAN Cloud OnRamp

2.0 Controller Document

2.1 Describe controller cloud deployment

2.2 Describe controller on-premises deploy ment

2.3 Configure certificates and device lists

2.4 Troubleshoot control plane connectivity

3.0 Router Deployment

3.1 Describe WAN Edge deployment

3.2 Configure Cisco SD-WAN data plane

3.3 Configure OMP

3.4 Configure TLOCs

3.5 Configure CLI and vManage feature configuration templates

3.6 Describe multicast support in Cisco SD-WAN

3.7 Describe configuration groups, feature profiles, and workflows

4.0 Policies

4.1 Configure control policies

4.2 Configure data policies

4.3 Configure end-to-end segmentation

4.4 Configure Cisco SD-WAN application aware routing

4.5 Configure direct Internet access

5.0 Security and Quality of Service

5.1 Configure service insertion

5.2 Describe Cisco SD-WAN security features

5.3 Describe Cloud security integration

5.4 Configure QoS treatment on WAN Edge routers

5.5 Describe Application Quality of Experience (App-QoE)

6.0 Management and Operations

6.1 Describe authentication, monitor ing, and reporting from vManage

6.2 Configure authentication, monitor ing, and reporting

6.3 Describe REST API monitoring

6.4 Describe software image manage ment from vManage

1.0 Advanced Addressing and Routing Solutions

1.1 Create structured addressing plans for IPv4 and IPv6
1.2 Create stable, secure, and scalable routing designs for IS-IS
1.3 Create stable, secure, and scalable routing designs for EIGRP
1.4 Create stable, secure, and scalable routing designs for OSPF
1.5 Create stable, secure, and scalable routing designs for BGP
1.6 Determine IPv6 migration strategies

2.0 Advanced Enterprise Campus Networks

2.1 Design campus networks for high availability (FHRP)
2.2 Design campus Layer 2 infrastructures
2.3 Design multicampus Layer 3 infrastructures
2.4 Describe SD-Access Architecture (underlay, overlay, control and data plane, automation, wireless, and security)
2.5 Describe SD-Access fabric design considerations for wired and wireless access (overlay, fabric design, control plan design, border design, segmentation, virtual networks, scalability, over the top and fabric for wireless, multicast)

3.0 WAN for Enterprise Networks

3.1 Describe WAN connectivity options for on-premises, hybrid, and cloud solutions
3.2 Design site-to-site VPN for on-premises, hybrid, and cloud solutions
3.3 Design high availability for enterprise WAN for on-premises, hybrid, and cloud solutions
3.4 Describe Cisco SD-WAN architecture (orchestration plane, management plane, control plane, data plane, on-boarding and provisioning, security)
3.5 Describe Cisco SD-WAN design considerations (control plane design, overlay design, LAN design, high availability, redundancy, scalability, security design, QoS and multicast over SD-WAN fabric)

4.0 Network Services

4.1 Select QoS strategies to meet customer requirements (DiffServ, IntServ)
4.2 Design end-to-end QoS policies
4.3 Design network management techniques
4.4 Describe multicast routing concepts (source trees, shared trees, RPF, rendezvous points)
4.5 Design multicast services (SSM, PIM bidirectional, MSDP)

5.0 Automation

5.1 Differentiate between IETF, OpenConfig, and Cisco YANG models

5.2 Differentiate between NETCONF and RESTCONF

5.3 Describe the impact of model-driven telemetry on the network

5.4 Describe GRPC and GNMI

5.5 Describe cloud connectivity options such as direct connect, cloud on ramp, MPLS direct connect, and WAN integration

5.6 Describe cloud-based services model in private, public, and hybrid deployments (Saas, PaaS, IaaS)

300-430 ENWLSI v1.1 – Implementing Cisco Enterprise Wireless Networks (ENWLSI)

1.0 Wireless Site Survey

1.1 Collect design requirements and evaluate constraints

1.2 Describe material attenuation and its effect on wireless design

1.3 Perform and analyze a Layer 1 site survey

1.4 Perform a pre-deployment site survey

1.5 Perform a post deployment site survey

1.6 Perform a predictive site survey

1.7 Utilize planning tools and evaluate key network metrics (Ekahau, AirMagnet, PI, Chanalyzer, Spec trum Analyzer)

2.0 Wired and Wireless Infrastructure

2.1 Determine physical infrastructure requirements such as AP power, cabling, switch port capacity, mounting, and grounding

2.2 Determine logical infrastructure requirements such as WLC/AP licensing requirements based on the type of wireless architecture

2.3 Design radio management

2.4 Apply design requirements for these types of wireless networks

2.5 Design high-density wireless net works and their associated compo nents

2.6 Design wireless bridging (mesh)

3.0 Mobility

3.1 Design mobility groups based on mo bility roles

3.2 Optimize client roaming

3.3 Validate mobility tunneling for data and control path

4.0 WLAN High Availability

4.1 Design high availability for controllers

4.2 Design high availability for Aps

300-435 ENAUTO v1.1 – Implementing Automation for Cisco Enterprise Solutions (ENAUI)

1.0 Network Programmability Foundation

1.1 Utilize common version control operations with git (add, clone, push, commit, diff, branching, merging conflict)

1.2 Describe characteristics of API styles (REST and RPC)

1.3 Describe the challenges encountered and patterns used when consuming APIs synchronously and asynchronously

1.4 Interpret Python scripts containing data types, functions, classes, conditions, & looping

1.5 Describe the benefits of Python virtual environments

1.6 Explain the benefits of using network configuration tools such as Ansible and Terraform for automating IOS XE platforms

2.0 Automate APIs and Protocols

2.1 Identify the JSON instance based on a YANG model (including YANG Suite)

2.2 Identify the XML instance based on a YANG model (including YANG Suite)

2.3 Interpret a YANG module tree generated per RFC8340

2.4 Compare functionality, benefits, and uses of OpenConfig, IETF, and native YANG models

2.5 Compare functionality, benefits, and uses of NETCONF and RESTCONF

3.0 Network Device Programmability

3.1 Implement device management and monitoring using NetMiko

3.2 Construct a Python script using ncclient that uses NETCONF to manage and monitor an IOS XE device

3.3 Configure device using RESTCONF API utilizing Python requests library

3.4 Utilize Ansible to configure an IOS XE device

3.5 Configure a subscription for model driven telemetry on an IOS XE device (CLI, NETCONF, and RESTCONF)

3.6 Compare publication and subscription telemetry models

3.7 Describe the benefits and usage of telemetry data in troubleshooting the network

3.8 Describe Day 0 provisioning methods

4.0 Cisco DNA Center

4.1 Compare traditional versus software-defined networks

4.2 Describe the features and capabilities of Cisco DNA Center

4.3 Implement Cisco DNA Center event outbound webhooks

4.4 Implement API requests for Cisco DNA Center to accomplish network management task

4.5 Implement API requests for Cisco DNA Center to accomplish network management tasks using these APIs

4.6 Troubleshoot Cisco DNA Center automation process using Intent APIs

5.0 Cisco SD-WAN

5.1 Describe features and capabilities of Cisco SD-WAN vManage APIs

5.2 Implement a Python script to perform API requests for Cisco SD-WAN vManage Device Inventory APIs to retrieve & display data

5.3 Construct API requests for Cisco SD-WAN vManage Administration APIs

5.4 Implement a Python script to perform API requests for Cisco SD-WAN vManage Configuration APIs to modify Cisco SD-WAN fabric configuration

5.5 Construct API requests for Cisco SD-WAN vManage Monitoring APIs (including real-time)

5.6 Troubleshoot a Cisco SD-WAN deployment using vManage APIs

6.0 Cisco Meraki

6.1 Describe features and capabilities of Cisco Meraki

6.2 Create a network using Cisco Meraki APIs

6.3 Configure a network using Cisco Meraki APIs

6.4 Implement a Python script for Cisco Meraki Alert WebHooks

300-440 ENCC v1.0 - Designing and Implementing Cloud Connectivity

1.0 Architecture Models

1.1 Describe internet-based connectivity to cloud providers (AWS, Azure, and Google Cloud)

1.2 Describe private connectivity to cloud providers (AWS, Azure, and Google Cloud)

1.3 Describe connectivity to SaaS cloud providers (AWS, Azure, and Google Cloud)

2.0 Design

2.1 Recommend the connectivity model to provide high availability, resiliency, SLAs, and reliability based on business and technical requirements

2.2 Recommend the connectivity model based on network architecture requirements such as bandwidth, QoS, dedicated vs shared, multi-homing, and routing needs based on business and technical requirements

2.3 Recommend a connectivity model to meet regulatory compliance (NIST, FEDRAMP, ISO) based on business and technical requirements

2.4 Describe cloud-native security policies for AWS, Azure, and Google Cloud, such as east/west traffic within the cloud provider, backhaul internet traffic, inbound connectivity to the internet

3.0 IPsec Cloud Connectivity

3.1 Configure IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router to a native AWS, Azure, and Google Cloud endpoint

3.2 Configure IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router and an AWS, Azure, or Google cloud-hosted Cisco IOS XE router

3.3 Configure routing on Cisco IOS XE to integrate with cloud networks using BGP and OSPF, including redistribution and static routing

4.0 SD-WAN Cloud Connectivity

4.1 Configure Cisco SD-WAN internet-based secure cloud connectivity for AWS, Azure, and Google Cloud

4.2 Configure Cisco SD-WAN OnRamp to a SaaS cloud provider

4.3 Configure Cisco SD-WAN policies (north/south and east/west)

5.0 Operation

5.1 Diagnose IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router to a native AWS, Azure, and Google Cloud endpoint

5.2 Diagnose routing issues on Cisco IOS XE to integrate with cloud networks using BGP and OSPF, including redistribution and static routing

5.3 Diagnose Cisco SD-WAN internet-based secure cloud connectivity for AWS, Azure, and Google Cloud

5.4 Diagnose Cisco SD-WAN policy issues (north/south and east/west)

LAB INFRASTRUCTURE

IPRulers has a fully equipped lab, specially designed for the **CCIE Enterprise Infrastructure training**, with an enhanced lab topology that represent real world network. Students will have the following equipment and software configured for their training; they may also get the chance to see newer hardware and software during this period.

CCNP ENTERPRISE EQUIPMENT AND SOFTWARE LIST

The practical exam tests candidates on solutions that can be configured using the below Equipment and software versions. Candidates may see more recent software versions during their attempt but will only be tested on features that are supported in the list below. Passing the exam requires a depth of understanding difficult to obtain without hands-on experience. Early in your preparation you should arrange access to equipment and software similar to that used on the exam.

Virtual machines

- **CISCO CATALYST 8000V ROUTERS WITH CISCO IOS XE SOFTWARE RELEASE 17.9**
- **CISCO IOSV WITH CISCO IOS SOFTWARE RELEASE 15.8**
- **CISCO IOSV-L2 WITH CISCO IOS SOFTWARE RELEASE 15.2**
- **CISCO SD-WAN (VMANAGE, VBOND, VSMART, CEDGE) SOFTWARE RELEASE 20.9**
- **CISCO DNA CENTER, RELEASE 2.3**

Physical Equipment

CISCO CATALYST 9300 SWITCHES WITH CISCO IOS XE SOFTWARE RELEASE 17.9

CISCO CATALYST SERIES SWITCHES

- CISCO CATALYST 9300 SERIES SWITCHES
- CISCO CATALYST 9200 SERIES SWITCHES
- CISCO CATALYST 3650 SERIES SWITCHES

CISCO DNA CENTER
CISCO WIRELESS ACCESS POINTS

- CISCO CATALYST 9115 SERIES ACCESS POINT
- CISCO AIRONET 3800 SERIES ACCESS POINTS
- CISCO AIRONET 3700 SERIES ACCESS POINTS
- CISCO AIRONET 1850 SERIES ACCESS POINTS

CISCO WIRELESS LAN CONTROLLERS

- EMBEDDED - CATALYST 9800 ON A CATALYST 9300 SWITCH
- MOBILITY EXPRESS - ON 1850
- PHYSICAL - 3504 WIRELESS CONTROLLER
- VIRTUAL - CISCO VIRTUAL WIRELESS CONTROLLER

MODE OF TRAINING

Classroom-based Training	Online Training	Corporate Training
Go old-school. Make friends and have fun, just like elementary grades. Follow lectures, turn in assignments and appear for exams in campus-style!	Sit in the comfort of your home as you move through the course. Instructors will guide you in predetermined sessions. Hundreds of supporting videos available, in case you want to outshine yourself.	Lectures and hands-on training for office employees, in the comfort of their own office. Sponsored by employers to push up their employees above the market competence.

One-on-One Training	Fast Track Training	Private Group Training
An instructor will train you in private – without any external intrusion. Ideal if you want to progress on your own. Schedule your classes according to your own timeline as you advance, without disruption to your daily routine.	No time to follow regular class timeline? Go fast track – speed through the course, whether it be alone, or online, in groups, on an accelerated timescale, to give the icing on the cake.	You and your friends like to be together in a class, but without any outsiders? You've got it! Feel as if you have hired your own instructor. A way to combat shyness, with the comfort your friend-circle.

TARGET AUDIENCE

- Network engineers seeking skill enrichment in specific technologies to nourish their passion and career.
- IT students and professionals seeking strong expertise in the subject and an internationally recognized qualification in the same for prospective jobs.

TRAINER'S PROFILE

- IP Rulers is managed by an expert team of trainers with over 15 years' experience in the industry and in hands-on training.
- All the trainers have multiple CCIEs in their respective areas of interest.
- Individual trainers' profiles can be provided upon request by email, along with demos and LinkedIn profiles.
- Online and classroom demos are also available upon request

BENEFITS

- Internationally valued certification from Cisco.
- Specialist Certification in any CCNP exam, whether it be core or concentration.
- Eligibility to attend the CCIE Enterprise (Infrastructure/Wireless) Lab Exam directly by passing the CCNP Core Examination.
- Combined benefits of CCNP Routing and Switching, CCNP Wireless and CCDP.
- Constant acquaintance to the dynamic technologies in the IT field.
- Refreshment in regular concepts of Enterprise Technologies along with Automation. Authority to link the CCNP Certification Badge to all social media profiles.

IP Rulers, 201, Wasl Business Central. 29B street, Sheikh Rashid Road.Port Saeed, Dubai.

www.iprulers.com

training@iprulers.com

+971559454771 | +97143346660