



NN-CCNA - IMPLEMENTING AND ADMINISTERING CISCO SOLUTIONS

CORSO CON DOCENTE

Durata	Prezzo	Orari	Calendario
5 giorni	2.700,00€ + IVA	9:00 - 13:00 14:00 - 17:00	

Questo corso è erogato grazie alla collaborazione con NovaNext, Cisco Learning Partner, centro autorizzato all'erogazione di corsi ufficiali Cisco.

Il corso **NN-CCNA – Implementing and Administering Cisco Solutions** offre un'ampia gamma di conoscenze fondamentali per tutte le carriere IT. Attraverso una combinazione di lezioni, laboratori pratici e studio autonomo, imparerete come installare, gestire, configurare e verificare le reti IPv4 e IPv6. Il corso tratta la configurazione dei componenti di rete come switch, router e controller LAN wireless, la gestione dei dispositivi di rete e l'identificazione delle minacce di base alla sicurezza. Il corso fornisce anche le basi per la programmabilità della rete, l'automazione e il networking software-defined.

Questo corso aiuta a prepararsi a sostenere l'[esame 200-301 Cisco® Certified Network Associate \(CCNA®\)](#). Superando questo esame, si ottiene la **certificazione CCNA**.

Si prega di notare che questo corso è una combinazione di studio guidato dall'istruttore e studio autonomo - 5 giorni in classe e circa 3 giorni di studio autonomo.

I contenuti di autoapprendimento saranno forniti come parte del courseware digitale che riceverete all'inizio del corso e dovranno essere parte della vostra preparazione per l'esame.

L'accesso al laboratorio è previsto sia per le sezioni in classe che per quelle di autoapprendimento; l'accesso al laboratorio è valido per 60 ore o 90 giorni, a seconda di quale sia il termine più breve, quindi assicuratevi di uscire dalle esercitazioni di laboratorio quando non le utilizzate.

Contenuti del corso

Exploring the Functions of Networking

- What is a Computer Network?
- Common Usage of a Computer Network
- Components of a Network
- Characteristics of a Network

MAIN PARTNERS



formazione@pipeline.it
www.pipeline.it/formazione



- Physical vs. Logical Topologies
- Interpreting a Network Diagram
- Impact of User Applications on the Network

Introducing the Host-To-Host Communications Model

- Host-To-Host Communications Overview
- ISO OSI Reference Model
- TCP/IP Protocol Suite
- Peer-To-Peer Communications
- Encapsulation and De-Encapsulation
- TCP/IP Stack vs OSI Reference Model

Operating Cisco IOS Software

- Cisco IOS Software Features and Functions
- Cisco IOS Software CLI Functions
- Cisco IOS Software Modes

Introducing LANs

- Local Area Networks
- LAN Components
- Need for Switches
- Characteristics and Features of Switches

Exploring the TCP/IP Link Layer

- Ethernet LAN Connection Media
- Ethernet Frame Structure
- LAN Communication Types
- MAC Addresses
- Frame Switching
- Duplex Communication

Starting a Switch

- Switch Installation
- Connecting to a Console Port
- Switch Components
- Switch LED Indicators
- Basic show Commands and Information
- Implement the Initial Switch Configuration

MAIN PARTNERS





Introducing the TCP/IP Internet Layer, IPv4 Addressing, and Subnets

- Internet Protocol
- Decimal and Binary Number Systems
- Binary-to-Decimal Conversion
- Decimal-to-Binary Conversion
- IPv4 Address Representation
- IPv4 Header Fields
- IPv4 Address Classes
- Subnet Masks
- Subnets
- Implementing Subnetting: Borrowing Bits
- Implementing Subnetting: Determining the Addressing Scheme
- Benefits of VLSM and Implementing VLSM
- Private vs. Public IPv4 Addresses
- Reserved IPv4 Addresses
- Verifying IPv4 Address of a Host

Explaining the TCP/IP Transport Layer and Application Layer

- TCP/IP Transport Layer Functions
- Reliable vs. Best-Effort Transport
- TCP Characteristics
- UDP Characteristics
- TCP/IP Application Layer
- Introducing HTTP
- Domain Name System
- Explaining DHCP for IPv4

Exploring the Functions of Routing

- Role of a Router
- Router Components
- Router Functions
- Routing Table
- Path Determination
- Cisco Router Models
- Routing Hierarchy on Internet

Configuring a Cisco Router

- Initial Router Setup

MAIN PARTNERS





- Configuring Router Interfaces
- Configuring IPv4 Addresses on Router Interfaces
- Checking Interface Configuration and Status
- Exploring Connected Devices
- Using Cisco Discovery Protocol
- Configure and Verify LLDP
- Implement an Initial Router Configuration

Exploring the Packet Delivery Process

- Layer 2 Addressing
- Layer 3 Addressing
- Default Gateways
- Address Resolution Protocol
- Host-To-Host Packet Delivery

Troubleshooting a Simple Network

- Troubleshooting Methods
- Troubleshooting Tools
- Troubleshooting Common Switch Media Issues
- Troubleshooting Common Switch Port Issues
- Troubleshooting Common Problems Associated with IPv4 Addressing

Introducing Basic IPv6

- IPv4 Address Exhaustion Workarounds
- IPv6 Features
- IPv6 Addresses and Address Types
- Comparison of IPv4 and IPv6 Headers
- Internet Control Message Protocol Version 6
- Neighbor Discovery
- IPv6 Address Allocation
- Verification of End-To-End IPv6 Connectivity

Configuring Static Routing

- Routing Operation
- Static and Dynamic Routing Comparison
- When to Use Static Routing
- IPv4 Static Route Configuration
- Default Routes

MAIN PARTNERS





- Verifying Static and Default Route Configuration
- IPv6 Static Route Configuration
- Implement IPv4 Static Routing
- Implement IPv6 Static Routing

Implementing VLANs and Trunks

- VLAN Introduction
- Creating a VLAN
- Assigning a Port to a VLAN
- Trunking with 802.1Q
- Configuring an 802.1Q Trunk
- VLAN Design Considerations
- Troubleshoot VLANS and Trunks

Routing Between VLANs

- Purpose of Inter-VLAN Routing
- Options for Inter-VLAN Routing
- Implement Multiple VLANS and Basic Routing Between the VLANs

Introducing OSPF

- Dynamic Routing Protocols
- Path Selection
- Link-State Routing Protocol Overview
- Link-State Routing Protocol Data Structures
- Introducing OSPF
- Establishing OSPF Neighbor Adjacencies
- OSPF Neighbor States
- SPF Algorithm
- Building a Link-State Database
- Routing for IPv6

Building Redundant Switched Topologies

- Physical Redundancy in a LAN
- Issues in Redundant Topologies
- Spanning Tree Operation
- Types of Spanning Tree Protocols
- PortFast, BPDU Guard and BPDU Filter
- Rapid Spanning Tree Protocol

MAIN PARTNERS





- STP Loop Guard
- STP Root Guard

Improving Redundant Switched Topologies with EtherChannel

- EtherChannel Overview
- EtherChannel Configuration Options
- Configuring and Verifying EtherChannel
- Improve Redundant Switched Topologies with EtherChannel

Explaining the Basics of ACL

- ACL Overview
- ACL Operation
- ACL Wildcard Masking
- Wildcard Mask Abbreviations
- Types of Basic ACLs
- Configuring Standard IPv4 ACLs
- Configuring Extended IPv4 ACLs
- Verifying and Modifying IPv4 ACLs
- Applying IPv4 ACLs to Filter Network Traffic
- Implement Numbered and Named IPv4 ACLs

Enabling Internet Connectivity

- Introducing Network Address Translation
- NAT Terminology and Translation Mechanisms
- Benefits and Drawbacks of NAT
- Static NAT and Port Forwarding
- Dynamic NAT
- Port Address Translation
- Configuring and Verifying Inside IPv4 NAT
- Implement PAT

Introducing AI and ML in Network Operations

- Basics of AI and ML
- Advanced AI Concepts
- Retrieval-Augmented Generation
- Role of AI and ML in Network Operations

Introducing System Monitoring

MAIN PARTNERS





- Introducing Syslog
- Syslog Message Format
- SNMP Overview
- Enabling Network Time Protocol
- Configure System Message Logging

Managing Cisco Devices

- Cisco IOS Integrated File System and Devices
- Stages of the Router Power-On Boot Sequence
- Loading and Managing System Images Files
- Loading Cisco IOS Configuration Files
- Validating Cisco IOS Images Using MD5/SHA512
- Managing Cisco IOS Images and Device Configuration Files
- Cisco IOS WebUI

Securing Administrative Access

- Network Device Security Overview
- Securing Access to Privileged EXEC Mode
- Securing Console Access
- Securing Remote Access
- Configuring the Login Banner
- Limiting Remote Access with ACLs
- External Authentication Options
- Secure Device Administrative Access

Implementing Device Hardening

- Securing Unused Ports
- Infrastructure ACL
- Disabling Unused Services
- Port Security
- Mitigating VLAN Attacks
- Dynamic ARP Inspection
- Mitigating STP Attacks
- Implement Device Hardening

Exploring Layer 3 Redundancy (Self-Study)

- Need for Default Gateway Redundancy
- Understanding FHRP

MAIN PARTNERS





- Understanding HSRP

Introducing WAN Technologies (Self-Study)

- Introduction to WAN Technologies
- WAN Devices and Demarcation Point
- WAN Topology Options
- WAN Connectivity Options
- Virtual Private Networks
- Enterprise-Managed VPNs

Introducing QoS (Self-Study)

- Converged Networks
- QoS Defined
- QoS Policy
- QoS Mechanisms
- QoS Models
- Deploying End-to-End QoS

Explaining Wireless Fundamentals (Self-Study)

- Wireless Technologies
- Wireless Radio Communication
- WLAN Architectures
- WI-FI Channels
- AP and WLC Management

Introducing Architectures and Virtualization (Self-Study)

- Introduction to Network Design
- Enterprise Three-Tier Hierarchical Network Design
- Spine – Leaf Network Design
- Cisco Enterprise Architecture Model
- Underlay and Overlay Network Concepts
- Cloud Computing Overview
- Network Device Architecture
- Virtualization Fundamentals

Explaining Software-Defined Networking (Self-Study)

- Software-Defined Networking
- Traditional versus Software-Defined Networks

MAIN PARTNERS





- Software-Defined Network Layers
- Introducing Cisco Catalyst Center
- Cisco Catalyst Center Dashboard and Tools
- Introducing Cisco SD-Access
- Introducing Cisco Catalyst SD-WAN
- Introducing Cisco Meraki

Introducing Network Programmability (Self-Study)

- Traditional Network Management
- Network Automation and Programmability
- Network Automation Use Cases
- Model-Driven Programmability
- Data Encoding Formats
- JavaScript Object Notation
- Extensible Markup Language
- YAML Data Serialisation Standard
- Network Management Protocols
- Configuration Management Tools Overview
- Ansible
- Terraform

Examining the Security Threat Landscape (Self-Study)

- Security Threat Landscape Overview
- Malware
- Hacking Tools
- DoS and DDoS
- Spoofing
- Reflection and Amplification Attacks
- Social Engineering
- Evolution of Phishing
- Password Attacks
- Reconnaissance Attacks
- Buffer Overflow Attacks
- Man-in-the-Middle Attacks
- Vectors of Data Loss and Exfiltration
- Other Considerations

Implementing Threat Defense Technologies (Self-Study)

- Information Security Overview

MAIN PARTNERS





- Firewalls
- Intrusion Prevention Systems
- Protection Against Data Loss and Phishing Attacks
- Defending against DoS and DDoS Attacks
- Introduction to Cryptographic Technologies
- IPsec Security Services
- Secure Sockets Layer and Transport Layer Security
- Wireless Security Protocols

Labs:

- Discovery 1: Get Started with Cisco Command-Line Interface (CLI)
- Discovery 2: Observe How a Switch Operates
- Discovery 3: Perform Basic Switch Configuration
- FAST Lab 1: Implement the Initial Switch Configuration
- Discovery 4: Inspect TCP/IP Applications
- Discovery 5: Configure an Interface on a Cisco Router
- Discovery 6: Configure and Verify Layer 2 Discovery Protocols
- FAST Lab 2: Implement an Initial Router Configuration
- Discovery 7: Configure Default Gateway
- Discovery 8: Explore Packet Forwarding
- Discovery 9: Troubleshoot Switch Media and Port Issues
- Discovery 10: Troubleshoot Port Duplex Issues
- Discovery 11: Configure Basic IPv6 Connectivity
- Discovery 12: Configure and Verify IPv4 Static Routes
- Discovery 13: Configure IPv6 Static Routes
- FAST Lab 3: Implement IPv4 Static Routing
- FAST Lab 4: Implement IPv6 Static Routing
- Discovery 14: Configure VLANs and Trunk
- FAST Lab 5: Troubleshoot VLANs and Trunk
- Discovery 15: Configure Inter-VLAN Routing
- FAST Lab 6: Implement Multiple VLANs and Basic Routing Between the VLANs
- Discovery 16: Configure and Verify Single-Area OSPF
- Discovery 17: Configure and Verify EtherChannel
- FAST Lab 7: Improve Redundant Switched Topologies with EtherChannel
- Discovery 18: Configure and Verify IPv4 ACLs
- FAST Lab 8: Implement Numbered and Named IPv4 ACLs
- Discovery 19: Configure a Provider-Assigned IPv4 Address
- Discovery 20: Configure Static NAT
- Discovery 21: Configure Dynamic NAT and Port Address Translation (PAT)

MAIN PARTNERS





- FAST Lab 9: Implement PAT
- Discovery 22: Configure and Verify NTP
- FAST Lab 10: Configure System Message Logging
- Discovery 23: Create the Cisco IOS Image Backup
- Discovery 24: Upgrade Cisco IOS Image
- Discovery 25: Secure Console and Remote Access
- Discovery 26: Enable and Limit Remote Access Connectivity
- FAST Lab 11: Secure Device Administrative Access
- Discovery 27: Configure and Verify Port Security
- FAST Lab 12: Implement Device Hardening
- Discovery 28: Log into and Monitor the WLC
- Discovery 29: Configure an Open Wireless Network
- Discovery 30: Define a RADIUS Server and Enable SNMP and Syslog
- Discovery 31: Configure a WLAN to Use WPA2 PSK

Partecipanti

Il **corso NN-CCNA – Implementing and Administering Cisco Solutions** è progettato per chiunque cerchi la certificazione CCNA. Il corso fornisce anche conoscenze fondamentali per tutti i tecnici di supporto coinvolti nell'installazione di base, nel funzionamento e nella verifica delle reti Cisco.

I ruoli lavorativi più adatti al materiale di questo corso sono:

- ingegnere di rete di primo livello;
- amministratore di rete;
- tecnico di supporto di rete;
- tecnico dell'help desk.

Prerequisiti

Prima di partecipare al **corso NN-CCNA – Implementing and Administering Cisco Solutions** dovresti avere:

- conoscenza di base del computer;
- conoscenza di base del sistema operativo del PC;
- abilità di base nell'uso di Internet;
- conoscenza di base degli indirizzi IP.

Non ci sono prerequisiti formali per la certificazione CCNA, ma dovresti assicurarti di avere una buona comprensione degli argomenti dell'esame.

Obiettivi

Dopo aver completato questo corso sarai in grado di:

MAIN PARTNERS





- identificare i componenti di una rete di computer e descrivere le loro caratteristiche di base;
- comprendere il modello di comunicazione host-to-host;
- conoscere le caratteristiche e le funzioni del software Cisco Internetwork Operating System (IOS®);
- descrivere le LAN e il ruolo degli switch all'interno delle LAN;
- conoscere Ethernet come livello di accesso alla rete del TCP/IP e descrivere il funzionamento degli switch;
- installare uno switch ed eseguire la configurazione iniziale;
- descrivere il livello Internet del TCP/IP, IPv4, il suo schema di indirizzamento e il subnetting;
- descrivere il livello di trasporto TCP/IP e il livello di applicazione;
- esplorare le funzioni del routing;
- implementare la configurazione di base su un router Cisco;
- spiegare le comunicazioni host-to-host attraverso switch e router;
- identificare e risolvere i problemi comuni della rete commutata e i problemi comuni associati all'indirizzamento IPv4;
- descrivere le caratteristiche e gli indirizzi principali di IPv6 e configurare e verificare la connettività IPv6 di base;
- descrivere il funzionamento, i vantaggi e i limiti del routing statico;
- definire, implementare e verificare le reti locali virtuali (VLAN) e i trunk;
- descrivere l'applicazione e la configurazione del routing inter-VLAN;
- spiegare le basi dei protocolli di routing dinamico e descrivere i componenti e i termini di Open Shortest Path First (OSPF);
- spiegare come funzionano lo Spanning Tree Protocol (STP) e il Rapid Spanning Tree Protocol (RSTP);
- configurare l'aggregazione dei link usando EtherChannel;
- descrivere lo scopo dei protocolli di ridondanza di livello 3;
- definire i concetti di base di WAN e VPN;
- descrivere il funzionamento delle Access Control List (ACL) e le loro applicazioni nella rete;
- configurare l'accesso a Internet utilizzando i client DHCP (Dynamic Host Configuration Protocol) e spiegare e configurare il NAT (Network Address Translation) sui router Cisco;
- descrivere i concetti di base della qualità del servizio (QoS);
- descrivere i concetti delle reti wireless, quali tipi di reti wireless possono essere costruite e come utilizzare i Wireless LAN Controller (WLC);
- conoscere le architetture di rete e dei dispositivi e introdurre la virtualizzazione;
- introdurre il concetto di programmabilità della rete e di Software-Defined Networking (SDN) e descrivere le soluzioni di gestione della rete intelligente come Cisco DNA Center™, Software-Defined Access (SD-Access) e Software-Defined Wide Area Network (SD-WAN);
- configurare gli strumenti di base di monitoraggio del sistema IOS;
- descrivere la gestione dei dispositivi Cisco;
- conoscere l'attuale panorama delle minacce alla sicurezza;
- descrivere le tecnologie di difesa dalle minacce;
- implementare una configurazione di sicurezza di base del piano di gestione dei dispositivi;
- implementare le fasi di base per rendere più resistenti i dispositivi di rete.

MAIN PARTNERS





Hai bisogno di chiarimenti o ulteriori informazioni?

Vuoi organizzare un corso personalizzato?

Chiamaci: 02/6074791 Scrivici: formazione@pipeline.it

MAIN PARTNERS



formazione@pipeline.it
www.pipeline.it/formazione