Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • Cisco Certified Support Technician – Networking

Cisco Certified Support Technician – Networking

Formation préparant à la certification Cisco Certified Support Technician – Networking, couvrant les bases des réseaux, équipements, médias et protocoles, et constituant une porte d'entrée vers les certifications Cisco pour débutants et techniciens réseau.

Distributeur officiel Certiport | Centre d'examen Certiport | Learn • Practice • Certify

Durée 23 h (recommandé)	**Examen** CCST Networking
Modalité Distanciel	**Niveau** Fondation / Technicien réseau débutant

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

- **Learn** : Bases structurées des réseaux : modèles OSI/TCP-IP, adressage IPv4/IPv6, topologies, infrastructures et notions de sécurité.
- **Practice** : Exercices pratiques incluant topologies, diagnostic, commandes Cisco de base et capture de paquets.
- **Certify** : Préparation complète aux objectifs de l'examen Cisco Certified Support Technician – Networking et passage de la certification sur site.

OBJECTIFS PÉDAGOGIQUES

- La formation couvre les concepts de base des réseaux, modèles, trames, paquets et adressage.
- Elle présente les types de réseaux, topologies et équipements d'infrastructure.
- Les participants apprennent le diagnostic réseau de base et les notions essentielles de sécurité.

PUBLIC CIBLE

- La formation s'adresse aux étudiants en réseaux, télécoms ou filières IT et aux techniciens réseaux juniors.
- Elle convient également aux stagiaires, assistants, support technique et personnes en reconversion vers les métiers du réseau et de l'infrastructure.

PRÉREQUIS

- Base en usage de l'ordinateur (environnement Windows/macOS) et navigation Internet.
- Notions d'adressage IP et de fonctionnement général d'un réseau local (un plus).
- Motivation pour les métiers de la technique, du support réseau et de la cybersécurité.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Standards et concepts

Identifier les blocs de construction conceptuels fondamentaux des réseaux

- Modèle TCP/IP, modèle OSI, trames et paquets, adressage.

Différencier bande passante et débit (throughput)

- Latence, délai, tests de vitesse (speed test) vs outils comme Iperf.

Différencier LAN, WAN, MAN, CAN, PAN et WLAN

- Identifier et illustrer les topologies physiques et logiques courantes.

Comparer les applications et services cloud et on-premises

- Cloud public, privé, hybride, SaaS, PaaS, IaaS, télétravail et travail hybride.

Décrire les applications et protocoles réseaux courants

- TCP vs UDP (connexion orientée vs non orientée), FTP, SFTP, TFTP, HTTP, HTTPS, DHCP, DNS, ICMP, NTP.

Adressage et formats de sous-réseaux

Comparer les adresses privées et publiques

- Classes d'adresses, concepts de NAT.

Identifier les adresses IPv4 et formats de sous-réseau

- Concepts de sous-réseau, utilisation d'une calculatrice de sous-réseau, notation CIDR (slash), masque de sous-réseau, domaine de broadcast.

Identifier les adresses IPv6 et les formats de préfixe

- Types d'adresses IPv6, concepts de préfixe.

Terminaux et types de médias

Identifier les câbles et connecteurs utilisés dans les réseaux locaux

- Types de câbles : fibre, cuivre, paires torsadées (twisted pair).
- Types de connecteurs : coaxial, RJ-45, RJ-11, connecteurs fibre (LC, SC, etc.).

Différencier les technologies Wi-Fi, cellulaires et filaires

- Cuivre et sources d'interférences ; fibre ; sans fil (802.11, bandes 2,4 GHz, 5 GHz, 6 GHz non licenciées) ; réseaux cellulaires licenciés et leurs sources d'interférences.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Décrire les terminaux (endpoints)

- Objets connectés (IoT), ordinateurs, appareils mobiles, téléphones IP, imprimantes, serveurs.

Configurer et vérifier la connectivité réseau sur différents OS

- Utilitaires réseau sur Windows, Linux, macOS, Android et iOS ; exécution de commandes de dépannage ; paramètres clients Wi-Fi (SSID, authentification, modes WPA).

Infrastructure

Identifier les voyants d'état sur un équipement Cisco

- Couleur et état (clignotant ou fixe) des voyants de lien (Link).

Utiliser un schéma réseau pour raccorder les câbles appropriés

- Câbles de brassage (patch), commutateurs et routeurs, petites topologies, alimentation, organisation en baie.

Identifier les différents ports sur les équipements réseau

- Port console, port série.
- Ports fibre.
- Ports Ethernet, modules SFP.
- Ports USB, ports PoE.

Expliquer les concepts de routage de base

- Passerelle par défaut.
- Différences entre commutateurs de couche 2 et de couche 3.
- Réseau local vs réseau distant.

Expliquer les concepts de commutation de base

- Tables d'adresses MAC.
- Filtrage basé sur les adresses MAC.
- VLAN (Virtual LAN).

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Diagnostic des problèmes

Appliquer des méthodologies de dépannage et bonnes pratiques help desk

- Politiques et procédures.
- Documentation complète et précise.
- Priorisation des tickets et gestion des incidents.

Réaliser une capture de paquets avec Wireshark et sauvegarder le fichier

- Objectif d'un analyseur de paquets.
- Enregistrement et ouverture de fichiers .pcap.

Exécuter des commandes de diagnostic de base et interpréter les résultats

- ping, ipconfig/ifconfig/ip, tracert/traceroute,nslookup; reconnaître l'influence des pares-feux sur les résultats.

Différencier les moyens d'accéder aux équipements pour collecter des données

- Accès distant (RDP, SSH, Telnet).
- VPN.
- Émulateurs de terminal, port console.
- Outils de gestion de réseau (NMS), réseaux gérés dans le cloud (Meraki).
- Scripts et automatisation.

Lancer des commandes show de base sur un équipement Cisco

- show run, show cdp neighbors,show ip interface brief, show ip route,show version, show inventory, show switch,show mac address-table, show interface, show interface x,show interface status ; niveaux de privilèges, aide en ligne des commandes, auto-complétion.

Sécurité

Décrire le fonctionnement des pares-feux pour filtrer le trafic

- Pare-feux filtrant ports et protocoles.
- Règles permettant ou refusant l'accès.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Décrire les concepts de sécurité fondamentaux

- Confidentialité, intégrité, disponibilité (CIA).
- Authentification, autorisation, audit (AAA).
- Authentification multifacteur (MFA).
- Chiffrement, certificats, complexité des mots de passe.
- Référentiels d'identité (Active Directory).
- Menaces et vulnérabilités.
- Spam, phishing, malware, attaques par déni de service.

Configurer la sécurité Wi-Fi de base sur un routeur domestique (WPAx)

- WPA, WPA2, WPA3.
- Choix entre modes Personal et Enterprise.
- Concepts de sécurité sans fil.