

Implémentation et administration des solutions Cisco (CCNA 200-301)

Date et durée
Code formation : CCNA Durée : 5 jours Nombre d'heures : 35 heures
Formation avec certification
CCNA (Cisco Certified Network Associate)
Description
Cette formation Cisco CCNA constitue une base de connaissances pour tous les techniciens informatiques qui sont amenés à utiliser les solutions Cisco. Grâce à des cours théoriques et des exercices pratiques, vous saurez comment installer, gérer, configurer et vérifier les paramètres IPv4 et IPv6 de base d'un réseau. En outre, les cours incluent la configuration des composants réseau CISCO comme les commutateurs, les routeurs, les contrôleurs de réseaux locaux sans fil, etc. Enfin, cette formation vous permet d'acquérir des connaissances sur la programmation des réseaux, l'automatisation et les réseaux SDN. Le programme de cette formation a pour objectif de vous préparer au passage de l'examen 200-301 Cisco. La réussite de celui-ci vous permettra d'obtenir le titre de Certified Network Associate (CCNA).
Objectifs
En suivant la formation CISCO CCNA, vous validerez les objectifs de compétence suivants : • identifier les différents composants d'un réseau et leurs fonctions. • découvrir et identifier des solutions possibles à mettre en œuvre sur un réseau local (LAN). • définir des méthodes d'interconnexion de réseaux à l'aide des routeurs CISCO. • configurer un routeur Cisco à l'aide de l'interface de commande en ligne (IOS). • étendre un réseau en utilisant plusieurs commutateurs avec support VLAN, trunking et spanning-tree. • comprendre les principes du routage et mettre en place un système de routage efficace sur un réseau. • être bien préparé pour l'examen 200-301 et obtenir la certification CISCO CCNA.
Points forts
Un formateur expert et certifié Cisco, des support de cours officiel avec des labs et une préparation à l'examen CCNA 200-301.
Certification
Cette formation vous prépare au passage de l'examen Cisco CCNA 200-301. Vous pouvez passer cet examen en ligne. Vous recevrez un voucher à l'issue de la formation, vous permettant de programmer votre examen à la date et heure de votre choix. Il teste vos connaissances et compétences sur les 6 domaines suivants : • les fondamentaux du réseau ;

- l'accès au réseau ;
- la connectivité IP ;
- les services IP ;
- les fondamentaux de la sécurité ;
- l'automatisation et la programmation.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Cisco CCNA** nécessite les prérequis suivants :

- des compétences de base en informatique, notamment en matière d'administration de systèmes d'exploitation ;
- des connaissances générales sur l'adressage IP.

Public

Cette formation s'adresse aux publics suivants :

- toute personne souhaitant obtenir ou maintenir sa qualification de Certified Network Associate (CCNA®) ;
- les techniciens de support chargés de l'installation, de l'exploitation et des tests de base des réseaux Cisco.

Cette formation s'adresse aux profils suivants

Administrateur réseaux - télécoms

Ingénieur réseaux - télécoms

Technicien Support / HelpDesk

Programme

Tour de table

- Introduction individuelle
- Exploration des attentes et des objectifs de chaque participant
- Introduction au cadre de la formation
- Alignement avec les objectifs et enjeux spécifiques
- Identification des attentes et des perspectives individuelles des participants

Domaine 1 : les fondamentaux du réseau

- Identification des composants d'un réseau informatique d'entreprise et de leurs fonctionnalités de base.
- Description des caractéristiques sur les architectures topologiques des réseaux.
- Identification des problèmes d'interface et de câble (collisions, erreurs, incompatibilité de duplex ou de vitesse).
- Comparaison entre TCP et UDP.
- Configuration et validation de l'adressage IPv4 et des sous-réseaux.
- Explication sur la pertinence d'un adressage IPv4 privé.
- Configuration et validation de l'adressage et du préfixage IPv6.

- Présentation des différents types d'adresses IPv6.
- Vérification des paramètres IP des systèmes d'exploitation clients (Windows, Mac OS, Linux).
- Explication à propos des principes des réseaux sans fil.
- Explication sur les principes de base de la virtualisation (virtualisation des serveurs, des conteneurs et des réseaux).
- Explication sur les concepts de commutation.

Domaine 2 : l'accès au réseau

- Configuration et validation des réseaux locaux virtuels (VLAN) sur plusieurs commutateurs.
- Configuration et validation de la connectivité entre les commutateurs.
- Configuration et validation des protocoles de découverte de la couche 2 (Cisco Discovery Protocol et LLDP).
- Configuration de Cisco Etherchannel (couche 2 et 3).
- Explication sur la nécessité du protocole Rapid PVST+ Spanning Tree et de son fonctionnement de base.
- Comparaison des architectures sans fil et des modes AP de Cisco.
- Description des connexions de l'infrastructure physique des composants WLAN (AP, WLC, ports d'accès/trunk et LAG).
- Description des connexions d'accès à la gestion des AP et WLC (Telnet, SSH, HTTP, HTTPS, console et TACACS+/RADIUS).
- Configuration des composants d'accès au réseau local sans fil pour la connectivité client avec l'interface graphique Cisco IOS (création d'un réseau local sans fil, paramètres de sécurité, profils de qualité de service et paramètres avancés).

Domaine 3 : la connectivité IP

- Interprétation des éléments de la table de routage.
- Compréhension du mode de décision de transfert par défaut d'un routeur.
- Configuration et contrôle du routage statique IPv4 et IPv6.
- Configuration et contrôle de l'OSPFv2 à zone unique.
- Compréhension du rôle, des fonctions et des concepts des protocoles de redondance de premier niveau.

Domaine 4 : les services IP

- Configuration et vérification du NAT source interne via des réseaux statiques et des pools.
- Configuration et vérification du fonctionnement de NTP en mode client et serveur.
- Explication sur le rôle du DHCP et du DNS au sein du réseau.
- Explication de la fonction du protocole SNMP dans l'exploitation du réseau.
- L'utilisation des fonctions syslog, incluant les facilités et les niveaux.
- Configuration et validation du client et du relais DHCP.
- Explication du principe de transfert de saut (PHB) pour la qualité de service, comme la classification, le marquage, la mise en file d'attente, l'encombrement, le maintien de l'ordre et la mise en forme.
- Configuration des périphériques réseau pour l'accès à distance à l'aide de SSH.
- Présentation des possibilités et de la fonction TFTP/FTP dans le réseau.

Domaine 4 : les fondamentaux de la sécurité

- Présentation des concepts fondamentaux de la sécurité (menaces, vulnérabilités, exploits et techniques d'atténuation).
- Description des étapes du programme de sécurité (sensibilisation des utilisateurs, formation et contrôle de l'accès physique).
- Configuration et validation du contrôle d'accès aux appareils en utilisant des mots de passe locaux.
- Description des éléments d'une politique de sécurité des mots de passe, tels que la gestion, la complexité et les alternatives aux mots de passe (authentification multifactorielle, certificats et biométrie).
- Explication sur les accès à distance IPsec et les VPN de site à site.

- Configuration et contrôle des listes de contrôle d'accès.
- Configuration des fonctions de sécurité de la couche 2 (surveillance DHCP, inspection ARP dynamique et sécurité des ports).
- Comparaison entre les concepts d'authentification, d'autorisation et de comptabilité.
- Présentation des protocoles de sécurité sans fil (WPA, WPA2 et WPA3).
- Configuration du WLAN avec WPA2 PSK à l'aide de l'interface graphique CISCO IOS.

Domaine 5 : l'automatisation et la programmation

- Explication sur les impacts de l'automatisation sur la gestion des réseaux.
- Comparaison sur les réseaux traditionnels et les réseaux à base de contrôleurs.
- Comparaison avec les architectures basées sur des contrôleurs et les architectures définies par logiciel (superposition, sous-couche et tissu).
- Comparaison entre la gestion traditionnelle des périphériques de campus et la gestion des périphériques basée sur le DNA Center de Cisco.
- Description des spécificités des API basées sur REST (CRUD, verbes HTTP et encodage des données).
- Identification des possibilités de gestion de la configuration des mécanismes Puppet, Chef et Ansible
- Interprétation des données codées en JSON.



Guide de certification
Cisco CCNA 200-301
[Télécharger la brochure](#)

Cisco est une marque déposée de Cisco Systems, Inc. aux Etats-Unis et dans d'autres pays.