

Cycle certifiant Administrateur Réseaux certificat professionnel FFP



SII-181 13 Jours (91 Heures)

Description

Ce cycle vous apportera toutes les connaissances nécessaires à la compréhension, l'installation et l'administration des réseaux d'entreprise. Vous apprendrez le fonctionnement et la mise en oeuvre des principaux protocoles réseaux tels que TCP/IP, DNS, HTTP, ainsi que des différents équipements d'interconnexion comme les commutateurs et les routeurs. Un module entièrement dédié à la sécurité des systèmes et des réseaux complètera ce cycle de formation.

À qui s'adresse cette formation ?

Pour qui

Techniciens informatiques.

Prérequis

Aucune

Les objectifs de la formation

Programme de la formation

Principes généraux et différents réseaux

- Un réseau pour quoi faire ? Les différents éléments et leur rôle.
- Classification des différents types de réseaux.
- Avantages et inconvénients des différentes technologies.
- Quelles technologies pour quels besoins ? Introduction au modèle client/serveur.
- Partager les ressources.
- Nature et objet d'un protocole.
- Le modèle ISO/OSI : quel intérêt ? Les sept couches.

Alternatives de raccordement et réseaux locaux (LAN)

- La paire torsadée, coaxial et fibre optique.
- Principe et règle de câblage.
- Le sans-fil.
- Pourquoi et quand utiliser un réseau local ? Le type d'adressage du standard Ethernet.
- Contraintes, avantages et mode de fonctionnement d'Ethernet (CSMA/CD).
- Plusieurs débits de 10 Mo à plusieurs Go (10/100 base T/Gigabit Ethernet/).
- Les réseaux locaux sans fil (802.11x).
- Les différents équipements, leurs rôles et leurs avantages respectifs.
- Travaux pratiques Création d'un réseau local avec des switchs et des stations de travail.
- Installation d'un analyseur réseau.
- Configuration des adresses paramètres IP sur les stations de travail.
- Identifier et travailler avec les adresses MAC, les requêtes ARP et la table ARP.
- Tests de connexion entre les stations.

TCP/IP et les protocoles de haut niveau

- Les contraintes d'adressage des réseaux.
- Le protocole IP.
- Le plan d'adressage.
- Le Broadcast et le Multicast.
- Les protocoles TCP et UDP.
- Notion de numéro de port.
- Le service de nom DNS.
- Rôle et intérêt.
- Les principes de fonctionnement.
- La notion de domaine.
- Le serveur DHCP.
- Les principes de base.
- Savoir attribuer des adresses IP dynamiquement.
- Les autres services rendus par DHCP.
- Les protocoles de messagerie SMTP, POP3, IMAP4.
- Le HTTP, HTTPS, FTP, TELNET et SSH.
- Travaux pratiques Exemple d'utilisation de FTP entre les postes de travail et le serveur FTP (prise de trace et analyse des trames et paquets).
- Connexion en telnet sur les routeurs (prise de trace et analyse des trames et paquets).
- Intégration des postes de travail en tant que client DNS et DHCP.

Routeurs Cisco, mise en oeuvre sur IP

- L'architecture d'un routeur Cisco.
- Installation et configuration.
- Configuration des commutateurs Cisco.
- Configurer le routage IP.
- Les protocoles de routage.
- Routage à vecteurs de distance RIP v1 et v2.
- EIGRP.
- Principes de fonctionnement.
- Traitement des boucles.
- Les protocoles de routage OSPF.
- Base de données et topologie.
- Les états de liens.
- La convergence.
- Topologie, tables, boucles, routes, routage politique.
- Routage multicast.
- Configurer un routeur pour les réseaux WAN.
- La translation d'adresses.
- Les adresses publiques et les adresses privées.
- Les accès pour une application donnée.
- Les Access-List étendues.
- Travaux pratiques Raccordement physique des routeurs.
- Configuration des adresses IP sur les routeurs.
- Identifier et travailler avec les adresses MAC, les requêtes ARP et la table ARP des routeurs.
- Analyser la table de routage.
- Tests de connexion entre stations et routeurs.
- Configuration d'une table de translation.

Le routeur Cisco au quotidien

- Comment récupérer le mot de passe.
- Les états du registre de configuration.
- Télécharger une nouvelle version de pack logiciel.
- Sauvegarder via TFTP.
- Téléchargement d'une nouvelle configuration.
- La supervision du routeur.
- La vérification sur logiciel.
- La gestion des modifications et de la configuration.
- La sécurité.
- Les adresses publiques et les adresses privées.
- Les techniques de maintenance.
- Reconnaître et réparer des composants matériels défectueux.
- Maintenance matérielle.
- Tests des interfaces.
- Maintenance logicielle.
- Debugging.
- Travaux pratiques Sauvegarde et réinstallation de configuration et IOS via le réseau.
- Récupération après perte d'IOS en Flash.
- Récupération et remplacement de mot de passe.

Risques et menaces, architectures de sécurité

- Introduction à la sécurité.
- Les attaques "couches basses" et les attaques applicatives.
- Quelles architectures pour quels besoins ? Firewall : pierre angulaire de la sécurité.
- Proxy serveur et relais applicatif.
- Sécurité des données et des échanges.
- Sécuriser un système, le "Hardening".
- Audit et sécurité au quotidien.
- Travaux pratiques Installation et utilisation de Wireshark.
- Mise en oeuvre d'une attaque applicative.
- Installation d'un proxy Cache/Authentification.
- Déploiement d'un relais SMTP et d'un proxy HTTP/FTP Antivirus.
- Réalisation d'une attaque Man in the Middle sur une session SSL.
- Mise en oeuvre d'IPSec.