

▶▶▶ **TECHNICIEN D'ASSISTANCE INFORMATIQUE – BC02 – RNCP-37681**

Objectifs pédagogiques

Cette Formation est composée de :

- **La formation Administration Réseau :**
- **La formation Cybersécurité :**

Vous apprendrez les fondamentaux de l'administration d'un réseau : routeur, adressage d'IP et virtualisation, gestion des protocoles, architecture des différents réseaux, les fondamentaux d'HTTP, les modèles réseaux et les notions liées à la Cybersécurité.

Temps moyen de formation

68 heures

Système d'évaluation

OUI

Pré requis technique

- Navigateur web : Edge, Chrome, Firefox, Safari
- Système d'exploitation : Mac ou PC

Technologie

- HTML5
- Norme SCORM

Administration Réseau

Objectifs pédagogiques

Avec cette formation **Administration Réseau** de **28 modules**, vous apprendrez les fondamentaux de l'administration d'un réseau : routeur, adressage d'IP et virtualisation, gestion des protocoles, architecture des différents réseaux.

Temps moyen de formation

42 heures

Système d'évaluation

OUI

Niveau de granularisation

28 Modules soit 165 chapitres

Pré requis technique

- Navigateur web : Edge, Chrome, Firefox, Safari
- Système d'exploitation : Mac ou PC

Technologie

- HTML5
- Norme SCORM

ONLINE Les fondamentaux du réseau 1/2

Chapitres

- 1 Réseau Informatique
- 2 Protocoles réseaux
- 3 Recherche des et protocole TCP/IP
- 4 Communication Point à Point
- 5 Réseaux des bases du réseau

Réseau Informatique

Qu'est-ce qu'un réseau informatique ?

Le mot **réseau** est un mot assez familier qui peut se retrouver dans différents contextes.

Par exemple, on a :

- des réseaux informatiques
- des réseaux de télécommunication
- des réseaux sociaux, que tout le monde connaît de nos jours

ONLINE

Les adresses IPv6 sont représentées sous la forme d'une série de...

Choisissez la bonne réponse.

- 4 champs hexadécimaux de 16 bits séparés par deux points
- 8 champs hexadécimaux de 16 bits séparés par deux points
- 16 champs hexadécimaux de 16 bits séparés par deux points

VALIDER

QUESTION 15/48

ONLINE Adressage IPv4 1/2

Chapitres

- 1 Adresse et en 16bits IPv4
- 2 Système décimal et binaire
- 3 8M Bits et Octet
- 4 Classes d'adressage IP
- 5 Les adresses IPv4 classées
- 6 Masque de sous-réseau

Masque de sous-réseau

Classe	Bits de réseau	Classe	Bits	Classe	Bits	Classe	Bits
A	8	B	16	C	24	D	32

Vous ne pouvez créer aucune partie des sous-réseaux ou vous devez utiliser avec une adresse IP de classe C.

Classe	Bits de départ	Début	Fin	CIDR	Masque s. sous-réseau
A	8	0	255	8	255.0.0.0
B	16	0	255	16	255.255.0.0
C	24	0	255	24	255.255.255.0

ONLINE Sécurité 1/2

Chapitres

- 1 Différents types de logiciels
- 2 Les attaques d'usurpation d'identité
- 3 Les autres types d'attaques
- 4 Vulnérabilités par mots de passe
- 5 Sécurité AAA, SERVICES DE TRAJETS
- 6 Sécurité de FQDN Classé
- 7 Sécurité FQDN Classé

Vulnérabilités par mots de passe

Le plaisir des systèmes d'un réseau d'entreprise est un type d'authentification pour accéder ou refuser l'accès des utilisateurs.

Lorsque les utilisateurs accèdent à un système, on leur demande généralement un nom d'utilisateur et un mot de passe.

►►► **Détail formation : Administration Réseau**

Les fondamentaux du réseau 1/2

- Réseau informatique
- Topologies réseaux
- Couche Osi et protocole TCP IP
- Communication Peer to Peer
- Résumons les bases du réseau

Les fondamentaux du réseau 2/2

- LAN
- Médias de connexion LAN/Ethernet
- Trame Ethernet
- Pour résumer : Média Ethernet
- TCP et UDP
- Couche Réseau
- ARP (Address Resolution Protocol)
- Couche de transport TCP/IP
- TCP versus UDP

Switch et IOS Cisco

- Les bases de l'IOS Cisco
- Logiciel IOS et fonction CLI
- Commande IOS Cisco de base
- Configuration IOS
- Hubs, ponts et commutateurs
- Commutateur et communication duplex
- Démarrage d'un switch
- Full-duplex et half-duplex
- Dépanner un switch

Routeur et routage 1/2

- Composants d'un routeur
- Différence switch et routeur
- Fonctionnement du routeur
- Protocole de routage dynamique
- Configuration de base du routeur
- Commandes de types show

Routeur et routage 2/2

- ARP et Gateway
- Livraison d'un paquet IP
- Dépannage des problèmes courants
- Vecteur de distances et état de lien
- Résumé du routeur et du routage

Virtual LAN et Trunk 1/2

- VLAN (Virtual LAN)
- TRUNKING (802.1Q)
- Routage Inter-VLAN
- Introduction VLAN
- VLAN-Mode ACCESS et TRUNK

Virtual LAN et Trunk 2/2

- Router On A Stick et DTP VLAN
- Introduction VTP
- DTP et VTP
- Configuration VTP
- Danger VTP

Spanning Tree Protocol (STP)

- La solution STP
- Introduction au Spanning Tree
- Spanning Tree par VLAN
- Élection STP
- Analyse du Spanning Tree
- Coût et priorité du port
- VLAN multiple
- PortFast et BPDU Guard

EtherChannel

- Les bases de l'EtherChannel
- Introduction EtherChannel
- Configuration EtherChannel

Adressage IPv4 1/2

- Adresse et en-tête IPv4
- Système décimal et binaire
- Bit Byte et Octet
- Classes d'adresses IP
- Les adresses IPv4 réservées
- Masque de sous-réseau

Adressage IPv4 2/2

- DNS et IP privées/publiques
- Subnetting binaire
- Subnetting décimal
- Calcul binaire et méthode magique
- Bits de sous-réseau
- VLSM

Access List (ACL)

- Fonctionnement ACL
- Wildcard Mask
- Configuration ACL standard
- Configuration ACL étendue

Services IP 1/2

- DHCP
- Configuration DHCP et DNS
- CDP et SNMP

Services IP 2/2

- QoS
- Les principes de la QoS
- Les outils de la QoS
- Supervision
- CDP et LLDP
- Services non utilisés et NTP

Network Address Translation (NAT)

- Adresses publiques et privées
- Les 3 types de NAT
- Dépannage NAT
- Résumé NAT et PAT

Protocoles FHRP et HSRP

- FHRP HSRP redondance Gateway
- Load balancing HSRP
- Différence HSRP VRRP et GLBP

Routage statique

- Opération de routage
- Protocole de routage Classfull et Classless
- Configuration d'une route statique
- Route statique par défaut
- RIP protocole de routage à vecteur de distance
- Configuration RIP : Routing Information Protocol

Protocole Open Shortest Path First (OSPF)

- Introduction OSPF
- Paquet Hello OSPF
- Métrique et en-tête
- Zone OSPF
- Dépannage OSPFv2 et OSPFv3
- Résumé OSPF

Wifi 1/2

- Comparaison des réseaux câblés et sans fil
- Les différentes topologies LAN sans fil
- Les autres topologies sans fil
- Radio fréquence
- Bandes et canaux sans fil
- AP autonome et Cloud
- AP autonome versus AP léger

Wifi 2/2

- Contrôleur WAN et mode AP
- Sécurisation des réseaux sans fil
- Méthodes d'authentification
- Méthodes sans fil de cryptage
- Construire un LAN sans fil
- Configurer un LAN sans fil

Gestion IP et dépannage 1/2

- Composants internes du routeur
- Image IOS et fichier de configuration
- IFS Gestion des IOS
- Sauvegarde et upgrade IOS
- Running-config et startup-config
- Mémoire et password recovery

Gestion IP et dépannage 2/2

- Licences IOS Cisco et configuration
- Guide de dépannage
- SPAN sniffer de trafic
- Syslog
- IP SLA ping traceroute telnet

Sécurité 1/2

- Qu'est-ce que la sécurité
- Les attaques d'usurpation d'identité
- Les autres types d'attaques
- Vulnérabilités par mots de passe
- Serveur AAA_RADIUS et TACACS
- Sécurité de l'IOS Cisco
- Sécuriser l'IOS Cisco

Sécurité 2/2

- Telnet et SSH
- Configuration SSH
- Firewall et IPS
- Port Security - Fonctionnement
- Port Security - Configuration
- DHCP Snooping
- DAI : Dynamic ARP Inspection

Adressage IPv6

- Différences IPv4 et IPv6
- Types d'adresse et préfixe IPv6
- Type d'adresse IPv6 et EUI-64
- Méthode EUI-64
- En-tête IPv6, ICMPv6 et NDP
- NDP SLAAC et DHCPv6
- Routage statique IPv6
- Route statique OSPFv3 et EIGRPv6

Architecture réseau LAN WAN Cloud 1/2

- Couche d'accès, distribution et core
- LAN SOHO
- POE : Power Over Ethernet
- Metro Ethernet
- WAN
- HDLC

Routage statique

- VPN MPLS
- Résumé : WAN et VPN
- PPPoE Tunnel GRE et EBGP
- Virtualisation
- Cloud Computing
- Cloud / WAN / VNF

Automation réseau

- NetFlow, StackWise, Cloud et SDN
- SDN (Software Defined Networking) - 1
- SDN (Software Defined Networking) - 2
- SD-Access et DNA Center
- API (Application Program Interface)
- Données et variables
- XML, JSON et YAML
- Puppet, Chef et Ansible

Cybersécurité

Objectifs pédagogiques

Cette formation **Cybersécurité** vous permettra, en **125 modules**, de vous sensibiliser et vous initier à la cybersécurité ; quel que soit votre niveau, apprenez et assimilez des notions de base de la SSI utiles au travail comme à la maison.

Temps moyen de formation

26 heures

Système d'évaluation

Oui

Niveau de granularisation

- 125 modules répartis en 4 domaines de 5 unités chacun

Pré requis technique

- Navigateur web : Edge, Chrome, Firefox, Safari
- Système d'exploitation : Mac ou PC, smartphone

Technologie

- HTML5
- Norme SCORM



▶▶▶ **Détail formation : CyberSécurité**

PANORAMA DE LA SSI

Unité 1 - Un monde numérique hyper-connecté

- Une diversité d'équipements et de technologies
- Le cyberspace, nouvel espace de vie
- Un espace de non-droits ?

Unité 2 - Un monde à hauts risques

- Qui me menace et comment ?
- Les attaques de masse
- Les attaques ciblées
- Les différents types de menaces
- Plusieurs sources de motivation
- Les conséquences pour les victimes de cyberattaques
- Conclusion

Unité 3 - Les acteurs de la cybersécurité

- Le livre blanc pour la défense et la sécurité nationale
- La stratégie nationale pour la sécurité du numérique
- L'ANSSI
- Autres acteurs de la cybersécurité
- D'autres experts pour m'aider
- Conclusion

Unité 4 - Protéger le cyberspace

- Les règles d'or de la sécurité
- Choisir ses mots de passe
- Mettre à jour régulièrement ses logiciels
- Bien connaître ses utilisateurs et ses prestataires
- Effectuer des sauvegardes régulières
- Sécuriser l'accès Wi-fi de son entreprise ou son domicile
- Être prudent avec son smartphone ou sa tablette
- Protéger ses données lors de ses déplacements
- Être prudent lors de l'utilisation de sa messagerie
- Télécharger ses programmes sur les sites officiels des éditeurs
- Être vigilant lors d'un paiement sur Internet
- Séparer les usages personnels et professionnels
- Prendre soin de ses informations et de son identité numérique
- Conclusion

Unité 5 - Mon rôle dans la sécurité numérique

- Introduction
- Les données
- Risques sur les données
- Protéger les données
- Responsabilités face aux risques

SÉCURITÉ DE L'AUTHENTIFICATION

Unité 1 - Principes de l'authentification

- Introduction
- Objectif de l'authentification
- Facteurs d'authentification
- Les types d'authentification
- Limites des facteurs d'authentification
- Les risques liés aux mots de passe

Unité 2 - Attaques sur les mots de passe

- Introduction
- Les attaques directes
- Les attaques indirectes
- Conclusion

Unité 3 - Sécuriser ses mots de passe

- Introduction
- Un bon mot de passe
- Comment mémoriser un mot de passe fort ?
- Comment éviter la divulgation de mot de passe ?
- Conclusion

Unité 4 - Gérer ses mots de passe

- Introduction
- Gérer la multiplication des mots de passe
- Configurer les logiciels manipulant les mots de passe
- Transmettre des mots de passe sur le réseau
- Conclusion

Unité 5 - Notions de cryptographie

- Introduction
- Principe général
- Chiffrement symétrique
- Chiffrement asymétrique
- Signature électronique, certificats et IGC
- Conclusion

►►► **Détail formation : CyberSécurité**

SÉCURITÉ SUR INTERNET

Unité 1 - Internet : de quoi s'agit-il ?

- Introduction
- Internet schématisé
- Cyber-malveillance
- Ingénierie sociale
- Contre-mesures possibles
- En cas d'incident
- Réseaux sociaux
- Conclusion

Unité 2 - Les fichiers en provenance d'Internet

- Introduction
- Les formats et les extensions d'un fichier
- Y a-t-il des formats plus risqués que d'autres ?
- Y a-t-il des sources plus sûres que d'autres ?
- J'ai déjà eu recours à une pratique déconseillée sans aucun problème
- Se protéger des rançongiciels
- Conclusion

Unité 3 - La navigation Web

- Introduction
- Comment fonctionne concrètement un navigateur ?
- Vous avez dit "typosquatting" ?
- Le moteur de recherche, la porte d'entrée du web
- Et les "cookies" alors ?
- Le navigateur bienveillant pour la santé de votre ordinateur
- Le contrôle parental
- Conclusion

Unité 4 - La messagerie électronique

- Introduction
- Présentation
- Panorama des menaces
- Bonnes pratiques de messagerie
- Les clients de messagerie
- Les messageries instantanées
- Cas particuliers

Unité 5 - L'envers du décor d'une connexion Web

- Introduction
- Fonctionnement basique d'une connexion web
- Utilisation d'un serveur mandataire
- HTTPS et les certificats
- Conclusion

SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME

Unité 1 - Applications et mises à jour

- Introduction
- Concept de vulnérabilité en sécurité informatique
- Mise à jour
- Installation d'applications

Unité 2 - Options de configuration de base

- Premier démarrage
- Déverrouillage et authentification
- Logiciels de sécurité
- Recommandations spécifiques aux terminaux mobiles
- Données spécifiques aux terminaux mobiles
- Chiffrement de l'appareil
- Conclusion

Unité 3 - Configurations complémentaires

- Introduction
- Gestion de base des comptes utilisateurs
- Gestion avancée des comptes utilisateurs
- Sauvegarde et connexion de l'appareil
- Conclusion

Unité 4 - Sécurité des périphériques amovibles

- Introduction
- Risques au branchement
- Chiffrement des périphériques de stockage amovible
- Durabilité
- Séparation des usages
- Effacement sécurisé
- Conclusion

Unité 5 - Séparation des usages

- Introduction
- Qu'est-ce que le mélange des usages ?
- Le danger du mélange des usages
- Étude de cas
- Bonnes pratiques
- Conclusion