BTS CIEL

16 Fiches de Révision

BTS CIEL

Étude et conception de réseaux informatiques

- Fiches de révision
- Fiches méthodologiques
- Tableaux et graphiques
- Retours et conseils

Conforme au Programme Officiel

Garantie Diplômé(e) ou Remboursé

4,6/5 selon l'Avis des Étudiants

www.coursbtsciel.fr

Préambule

1. Le mot du formateur :

Hello, moi c'est **Pierre Leclerc** 👏

D'abord, je tiens à te remercier de m'avoir fait confiance et d'avoir choisi www.coursbtsciel.fr.

Si tu lis ces quelques lignes, saches que tu as déjà fait le choix de la **réussite**.

Dans cet E-Book, tu découvriras comment j'ai obtenu mon **BTS Cybersécurité, informatique et réseaux, électronique (CIEL)** avec une moyenne de **16.49/20** grâce à ces **fiches de révisions**.

2. Pour aller beaucoup plus loin :

Si tu lis ces quelques lignes, c'est que tu as déjà fait le choix de la réussite, félicitations à toi.

En effet, tu as probablement déjà pu accéder aux 62 Fiches de Révision et nous t'en remercions.

Vous avez été très nombreux à nous demander de créer une **formation 100% vidéo** axée sur l'apprentissage de manière efficace de toutes les informations et notions à connaître.

Chose promise, chose due : Nous avons créé cette formation unique composée de **5 modules ultra-complets** afin de vous aider, à la fois dans vos révisions en BTS CIEL, mais également pour toute la vie.

En effet, dans cette formation vidéo de **plus d'1h20 de contenu ultra-ciblé**, nous abordons différentes notions sur l'apprentissage de manière très efficace. Oubliez les "séances de révision" de 8h d'affilés qui ne fonctionnent pas, adoptez plutôt des vraies techniques d'apprentissages **totalement prouvées par la neuroscience**.

3. Contenu de la formation vidéo :

Cette formation est divisée en 5 modules :

1. **Module 1 - Principes de base de l'apprentissage (21 min) :** Une introduction globale sur l'apprentissage.

2. **Module 2 - Stéréotypes mensongers et mythes concernant l'apprentissage (12 min) :** Pour démystifier ce qui est vrai du faux.

3. **Module 3 - Piliers nécessaires pour optimiser le processus de l'apprentissage (12 min) :** Pour acquérir les fondations nécessaires au changement.

4. **Module 4 - Point de vue de la neuroscience (18 min) :** Pour comprendre et appliquer la neuroscience à sa guise.

5. **Module 5 - Différentes techniques d'apprentissage avancées (17 min) :** Pour avoir un plan d'action complet étape par étape.

6. **Bonus - Conseils personnalisés, retours d'expérience et recommandation de livres :** Pour obtenir tous nos conseils pour apprendre mieux et plus efficacement.

Découvrir Apprentissage Efficace

E4 : Étude et conception de réseaux informatiques

Présentation de l'épreuve :
L'épreuve E4 « Épreuve professionnelle » est une épreuve variant en fonction de l'option du BTS CIEL choisie, à savoir :

- **Option A « Informatique et réseaux » :** Épreuve E4 « Étude et conception de réseaux informatiques » ;
- **Option B « Électronique et réseaux » :** Épreuve E4 « Étude et conception de produits électroniques ».

Peu importe l'option choisie, l'épreuve E4 se déroule sous forme ponctuelle écrite au travers d'un examen de 6 heures et dispose d'un coefficient de 4, ce qui représente 19 % de la note finale, d'où son importance.

De plus, il s'agit d'une épreuve « pilier » : L'ensemble des notions évoquées au travers de celle-ci seront réutilisées pour la réussite des autres épreuves.

Conseil :
L'épreuve E4 « Épreuve professionnelle » est une épreuve cruciale pour réussir le BTS CIEL. En effet, elle compte pour près du cinquième de la note finale, ce qui signifie que ces points peuvent être déterminants pour l'obtention du diplôme. Il est donc essentiel de ne pas la négliger et de disposer des bonnes clés pour réussir avec facilité.

Pour la réussir, n'hésite pas à t'entraîner grâce aux annales d'épreuves pour être sûr d'être prêt(e) à 100 %.

Lors de tes entraînements, mets-toi dans des conditions similaires à celles de l'examen réel. Cela signifie prendre le temps de réfléchir aux questions posées, d'analyser les informations disponibles, de proposer des solutions argumentées et de savoir les présenter de manière claire et concise.

Table des matières

Chapitre 1 : Matériel de réseau et infrastructure

1. Les réseaux informatiques :

Qu'est-ce qu'un réseau informatique ?
Un réseau informatique est un ensemble de dispositifs connectés qui permettent le partage de ressources et d'informations entre les utilisateurs. Ces dispositifs comprennent des ordinateurs, des serveurs, des routeurs, des commutateurs, des câbles et d'autres équipements réseau.

L'importance de l'infrastructure réseau :
L'infrastructure réseau est essentielle pour assurer la connectivité et la communication efficace au sein d'un réseau informatique. Elle permet de transférer des données de manière sécurisée, de garantir la disponibilité des services réseau et de soutenir les besoins des utilisateurs.

2. Les éléments du matériel de réseau :

Les serveurs :
Les serveurs jouent un rôle central dans un réseau informatique. Ils fournissent des services (stockage de données, hébergement de sites web, gestion des comptes d'utilisateurs, etc...). Les serveurs peuvent être physiques (matériels) ou virtuels (machines virtuelles).

Les routeurs :
Les routeurs sont des dispositifs qui dirigent le trafic réseau entre différents réseaux. Ils permettent la transmission de données entre des réseaux locaux (LAN) ou des réseaux étendus (WAN). Les routeurs prennent des décisions sur la meilleure route à emprunter pour acheminer les données vers leur destination.

Les commutateurs :
Les commutateurs sont utilisés pour connecter différents dispositifs au sein d'un réseau local (LAN). Ils permettent de transférer les données uniquement vers les destinataires appropriés, ce qui augmente l'efficacité du réseau. Les commutateurs peuvent être gérés ou non gérés, en fonction des besoins du réseau.

Les câbles et connecteurs réseau :
Les câbles et connecteurs réseau sont utilisés pour établir des connexions physiques entre les différents dispositifs d'un réseau. Les types de câbles couramment utilisés sont les câbles Ethernet, les câbles coaxiaux et les câbles à fibre optique. Les connecteurs réseau (connecteurs RJ45) assurent la connexion fiable des câbles aux dispositifs.

Les pares-feux :
Les pares-feux sont des dispositifs de sécurité qui contrôlent le flux de trafic réseau. Ils filtrent les données entrantes et sortantes pour protéger le réseau contre les menaces

potentielles comme les attaques de piratage ou les logiciels malveillants. Les pares-feux peuvent être mis en place au niveau du réseau ou de l'ordinateur.

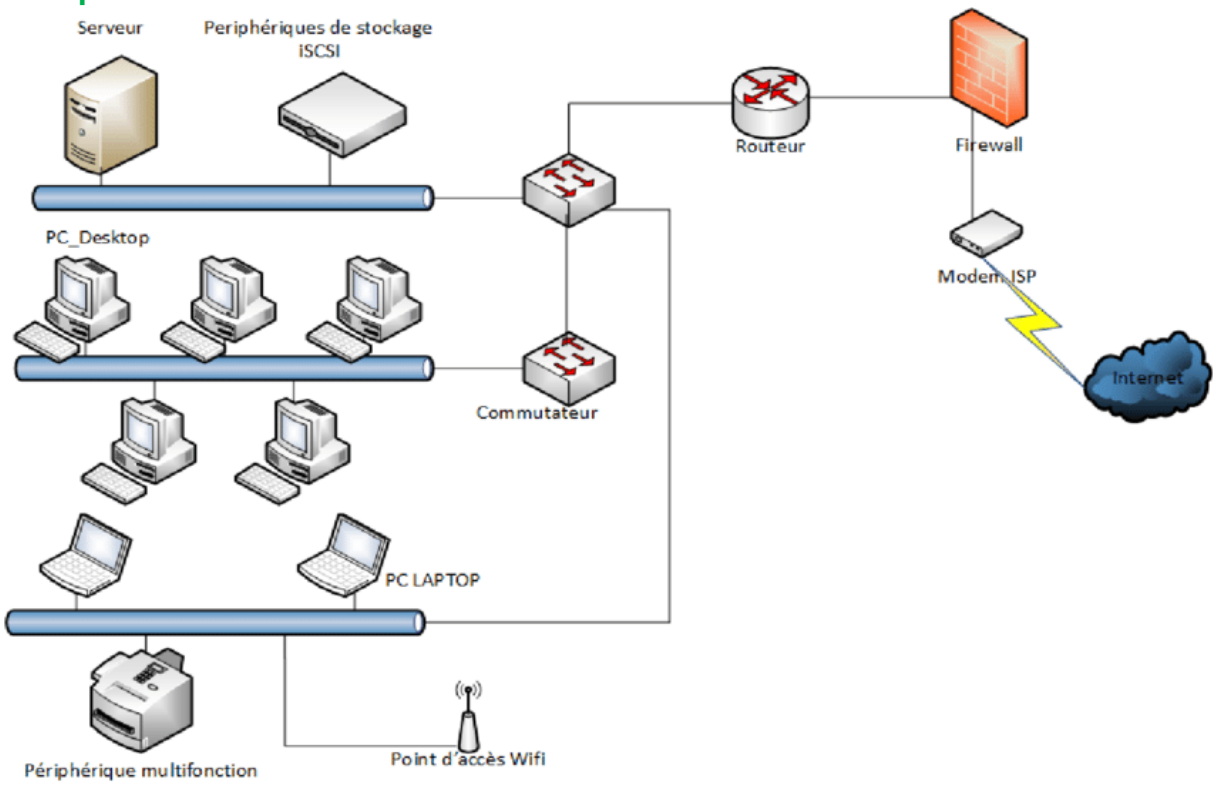
3. L'architecture du réseau :

Topologies de réseau :
Les topologies de réseau décrivent la structure physique ou logique d'un réseau informatique. Les topologies couramment utilisées comprennent l'étoile, le bus, l'anneau et la maillée. Chaque topologie a ses propres avantages et inconvénients en termes de coût, de fiabilité et de facilité de gestion.

Adressage IP :
L'adressage IP est un système utilisé pour identifier et localiser les dispositifs connectés à un réseau. Chaque dispositif reçoit une adresse IP unique, qui peut être une adresse IPv4 ou une adresse IPv6. L'adressage IP permet le routage des paquets de données à travers le réseau.

Protocoles réseau :
Les protocoles réseau sont des règles et des normes qui régissent la communication entre les dispositifs d'un réseau. Des protocoles couramment utilisés incluent TCP/IP (Transmission Control Protocol/Internet Protocol), DHCP (Dynamic Host Configuration Protocol) et DNS (Domain Name System). Chaque protocole a un rôle spécifique dans l'acheminement et la gestion des données.

Exemple d'architecture de réseau :



Exemple d'architecture de réseau

4. La sécurité du réseau :

Les menaces du réseau :
Les réseaux informatiques sont confrontés à de nombreuses menaces comme par ex. les attaques par déni de service (DDoS), les virus informatiques, les usurpations d'identité et le vol de données. Il est essentiel de mettre en place des mesures de sécurité appropriées, telles que des pares-feux, des antivirus et des politiques de sécurité, pour protéger le réseau contre ces menaces.

Les mécanismes de sécurité :
Les mécanismes de sécurité réseau comprennent l'authentification des utilisateurs, le cryptage des données, les réseaux privés virtuels (VPN) et les sauvegardes régulières des données. Ces mécanismes aident à prévenir les accès non autorisés, à sécuriser les communications et à garantir l'intégrité des données.

Les bonnes pratiques en matière de sécurité :
L'application de bonnes pratiques en matière de sécurité est essentielle pour maintenir la sécurité du réseau. Cela inclut la gestion des mots de passe, la mise à jour régulière des logiciels, la sensibilisation des utilisateurs aux menaces de sécurité et la sauvegarde régulière des données importantes.

Chapitre 2 : Les protocoles de réseau

1. Les types de protocoles de réseau :

Protocoles de réseau filaire :
Les protocoles de réseau filaire sont utilisés dans les réseaux qui utilisent des câbles physiques pour transmettre les données. Ils incluent des normes comme Ethernet, Fast Ethernet et Gigabit Ethernet, qui sont couramment utilisées dans les réseaux locaux (LAN).

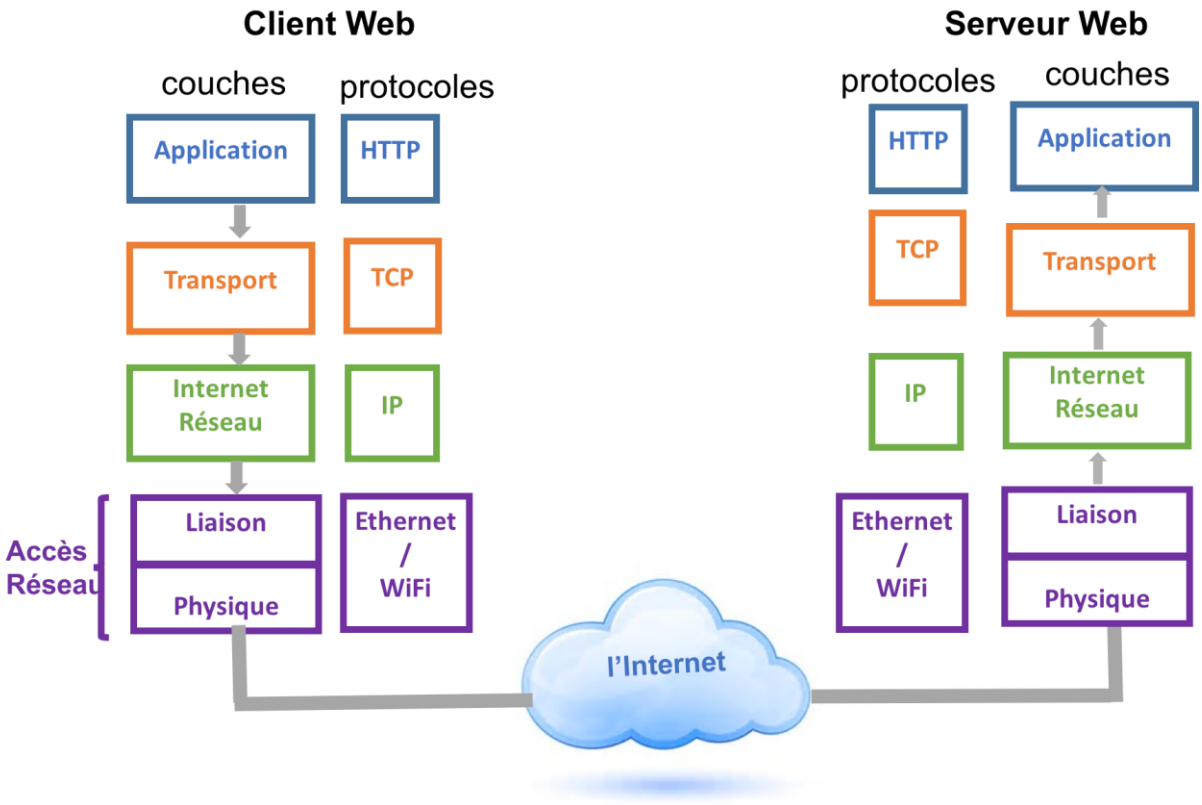
Protocoles de réseau sans fil :
Les protocoles de réseau sans fil sont conçus pour les réseaux qui utilisent des ondes radio pour transmettre les données. Ils comprennent des normes telles que Wi-Fi (802.11), qui est largement utilisée pour la connectivité sans fil dans les environnements locaux.

Protocoles de réseau de longue distance :
Les protocoles de réseau de longue distance sont utilisés pour les communications à grande échelle sur des distances étendues. Parmi les protocoles les plus connus figurent le protocole Internet (IP) et le protocole de contrôle de transmission (TCP), qui constituent les fondements d'Internet.

2. Fonctionnement des protocoles de réseau :

Les couches du modèle OSI :
Le modèle OSI (Open Systems Interconnection) divise les protocoles de réseau en différentes couches, chacune ayant un rôle spécifique dans la transmission des données. Les sept couches du modèle OSI comprennent la couche physique, la couche de liaison de données, la couche réseau, la couche transport, la couche session, la couche présentation et la couche application.

Exemple : Prenons l'exemple d'un utilisateur qui envoie un e-mail à un destinataire distant. Le message passe par chaque couche du modèle OSI, de la couche application où il est créé, à la couche physique où les données sont converties en signaux électriques ou en ondes radio pour la transmission.



Les protocoles client et serveur

3. Principaux protocoles de réseau :

Le protocole TCP/IP :
Le protocole TCP/IP est le fondement d'Internet. Il assure un transport fiable des données en les divisant en paquets, en les envoyant via le protocole IP et en les réassemblant à la destination finale.

Le protocole HTTP :
Le protocole HTTP (Hypertext Transfer Protocol) est utilisé pour le transfert de pages Web. Il permet aux navigateurs Web de demander des ressources aux serveurs et de les afficher sur les écrans des utilisateurs.

Le protocole DNS :
Le protocole DNS (Domain Name System) est responsable de la conversion des noms de domaine en adresses IP. Il permet aux utilisateurs d'accéder à des sites Web en saisissant des noms de domaine compréhensibles plutôt que des adresses IP numériques.

4. Sécurité des protocoles de réseau :

Les menaces et les vulnérabilités des protocoles de réseau :
Les protocoles de réseau peuvent être sujets à des attaques comme le vol de données, les attaques de déni de service (DDoS) et les attaques par débordement de tampon. Il est

essentiel de mettre en place des mécanismes de sécurité (chiffrement et pare-feu) pour protéger les réseaux contre ces menaces.

Exemple : Le protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) est utilisé pour sécuriser les communications sur Internet, notamment les transactions en ligne et les échanges d'informations sensibles. Il utilise le chiffrement pour assurer la confidentialité et l'intégrité des données.

Chapitre 3 : Sécurité des réseaux

1. Les menaces pour la sécurité des réseaux :

Les différentes formes de menaces :

- Les attaques par déni de service distribué (DDoS) ;
- Les attaques de force brute ;
- Les attaques de phishing ;
- Les logiciels malveillants ;
- Les virus informatiques ;
- Les chevaux de Troie ;
- Les failles de sécurité des systèmes d'exploitation et des applications.

La détection et la correction :
Les menaces pour la sécurité des réseaux peuvent être détectées à l'aide de diverses techniques (analyse des journaux, surveillance du trafic réseau et tests de pénétration).

Procédures mises en place pour les corriger :

- Mise à jour des logiciels et des systèmes ;
- Modification des politiques de sécurité ;
- Mise en place de contrôles supplémentaires.

2. Les protocoles de sécurité :

Les différents types de protocoles de sécurité :

Protocoles de sécurité	Description
SSL/TLS	Protocoles de cryptage pour la communication en ligne
PGP	Protocoles de cryptage pour la sécurisation des mails
SSH	Protocoles de sécurisation des connexions distantes
VPN	Protocoles pour la sécurisation des connexions à distance

Les protocoles de contrôle d'accès :
Les protocoles de contrôle d'accès sont utilisés pour assurer la sécurité des réseaux en contrôlant les accès des utilisateurs.

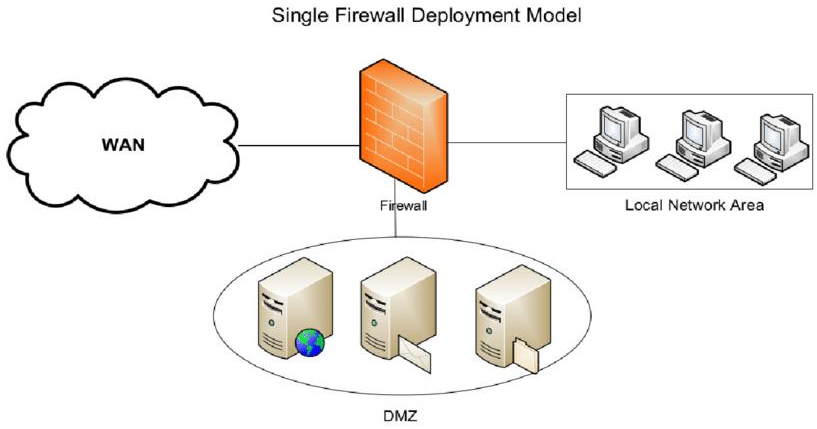
Exemples :

- Le protocole LDAP ;
- Le protocole SAML ;
- Le protocole OAuth.

3. Les pares-feux :

Les fonctions des pares-feux :
Les pares-feux permettent de protéger les réseaux en filtrant le trafic entrant et sortant. Les pares-feux peuvent être des dispositifs matériels ou logiciels et ils fonctionnent en bloquant le trafic qui ne répond pas à des règles spécifiques.

Les architectures des pares-feux :



Architecture des pares-feux

4. Les VPN :

A quoi servent les VPN ?
Les VPN sont utilisés pour sécuriser les connexions à internet et protéger les données échangées entre les différents équipements d'un réseau, en les cryptant.

Exemple de protocoles de VPN :

Protocole de VPN	Description	Avantages	Inconvénients
PPTP	Point-to-Point Tunneling Protocol	Facile à configurer, rapide	Faible niveau de sécurité
IPsec	Internet Protocol Security	Sécurisé, cryptage de bout en bout	Configuration complexe
SSL	Secure Sockets Layer	Compatible avec différents systèmes, sécurisé	Peut être plus lent que d'autres protocoles
OpenVPN	Open-source VPN	Très sécurisé, personnalisable	Configuration complexe, requiert des compétences en informatique

5. Les bonnes pratiques :

Les bonnes pratiques pour les utilisateurs :

- Utiliser des mots de passe forts et uniques pour chaque compte ;
- Éviter de partager des informations personnelles ou confidentielles sur des réseaux publics ;
- Ne pas cliquer sur des liens suspects ;
- Garder à jour les logiciels et les systèmes d'exploitation ;
- Installer un antivirus et un pare-feu ;
- Sauvegarder régulièrement les données importantes.

Les bonnes pratiques pour les réseaux :

- Limiter l'accès aux informations sensible ;
- Installer et mettre à jour régulièrement des logiciels antivirus et antimalwar ;
- Établir des politiques d'utilisation des réseaux pour les employés et les visiteurs ;
- Assurer la sécurité des connexions Wi-Fi en utilisant WPA2 ;
- Établir des sauvegardes régulières des données.

Comment bien gérer la sauvegarde et la récupération des données ?

- Établir une stratégie de sauvegarde et de récupération des données ;
- Réaliser des sauvegardes régulières des données ;
- Stocker les sauvegardes dans des endroits sûrs ;
- Tester régulièrement les sauvegardes ;
- Mettre en place des procédures d'urgence pour restaurer rapidement les données.

Chapitre 4 : Réseaux sans fil et mobiles

1. Les réseaux sans fil et mobiles :

Qu'est-ce qu'un réseau sans fil et mobile ?
Un réseau sans fil et mobile est un système de communication qui permet aux appareils de se connecter et de communiquer sans l'utilisation de câbles physiques. Il offre une flexibilité et une mobilité accrues, permettant aux utilisateurs de se déplacer librement tout en restant connectés au réseau.

Les avantages des réseaux sans fil et mobiles :

- **Mobilité :** Les utilisateurs peuvent accéder au réseau depuis n'importe quel endroit dans la zone de couverture ;
- **Flexibilité :** Les appareils peuvent être déplacés facilement sans avoir à reconfigurer les connexions physiques ;
- **Évolutivité :** Les réseaux sans fil et mobiles peuvent être étendus ou mis à jour plus facilement que les réseaux câblés ;
- **Connectivité étendue :** Les réseaux sans fil et mobiles permettent de connecter un grand nombre d'appareils simultanément.

2. Les technologies sans fil :

Les principaux types de technologies sans fil :
Il existe plusieurs types de technologies sans fil utilisées dans les réseaux sans fil et mobiles :

- **Wi-Fi :** Permet la connexion sans fil à Internet ou à un réseau local ;
- **Bluetooth :** Utilisé pour les connexions sans fil entre appareils à courte distance ;
- **4G/5G :** Fournit une connectivité haut débit pour les appareils mobiles ;
- **Réseaux satellites :** Utilisés pour la communication à grande distance lorsque les infrastructures terrestres ne sont pas disponibles.

Les caractéristiques des technologies sans fil :

- **Portée :** La distance maximale sur laquelle les appareils peuvent se connecter au réseau sans fil ;
- **Débit :** La vitesse de transmission des données à travers le réseau sans fil ;
- **Sécurité :** Les mesures mises en place pour protéger les données échangées sur le réseau sans fil ;
- **Interférences :** Les perturbations qui peuvent affecter la qualité de la connexion sans fil.

3. La conception des réseaux sans fil et mobiles :

L'analyse des besoins et des contraintes :
Avant de concevoir un réseau sans fil et mobile, il est important de comprendre les besoins spécifiques de l'utilisateur, ainsi que les contraintes techniques et budgétaires.

Cela permettra de définir les objectifs du réseau et de choisir les technologies appropriées.

La planification de la couverture réseau :
La planification de la couverture réseau consiste à déterminer l'emplacement optimal des points d'accès sans fil pour assurer une couverture adéquate dans la zone cible. Des outils de simulation peuvent être utilisés pour optimiser la disposition des points d'accès et minimiser les zones sans couverture.

La gestion de la capacité et de la qualité de service :
La gestion de la capacité est essentielle pour garantir des performances optimales du réseau sans fil et mobile. Cela implique de surveiller la charge du réseau, d'ajuster la capacité en fonction du trafic et de mettre en place des mécanismes de priorisation pour garantir une qualité de service satisfaisante.

4. Les défis des réseaux sans fil et mobiles :

La sécurité des réseaux sans fil et mobiles :
La sécurité est une préoccupation majeure dans les réseaux sans fil et mobiles. Il est essentiel de mettre en place des mesures de protection comme le chiffrement des données, l'authentification des utilisateurs et la détection des intrusions pour prévenir les attaques et les violations de la confidentialité.

La gestion de la mobilité :
La mobilité des utilisateurs dans un réseau sans fil et mobile nécessite une gestion efficace. Il est important de permettre une transition transparente entre les points d'accès et de maintenir une connexion stable lors des déplacements.

Les problèmes de performance :
Les réseaux sans fil et mobiles peuvent être sujets à des problèmes de performance (latence, perte de paquets et interférences). Il est nécessaire de surveiller et d'optimiser régulièrement le réseau pour garantir des performances optimales.

Chapitre 5 : L'administration des systèmes

1. Les objectifs :

Les objectifs de l'administrateur des systèmes :

- Assurer la disponibilité des systèmes ;
- Maintenir la sécurité des systèmes ;
- Optimiser les performances des systèmes ;
- Gérer les ressources des systèmes ;
- Fournir un support technique aux utilisateurs.

Domaine de l'administration des systèmes :

Domaine de l'administration des systèmes	Outils et techniques
Gestion des utilisateurs et des groupes	Active Directory, LDAP
Gestion de la base de données	Oracle, MySQL, PostgreSQL, MongoDB
Sécurité	Firewall, antivirus, chiffrement
Virtualisation	VMware, Hyper-V
Cloud computing	AWS, Azure, Google Cloud Platform
Gestion des systèmes d'exploitation	Windows Server, Linux

2. Les compétences requises :

Administration des systèmes - Les compétences techniques requises :

- Analyser les besoins d'un système d'informations ;
- Installer, configurer et utiliser un logiciel de prise de contrôle à distance afin de diagnostiquer et résoudre un problème (assistance à l'utilisateur) ;
- Configurer une maquette pour valider une solution (virtualisation) ;
- Configurer les éléments d'interconnexion permettant de séparer les flux, d'établir des périmètres de sécurité d'assurer la communication avec des réseaux externes (routeur, pare-feu, proxy, etc.) ;
- Caractériser, installer et administrer les éléments nécessaires à la qualité, à la continuité et à la sécurité d'un service (gérer des serveurs) ;
- Superviser et améliorer les performances d'une infrastructure réseau.