MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT

ENSEIGNEMENT DE PROMOTION SOCIALE

DOSSIER PEDAGOGIQUE

UNITE D'ENSEIGNEMENT

ADMINISTRATION, GESTION ET SECURISATION DES RESEAUX ET SERVICES

ENSEIGNEMENT SUPERIEUR DE TYPE COURT
DOMAINE : SCIENCES ECONOMIQUES ET DE GESTION

CODE : 7532 47 U32 D4

CODE DU DOMAINE DE FORMATION : 710
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du 16 août 2023,
sur avis conforme du Conseil général

ADMINISTRATION, GESTION ET SECURISATION DES RESEAUX ET SERVICES

ENSEIGNEMENT SUPERIEUR DE TYPE COURT

1. FINALITES DE L'UNITE D'ENSEIGNEMENT

1.1. Finalités générales

Dans le respect de l'article 7 du décret du 16 avril 1991 organisant l'enseignement de promotion sociale de la Communauté française, cette unité de formation doit :

- concourir à l'épanouissement individuel en promouvant une meilleure insertion professionnelle, sociale, culturelle et scolaire ;
- répondre aux besoins et demandes en formation émanant des entreprises, des administrations, de l'enseignement et d'une manière générale des milieux socio-économiques et culturels.

1.2. Finalités particulières

L'unité d'enseignement vise à permettre à l'étudiant:

- de mettre en œuvre, d'une manière appropriée, un ensemble de compétences, de techniques, de procédures et de méthodes spécifiques pour administrer, gérer et sécuriser un réseau local, des applications ou services pour :
  - administrer le serveur ;
  - administrer les périphériques des réseaux tels que routeurs, switches, etc. ;
  - administrer un poste de travail ;
  - administrer une solution d'hébergement dans un Cloud
  - …
- d'autoriser, de gérer et de sécuriser les accès à différents réseaux ou services tels que routeurs, répartiteurs de charges, serveurs et web serveurs, postes de travail, etc. ;
- de développer des compétences de travail en équipe pour des applications plus larges ;
- d'agir avec une marge d'initiative étendue dans l'optimalisation du travail réalisé ou de la gestion des tâches ;
- d'acquérir des compétences pour répondre d'une manière appropriée à l'évolution des techniques et des besoins de la clientèle.

2. CAPACITES PREALABLES REQUISES

2.1. Capacités

Pour Bases des réseaux

en disposant du matériel informatique nécessaire (routeurs, switches, câbles informatiques,…), de la documentation requise et d'une station informatique opérationnelle connectée à Internet,

- de décrire les principales notions de base des réseaux : le câblage, l'adressage IP, le modèle OSI, …;
- de décrire le fonctionnement d'un commutateur Ethernet et d'un routeur IPv4;
- d'établir un plan d'adressage d'un réseau simple sous IPv4 avec un accès vers l'Internet ;
- de remédier à un dysfonctionnement simple (par ex : erreur d'adressage, câble débranché, …).

2.2. Titre pouvant en tenir lieu

Attestation de réussite de l'unité d'enseignement « Bases des réseaux », n° de code 2983 10 U31 D2, classée dans l'enseignement supérieur de type court.

3. ACQUIS D'APPRENTISSAGE

Pour atteindre le seuil de réussite, l'étudiant sera capable,

en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...), de la documentation requise et d'un réseau,

face à un système informatique installé ou à installer, des consignes précises lui étant communiquées,

- de mettre en œuvre les procédures appropriées d'installation et de configuration d'un service déterminé ;
- de configurer le service sur le plan des fonctionnalités et de la sécurité, afin de respecter les objectifs à atteindre ;
- d'identifier l'origine d'un problème rapporté par un utilisateur du système et de lui apporter une solution ;
- d'identifier les différentes failles de sécurité présentes dans l'environnement réseau et applicatif et de leur apporter une solution ;
- de mettre en place une stratégie cohérente de sécurité tant au niveau accès, serveur, poste de travail, application ;
- de mettre en place un service hébergé dans une solution d'informatique dans le nuage (Cloud).

Pour la détermination du degré de maîtrise, il sera tenu compte :

- le niveau de cohérence : la capacité à établir une majorité de liens logiques pour former un ensemble organisé,
- le niveau de précision : la clarté, la concision, la rigueur au niveau de la terminologie, des concepts et des techniques/principes/modèles,
- le niveau d'intégration : la capacité à s'approprier des notions, concepts, techniques et démarches en les intégrant dans son analyse, son argumentation, sa pratique ou la recherche de solutions,

- le niveau d'autonomie : la capacité à faire preuve d'initiatives démontrant une réflexion personnelle basée sur une exploitation des ressources et des idées en interdépendance avec son environnement.

4. PROGRAMME

L'étudiant sera capable :

en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...), de la documentation requise et d'un réseau,

Laboratoire : Administration et gestion des réseaux et services :

- de décrire le fonctionnement des réseaux sans fil (WiFi et mobile à large bande) ;
- de situer et d'expliciter les rôles des différents composants d'une solution multi-tiers (rôle du navigateur, serveur web, moteur d'application, base de données) ;
- de décrire les différentes étapes du traitement d'un message envoyé dans une logique de « store and forward » (p.ex. courrier électronique) ainsi que les composants matériels, logiciels et protocoles mobilisés à chaque étape ;
- de configurer les piles de protocoles nécessaires à la mise en réseau d'un serveur et d'un poste de travail ;
- d'installer et de configurer les applications de gestion technique du réseau (p.ex. DHCP, DNS ….) ;
- de gérer des applications de manière centralisée telles que Antivirus, applicatifs divers ... ;
- de gérer des serveurs et des postes de travail virtuels hébergés dans une solution de virtualisation ;
- de décrire et de mettre en œuvre une politique de sauvegarde et de restauration ;
- de décrire et de mettre en œuvre une interconnexion de sites distants tels que succursales, filiales à l'étranger, etc. ;
- d'installer et de configurer un service standard de type Internet :
    - courrier électronique (y compris la configuration d'un client de référence),
    - serveur web (y compris la mise en place des connecteurs vers les moteurs applicatifs et les systèmes de gestion de base de données),
    - serveur d'application basé sur un environnement standard (Java …) ;
    - ...
- d'installer et de connecter des nœuds ;
- de configurer des réseaux virtuels et d'utiliser des protocoles ad hoc ;
- de mesurer les performances du réseau ;
- de réaliser le plan d'adressage d'un réseau segmenté simple en IPv4 et IPv6 (approche en double pile « Dual Stack »).

Laboratoire : Sécurisation des réseaux et services :

- de comprendre les risques, les menaces et les fonctionnements des protocoles de communication des différentes couches du modèle OSI:
    - de décrire le fonctionnement des protocoles de sécurisation tels que SSL, TLS (algorithmes de cryptage et d'authentification), etc.,
    - des protocoles utilisateurs tels que SSH, SFTP, HTTPS,
    - de chacune des couches basses (1, 2, 3, 4) ;
- d'expliquer les notions, technologies et outils liés à la sécurité de l'information ainsi que les conséquences de leurs usages (prérequis, coûts, organisation) : Firewall, IDS, NAC, Proxy, SWITCH, Routeur, VLAN, authentification de type 802.1x (host & network based), DMZ, UTM, Honeypots, Captive Portals, IPSec, VPN, risques d'impersonnalisation (spoofing), renforcement ("hardening"),… ;
- de caractériser le rôle d'un équipement (basé sur l'hôte et le réseau) de filtrage (pare-feu, IDS, IPS, proxy, …), authentification, autorisation d'accès (accès réseau authentifié (physique et logique), sanity check, …), d'accounting et d'en formuler les règles de fonctionnement ;
- de configurer les pares-feux centralisés et locaux du système afin de permettre l'établissement des connexions nécessaires pour un service standard et sécurisé ;
- d'argumenter l'intérêt de l'intégration d'un poste de travail dans un système d'authentification centralisé (utilisation des ACL, problèmes de « hacking ») ;
- d'installer et de configurer un système d'authentification distribuée entre autres :
    - Active Directory,
    - LDAP et/ou Kerberos,
    - etc. ;
- de mettre en œuvre un serveur de partage de fichiers, de l'intégrer à un système d'authentification distribué, d'en configurer les partages et d'en régler la sécurité ;
- de décrire et de mettre en œuvre un contrôle d'accès par VLAN ;
- de décrire, de mettre en œuvre une politique d'antivirus et d'antispam au niveau des postes clients, serveurs et messagerie, etc. ;
- de décrire et de mettre en œuvre des règles de stratégie de groupe (GPO) ;
- de décrire et de mettre en œuvre une politique d'accès sécurisé à distance tels que VPN ou accès à un bureau/application à distance de type Citrix, Microsoft Remote Desktop, etc.

5. CHARGE(S) DE COURS

Un enseignant ou un expert.

L'expert devra justifier de compétences issues d'une expérience professionnelle actualisée dans le domaine en relation avec le programme du présent dossier pédagogique.

6. CONSTITUTION DES GROUPES OU REGROUPEMENT

Il est recommandé de ne pas dépasser un étudiant par poste de travail.

7. HORAIRE MINIMUM DE L'UNITE D'ENSEIGNEMENT

7.1. Dénomination du cours	**Classement**	**Code U**	**Nombre de périodes**
Laboratoire : Administration et gestion des réseaux et services	CT	S	48
Laboratoire : Sécurisation des réseaux et services	CT	S	32
7.2. Part d'autonomie		P	20
Total des périodes			100
Nombre d'ECTS			8