UE T8-J - UVT8B2 - Réseaux et Sécurité

ECTS
6 crédits

Composante
ENSEIRB-MATMECA

Présentation

Code interne : ET8B2

Description

Niveau de connaissances (savoirs) :
N1 : débutant
N2 : intermédiaire
N3 : confirmé
N4 : expert
Les connaissances (savoirs) attendues à l'issue des enseignements de l'UE
Connaître les notions de ponts, de commutateurs et de routeurs et apprendre les principaux algorithmes de routage afin d'être capable d'interconnecter des réseaux de niveau 2 et de niveau 3 du modèle OSI. Appréhender la notion de qualité de service dans les réseaux et connaître les principaux modèles et algorithmes utilisés. (C1,N3) (C2,N3)
Connaître les principales notions et propriétés de sécurité de l'information et appréhender leurs enjeux dans l'entreprise et la société numériques. Apprendre les propriétés des principaux outils cryptologiques utiles pour assurer la sécurité des informations comprendre leur utilisation dans le contexte de la sécurité des réseaux. Connaître les principaux protocoles de sécurisation des communications électroniques, tels qu'IPSec et TLS. Appréhender la notion de VPN. (C1,N2) (C2,N2) (C9,N2) (C11,N2)
Les acquis d'apprentissage en termes de capacités, aptitudes et attitudes attendues à l'issue des enseignements de l'UE
être capable d'interconnecter des réseaux Ethernet en utilisant des ponts supportant l'évitement de boucles à l'aide du Spanning Tree Protocol (IEEE 802.1D) et de partager des liens à l'aide de VLAN (réseaux locaux virtuels, norme IEEE 802.1Q). être capable d'interconnecter des réseaux IP par routage statiques et dynamiques (protocoles RIP, OSPF et BGP) en concevant les plans d'adressage adéquats. Réunir les deux notions précédentes afin d'effectuer du routage inter-VLAN. être capable de construire de tels réseaux à l'aide d'équipements professionnels. être capable de définir une architecture réseau respectueuse de la qualité de service. (C3,N3) (C4,N3) (C5,N3) (C7,N2)
être capable de choisir les bons outils cryptologiques afin d'assurer les objectifs de sécurité souhaitée pour des communications électroniques. être capable de détecter les attaques de base, par exemple fondée sur le hameçonnage (phishing), et de manipuler la notion de certificat de clé publique, y compris dans les cas de chaînage de certifications et de certifications croisées. être capable de construire, à l'aide d'équipements professionnels, un système de VPN utilisant IPSec pour la connexion sécurisée d'utilisateurs nomades à un site central. (C3,N2) (C4,N2) (C5,N2) (C7,N2)

Liste des enseignements

	Nature	CM	CI	TP	TI	ECTS
Module - Cultures de l'ingénieur (au choix)	Module à choix					
Intelligence Economique	Module					
Initiation à la finance de marché	Module					
Sciences techniques et sociétés	Module					
Parcours entrepreneur	Module					
Management humain et performant	Module					
Management de projet digital et innovant	Module					
Management & santé au travail	Module					
Participation à un challenge/concours	Module					
S8 TOEIC (Rattrapage obligatoire)	Module					
Initiation à la recherche - Parcours PhD	Module					
Introduction à la sécurité de l'information et des réseaux	Module					
Interconnexion de réseaux	Module					

Infos pratiques

Contacts

Xavier Delord

Xavier.Delord@bordeaux-inp.fr