

Intitulé de l'UE	Networks : Connected and secure
Section(s)	- (10 ECTS) Bachelier en Informatique et Systèmes orientation Réseaux et Télécommunications / Cycle 1 Bloc 3 option Sécurité

Responsable(s)	Heures	Période
Denis MANDOUX	95	Quad 1

Activités d'apprentissage	Heures	Enseignant(s)
Connecting networks - théorie	30h	Denis MANDOUX
Connecting networks - travaux pratiques	40h	Denis MANDOUX
Cybersécurité 2	25h	Denis MANDOUX

Prérequis	Corequis

Répartition des heures
Connecting networks - théorie : 30h de théorie
Connecting networks - travaux pratiques : 40h d'exercices/laboratoires
Cybersécurité 2 : 20h de théorie, 5h d'exercices/laboratoires

Langue d'enseignement
Connecting networks - théorie : Français, Anglais
Connecting networks - travaux pratiques : Français, Anglais
Cybersécurité 2 : Français, Anglais

Connaissances et compétences préalables
Aucun prérequis n'est demandé, il est cependant fortement conseillé d'avoir réussi les activités d'apprentissage "Télécommunications et réseaux (théorie et travaux pratiques)", "Télécommunications et réseaux avancés (théorie et travaux pratiques)", "Concepts de routage et commutation (théorie et travaux pratiques)" ainsi que "Cybersécurité 1".

Objectifs par rapport au référentiel de compétences ARES
Cette UE contribue au développement des compétences suivantes
<ul style="list-style-type: none"> • Communiquer et informer <ul style="list-style-type: none"> ◦ Choisir et utiliser les moyens d'informations et de communication adaptés • Collaborer à la conception, à l'amélioration et au développement de projets techniques <ul style="list-style-type: none"> ◦ Elaborer une méthodologie de travail

- Planifier des activités
- Analyser une situation donnée sous ses aspects techniques et scientifiques
- Rechercher et utiliser les ressources adéquates
- Proposer des solutions qui tiennent compte des contraintes
- S'inscrire dans une démarche de respect des réglementations
 - Respecter les normes, les procédures et les codes de bonne pratique
- Collaborer à l'analyse et à la mise en œuvre d'un système informatique
 - Sur base de spécifications issues d'une analyse : (1) développer une solution logicielle ; (2) mettre en œuvre une architecture matérielle
 - Assurer la sécurité du système
- Intégrer des solutions télécoms sécurisées autour des réseaux locaux en y incluant la qualité de service
 - Mettre en place des solutions sécurisées d'accès aux réseaux (sans fil, ADSL, ...)
 - Interconnecter des réseaux de manière sécurisée, en gérant correctement des plans d'adressage et les aspects de sécurité (routage, ...)
 - Analyser le comportement d'un réseau en utilisant des outils de supervision et d'audit. mettre en oeuvre des solutions de qualité de service

Acquis d'apprentissage spécifiques

A l'issues des activités d'apprentissage, les étudiants seront notamment capable de

- Expliquer les différentes technologies WAN et leurs caractéristiques.
- Expliquer le fonctionnement et les avantages des réseaux privés virtuels (VPN) et du tunneling.
- Surveiller les fonctions réseau et assurer la résolution des problèmes avec Syslog, SNMP et NetFlow.
- Expliquer les concepts et mécanismes de la qualité de service dans les réseaux.
- Expliquer les composants d'une infrastructure de téléphonie mobile.
- Configurer et dépanner syslog et NTP.
- Configurer et dépanner des connexions série.
- Configurer et dépanner des réseaux sans fil.
- Configurer et dépanner des VPN IPsec et SSL.
- Configurer et dépanner la qualité de service dans un réseau.
- Configurer et dépanner les différentes fonctions d'un UTM, notamment
 - La virtualisation de pare-feux (VDM).
 - Le mode transparent.
 - La haute disponibilité.
 - Les VPN IPsec et SSL.
 - Mode transparent.
 - La fonction IPS.
 - Le Single Sing On.
- Respecter les méthodologies et règles de bonnes pratiques de l'administrateur réseau et sécurité.

Contenu de l'AA Connecting networks - théorie

Le contenu de l'activité est principalement basée sur :

- Les réseaux sans fil (Wi-Fi).
- Les technologies WAN.
- Les connexions séries point à point (protocoles HDLC et PPP).
- La surveillance du réseau (syslog, SNMP, Netflow).
- La qualité de service (gestion des files d'attente, traffic shaping).
- Les réseaux téléphoniques mobiles.
- Configurer et dépanner les connexions série.
- Configurer et dépanner des réseaux sans fil.
- ...

Contenu de l'AA Connecting networks - travaux pratiques

Projet commun de déploiement et sécurisation d'un réseau mettant en application les notions abordées dans les activités d'apprentissage "télécommunication et réseaux - routing and switching", "Network : Connected and secure" et "Cybersécurité 1 et 2".

Contenu de l'AA Cybersécurité 2

Ce cours vous apprendra à déployer une solution de sécurité de type UTM/NGFW et à maîtriser les éléments essentiels de sa configuration.

Configurer et dépanner les différentes fonctions d'un UTM, notamment :

- Le mode transparent.
- La haute disponibilité.
- Les VPN IPsec et SSL.
- Le contrôle d'application.
- La fonction IPS.
- L'authentification.
- ...

Méthodes d'enseignement

Connecting networks - théorie : cours magistral, approche interactive

Connecting networks - travaux pratiques : approche par projets

Cybersécurité 2 : cours magistral, approche interactive

Supports

Connecting networks - théorie : copies des présentations, Coursus CCNA routing and switching accessible en ligne

Connecting networks - travaux pratiques : notes d'exercices, protocoles de laboratoires, activités sur eCampus, Coursus CCNA routing and switching accessible en ligne

Cybersécurité 2 : copies des présentations, notes d'exercices, Documentation des éditeurs de solution de sécurité

Ressources bibliographiques de l'AA Connecting networks - théorie

- Support de notes : Mandoux D., *Connecting Networks*, HEH Campus Technique.
- Odom W., *CCNA Routing and Switching 200-125: Official Cert Guide*, CiscoPress, juillet 2016

Ressources bibliographiques de l'AA Connecting networks - travaux pratiques

- Protocoles de laboratoire.
- Odom W., *CCNA Routing and Switching 200-125: Official Cert Guide*, CiscoPress, juillet 2016

Ressources bibliographiques de l'AA Cybersécurité 2

- Support de notes, Mandoux D. *Cybersécurité 2*, HEH Campus Technique.
- Fortinet, Inc., FortiOS™ Handbook - System Administration VERSION 6.0.6, [En ligne] <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/admin-toc-final.pdf>.
- O. Santos, J. Stuppi, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.

Évaluations et pondérations

Évaluation	Épreuve intégrée
Langue(s) d'évaluation	Français, Anglais
Méthode d'évaluation	Examen oral 70% Autre 30% (non remédiable en 2e session) : Evaluation continue lors des activités d'apprentissage.

