Licence Professionnelle Métier des Réseaux Informatiques & Télécommunications

Parcours Administration et sécurité des systèmes

Programme Pédagogique 2021–2022

Rushed KANAWATI

9 février 2021

Table des matières

1 Introduction **2**
M11 Anglais . . . 4
M12 Expression . . . 5
M13 Droit . . . 6
M21 Introduction à la programmation . . . 7
M22 Introduction aux Systèmes d'exploitation . . . 8
M23 Gestion de Projet . . . 9
M24 Notions de risques . . . 10
M31 Administration UNIX . . . 11
M32 Programmation client/serveur . . . 12
M41 Services réseaux . . . 13
M42 Administration Windows . . . 14
M51 Réseaux . . . 15
M52 Qualité de Service et VoIP . . . 16
M61 Routage . . . 17
M62 Réseaux sans fils . . . 18
M71 Supervision des réseaux . . . 19
M72 Introduction à la cryptographie . . . 20
M81 Techniques d'attaques . . . 21
M82 Cryptographie avancée . . . 22
M83 Cybersécurité . . . 23
M91 Projet Tutoré . . . 24

1 Introduction

Ce document décrit le programme pédagogique de licence professionnelle Métiers des Réseaux Informatiques et télécommunication (LP MRIT) - Parcours Administration et sécurité des systèmes.
L'essor actuel de l'économie numérique requiert la formation de professionnels experts capables d'appréhender des problématiques liées à la production, à la transmission à la sécurisation et au traitement des données numériques. La licence MRIT répond à ces enjeux en formant des techniciens supérieurs disposant de compétences technologiques fortes mais capables d'évoluer et d'avoir une vision d'ensemble des systèmes d'informations. La licence MRIT comprendra cinq parcours types :

1. Administration et sécurité des réseaux et des systèmes (ASUR)
2. Réseaux très haut débit (RTHD)
3. Électronique, optique et nanotechnologies (EON)
4. Internet des objets : réseaux & capteurs (IoT-D)
5. Internet des objets : de la collecte à l ?analyse des données (IoT-R)

Cette licence adresse donc un large spectre des problématiques citées ci-dessus. Elle propose un couplage original qui permet d'adresser, à travers les différents parcours, la chaîne complète des données numériques : dès la fabrication des capteurs jusqu'au traitement des données en passant par la transmission efficace et sécurisée des données numériques.
Les cinq parcours partagent un tronc commun et des différents modules sont mutualisés entre les différents parcours. La figure suivante illustre le recouvrement et la mutualisation entre les différents parcours de la licence MRIT.

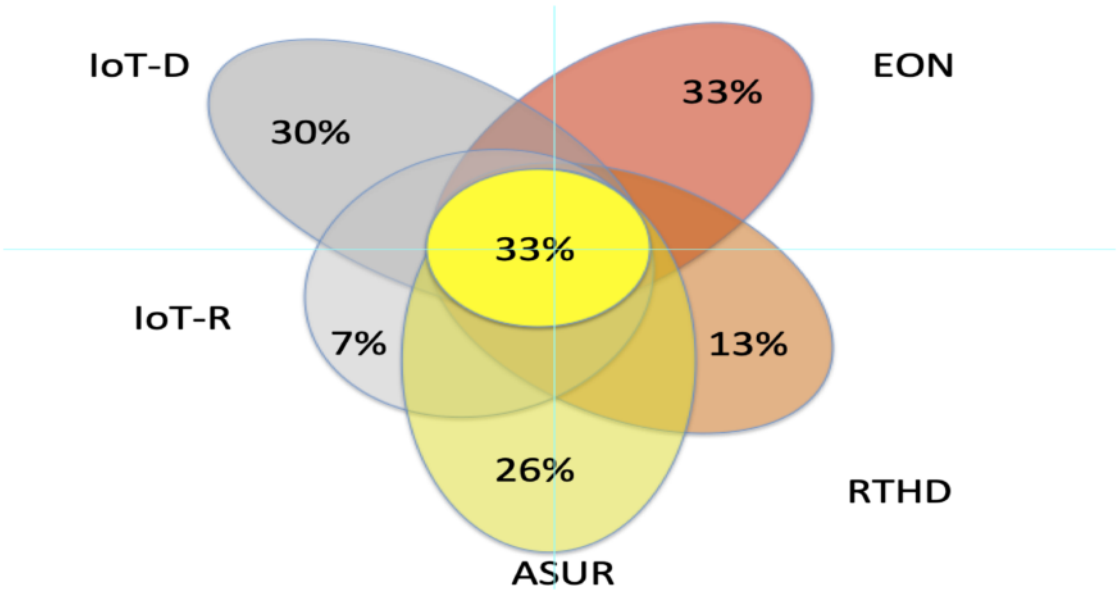

FIGURE 1 – Organisation des parcours de la licence MRIT

Dans la suite de ce document nous présentons le contenu pédagogique du parcours : Administration et sécurité des réseaux et des systèmes (ASUR). Ce parcours est organisé en 10 unités d'enseignements, pour un volume total de 550 H d'enseignements.

Le tableau suivant donne l'ensemble des unités d'enseignements du parcours :

Unité d'Enseignement	ECTS	Coeff.	Disciplines concernées	Modalités de l'enseignement (CM/TD/TP)	Durée totale d'enseignement en présentiel	
					CM	TD/TP
UE1: Enseignements généraux	4	2	anglais, communication	TD/TP	18,75	56,25
UE2: Enseignements généraux techniques	4	2	Informatique/mathématiques/physique	TD/TP	18,75	56,25
UE 3.1 Système 1	5	2	Informatique	CM/TD/TP	11,25	33,75
UE 3.2 Système avancé	5	2	informatique	CM/TD/TP	11,25	33,75
UE 4.1 réseaux informatiques	5	2	informatique	CM/TD/TP	11,25	33,75
UE 4.2 réseaux avancés	5	2	informatique	CM/TD/TP	11,25	33,75
UE 5.1 Sécurité des SI	6	2	info/maths	CM/TD/TP	11,25	33,75
UE 5.2 Sécurité avancée	8	3	info/maths	CM/TD/TP	18,75	56,25
UE 6 : projet tutoré	6	3			0	100
UE 7: stages	12	5			-	0
	60			**Total**	**550**	

FIGURE 2 – Maquette pédagogique de la LP MRIT - Parcours ASUR

Les modules inclus dans chaque unité d'enseignement sont détaillés dans la suite de ce document.

M11 Anglais

Durée: 25h

Résumé: Anglais technique pour l'informatique et les réseaux.

- Communication professionnelle en anglais (courriels) ;
- le vocabulaires de l'informatique et des réseaux ;
- lecture et rédaction de documentation technique ;
- péparation de la certification TOEIC.

Évaluation: contrôle continu.

M12 Expression

Durée: 25h

Résumé: Expression et communication, insertion professionnelle

- techniques de recherche d'emplois : CV, lettre de motivation, recherche d'emplois et stage ;
- pratiques de communication en milieu professionnel (prise de parole en réunion, courriel, etc.) ;
- préparation au rapport et à la soutenance de stage.

Évaluation: contrôle continu (exposés, préparation de documents).

M13 Droit

Durée: 15h

Résumé:
Ce module permet aux étudiants d'acquérir les notions juridiques indispensables au bon déroulement de leur activité opérationnelle.

Principales notions abordées :

1. la responsabilité pénale ;
2. la fraude informatique : intrusion et atteintes matérielles et virtuelles au système/ utilisation du systèmeà des fins frauduleuses ;
3. la protection des données personnelles : RGPD [1], CNIL [2], infractions relatives aux données personnelles (collecte et traitement) ;
4. le droit d'auteur sur Internet ;
5. principes éthiques pour les administrateurs de systèmes d'informations.

Évaluation: examen écrit.

1. règlement général sur la protection des données
2. Commission nationale de l'informatique et des libertés

M21 Introduction à la programmation

Durée: 30h

Résumé:

Les notions abordées sont les suivantes :

- variables, structures de contrôle ;
- algorithmes simples, manipulations de structures de données basiques (séquences, chaines de caractères) ;
- entrées/sorties et lecture/écriture de fichiers textes ;
- très brève introduction à la notion d'objet.

Ces notions seront présentées à la fois d'une manière généraliste, afin d'être utilisables dans un contexte général, et illustrées au moyen de l'utilisation du langage Python.

Recommandation de mise en œuvre : travaux pratiques, expérimentation, utilisation intensive de l'interpréteur.

Évaluation: contrôle continu (TP) et final.

M22 Introduction aux Systèmes d'exploitation

Durée: 25h

Résumé: Introduction aux systèmes de la famille Unix et au shell Bash.

Système de fichiers, processus, commandes de base, principes du shell Bash, expressions réguliéres, bases de la programmation de scripts (variables, conditionnelle, boucles for et while, fonctions).

Déroulement:

1. Cours : rappel notions UNIX, fichiers, commandes de base ;
2. TP 1 : Utilisation de base d'UNIX (commandes, redirection, méta-caractères, find, variables d'environnement).
3. Cours : permissions, processus et jobs.
4. TP 2 : Droits d'accès, jobs et processus (ps, kill).
5. Cours : scripts bash
6. TP 3 : Bash : scripts simples, itérations.

Compléments possibles : liens Bash/Python ; compilation d'un programme C.

Évaluation: TP, contrôle final.

M23 Gestion de Projet

Durée: 20h

Résumé:
Le module aborde les bases de la gestion de projet :

- les fondamentaux :
  - définition d'un projet
  - les acteurs
  - les types d'organisation
  - les phases d'un projet
- les étapes du management de projet ;
- la maitrise des coûts ;
- la maîrise des risques ;
- leadership du chef de projet ;
- réseau PERT, diagramme de GANTT ;
- Outils de résolution de problèmes.

Évaluation: examen écrit.

M24 Notions de risques

Durée: 15h

Résumé: Ce module est une introduction générale aux problématiques liées à la sécurité informatique.

1. Notions de sécurité, de risque, de qualité.
2. Les éléments de la sécurité
3. Sécurité physique
4. Sécurité des postes clients
5. Sécurité réseau
6. Sécurité des logiciels
7. Sécurité humaine
8. Sauvegardes des données
9. Analyse des risques
10. Protection de l'environnement (*green IT*)

Mise en œuvre : cours, travaux de recherche des étudiants, exposés.

Évaluation: exposés.

M31 Administration UNIX

Durée: 30h

Résumé: Le but de ce module est d'acquérir de solides connaissances en administration de systèmes Unix.

Les notions abordées sont les suivantes :

- Rappels et compléments : processus, usage de ssh, sécurité humaine, veille.
- Installation et configuration d'un système Linux.
- SGF, liens, droits, partitions, MBR. Caractéristiques des SGF les plus courants (exemples : ext4, VFAT) et tendances futures (exemple : Btrfs). Notion de journalisation.
- Processus, exécution de commandes, Shells (approfondissement de M01).
- Utilisateurs. Création d'un utilisateur. Groupes. Bon usage de su et sudo.
- Tâches périodiques (cron). Scripts de démarrage.
- Maintenance d'un système UNIX : journaux (logs), mises à jour, veille.
- Réseau local UNIX : RPC, NFS, NIS (on mentionnera d'autres solutions comme SAMBA).
- Sécurité des données et sauvegardes (locales et distantes). Outils de base (tar, rsync). Stratégies de sauvegardes (incrémentales) et solutions utilisées en entreprises (logiciels de gestion des sauvegardes, RAID, SAN).
- Notion de machine virtuelle (usage de VirtualBox ou logiciel similaire). Usages de la virtualisation en entreprise.
- Sécurisation du système : pare-feu (Netfilter sur un poste client).
- Administration distante : installation, configuration et bon usage d'un serveur SSH. Outils associés (par exemple : nc, screen).

Évaluation: contrôle continu en TP, contrôle terminal.

M32 Programmation client/serveur

Durée: 15h

Résumé:

Contenu :

1. rappels programmation en langage Python ;
2. rappels sur les protocoles IP, ARP, UDP et TCP ;
3. programmation client et serveur UDP ;
4. programmation client et serveur TCP ;
5. protocoles applicatifs simples (exemple : telnet, finger, ftp ou http) ;
6. utilisation de services Web (exemple : interrogation de l'API Twitter).

Pré-requis : bases de programmation (Python), protocoles TCP et UDP. Indication : travaux pratiques en langage Python.

Évaluation: contrôle continu en TP, contrôle terminal.

M41 Services réseaux

Durée: 30h

Résumé: Dans ce module, on aborde les principes et la mise en œuvre des principaux services réseaux. Chaque service fait l'objet d'une présentation (rôle, cas d'utilisation) et d'une description des protocoles réseaux associés. Les principales solutions (logiciels) rencontrés en entreprise sont présentés, en insistant si besoin sur les problèmes d'interopérabilité. Une mise en œuvre est effctuée sous forme de travaux pratiques. On insiste sur les problèmes de sécurité (intrusions, divulgation d'information) et de qualité (robustesse aux pannes, continuité du service, sauvegardes).

Services étudiés :

1. Service de nom IPv4 : DNS. Gestion des noms de domaines (*registrars*. Installation et configuration d'un serveur simple (*bind*).
2. Messagerie électronique. Protocoles SMTP, IMAP(s), POP3(s). Format MIME.
3. Serveur Web. principes d'une application Web. Notions d'HTML, CSS, JavaScript. Protocole HTTP(s). Installation et configuration d'un serveur simple (*Apache*).
4. Annuaire LDAP. Principes et cas d'utilisation. Configuration client. Serveur simple (OpenLDAP). Interopérabilité (UNIX/Windows).
5. Serveur de fichiers et intégration UNIX/Windows : SAMBA, partages, *Active Directory*.

Évaluation: contrôle continu en TP, contrôle terminal.

M42 Administration Windows

Durée: 15h

Résumé: Principes du système d'exploitation Windows. Mise en réseau. Administration et sécurisation.

Points abordés dans ce module :

1. Poste client Windows
   - historique
   - système de fichier
   - scripts dos
   - profil utilisateur
   - base de registre
   - amorçage
2. Serveur Windows
   - Active Directory (DNS/WINS)
   - Groupes/OU
   - Stratégie de groupe (GPO)/réglages
   - DFS/EFS
   - contrôleur RAID
   - déploiement logiciels
   - clichés instantanés
   - quotas disque
   - DHCP
   - WSUS
   - Network Access Protection (NAP)

Indication : travaux pratiques sur machines virtuelles.

Évaluation: contrôle continu en TP, contrôle terminal.

M51 Réseaux

Durée: 30h

Résumé: Réseaux locaux, réseaux IP.

1. Cours : pile de protocoles TCP/IP (sur Ethernet).
2. Adressage IPv4 (classes, masques)
3. Protocoles ARP, ICMP, IP (v4), TCP, UDP.
4. Cours : réseaux locaux ethernet : commutation, VLAN, *spanning tree*, 802.1q.
5. TP : analyse de trames sur Ethernet ;
6. TP : service DHCP (client et serveur Linux) ;
7. routage statique ;
8. pare feu : SNAT, DNAT, mise en œuvre avec *Netfilter* ;
9. Introduction à IPv6

Indications de mise en œuvre : TP sur commutateurs Ethernet. Simulations avec le logiciel *Marionnet*.

Évaluation: contrôle continu en TP, contrôle terminal.

M52 Qualité de Service et VoIP

Durée: 15h

Résumé: Dans ce module, les élèves se familiarisent avec la notion de QoS réseau et ses fonctions. Applications multimédia –vidéo et VoIP– et Téléphonie sur IP.

Les principaux points abordés sont les suivants :

- applications multimédia sur internet ;
- streaming mutimédia et protocole RTP/RTCP ;
- paramètres de la QoS IPv4 et les sources de dégradation, l'apport de TCP et de RTP ;
- gestion des ressources dans un routeur (le modèle DiffServ, les mécanismes de la QoS) et dans un switch ;
- gestion des défaillances dans un routeur (le protocole HSRP) et dans un switch (le protocole STP) ;
- voix et téléphonie sur IP : VoIP, ToIP, SIP ;
- en pratique : mise en ?uvre d'un proxy SIP, analyse des mécanismes pour la ToIP, et interconnexion de technologies hétérogènes. (Utilisation d'un PIBX Aastra permettant de mettre en œuvre tous les types d'architecture évoqués dans ce module).

Indication : la QoS IP pourra être étudiée pratiquement à l'aide d'iproute2/TC dans le logiciel Marionnet.

Évaluation: contrôle continu en TP, contrôle terminal.

M61 Routage

Durée: 20h

Résumé: Routage dynamique dans les réseaux IP

Les notions abordées sont les suivantes :

- bref rappel sur la couche IP et routage statique ;
- routage à vecteur distant (RIP en TP) ;
- routage à états de liens (OSPF en TP + multizone) ;
- notions sur les protocoles de routage longue distance X25, Frame Relay.
- routage de bord.

Recommandation de mise en œuvre : travaux pratiques sur routeurs.

Évaluation: contrôle continu en TP, contrôle terminal.

M62 Réseaux sans fils

Durée: 25h

Résumé: Le but de ce module est de permettre une compréhension du monde sans fil, en se basant principalement sur les normes de communication 802.11 (a, b et g), et développer les mécanismes de sécurité applicables (WEP/WPA et 802.11i).

Les notions abordées sont les suivantes :

- notions de base (SSID, infrastructure sans fil) ;
- méthode de propagation des ondes ;
- algorithmes de chiffrement et d'authentification (RC4, EAS, EAP, 802.1x) ;
- normes et protocoles utilisables conjointement (802.1q, 802.11n) ;
- Sécurité et méthodes d'audit (principe de scan des réseaux et crackage de clef).

Évaluation: contrôle continu.

M71 Supervision des réseaux

Durée: 25h

Résumé: Techniques de surveillance et de protection des réseaux.

Les principaux points abordés sont les suivants :

- protection des données (IPSec) et la mise en place d'une association de sécurité (ISAKMP, DOI, IKE) ;
- infrastructures à clés publiques (PKI) ;
- révision : contrôle d'accès au switch et au point d'accès WiFi
- réseaux privés virtuels (VPN) : principes et implémentations. (Travaux pratiques sur IPSec) ;
- usages avancés de SSH (proxy) ;
- supervision réseau (TP avec NAGIOS) ;
- détection d'intrusions dans un réseau (IDS).

Prolongement possible :

- cloisonnement du réseau (MPLS-VPN).

Évaluation: contrôle continu en TP, contrôle terminal.

M72 Introduction à la cryptographie

Durée: 15h

Résumé: notions de cryptographie et applications.

Contenu du cours :

1. principes généraux : authenticité, confidenialité, intégrité ;
2. algorithmes élémentaires de chiffrement (décalage et substitution) ;
3. déroulement à la main et implémentation à l'aide d'un ordinateur (TP en python) ;
4. cryptanalyse de ces algorithmes par force brute (avec notion de complexité) et analyse fréquentielle ;
5. cryptographie asymètrique : notions de clé publique et privée ;
6. présentation du point de vue utilisateur de protocoles et techniques de chiffrement et sécurité (MD5, SHA, RSA, SSH, TLS) ;
7. robustesse des mots de passe et cryptanalyse (avec analyse de complexité) ;
8. infrastructure à clé publique ;
9. certificats (X509) ;
10. utilisation d'outils (exemple : OpenPGP).

Évaluation: contrôle continu en TP, contrôle terminal.

M81 Techniques d'attaques

Durée: 30h

Résumé: Techniques d'attaques des réseaux et systèmes.

— Cours sur les techniques d'attaques (réseaux et applicatives) vues sous l'angle d'un « pentester » (celui qui fait des tests d'intrusions), sans aborder les techniques qui nécessitent des notions de développement trop pointues pour le niveau des étudiants (ex. *buffer overflow*).
— TP sur *ARP Poisoning* (approfondissement de celui traité en R&T2) Utilisation de cette technique pour détourner des requêtes DNS clientes précises (par exemple www.fnac.fr) vers un serveur DNS fake, qui va donner une fausse réponse et rediriger la victime vers un faux serveur web, imitant le mieux possible le serveur usurpé. Ensuite ils doivent imiter le certificat (en sachant que la victime devra répondre à un message d'erreur) et détourner la session de la victime où lui voler ses identifiants.
— d'introduire des techniques d'évasion (comportementales) : c'est à dire qu'ils doivent, sans cesse, se demander ce que fait l'os ou l'application lorsqu'ils opèrent, de manière à adapter leur comportement, soit pour ne pas trop laisser de traces, soit pour ne pas stimuler une sonde de détection.

Pré-requis :
— Linux (et Windows) : shell, commande, configuration, droits ;
— base de données (ici MySQL) : SELECT ... les UNION SELECT ou les jointures, les tables `information_schema`, ...
— PHP, HTML et Javascript : savoir ce qu'est une variable, comment la filtrer ...
— protocoles applicatifs de base et en particulier HTTP (car on manipule les enêtes) et savoir configurer rapidement un serveur HTTP, FTP, TFTP, DNS ;
— connaître iptables (pour le SNAT et le DNAT en particulier).

Évaluation: contrôle continu en TP, contrôle terminal.

M82 Cryptographie avancée

Durée: 20h

Résumé: Cryptographie avancée

- Principe clé publique / clé privée (Illustration avec messagerie GnuPG)
- Présentation des certificats : Certificat auto signé, Manipulation en mettant en œuvre un service apache auto signé en https
- Présentation du concept de CA (amener les PKI en douceur) : Séquestre, Révocation, Manipulation en mettant en place une petite CA autour de notre serveur web
- Le certificat côté client : Authentification du client auprès du serveur, Manipulation en créant des certificats nominatifs pour les clients souhaitant accéder à notre serveur web

Évaluation: contrôle continu en TP, contrôle terminal.

M83 Cybersécurité

Durée: 25h

Résumé: L'objectif de ce module est de montrer aux étudiants les différents techniques de intrusion (pentesting) afin de mieux mette en place des stratégies de défense.

- Durant des TP, les étudiants se comportent comme des hackers. Ils ont une cible (une machine virtuelle) nous l'attaquons ensemble. Les 2 premirères cibles permettent :
  - de mettre en place le scénario (prises d'infos et mise en places de stratégies d'exploitation) : bases sur Whois, découverte des architectures de messagerie, découverte de routeurs filtrant, etc.
  - d'introduire des outils (nmap, dirbuster, john the ripper, ...) et donc de s'initier aux techniques de force brute (recherche de répertoires sur un serveur httpd, cassage de mots de passe, ...)
  - Obtention de privilèges (devenir root). Approfondissements sur les utilisateurs et les droits UNIX.
  - Attaques Web (Injection SQL, XSS, ...). (TP sur SQL et PHP, utilisation de machines virtuelles issue de HackFest. Travail en groupe).
  - Attaque d'une machine virtuelle : devenir root en cherchant et exploitant les vulnérabilités d'un serveur Web.
  - Utilisation des outils METASPLOIT et SET (Social Engineering). METASPLOIT est une référence chez les *pentesters* et permet d'introduire la notion d'EXPLOITS.

Évaluation: contrôle continu en TP, contrôle terminal.

M91 Projet Tutoré

Durée: 100h

Résumé: Le but de ce module est de permettre aux étudiants de développer une méthode de conduite de projet sur un sujet nouveau, d'effectuer des recherches et implémenter puis présenter une solution.
Les notions abordées sont les suivantes :
— gestion de mini-projet sous forme de ressources ;
— identification des tâches ;
— qualification et estimation des durées des tâches ;
— ingénierie et intégration de solution préexistence.
Cisco en auto-apprentissage :
— CCNA1 Fondamentaux du réseau (*Network fundamentals*)
  — chapitre 1 : notions générales sur les réseaux, usages, fonctions et données transportées
  — chapitre 2 : modèle en couches OSI//TCP/IP notion adresse physique/logique N° port encapsulation fragmentation+whireshark et paquet tracer
  — chapitre 3 : couche application : DNS, www, HTTP, SMTP, FTP, DHCP, SMB Gnutella Telnet tp installation apache et capture HTTP et SMTP
  — chapitre 4 : couche transport OSI (TCP et UDP)
  — chapitre 5 : couche Réseau OSI (IP)
  — chapitre 6 : adressage IPV4
  — chapitre 7 : liaison de données (CSMA/CD CSMA/CA)
  — chapitre 8 : couche physique
  — chapitre 9 : ethernet
  — chapitre 10 : planification et câblage des réseaux (plan adressage VLSM et fixe bien expliqués)
  — chapitre 11 : configuration et test du réseau
— CCNA2 Concepts et protocoles de routage *Routing protocol and concepts*)
  — chapitre 1 présentation routage
  — chapitre 2 protocoles et concepts de routage
  — chapitre 3 routage dynamique
  — chapitre 4 Protocoles à vecteurs de distance
  — chapitre 5 RIP V1
  — chapitre 6 VLSM et CIDR
  — chapitre 7 RIP V2
  — chapitre 8 tables de routage
  — chapitre 9 EIGRP
  — chapitre 10 Protocoles à état de liaison
  — chapitre 11 OSPF
— CCNA3 Sans fil et commutation LAN *LAN Switching and wireless*)
  — chapitre 1 Réseau hiérarchique (accès distribution coeur)
  — chapitre 2 concepts de commutation
  — chapitre 3 VLAN
  — chapitre 4 VTP
  — chapitre 5 STP
  — chapitre 6 inter VLAN routing
  — chapitre 7 Wireless lan
— CCNA4 WAN *Accessing the WAN*
  — chapitre 1 Réseaux étendus
  — chapitre 2 PPP

— chapitre 3 Frame Relay
— chapitre 4 Sécurité du réseau
— chapitre 5 ACL
— chapitre 6 Télétravail (VPN/IPSec)
— chapitre 7 adressage IP (DHCP/NAT/IPV6)
— chapitre 8 Problèmes/dépannage du réseau

Évaluation: examens en ligne.