h e g

Haute école de gestion
Genève

Descriptif de module

Domaine : Economie & Services
Filière : Informatique de gestion

1. Intitulé de module — CCNA — 2023-2024

Code :
650-3

Type de formation :
☒ Bachelor ☐ Master ☐ MAS ☐ DAS ☐ CAS ☐ Autres :

Niveau :
☐ Module de base
☐ Module d'approfondissement
☒ Module avancé
☒ Module spécialisé
☐ Autres :

Caractéristique :
☒ Module dont l'échec peut entrainer l'exclusion définitive de la filière selon l'art.15, al.1 des directives cadres "statut des étudiants-e-s"

Type :
☐ Module principal
☐ Module lié au module principal
☒ Module facultatif ou complémentaire
☐ Autres :

Organisation temporelle :
☒ Module sur 1 semestre
☐ Module sur 2 semestres
☒ Semestre d'automne
☒ Semestre de printemps
☐ Autres :

2. Organisation

Crédits ECTS
5

Langue principale d'enseignement :
☒ Français
☐ Allemand
☐ Autres :
☐ Italien
☐ Anglais

3. Prérequis

☐ Avoir validé le module
☐ Avoir suivi le module
☐ Pas de prérequis
☒ Autres : Il est fortement recommandé d'avoir validé le module 63-13 avant de s'inscrire au module 65-31

4. Compétences visées / Objectifs généraux d'apprentissage

L'étudiante ou l'étudiant doit être capable, en fin de module, de justifier des compétences professionnelles suivantes :

- Être capable de concevoir un réseau d'entreprise, de configurer les équipements en conséquence, de présenter l'état de l'installation, et le cas échéant, d'y rechercher les pannes et de les corriger.
- Acquérir les connaissances théoriques, techniques et pratiques dans le cadre de différentes solutions VPN, d'une authentification centralisée, d'un réseau basé sur l'identité, d'un protocole de routage à états de liens et d'une architecture redondante.
- Être capable de mettre en œuvre de bonnes pratiques de sécurité réseau.

5. Objectifs détaillés des enseignements

- Maitriser le protocole de routage OSPF
- Comparer les avantages et les inconvénients des différents protocoles de routage IGP
- Appréhender le concept de superposition
    - Configurer des tunnels génériques
- Décrire et activer les meilleures pratiques de protection d'un réseau.
    - Sécuriser les communications
        - Configurer des VPN site à site sécurisés par IPsec
        - Configurer un VPN d'accès à distance
    - Sécuriser les équipements
        - Configurer un serveur AAA
        - Mettre en oeuvre le protocole 802.1x

- Mettre en œuvre de protocoles pour gérer le réseau.
    - Mettre en œuvre le protocole NTP entre un client et un serveur
    - Expliquer le fonctionnement du protocole SNMP
    - Expliquer le fonctionnement de Syslog
- Expliquer les considérations relatives à la conception d'un réseau évolutif.
    - Concevoir des liaisons redondantes
    - Augmenter la bande passante avec des liens multiples
- Dépanner le réseau d'entreprise.
    - Comparer les méthodes de dépannage
    - Décrire et utiliser les différents outils de dépannage du réseau

6. Plan et chapitres des cours

- Rappels configuration de base routeurs et commutateurs, routage statique, vlan, ACL et protocoles de routage OSPF ainsi qu'EIGRP en dual-stack
- Routage et commutation avancés
- Configuration de réseaux privés interconnectés via internet par un tunnel générique (GRE)
- Notions de VPN et IPsec, VPN site à site, accès distant, configuration client
- Authentification centralisée
    - Authentification d'administrateur réseau centralisée basée sur Freeradius
    - Authentification d'administrateur réseau centralisée basée sur Active Directory
- Authentification clients vpn sur Active Directory
- Accès au réseau basé sur l'identité
    - Structure réseau avec commutateurs à accès sécurisé au vlan de l'entreprise (802.1x) par utilisateur
    - Structure réseau avec commutateurs à accès sécurisé au vlan de l'entreprise (802.1x) par machine
- Firewall d'entreprise avec DMZ
- Bonnes pratiques pour la sécurité du réseau
- Localisateur et protocole de séparation d'ID (LISP)
- Architecture VLAN avancée
- Protocoles NTP, SNMP et Syslog

7. Forme du cours et méthodes pédagogiques

De nombreux travaux pratiques sont proposés, durant les cours, individuellement ou par groupe. L'étudiant.e a l'opportunité de travailler avec du matériel professionnel, d'un équipementier connu mondialement, et veillera à utiliser les différents modèles d'équipements durant les TP (routeurs, commutateurs, firewall, AP).

En dehors des heures de cours, les salles Réseaux sont à disposition des étudiants sur demande pour effectuer des travaux pratiques. Elles doivent être refermées durant les pauses et en fin d'activités

L'assistant.e est également à disposition des étudiant.e.s sur rendez-vous pour répondre à des questions concernant le cours et/ou les exercices pratiques proposés.

De plus, le cours s'appuie sur le cours en ligne CCNA proposé par l'académie Cisco.

L'étudiant.e désirant obtenir une attestation CCNA devra effectuer des QCM et des exercices pratiques supplémentaires sur simulateur en dehors du cours

L'étudiant.e aura accès au logiciel Packet Tracer, développé par Cisco, qui permet de créer des simulations de réseaux.

8. Modalités d'évaluation et de validation

Acquis : A-E
Remédiation : Fx
Répétition : F

L'évaluation du module se fera en principe de la manière suivante :

Contrôle continu : 100%	**Examen : 0%**
1 contrôle continu individuel — coefficient 1 1 contrôle continu individuel ou un projet — coefficient 1	Pas d'examen.