# UTC505 - Introduction à la cyberstructure de l'internet : réseaux et sécurité

Mis à jour le 15-07-2024

## Code : UTC505

Unité d'enseignement de type mixte

3 crédits

Volume horaire de référence (+/- 10%) : **30 heures**

**Responsabilité nationale :**
EPN05 - Informatique / 1

**Contact national :**

EPN05 - Informatique

2 rue Conté
33.1.4A
75003 Paris
01 40 27 22 40
Agnès Lapierre
agnes.lapierre@lecnam.net

# Présentation

## Prérequis

Pas de pré-requis nécessaire dans l'absolu, mais avoir obtenu une UE comme NFA009 peut aider à exploiter plus pleinement le contenu du cours. Il faut bien sûr une culture de base en systèmes d'exploitation, en programmation et en mathématiques telle que demandée dans un DUT informatique. UTC505 est un pré-requis de RSX101, RSX102 et RSX112. Ces UE poursuivent le programme de UTC505 et ne le refont pas.

## Objectifs pédagogiques

L'objectif de l'UE est :

- d'introduire le domaine des réseaux à travers l'exemple de l'Internet, de décrire ses principaux ingrédients et les concepts clefs de son fonctionnement,
- et de présenter les propriétés de sécurité qui sont générales et pas seulement liées aux réseaux.

## Compétences

L'UE UTC505 dès sa conception avait une visée théorique comme l'a explicitement demandé la Commission du Titre de l'Ingénieur. Le Cnam, en particulier, l'équipe IRSM, a respecté cette exigence. Cette UE apporte donc d'abord des connaissances dans le domaine des réseaux et de la sécurité. Les compétences découlent des exercices et des cours qui s'inspirent de situations réelles ou proches de la réalité.

- Connaissances associées aux concepts, protocoles, architectures du Modèle en couche OSI ou Internet. L'auditeur pourra, à l'issue du cours, évaluer les principales contraintes réseaux et leur impact sur une application de type client/serveur,
- L'auditeur sera en mesure de participer à la définition des principaux éléments d'un cahier des charges fonctionnel à destination d'une maîtrise d'ouvrage dont l'objectif est d'urbaniser une application ou un système d'information distribués.
- L'auditeur disposera de repères pour évaluer fonctionnellement une livraison d'équipements réseaux, et mettre en place une procédure de recette de ceux-ci dans un cadre applicatif.
- L'auditeur ayant suivi le cours devrait savoir exploiter l'outil Wireshark dans un mode normal, et s'il a suivi les vidéos optionnelles en plus il pourra avancer vers un niveau expert.

*Savoirs :* Protocoles et normes télécoms, Protocoles de l'Internet, Technologies clefs des réseaux de données, Règles de sécurité Informatique et Télécoms, CyberSécurité, Architectures réseau, Réseaux de données et télécoms.

# Programme

## Contenu

Sujets traités pour la partie Réseaux (2/3 du volume de l'enseignement) :

- **Diviser pour régner / Modèles en couches OSI vs Internet / Encapsulation**
  - Découverte de l'architecture de communication en couches : du modèle OSI à l'architecture Internet ;
  - L'outil d'analyse de traces Wireshark pour comprendre l'encapsulation et l'articulation entre les couches.
  - La couche physique et la couches liaisons sont abordées ici, très succinctement à travers la présentation des couches de protocoles, pas plus
- **Carrefours, itinéraires et destinations / Couche Réseau /**
  - Protocole IP.
  - Adressage IPv4 sans classe (CIDR, Classless Inter-Domain Routing) : adresse

d’interface, adresse de réseau, masques, broadcast sur sous-réseau.
    - Tables de routage (plan de données et commutation/forwarding) et acheminement de datagrammes dans un réseau IP.
    - D’IPv4 à IPv6 : le point de vue du datagramme et des adresses IPv6, le cours est centré IPv4 car beaucoup de mécanismes sont plus faciles à comprendre avec les adresses IPv4 mais certains principes restent les mêmes avec IPv6. Le public de l'UE a d'ailleurs souhaité qu'on enseigne les concepts clefs de la couche IP à partir d'IPv4 plutôt qu'à partir d'IPv6.
    - Algorithme du plus court chemin de Dijkstra pour le routage dynamique qui est sous-jacent à OSPF est parfois abordé à la demande du public mais ce n'est pas systématique.
- **Une lettre ou un appel ?  / Couche Transport /**
    - Transport de données entre un client et un serveur
    - Mode connecté TCP : ouverture de connexion, transfert de données, fermeture de connexion, contrôle de flux et fenêtre glissante
- **Quelques protocoles de la couche application**
    - Introduction aux protocoles dédiés aux applications : HTTP, DNS
- **Course d'obstacles en tous genres /les boitiers divers et variés encore appelés “middleboxes”**
    - Etude de l'impact des équipements NAT/Firewall et protocoles associés dont DHCP

Sujets traités pour la partie Sécurité (1/3 du volume de l'enseignement) :

- **Introduction à la sécurité**
    - Bonnes pratiques de sécurité personnelle
    - Droit du numérique
    - Côté entreprises : normes et règlementation : RGPD, SOx, PCI DSS, OIV, ISO 27000
- **Menaces**
    - Études de cas : Stuxnet, TV5Monde, Banque du Bangladesh, EternalBlue/WannaCry/NotPetya, Carbanak/Cobalt, fraude au président (Pathé), SolarWinds.
    - Rançongiciels : Colonial Pipeline, HSE, Kaseya VSA
    - Processus d’attaque : MITRE ATT&CK Framework, Unified Kill Chain, menaces persistantes avancées (APT)
- **Mesures de sécurité**
    - Vulnérabilités : failles 0-day, échelle de sévérité, CVE MITRE, score CVSS
    - Processus de déploiement des correctifs de sécurité. Séparation des environnements.
    - Scan de vulnérabilités, durcissement de configuration, vérification de la conformité technique
    - Modélisation des menaces
    - Sécurité du code pour les développements logiciels : débordement de tampon ou d’entiers, MITRE CWE. Bonnes pratiques de développement et d’amélioration de la qualité du code. Fuzzing, tests d’intrusion, exercices red/blue team.
    - Impacts : bilan d’impact sur l’activité (BIA), temps et point de rétablissement (RTO et RPO), Data Protection/Privacy Impact Assessment (D)PIA, plans de reprise (PRA), de continuité (PCA), d’urgence et de poursuite d’activité (PUPA)
    - Gestion des risques informatiques : ISO 27000, méthodologies EBIOS et MEHARI
    - Organisation de la sécurité : SOC, surveillance des événements de sécurité (SEM)
    - Sensibilisation des utilisateurs à la sécurité informatique
    - Sécurité des authentifications : biométrie, mots de passe, possession. Authentification forte multi-facteurs.
    - Défense en profondeur, modèle du château fort, dépérimétrisation de l’infrastructure informatique et réseaux ‘zéro trust’.
- **Primitives cryptographiques**
    - Propriétés de sécurité, de contrôle d’accès et de sûreté de fonctionnement
    - Approches historiques : codage, stéganographie, chiffrement
    - Principe de Kerckhoffs
    - Taxinomie des techniques de cryptanalyse : KPA, CPA, CCA. Exemple d’attaque sur la

carte à puce via l'horloge.
    - Niveau de sécurité
    - Analyse des fréquences (Al-Kindi). Indice de coïncidence de Friedman
    - Algorithmes historiques : César, Vigenère, Playfair, ADFGVX, Enigma.
    - Sécurité inconditionnelle de l'algorithme du masque à usage unique (chiffre de Vernam)
    - Principe des chiffres symétriques (en continu ou par blocs) et à clé publique.
    - Cryptosystèmes hybrides. Infrastructures de clés publiques et autorités de certification.

Suivant l'enseignant, le cours peut démarrer par la partie sécurité ou par la partie réseaux, il y a des articulations dans les deux cas. Pour la partie réseaux, en général on commence par le modèle ISO, puis on peut décrire en commençant par la couche application en allant vers la couche réseau, ou le contraire. A paris, on démarre souvent après le modèle en couches et l'encapsulation, mais pas toujours, par la couche Réseau et IP car c'est la clef de voute de l'Internet.

L'enseignant est libre aussi de proposer des extensions optionnelles au cours qui ne comptent pas pour l'examen mais qui peuvent intéresser une partie du public. A Paris, le cours s'appuie sur différents types de ressources : supports de cours, exercices corrigés : vus en séance, à faire soi-même ou pour s'auto-évaluer, animations power point et vidéos. Les vidéos du cours sont enrichies par des vidéos de youtubeurs du domaine qui complètent le contenu du cours sur certains thèmes et peuvent répondre à la curiosité des auditeurs souhaitant se spécialiser en réseaux ou en cybersécurité. Le cours se découpe en 5 séquences Réseaux et 5 séquences Sécurité. Ces séquences se subdivisent elles-mêmes en séances. Le nombre de séances par séquence est variable. Les contenus par séquence sont divisés en partie principale et en parties optionnelles. Les parties optionnelles sont identifiables par l'expression « pour aller plus loin » ou plus clairement par « optionnel ». Les contenus optionnels sont offerts aux curieux soit pour creuser le sujet du cours, soit pour préparer aux unités d'enseignement qui suivent comme RSX101, RSX102, RSX112. Il est rappelé que les contenus optionnels ne font pas l'objet de questions à l'examen. Tous les contenus sont consultables jusqu'au 30 septembre de l'année académique en cours, ils sont tous sur l'espace numérique de formation (ENF). Toutes et tous disposent des mêmes contenus. L'ENF contient aussi des sujets d'examens parfois corrigés et sont en libre accès aux inscrits à UTC505.

Evolution du cours : la couche physique et la couche liaison ont disparu du contenu du cours et ont été remplacées par une partie "middleboxes" qui aborde le NAT, le firewall et les protocoles associés. Liaison et Physique ont été déplacées dans RSX101. Certains enseignants de réseaux trouveront que ça peut être une hérésie, mais le domaine des réseaux évolue, les besoins du public du Cnam évoluent, et les métiers évoluent. Liaison et Physique sont du ressort d'équipes plus spécialisées dans les entreprise, et, l'impact des boitiers intermédiaires sur les communications applicative est devenu plus conséquent. Par ailleurs, pour beaucoup, la couche physique et la couche liaison sont perçues comme des tuyaux relativement fiables dont on ne se préoccupe plus que quand on se soucie d'architecture de réseaux de communication.

Ces boitiers participent à l'ossification de l'Internet, il est donc bon d'en connaître un minimum sur leur impact. Typiquement, un cours à distance fait avec Teams entre les auditeurs/auditrices et l'enseignant qu'il soit chez lui ou dans son bureau au Cnam, est complètement assujetti à la traversée de ces middleboxes.

## Modalités de validation

- Contrôle continu
- Examen final

## Description des modalités de validation

A Paris, on pratique un contrôle continu sur le thème de la sécurité, ⅓ des points, on a adopté la forme QCM pour l'évaluation en contrôle continu. Et un examen de 2h00 écrit sur la partie réseaux ⅔ des points. Les deux formes d'examen se complètent car elles ne convoquent pas les aptitudes.