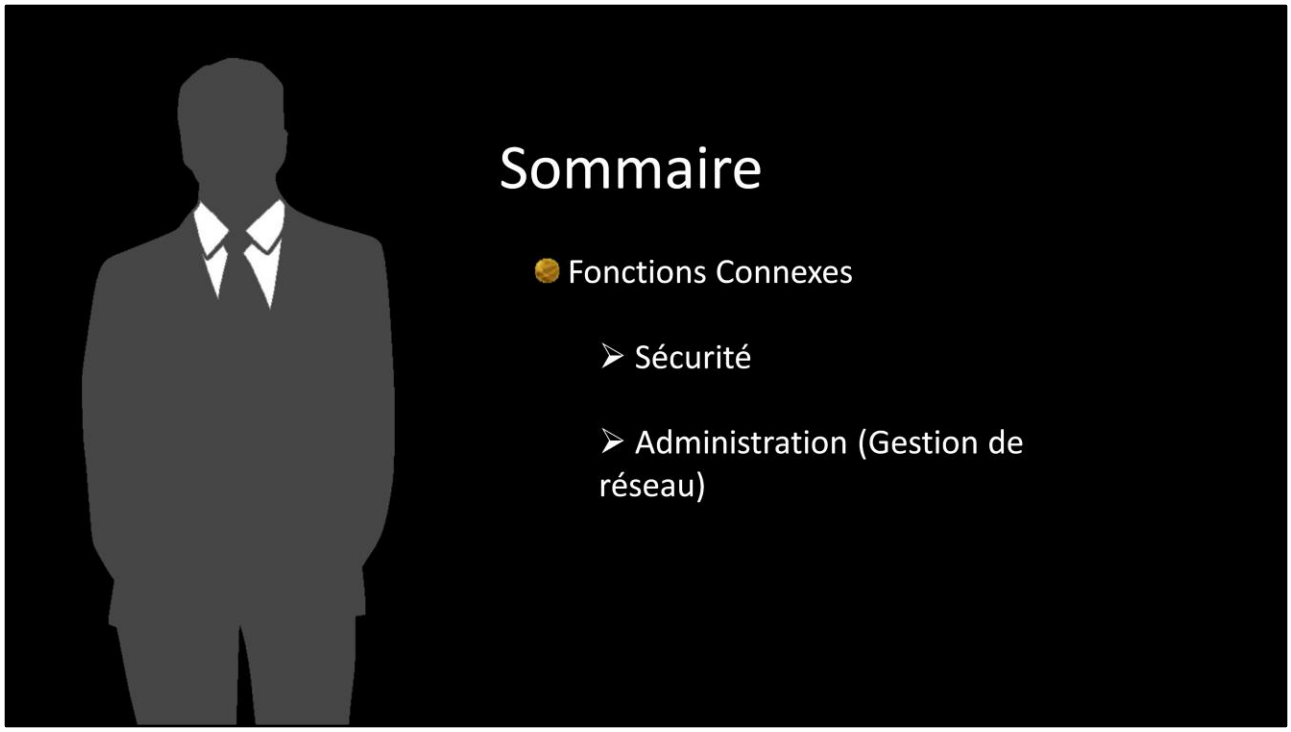
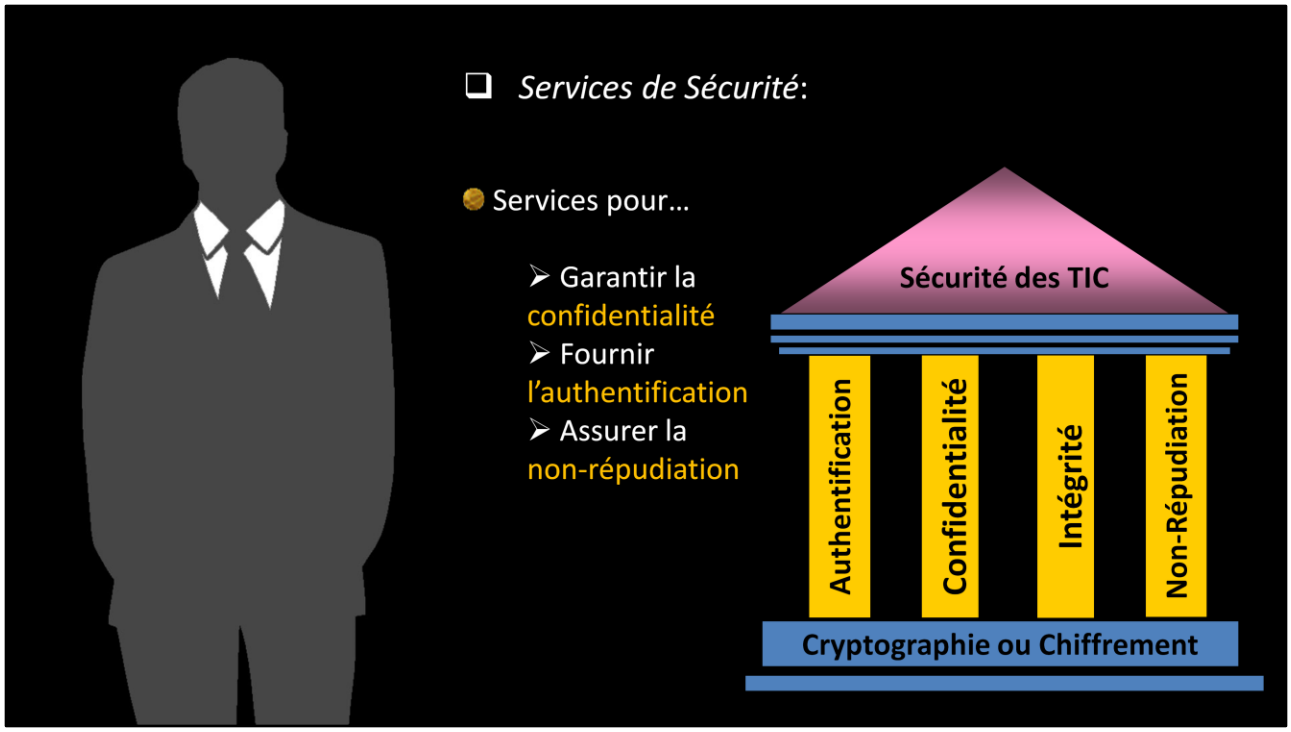


Cette séquence va permettre de donner quelques définitions propres à introduire des notions sans lesquelles le fonctionnement des réseaux serait beaucoup plus problématique.
Deux fonctions sont particulièrement importantes dans le cadre de la vie des réseaux : la sécurité, vue ici dans le sens protection des données et non fiabilité des réseaux, et l'administration, prise ici dans le sens de la gestion des réseaux et des équipements connectés.



La sécurité dans les réseaux de communication est basée sur un ensemble de services destinés à :

- garantir la confidentialité et l'intégrité des messages transmis - fournir l'authentification des utilisateurs et des services.
- s'assurer de la non–répudiation par les utilisateurs et le non-déni de services.

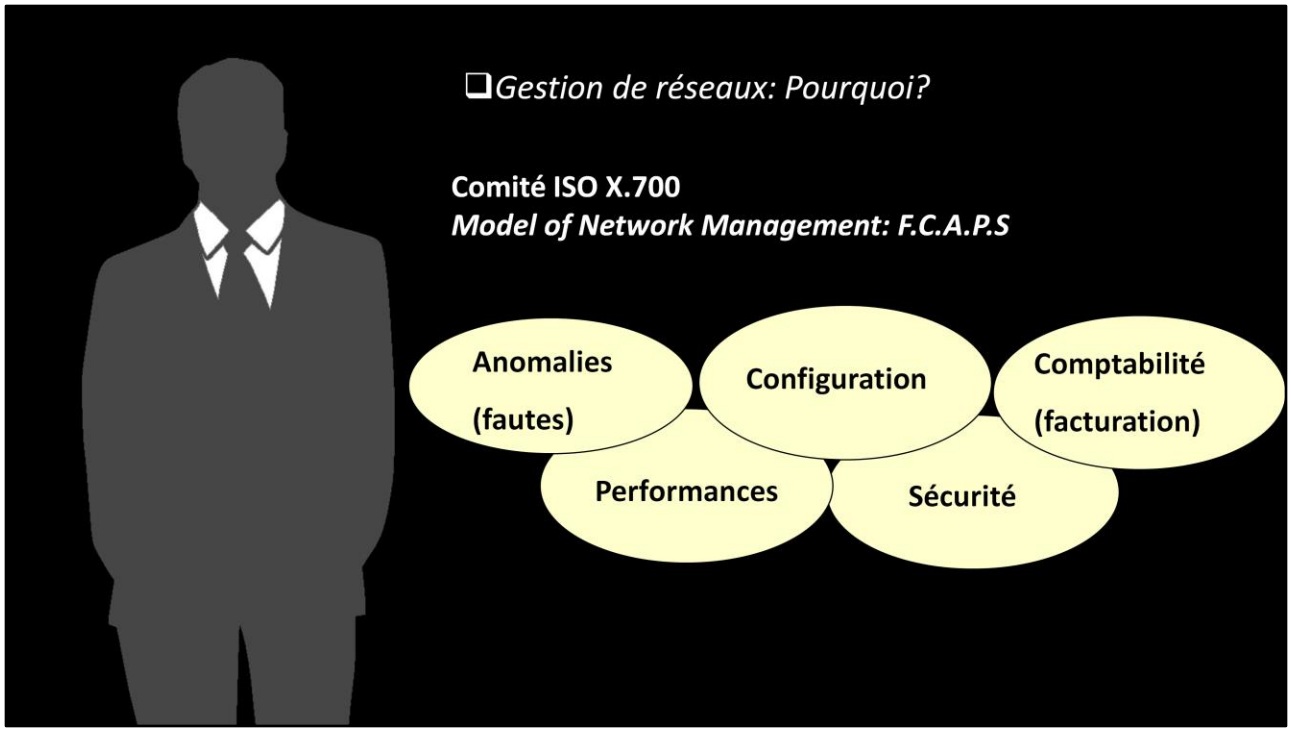
Les services de sécurité à mettre en oeuvre pour assurer la sécurité des communications sont :
La c*onfidentialité* : fournit la protection des données contre toute tentative d'accès au contenu des messages.
L'*intégrité* : fournit la preuve de non modification des données et permet la détection de toute manipulation frauduleuse du contenu des messages.
L'*authentification mutuelle* : garantit les identités des entités communicantes. Ce service est utilisé pour la protection contre la mascarade et le rejeu.
La *non–répudiation* : fournit la preuve d'intégrité et d'origine des données qui peut être vérifiable par un tiers à tout moment.
Le *contrôle d'accès* : fournit la protection contre tout usage non autorisé des ressources.
L'ensemble des mécanismes permettant de mettre en place ces différents services repose principalement sur la mise en oeuvre des systèmes cryptographiques.

Il est important d'identifier les menaces contre lesquelles le réseau doit être protégé. Une menace est une violation potentielle de la sécurité. On distingue 2 familles de menaces :

Les menaces passives qui n'introduisent aucune modification sur les informations transmises ou sur le fonctionnement normal du système. On peut citer :
L'accès au contenu du message, qui concerne généralement les informations sensibles ou confidentielles contenues dans une conversation téléphonique, dans un message électronique ou dans un fichier transféré.
L'analyse de trafic, qui consiste à exploiter les parties non chiffrées du message pour déduire des informations utiles sur l'identité et la localisation des entités qui communiquent, ou observer la fréquence et la longueur des messages échangés, en examinant des messages ou le flot de messages.

Les menaces actives qui se traduisent souvent par des modifications des informations ou du fonctionnement normal du système. On peut citer :

La mascarade, où un intrus prétend être une entité légitime et acquiert ainsi les droits d'accès correspondants.
Le rejeu, correspond à la capture d'une unité de données puis à sa retransmission ultérieurement pour générer un message sans source légitime.
La modification, qui se traduit par la modification partielle ou totale, l'effacement ou le re-séquencement de messages.
Le déni de service, qui vise à empêcher l'usage ou la gestion normale des moyens de communication à travers une cible spécifique.
L'interruption, qui vise généralement la destruction ou la mobilisation d'un élément du réseau, le rendant ainsi indisponible. C'est une atteinte à la *disponibilité*.
L'interception, qui se traduit par un accès illicite au contenu d'un message.
La création, qui se traduit par l'insertion d'informations crées de toutes pièces par l'intrus . C'est une atteinte à l'*authentification*.



L'administration de réseaux a pour objectif d'englober un ensemble de techniques de gestion mises en oeuvre, pour offrir aux utilisateurs une certaine qualité de service, pour permettre l'évolution du système en incluant de nouvelles fonctionnalités, et pour rendre opérationnel un système.

L'administration de réseaux, ou Network Management, en anglais, ne peut pas être isolée de son environnement. Il s'agit d'une partie intégrante d'un système plus général constitué de trois parties.

La première partie est l'utilisateur, auquel il faut fournir un ensemble de mécanismes pour lui permettre l'accessibilité aux applications, aux serveurs de noms pour localiser les ressources, et lui assurer la confidentialité et la sécurité ainsi que la qualité de service.

La seconde partie concerne l'administration des serveurs, pour permettre la distribution des applications et des données avec un maximum de fiabilité, et la mise en place d'outils de contrôle et de protection des accès à ces applications et données.

La troisième partie concerne les équipements de transport de l'information, et l'ensemble des mécanismes permettant d'intervenir sur le fonctionnement du réseau, les performances, la configuration et autres éléments comme l'inventaire et la gestion des changements.

La norme ISO X700 définit 5 groupes de fonctions, nommés domaines fonctionnels, afin de satisfaire au minimum des besoins de gestion, dit FCAPS pour Fault, Configuration, Accounting, Performances Security.

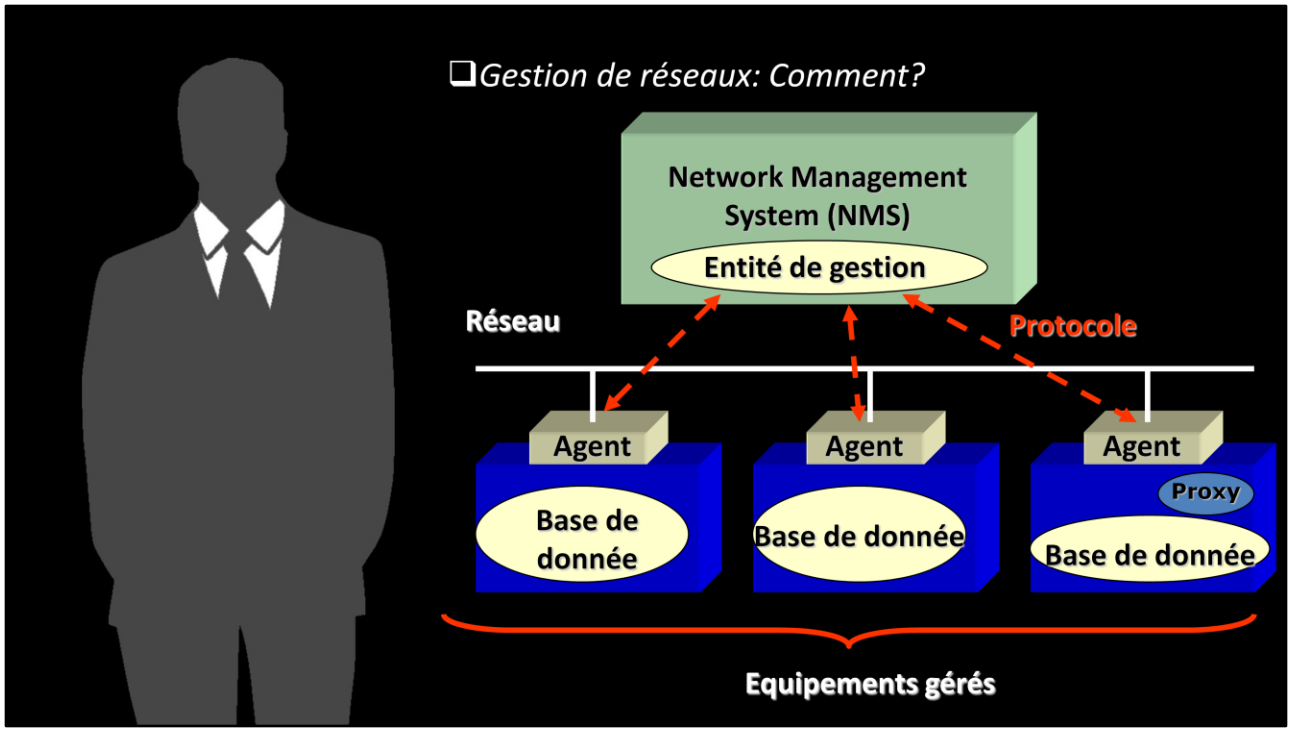
Le premier de ces groupes correspond à la gestion des fautes, qui concerne la fonction de surveillance (monitoring), la localisation et la détermination des pannes.

Le second est la gestion des configurations et des noms, qui concerne la fonction d'installation de composants, la fonction de contrôle et surveillance puis la fonction de gestion des noms.

Le troisième s'intéresse à la gestion des performances, qui concerne la fonction de collecte de données, de gestion de trafic et la fonction d'observation de la qualité de service.

Le quatrième porte sur la gestion de la facturation, qui concerne la fonction de surveillance de la charge et des coûts des ressources.

Le cinquième se rapporte à la gestion de la sécurité, qui concerne la confidentialité, l'audit et l'enregistrement, et la gestion d'abonnés.



La gestion de réseau est basée sur un modèle tel que représenté ici. Ce modèle a été défini par le Network Management Forum, également connu sous le nom TeleManagement Forum ou TM Forum, une entité de l'OSI, et est basé sur un modèle client-serveur.

Le client est le système de gestion de réseau, ou Network Management System, le Manager, qui produit la demande de gestion de réseau.

Le serveur est un logiciel de gestion présent sur l'entité à gérer. Appelé agent, il a pour rôle de répondre aux demandes du Manager.

L'agent proxy traduit la demande du Manager en quelque chose qui sera compris par l'entité.

D'après OSI, les informations de gestion sont documentées à l'aide d'un ensemble de formulaires, appelés GDMO pour Guidelines for Definition of Manager Objects.

Les protocoles permettant les échanges entre Manager et Agent dépendent de l'environnement de travail. On peut citer CMIP, Common Management Information Protocol, dans le monde OSI et SNMP, Simple Network Management Protocol dans le monde TCP/IP.