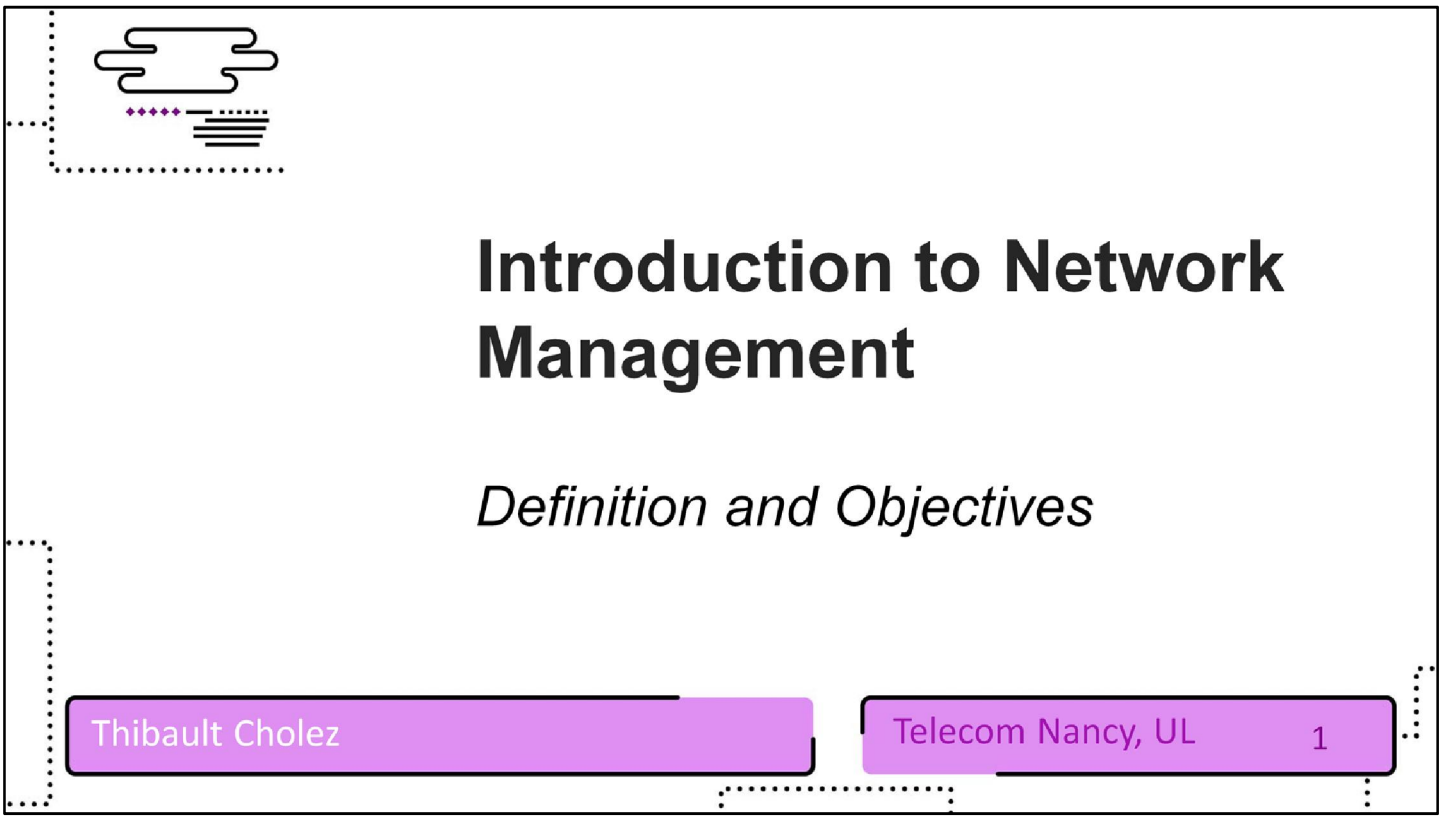
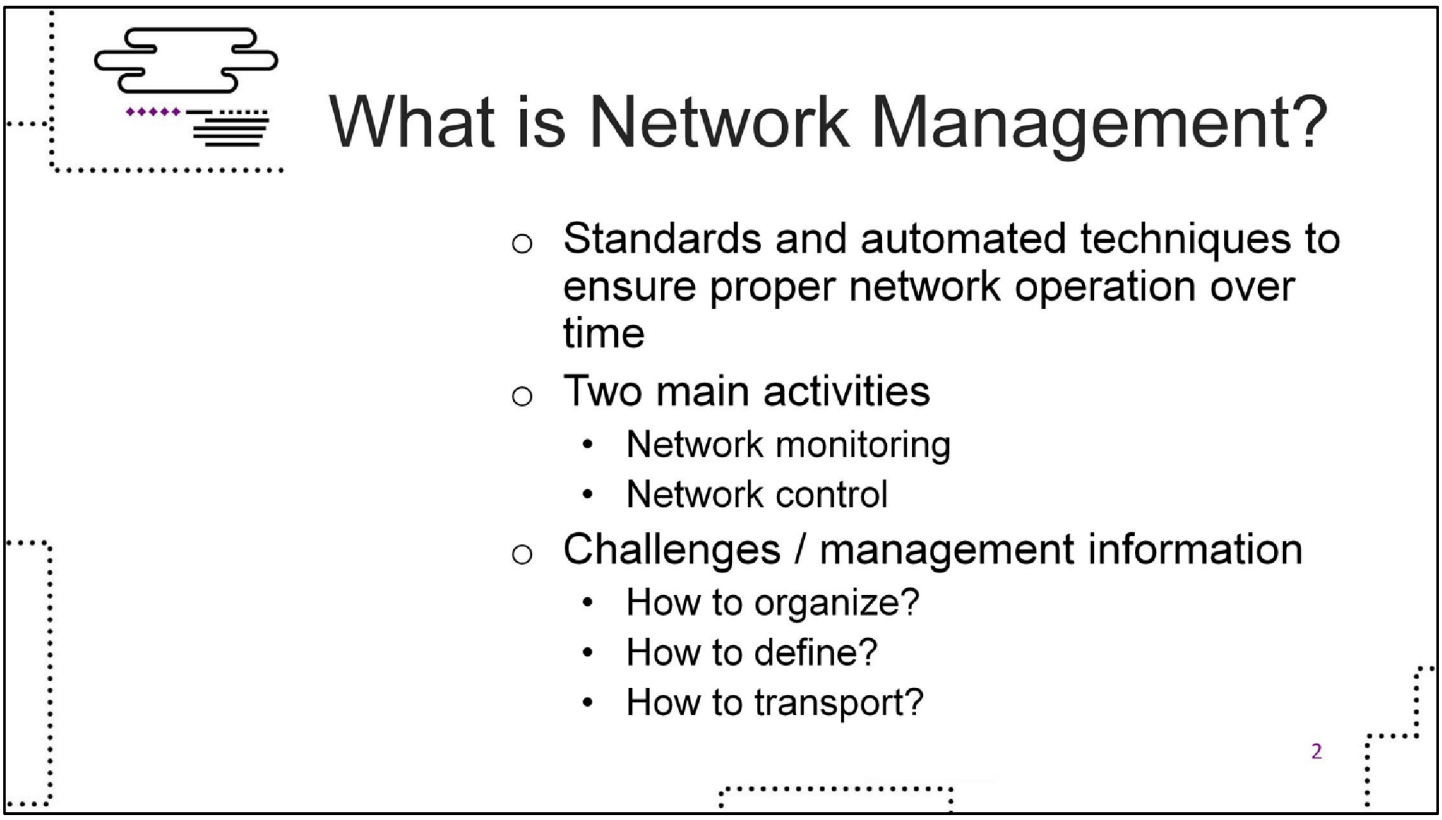


Nous allons découvrir, lors de cette première semaine d'introduction, quels sont les objectifs de la gestion de réseaux.

Nous allons notamment appréhender les différents objectifs de ce domaine à travers les aires fonctionnelles de la gestion de réseaux, puis nous les illustrerons à travers plusieurs interviews de professionnels.

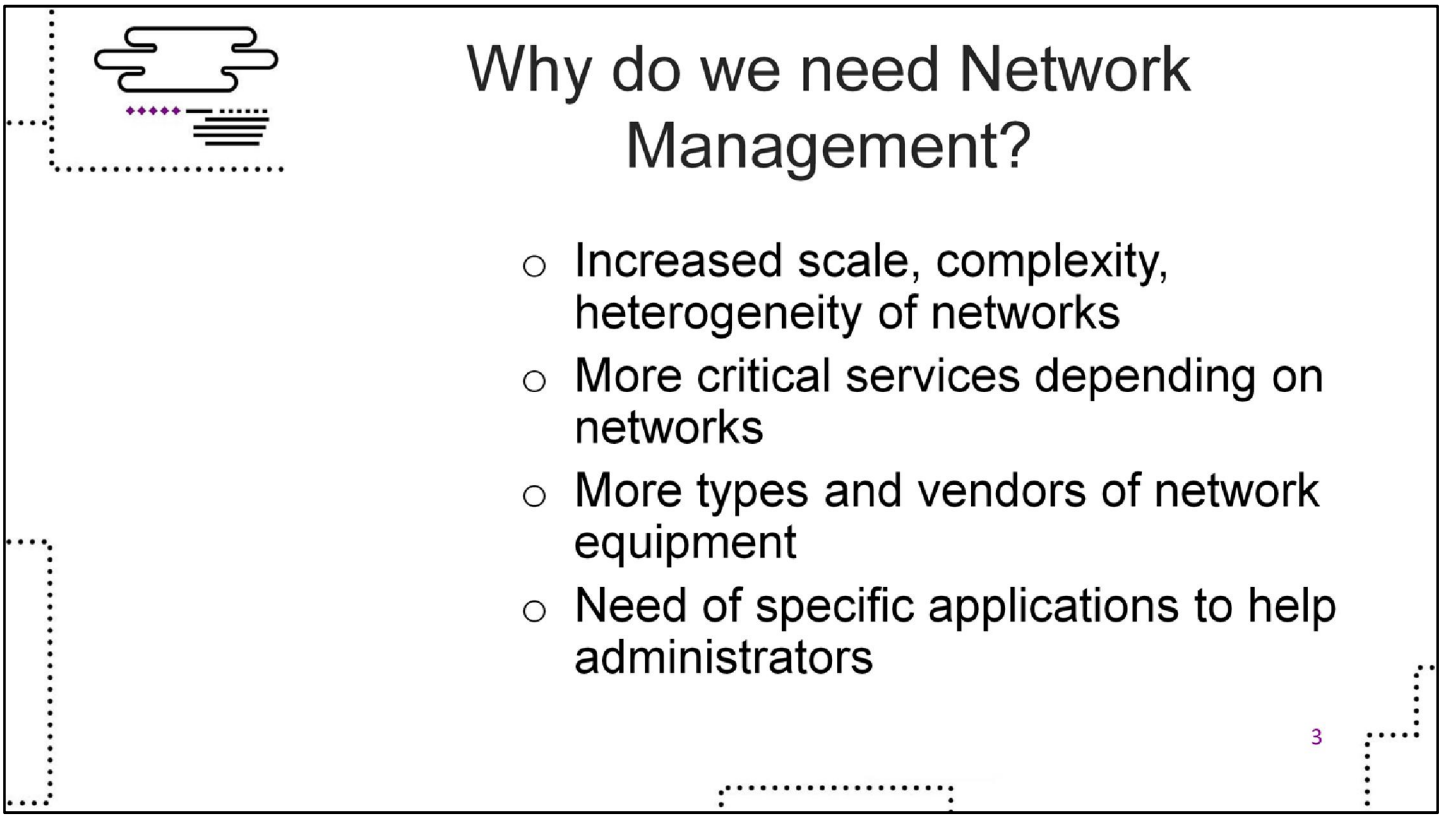


Pour commencer, qu'est-ce que la gestion de réseaux ?
La gestion de réseaux est définie par l'ensemble des normes et des techniques automatisées permettant d'assurer un bon fonctionnement du réseau au fil du temps.

Elle est constituée de deux activités principales :
- la supervision de réseau, qui consiste à collecter des informations sur l'état et le fonctionnement des nœuds;
- le contrôle du réseau, qui consiste à changer des paramètres de configuration.

Ces activités ont vocation à être automatisées autant que faire se peut, par exemple, en définissant et en exécutant des routines prédéfinies.

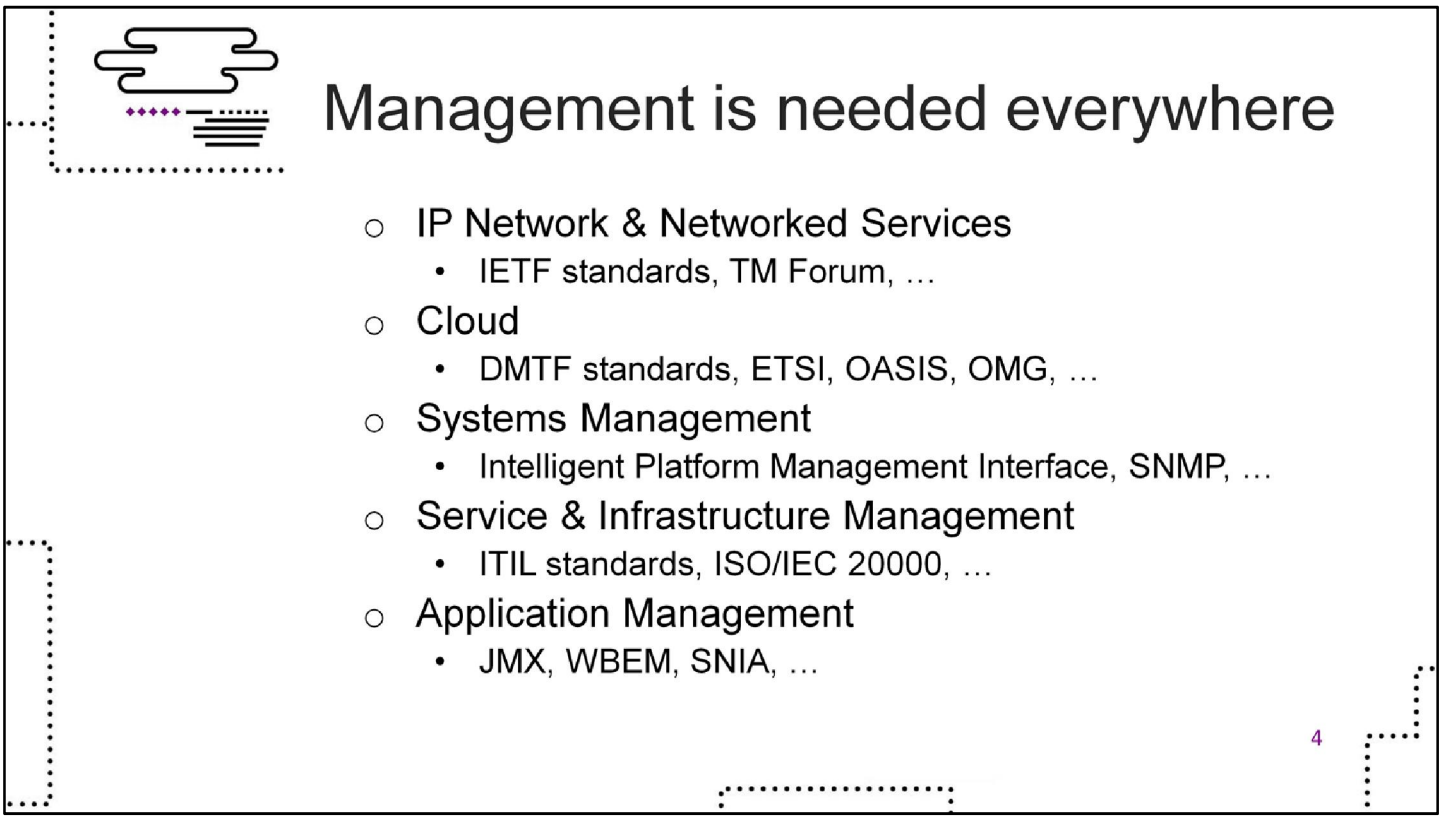
Ce qui nous amène à nous poser trois questions essentielles au sujet des informations nécessaires pour la gestion et qui trouveront leur réponse dans ce cours :
- Comment organiser les informations de gestion ? -> SMI
- Comment en définir de nouvelles ? -> MIBs
- Comment les transporter ? -> SNMP



Pourquoi a-t-on besoin de gestion de réseaux ?

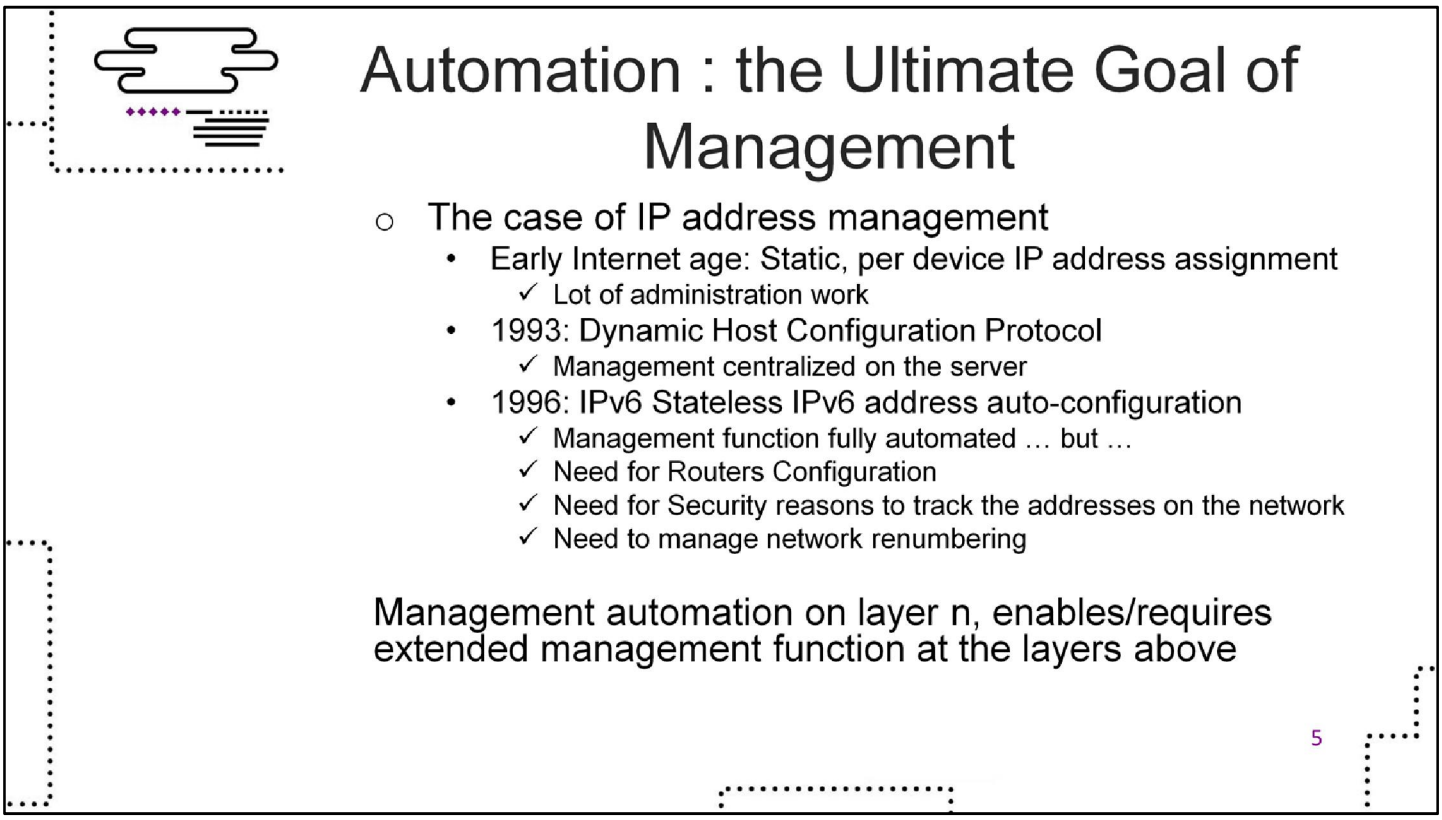
Le développement de l'informatique a induit une augmentation de la taille, de la complexité, et de l'hétérogénéité des réseaux informatiques. Par exemple récemment, avec le déploiement du très haut débit mobile ou de l'internet des objets.
De nombreux services critiques dépendent des réseaux, et ce, dans de nombreux domaines : la santé, les banques, la sécurité des personnes, etc.

En même temps, le nombre d'équipements et de protocoles a augmenté afin de répondre au divers besoins de communication, ce qui rend la maîtrise des réseaux de plus en plus difficile. Il y a donc besoin d'applications spécifiques pour aider les administrateurs à maîtriser l'exploitation de leur réseau.



De fait, il y a besoin de gestion dans tous les secteurs de l'informatique, qu'il s'agisse des réseaux, des systèmes, des applications, etc. Pour chaque domaine, des organismes sont chargés de définir les standards et les bonnes pratiques appropriés.

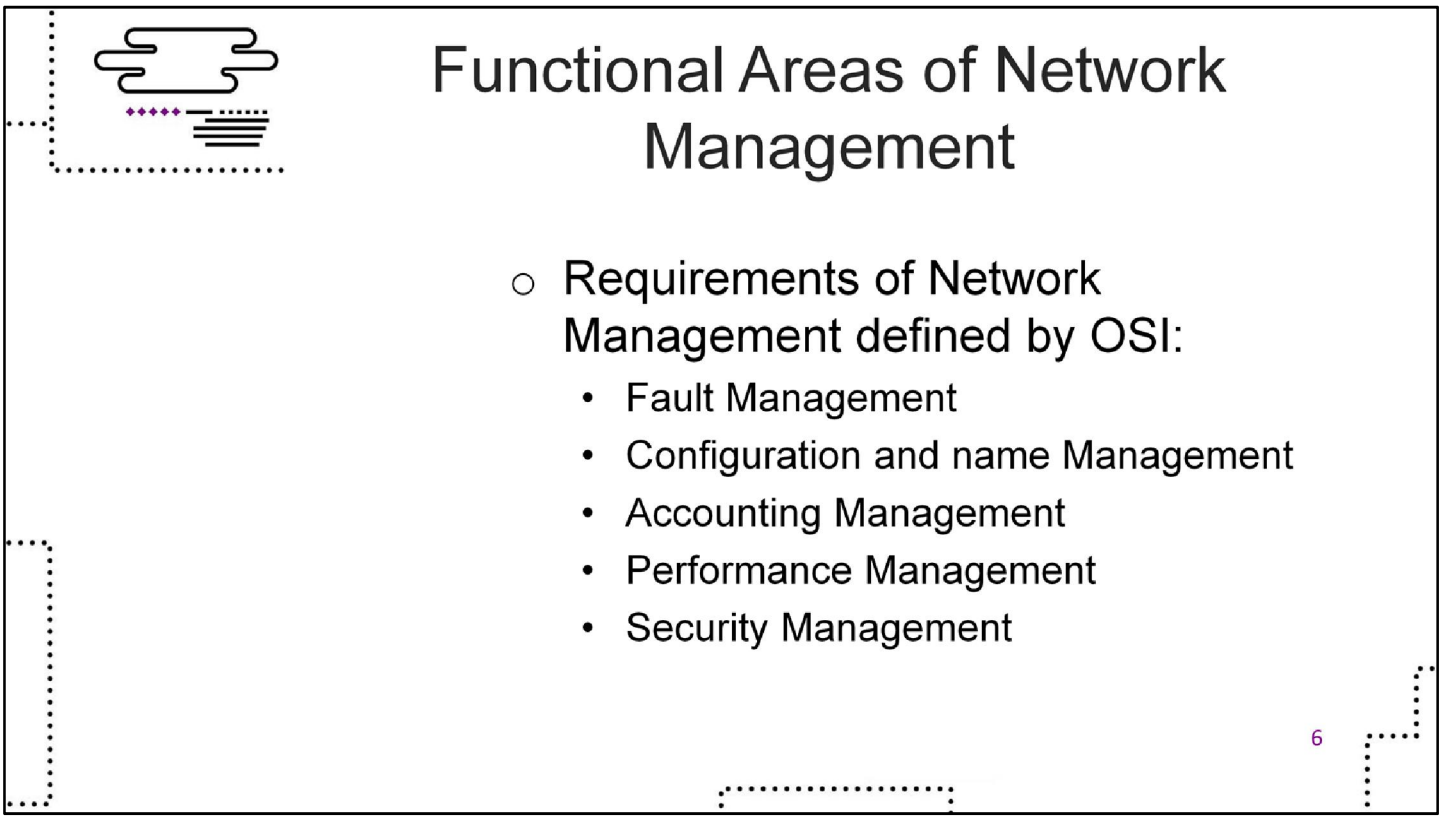
Nous pouvons notamment citer l'IETF (Internet Engineering Task Force), qui s'occupe de définir les standards autour des réseaux IP, ou encore l'ETSI (European Telecommunications Standards Institute) qui est très actif dans des domaines émergeants comme le cloud ou la 5G.



L'automatisation est donc le but ultime de la gestion de réseaux.
Nous pouvons prendre l'exemple de la configuration des adresses IP, qui illustre bien le besoin croissant de gestion et d'automatisation.

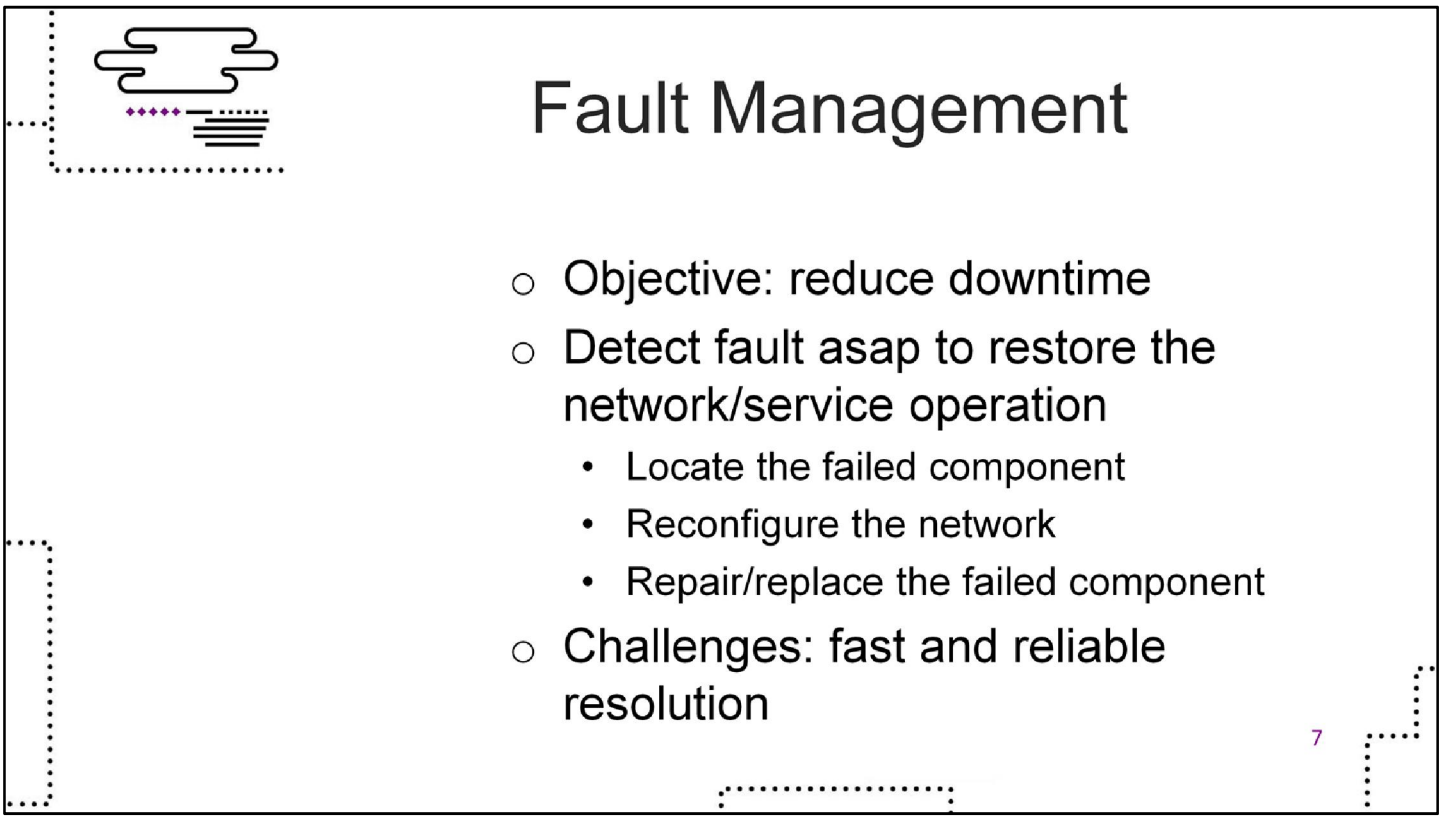
Au début d'Internet, les adresses IP étaient statiques et assignées manuellement à chaque équipement, ce qui engendrait une charge importante d'administration, incompatible avec la croissance rapide des réseaux. En 1993 a été créé le protocole DHCP (Dynamic Host Configuration Protocol) qui a permis de centraliser sur un serveur la gestion dynamique des adresses IP. Désormais, avec IPv6, la configuration des adresses IP peut se faire automatiquement avec ICMPv6 et n'a plus besoin de protocole externe. Néanmoins, d'autres besoins ne sont pas couverts et nécessitent encore des outils spécifiques, tels que la configuration des routeurs, la sécurité, etc.

L'automatisation au niveau d'une couche N du modèle OSI ne rend donc pas la gestion caduque mais permet en réalité d'accroître les possibilités de gestion des couches supérieures.



Une manière de bien comprendre à quoi sert la gestion de réseaux est de considérer ses principaux objectifs tels que définis par l'OSI, aussi appelés « aires fonctionnelles ». Il y a la gestion de fautes, la gestion de la configuration et des noms des équipements, la gestion de la volumétrie, la gestion des performances, et enfin, la gestion de la sécurité. L'acronyme « FCAPS », obtenu en prenant la première lettre de chaque objectif permet de retenir plus facilement les aires fonctionnelles.

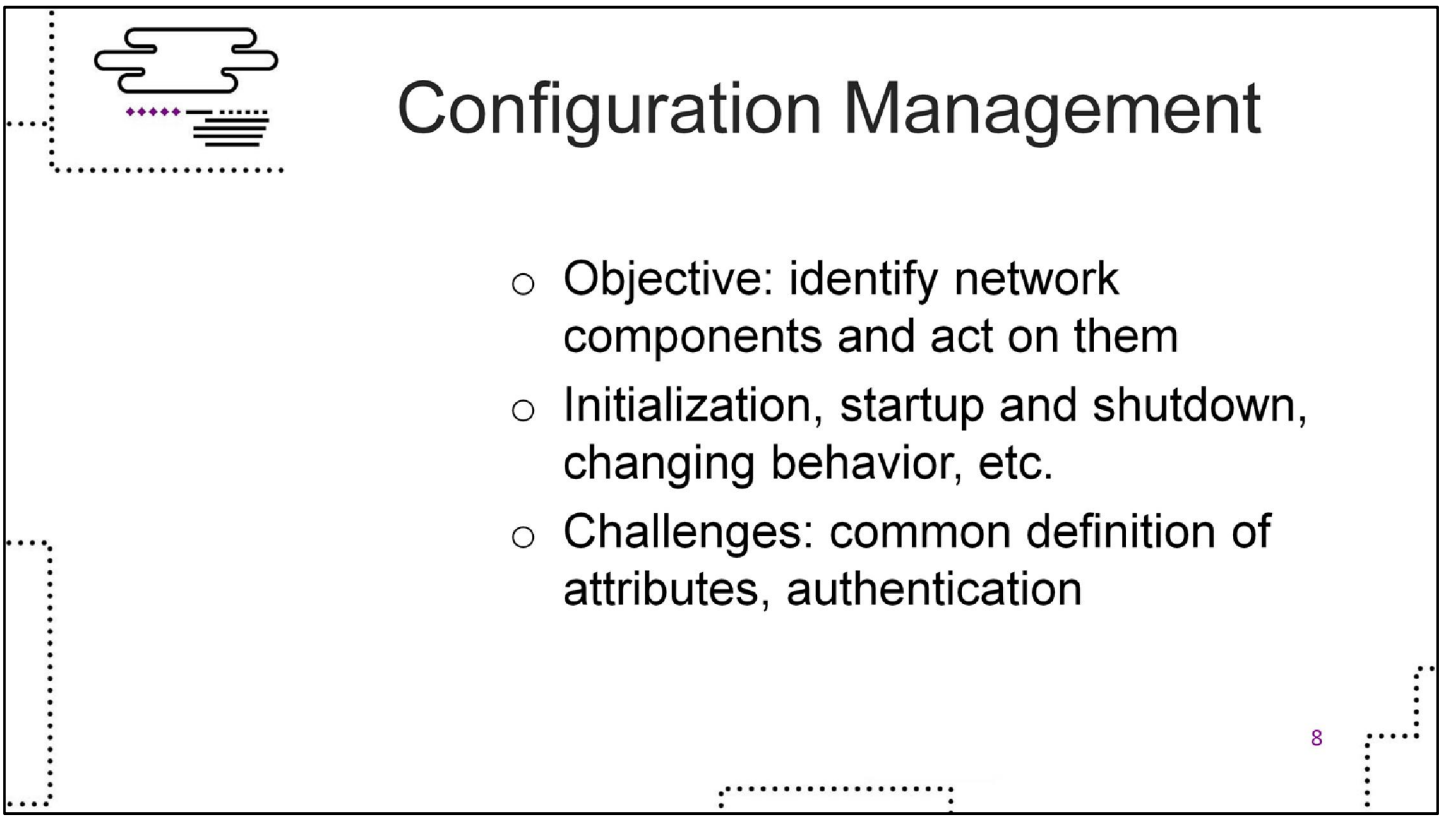
On remarquera que les 3 premiers objectifs « FCA » sont davantage orientés supervision, alors que les deux derniers « PS » sont davantage orientés contrôle. Nous allons maintenant passer en revue chacune de ces aires fonctionnelles pour bien comprendre leurs enjeux.



L'objectif de la gestion de fautes est de réduire le temps d'arrêt du système dû à un problème. Il convient de faire la distinction entre une faute et une erreur. Une erreur est un évènement isolé qui n'implique pas forcément un danger pour le système. Une faute, quant à elle, est une condition anormale nécessitant une intervention et engendrant des erreurs dans le système.

La gestion de fautes consiste donc à détecter dès que possible quand une faute se produit afin de rétablir au plus vite le fonctionnement du système. Cela implique par exemple de 1) localiser un équipement fautif, 2) reconfigurer le réseau pour pallier la défaillance, et 3) remplacer l'équipement fautif. Pour faciliter la gestion de faute, il faut notamment prévoir de la redondance pour les équipements et les services critiques.

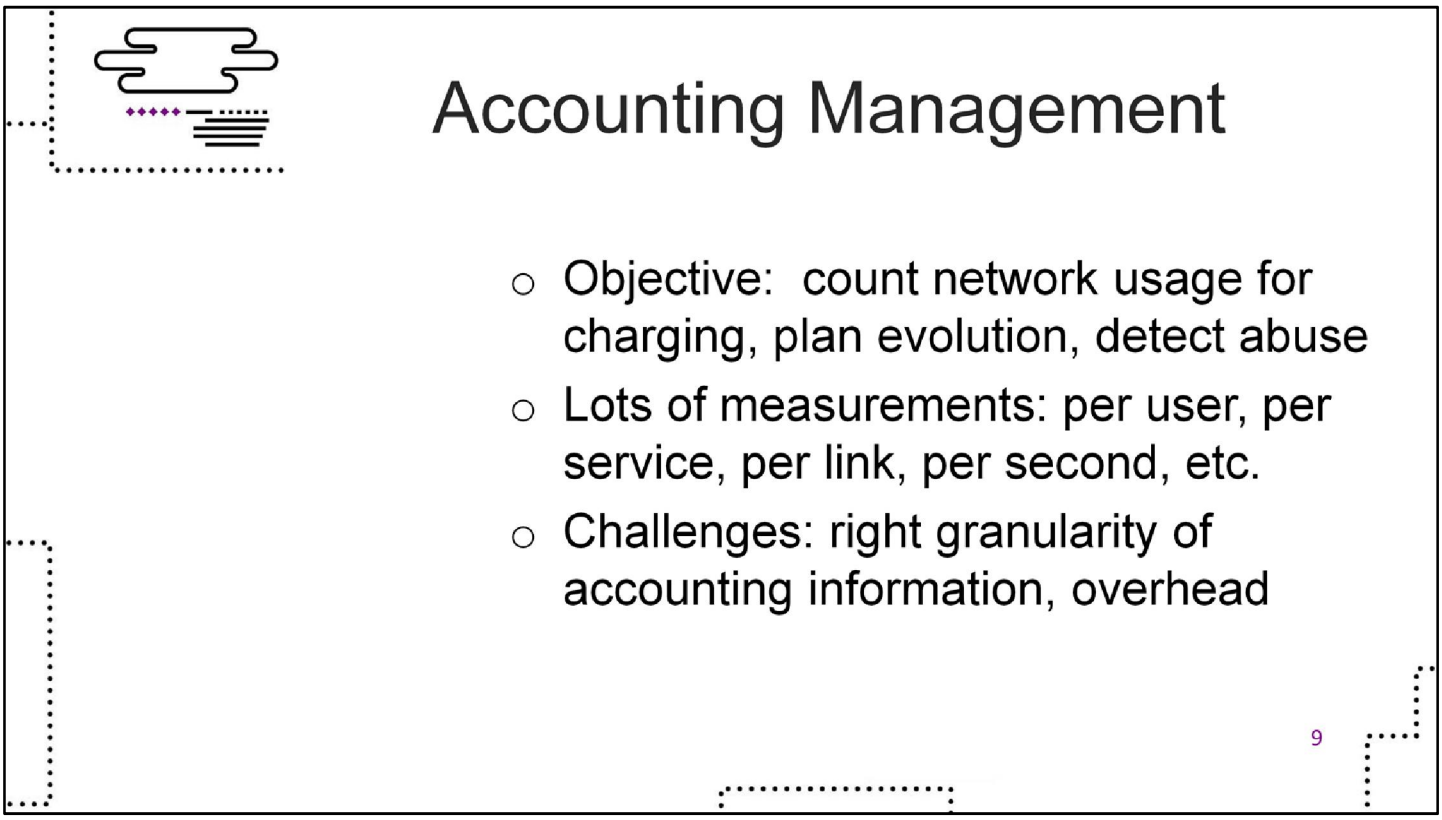
Le défi lié à cet objectif est d'avoir une résolution rapide et fiable des fautes. Un des problèmes est de pouvoir remonter l'information de supervision en cas de fautes lorsque le réseau lui-même est défaillant. C'est pour cela qu'en général un réseau spécifique est dédié au management.



Le second objectif concerne la gestion de la configuration et des noms des équipements. Il s'agit d'être capable d'identifier précisément un équipement réseau et de pouvoir agir dessus.

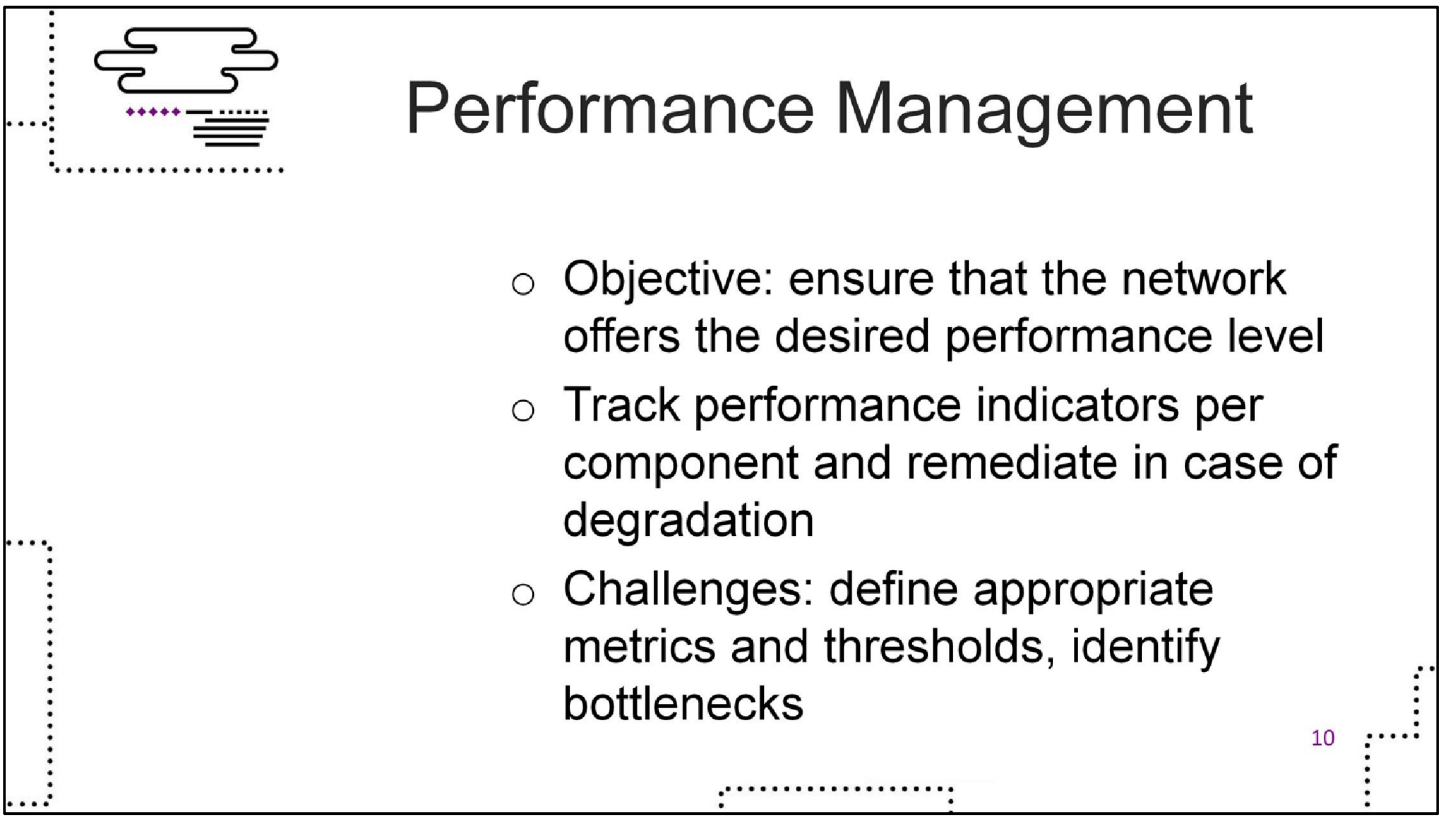
Les actions à effectuer sur un équipement peuvent être diverses à commencer par le chargement des configurations pré-établies pour initialiser le réseau. Il y a bien sûr d'autres actions essentielles comme le fait de pouvoir démarrer ou arrêter un équipement à distance.

Les défis concernent ici deux aspects. D'une part, la définition standardisée des attributs d'un type d'équipement sur lesquels un administrateur peut agir, par exemple : comment définir la table de routage d'un routeur ? D'autre part, l'authentification préalable à la réalisation des actions de configuration car celles-ci peuvent avoir un impact important sur le réseau.



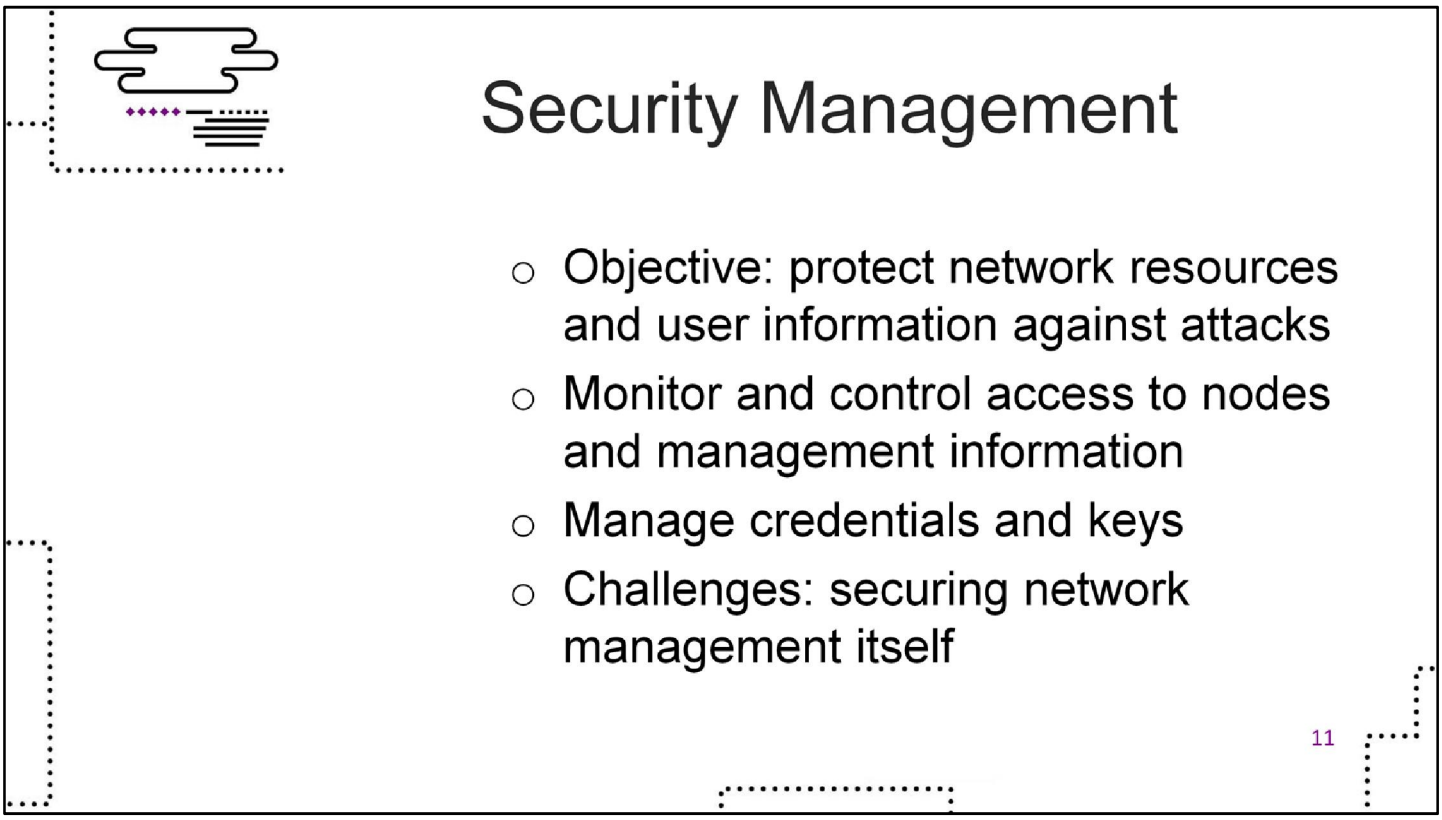
La gestion de la volumétrie a pour but de pouvoir comptabiliser précisément les diverses utilisations du réseau, et ce, à plusieurs fins tel que le fait de faire payer certains usages – on pense notamment aux fournisseurs d'accès à internet – sinon pour anticiper l'évolution de l'infrastructure lorsque l'on constate que l'on s'approche régulièrement de la capacité maximale, ou encore pour détecter des abus comme les dénis de services.

Cela implique d'effectuer de nombreuses mesures, potentiellement par utilisateur, par service, par lien, par seconde, etc. On perçoit rapidement quel va être tout l'enjeu de la gestion de la volumétrie, à savoir comment obtenir une granularité des mesures suffisante pour les besoins opérationnels, tout en essayant de contenir le surcoût lié à la supervision : à la fois le surcoût CPU pour traiter les informations, mais aussi le surcoût réseau pour remonter les mesures au gestionnaire.



La gestion des performances doit garantir le fait que le réseau offre en permanence le niveau de performance adéquat. Cela implique de suivre de nombreux indicateurs de performance au niveau des équipements et d'agir en cas de dégradation constatée des performances. Il existe de nombreux indicateurs généraux des performances d'un réseau tels que le débit, la latence, le taux de perte de packets, le taux de retransmission, etc. Et encore bien d'autres métriques spécifiques à tel ou tel service en particulier.

Les défis ici sont de définir les indicateurs à suivre et les seuils d'alerte, afin d'identifier les goulots d'étranglement et de pouvoir y remédier.
Un exemple d'action peut être le fait d'effectuer un changement dans des tables de routage pour améliorer la répartition de charge entre des équipements. La gestion des performances permet également de prévoir les évolutions et les investissements à venir quand la limite des performances est régulièrement atteinte.



Pour finir, la gestion de la sécurité vise à protéger les ressources du réseau et les informations des utilisateurs contre les attaques informatiques.
Les attaques peuvent être passives, comme l'interception et l'analyse de trafic en un point par un attaquant, ou actives, comme les dénis de services, l'usurpation d'identité, ou l'envoi de paquets forgés.

Dans ce contexte, la gestion de la sécurité consiste principalement à gérer les droits et les clés d'accès aux nœuds du réseau et aux informations de gestion, et à superviser et contrôler les accès en analysant les logs des équipements. Un des défis ici est de pouvoir sécuriser la gestion du réseau elle-même puisqu'elle permet de nombreuses opérations critiques.

Nous avons donc vu en quoi la gestion de réseaux est nécessaire aujourd'hui et les objectifs auxquels elle doit répondre à travers la description des aires fonctionnelles FCAPS (Fault, Configuration, Accounting, Performance, Security). Celles-ci sont illustrées par des interviews de professionnels dans la suite de ce cours.