Administration réseaux

Christian Bulfone
christian.bulfone@gipsa-lab.fr
www.gipsa-lab.fr/~christian.bulfone/MIASHS-L3

Master MIASHS L3
Année 2021/2022

Administration réseaux

- Ensemble des moyens mis en œuvre
  - pour garantir l'efficacité du système et sa disponibilité,
  - pour assurer la surveillance des coûts et la planification des évolutions
- L'administration d'un réseau suppose l'existence d'une base d'information décrivant l'ensemble des objets administrés
  - Grand nombres d'objets concernés
  - Nécessite un dialogue entre les composants

Administration réseaux

- L'ISO définit 5 domaines d'administration
  - Gestion des configurations
    - Paramétrage des équipements et de la topologie
  - Gestion des performances
    - Mesures, statistiques de la charge, des flux et des erreurs
  - Gestion des pannes
    - Détection et localisation des défaillances et contournement
  - Gestion de la comptabilité
    - Recensement, facturation, rentabilisation, contrat de maintenance
  - Gestion de la sécurité
    - Protection du réseau et des utilisateurs contre les intrusions et malveillances

Gestion des configurations

- Consiste à maintenir un inventaire précis des ressources matérielles (type, équipement,. . .) et logicielles (version, fonction,. . .)
- Connaître la répartition géographique des équipements gérés

Gestion des performances

- Mettre en œuvre des moyens permettant d'évaluer le comportement des objets gérés
- Déterminer si la qualité de service (QoS) est rendue aux utilisateurs
- On retrouve aussi :
  - La collecte d'information (audit)
    - Mesure de trafic
    - Temps de réponse
    - Taux d'erreurs
  - Le stockage (archivage)
  - L'interprétation des mesures (calcul de charge)

Gestion des pannes

- Optimisation des ressources et des moyens
- Diagnostic rapide de toute défaillance (externe, coupure d'un lien public, ou interne, panne d'un routeur)
- On retrouve aussi :
  - Surveillance et traitement des alarmes
  - Localisation et diagnostic des incidents
  - Mémorisation des anomalies (journalisation)
  - Définition des opérations curatives

Gestion de la comptabilité

- Cette fonction permet essentiellement d'imputer les coûts du réseau à ses utilisateurs selon l'usage réel des moyens (comptabilité analytique)
- On retrouve :
  - Définition des centres de coût
  - Mesure des dépenses (structure) et répartition
  - Mesure des consommations par service
  - Imputation des coûts

Gestion de la sécurité

- Regroupe tous les domaines de la sécurité afin d'assurer l'intégrité des informations traitées et des objets administrés
  - Contrôle d'accès au réseau
  - Confidentialité des données
  - Intégrité des données
  - Authentification
  - Non désaveu

Supervision de réseaux : le protocole SNMP

- SNMP (*Simple Network Management Protocol*)
  - Protocole créé en 1988 par l'IETF (*Internet Engineering Task Force*) pour répondre aux besoins d'administration du réseau Internet
- Objectifs de SNMP
  - Fédérer en un standard unique des protocoles multiples liés aux équipementiers
  - Déploiement rapide et à moindre coût

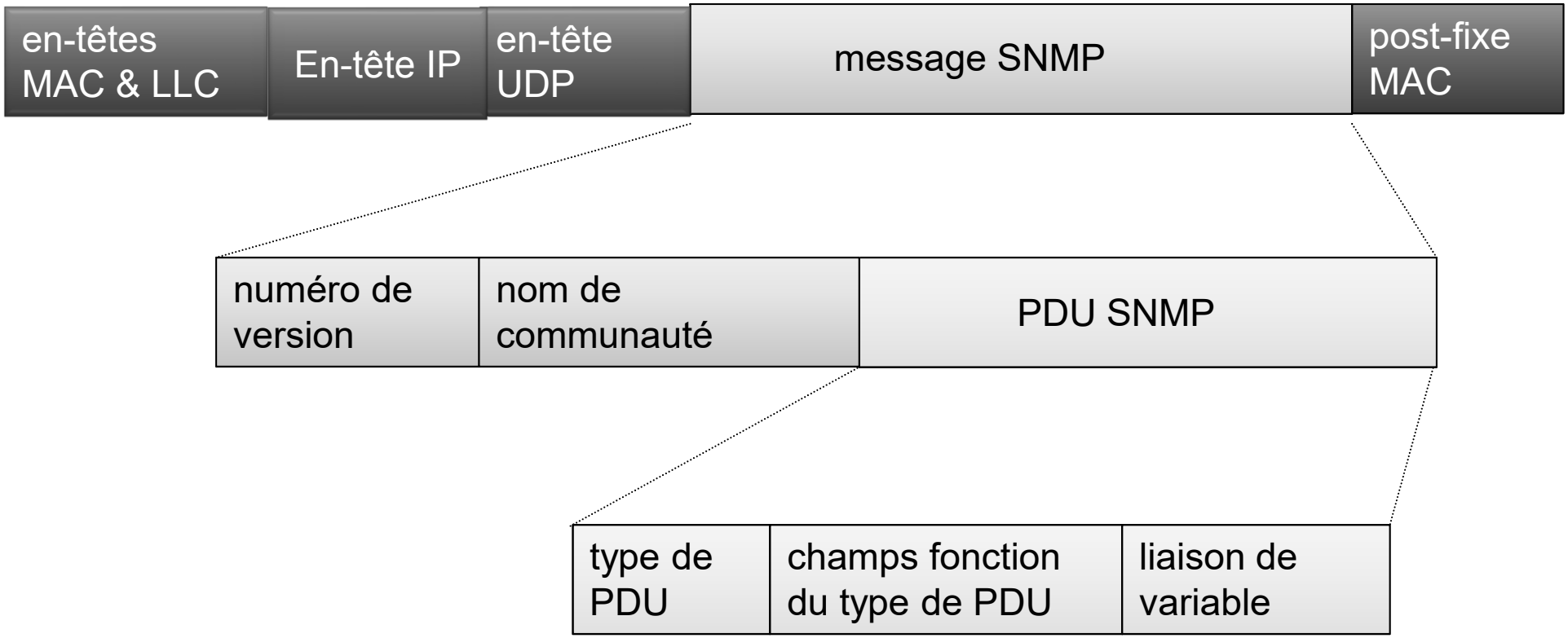
Supervision de réseaux : le protocole SNMP

- Permet aux administrateurs réseau
  - de gérer les équipements du réseau
  - de surveiller leur comportement
- Chaque élément potentiellement administrable est doté d'un **agent**
  - Programme fonctionnant sur un élément réseau (commutateurs, routeurs) et/ou stations de travail et serveurs
- Tous les agents sont contrôlés par une (ou des) **station(s) d'administration** ou station(s) maîtresse(s) (NMS : *Network Management System*)
- Les informations d'administration d'un élément du réseau sont stockées dans une structure arborescente appelée **MIB** (*Management Information Base*)

Le protocole SNMP

- SNMP est défini par 3 principaux RFC (1157, 1213 et 1155)
- Le protocole est basé sur l'échange de messages (requêtes et réponses) entre l'élément réseau à surveiller et la station d'administration
- Les messages SNMP sont encapsulés dans des paquets UDP (numéros de port 161 et 162)
  - Avantage : simplicité et peu de puissance nécessaire pour faire fonctionner l'agent
  - Inconvénient : protocole non fiable
    - Une écriture sera suivie d'une lecture de la valeur pour vérification
    - En cas de non réponse, la requête est réitérée

Format des données en SNMP



Le protocole SNMP

- La station maîtresse (*manager*)
  - Est chargée d'interroger régulièrement les agents
  - Est aussi la destinataire des alertes (*traps)* qui sont générés spontanément par les agents
    - Plus la fréquence d'interrogation est élevée, plus les informations remontées seront détaillées, mais plus le trafic sera important

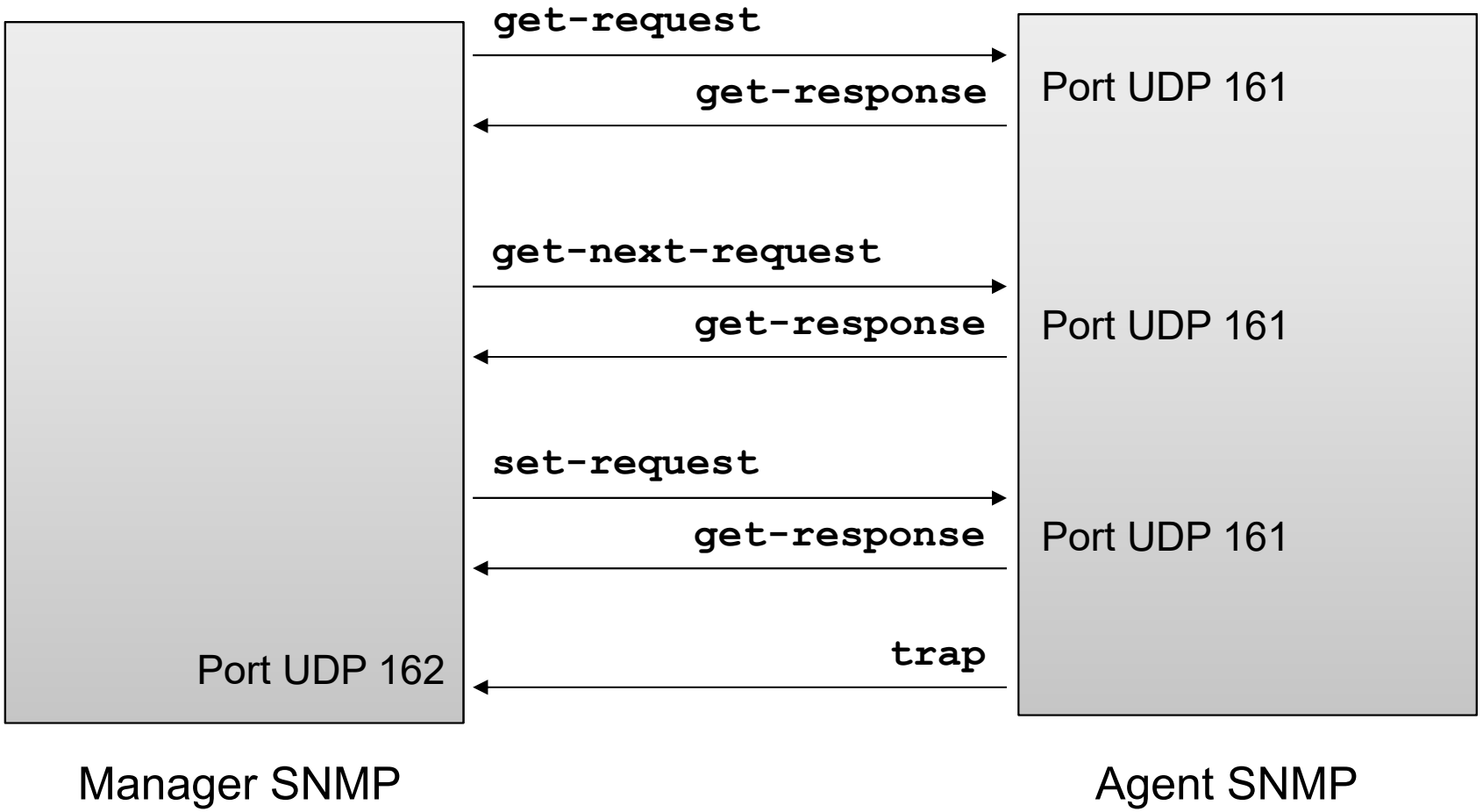
Le protocole SNMP

- Les agents
  - Répondent aux requêtes de la station maîtresse en renvoyant la valeur du paramètre recherché
  - Positionnent des variables aux valeurs qui lui leur sont envoyées
  - Emettent spontanément une alarme lors d'un événement critique
  - Ne peuvent fonctionner que sur un CPU ou avec des extensions dédiées
  - Possèdent des noms de communauté (« public » par défaut) pour se protéger des requêtes de lecture ou d'écriture indésirables

Le protocole SNMP

- 5 types de messages ou requêtes SNMP peuvent être échangés (SNMPv1) entre agent et manager
  - Get Request
    - demande de la valeur courante de la variable indiquée
  - Get Next Request
    - demande de la valeur « suivante » dans l'arborescence
  - Get Response
    - envoi de la valeur demandée
  - Set Request
    - configuration d'une variable à la valeur indiquée
  - Trap
    - indication autonome de l'agent

Le protocole SNMP



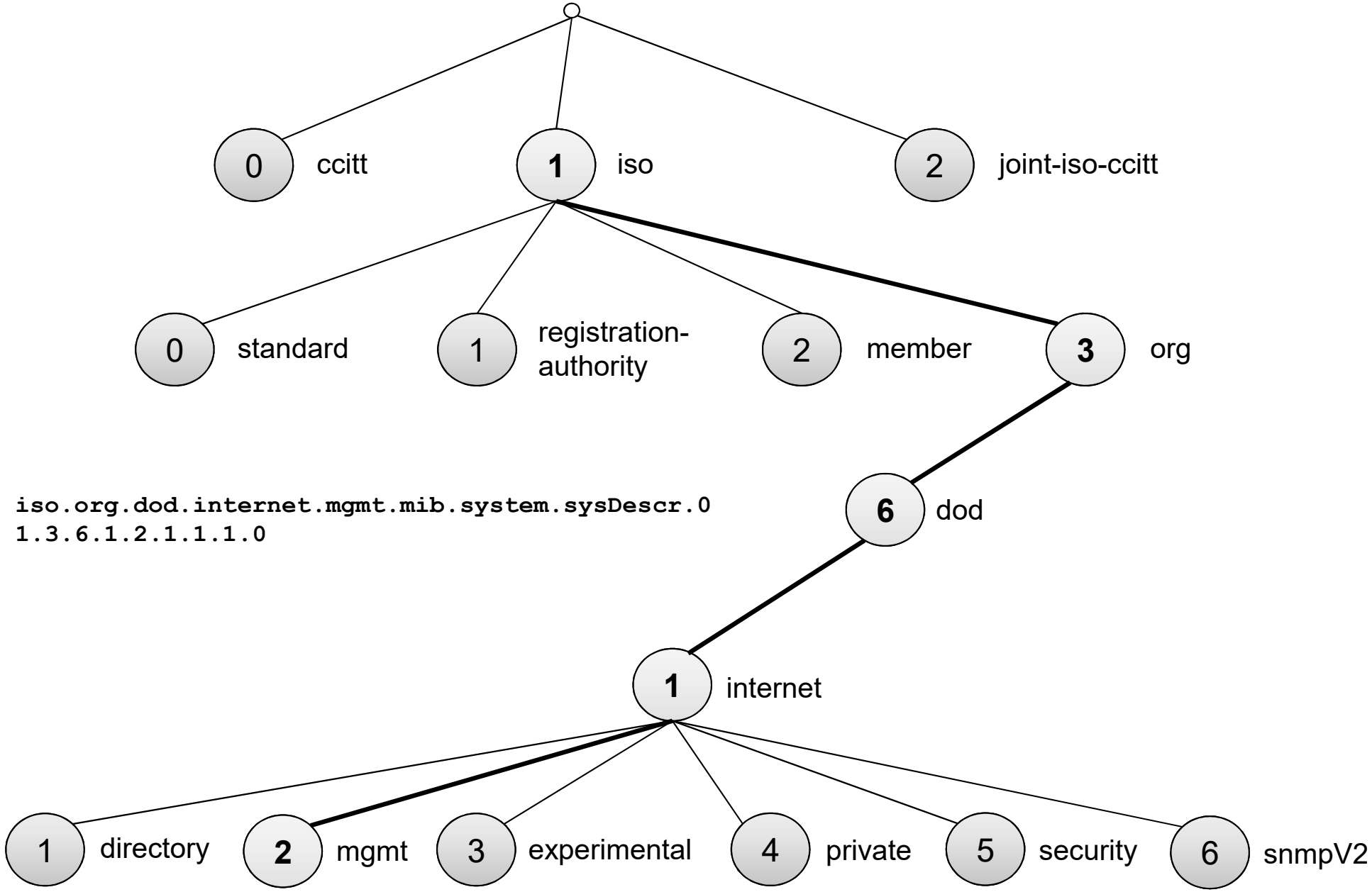
Le protocole SNMP

- MIBs
  - Stockent les informations d'administration d'un élément du réseau sous **forme arborescente**
  - Chaque objet de la MIB
    - possède un identificateur unique ou OID (*Object ID*)
    - se conforme au codage ASN.1 (*Abstract Syntax Notation*) de l'ISO et peut être de différents formats (numérique entier, suite de bits, suite d'octets, nul, identificateur d'objet, séquence de)
  - Une partie de la MIB, la MIB-II, doit toujours être présente
  - De multiples MIB ont été définies en complément
    - Par technologies : Ethernet, Token-Ring, FDDI, 100VG-AnyLan, X.25 …
    - Par équipements : répéteur Ethernet, Bridge, Source-Route bridge, sonde
    - Par protocole : BGP-4, PPP, RIP-2, OSPF, DNS, AppleTalk, DECnet …

Le protocole SNMP

- Structure de la MIB
  - Se compose d'une racine non nommée à partir de laquelle sont référencés de façon absolue les objets (nœuds de l'arbre)
  - Chaque nœud de l'arbre possède un **nom symbolique**
  - Chaque objet peut être identifié de façon symbolique ou en utilisant son OID

Structure de la MIB



iso.org.dod.internet.mgmt.mib.system.sysDescr.0
1.3.6.1.2.1.1.1.0

Logiciels de supervision

- Ont pour tâche de mettre en œuvre tous les mécanismes génériques autour de SNMP
  - enregistrement (log) avec filtrage divers et déclenchement d'actions sur événement (trap reçu)
  - découverte du réseau (IP) et maintient d'une base de données des éléments découverts (adresses MAC, adresses IP, type d'équipements …)
  - surveillance minimale de la présence de ces éléments (polling périodique)
  - aide à la construction de graphes par interrogation de variables spécifiques
  - mise en œuvre de script combinant polling, conditions et actions

Logiciels de supervision

- Auto-découverte
  - Ne consiste pas à localiser physiquement les machines, mais à connaître leur existence par
    - **écoute** des adresses réseau qui communiquent
    - **interrogation** des adresses potentielles à l'aide de **ping**
    - **interrogation SNMP**
      - requête Get sur une valeur élémentaire de la MIB II (par exemple sysObjetctID dans System)
  - Processus tournant sans arrêt en tâche de fond
  - Prise en compte dynamique de
    - l'apparition des nouveaux nœuds dans le réseau
    - la disparition (temporaire ou non) de certains autres (signalée par une alarme)

Logiciels de supervision

- Plusieurs logiciels d'administration disponibles
  - Commerciaux
    - OpenView d'HP
    - Tivoli Netview d'IBM
    - PRTG de Paessler
    - WhatsUp Gold d'Ipswich
  - Open source
    - Zabbix
    - Zenoss
    - Nagios
    - ...

SNMP et sécurité

- Les versions SNMP 1 et 2c ne sont pas sûres
  - Les trames circulent en clair sur le réseau, le nom de communauté peut être facilement récupéré
  - Même si l'agent est paramétré pour ne répondre qu'à certaines adresses IP, le spoofing d'adresse IP est possible ; il n'y a pas de notion d'*« utilisateur authentifié »*
- La version 3 de SNMP a été créée pour résoudre ce problème
- Composants
  - Dispatcher (répartiteur)
  - Sous-système de traitement des messages
  - Sous-système de sécurité
  - Sous-système de contrôle d'accès

SNMP version 3 (SNMPv3)

- Le module le plus commun repose sur l'utilisateur ou un « modèle de sécurité utilisateur »
  - **Authenticité et intégrité** :
    - des utilisateurs peuvent être créés, chacun disposant d'un identifiant et d'un mot de passe personnel
    - les messages ont une signature numérique générée par hachage (MD5 ou SHA)
  - **Confidentialité** :
    - les messages peuvent être chiffrés au moyen d'un algorithme (DES) à clé secrète (privée)
  - **Validité temporaire** :
    - Utilise une horloge synchronisée avec une fenêtre 150 secondes et contrôle de séquence pour éviter toute tentative de rejoue (« replay attack »)

Niveaux de sécurité

- **noAuthPriv**
  - Pas d'authentification, pas de confidentialité
- **authNoPriv**
  - Authentification sans confidentialité
- **authPriv**
  - Authentification avec confidentialité

Métrologie

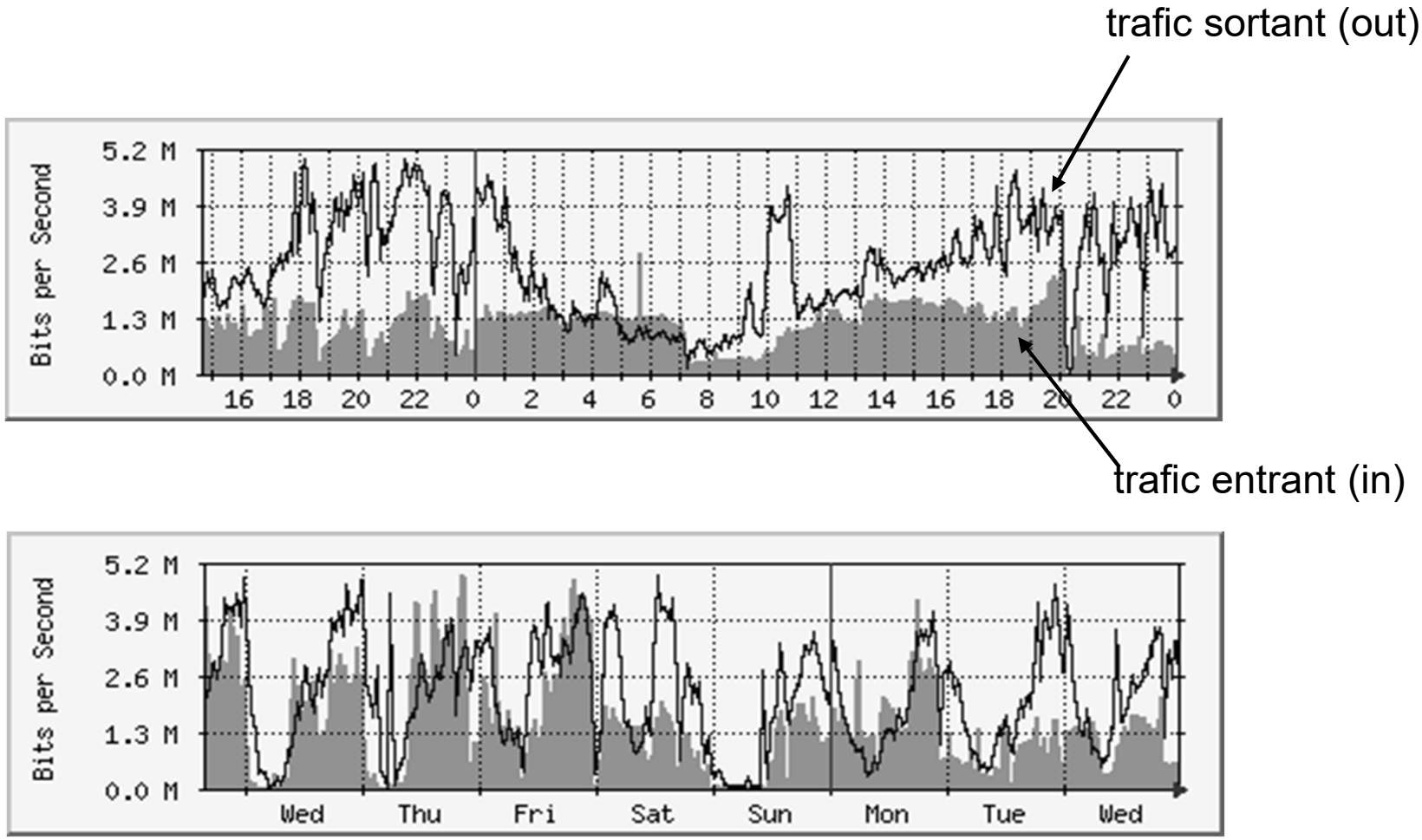
- Par définition, désigne la science des mesures
- Dans le cadre des réseaux informatiques, son objectif est de « connaître et comprendre le réseau » afin de pouvoir
  - intervenir dans l'urgence en cas de problème,
  - anticiper l'évolution du réseau,
  - planifier l'introduction de nouvelle applications,
  - améliorer les performances pour les utilisateurs

Métrologie

- Protocoles utilisés
  - SNMP
    - Récupération à intervalles réguliers des valeurs des compteurs sur les équipements actifs
    - Mise à jour d'histogrammes à partir des données collectées
  - NetFlow
    - Protocole développé par Cisco permettant la comptabilisation de flux réseaux
    - Supporté par la majorité des vendeurs d'équipements réseaux
    - Il existe des protocoles similaires (sFlow chez InMon, LFAP chez Riverstone notamment)

Métrologie

- Programme MRTG



Autres outils

- Protocole HTTP
  - Utilisation d'un navigateur Web comme outil d'interrogation
  - L'agent est plus autonome (mini-serveur Web) mais doit prendre en charge une partie des fonctions de mises en forme des informations
  - Un protocole légèrement mieux adapté que HTTP doit être adopté pour gérer plus complètement les aspects liés à la sécurité (HTTPS par exemple)
- Téléchargement
  - Mise à jour des OS et des fichiers de configuration par TFTP (*Trivial File Transfert Protocol*)

Autres outils

- Telnet/SSH
  - Permet d'accéder à l'interface de configuration des matériels réseau (switch, routeur …)
- Analyseurs de protocoles
  - Logiciel permettant d'intercepter et de décoder le trafic réseau
  - La connexion réseau est placée dans un mode d'opération « libéral » (promiscuous)
    - tous les paquets transitant par le segment du réseau sont acceptés, y compris ceux à destination des autres nœuds
  - Utile pour comprendre les protocoles de réseau et en corriger les dysfonctionnements, mais pose des problèmes de sécurité