



Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre Universitaire de Mila
Institut des Sciences et de la Technologie



Administration des Réseaux

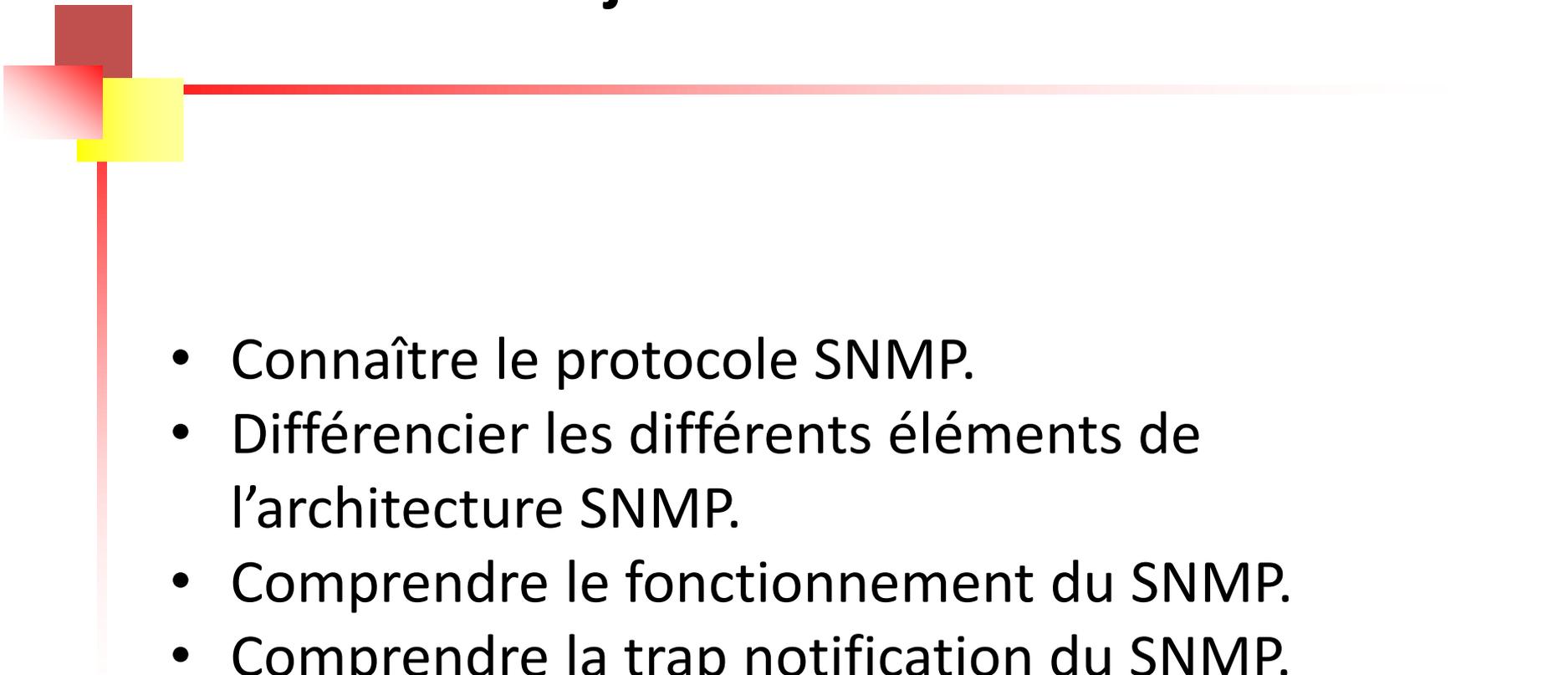
– Chapitre 2 – Le protocole SNMP

Département MI

s.meghzili@centre-univ-mila.dz

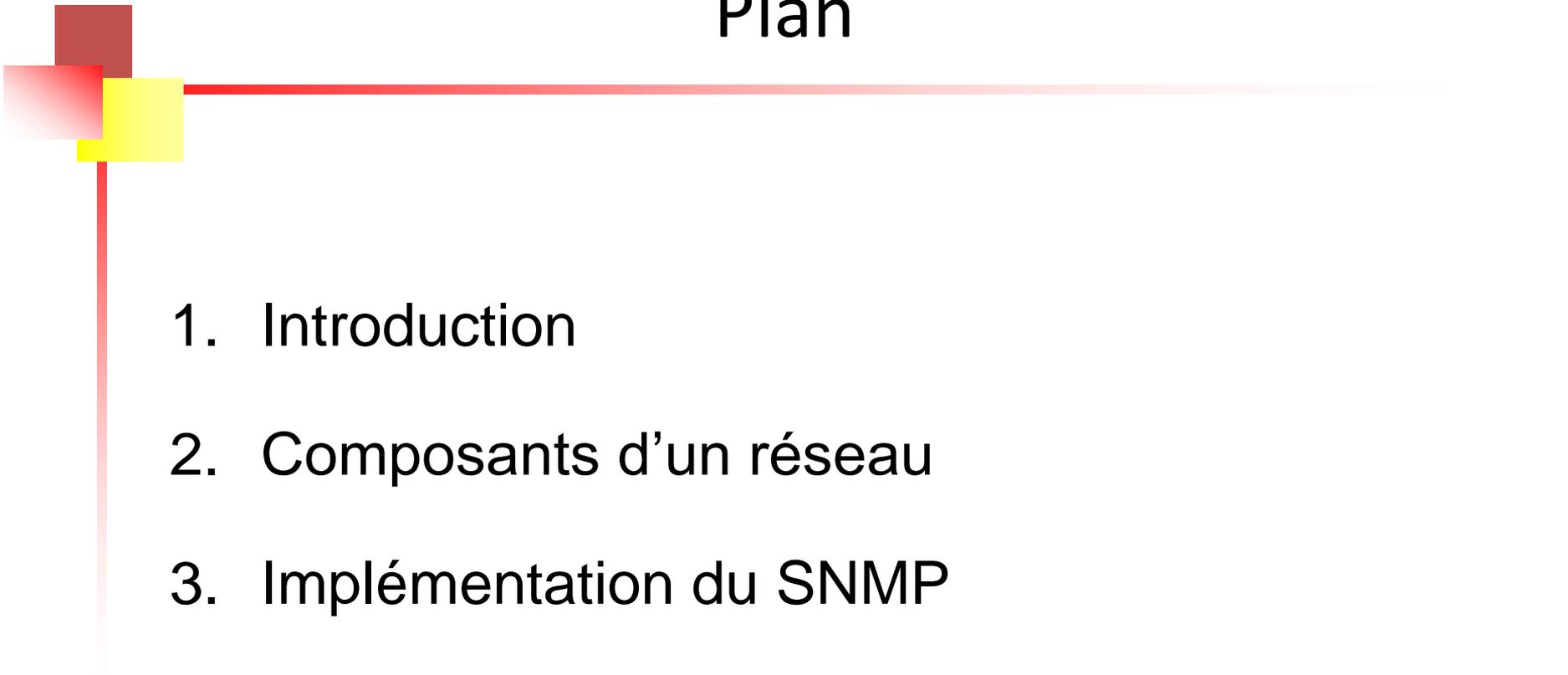


Objectifs du cours



- Connaître le protocole SNMP.
- Différencier les différents éléments de l'architecture SNMP.
- Comprendre le fonctionnement du SNMP.
- Comprendre la trap notification du SNMP.
- Connaître quelques logiciels de supervision.

Plan

A decorative graphic on the left side of the slide. It consists of three overlapping squares: a dark red one at the top, a lighter red one to the left, and a yellow one at the bottom. A horizontal red line extends from the right side of the yellow square across the top of the slide. A vertical red line extends downwards from the bottom of the yellow square.

1. Introduction
2. Composants d'un réseau
3. Implémentation du SNMP
4. Trap notification du SNMP
5. Logiciel de supervision (Monitoring Software)

Qu'est-ce que SNMP?

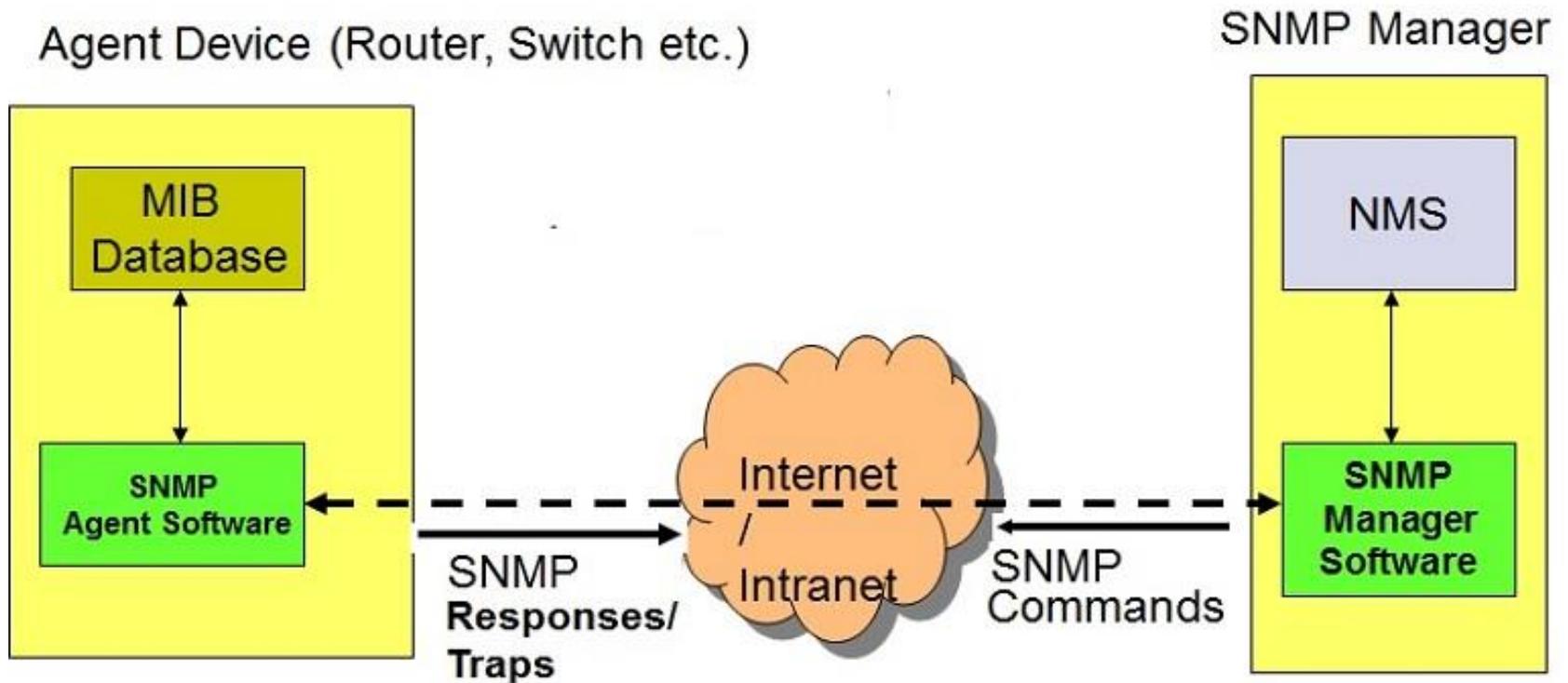
- Protocole Internet standard (Internet standard protocol) défini par IETF (Internet Engineering Task Force).
- Protocole de la couche **application** qui permet de **gérer** des dispositifs (*routeur, commutateurs, imprimantes, etc.*) sur des réseaux **IP**.
- Permet à un manager de:
 - **Récupérer** la valeur d'un **objet** défini au niveau d'un **agent**.
 - **Stocker** une valeur dans un **objet** défini au niveau d'un **agent**.
- Permet à un agent d'**envoyer** des informations d'**alarme** appelées **trap** événements.

Version du SNMP

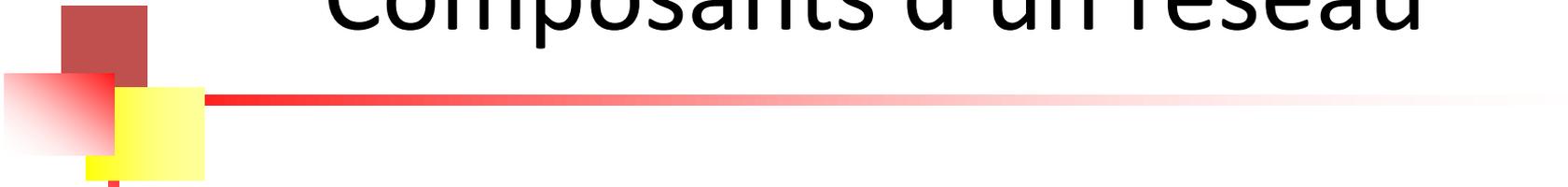
- Plusieurs versions
- SNMPv1 et SNMPv2c :
 - Faible sécurité (insecure).
 - Basée sur des community strings utilisées comme des mots de passe.
- Nouveautés de SNMPv3 :
 - Sécurité
 - Authentification et cryptage
 - Autorisation et contrôle d'accès
 - Administration
 - Nommage des entités
 - Gestion de la comptabilité
 - Destinations des notifications
 - Configuration à distance

Architecture SNMP

SNMP Architecture

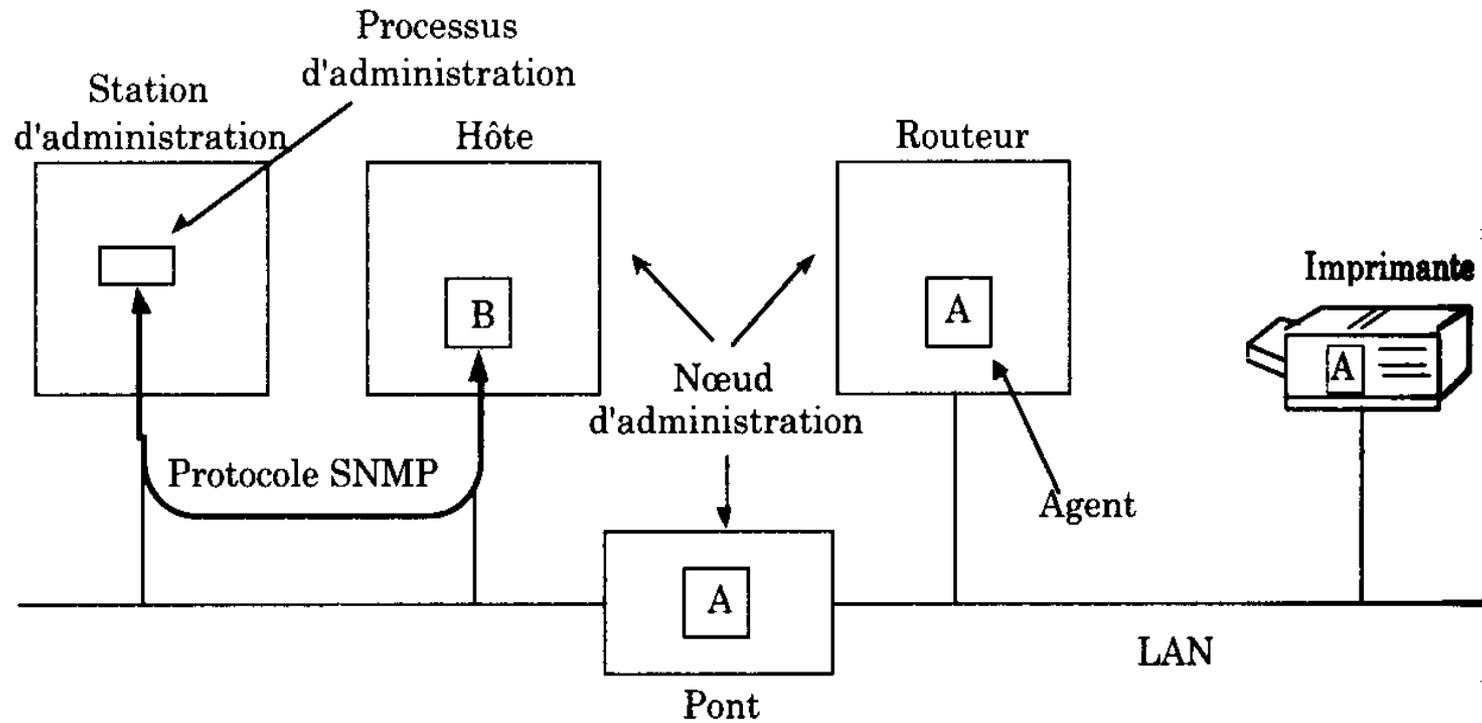


Composants d'un réseau



- **Nœuds** administrés
- **Stations** d'administration
- **Information** d'administration
- **Protocole** d'administration

Exemple: des composants d'un réseau





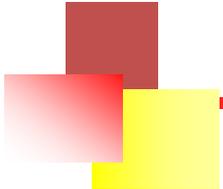
Nœud administré

- **Entité** capable de **communiquer** des **informations d'état**
 - Hôtes, routeurs, ponts, imprimantes...
- Exécute un agent **SNMP**
 - Processus d'administration SNMP gérant une **base de données** locale de variables donnant l'**état** et l'**historique**



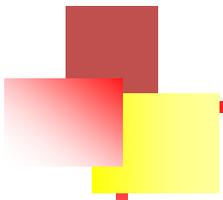
Station d'administration

- Ordinateur exécutant un **logiciel** particulier
- Communique avec les agents
 - **Envoi** de commandes/**réception** de réponses
- **Avantage:**
 - Agents très simples



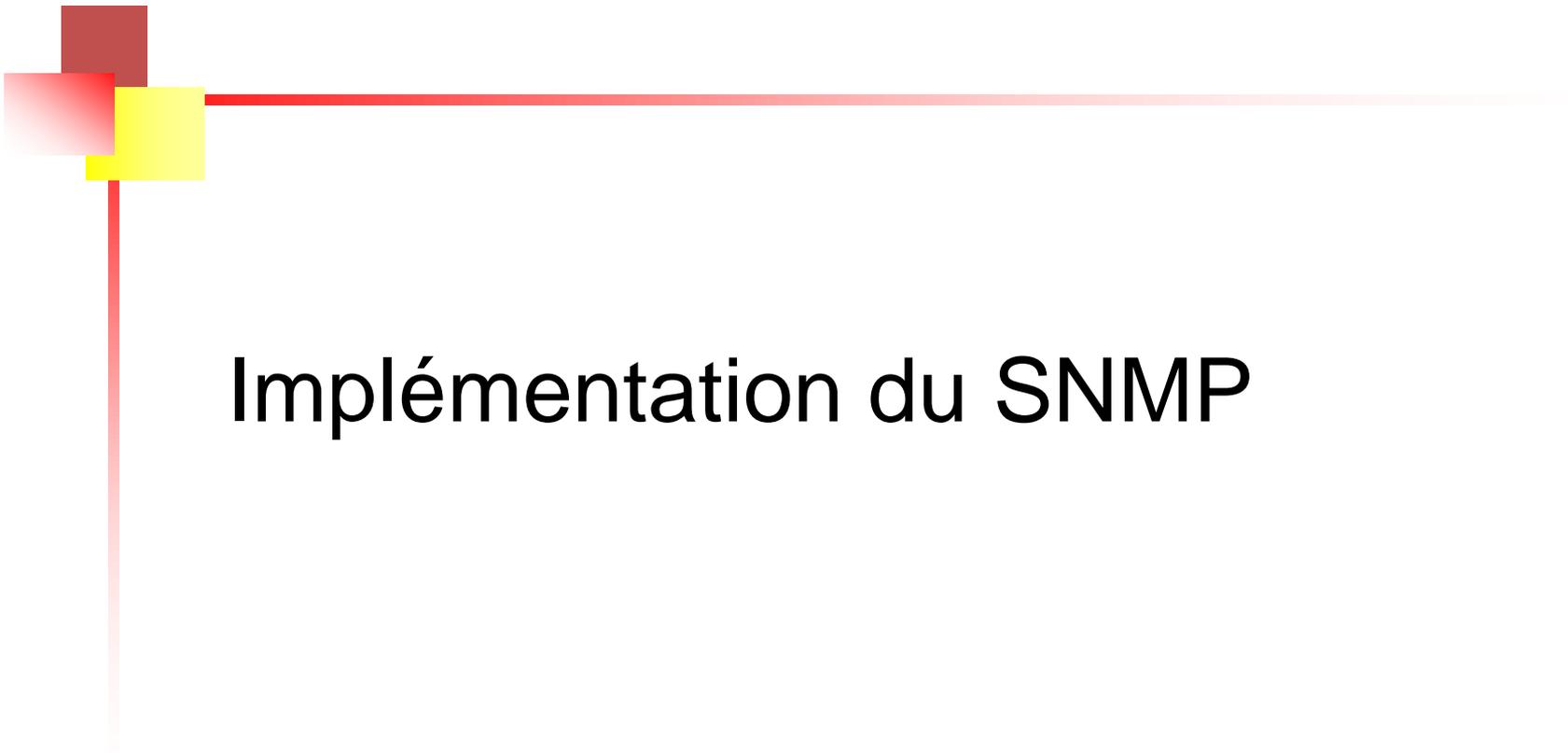
Information d'administration

- Chaque entité gère des variables décrivant son **état**
- Une variable est appelée **objet**
- L'ensemble des **objets** d'un réseau se **trouve** dans la **MIB (Management Information Base)**



Protocole d'administration

- La station d'administration interagit avec les agents (synchrone):
 - **Communication** type question/réponse
 - **Interrogation** de l'état des **objets** locaux d'un agent
 - **Changement** de l'état d'un objet
- Cas d'événement **non planifié** (Asynchrone):
 - Plantage, démarrage, rupture de liaison...
 - L'agent **signale** l'événement à la station d'administration

A decorative graphic in the top-left corner consisting of three overlapping squares: a dark red one on top, a lighter red one to the left, and a yellow one to the right. A red line extends horizontally from the right side of the yellow square across the top of the slide, and another red line extends vertically downwards from the bottom of the yellow square.

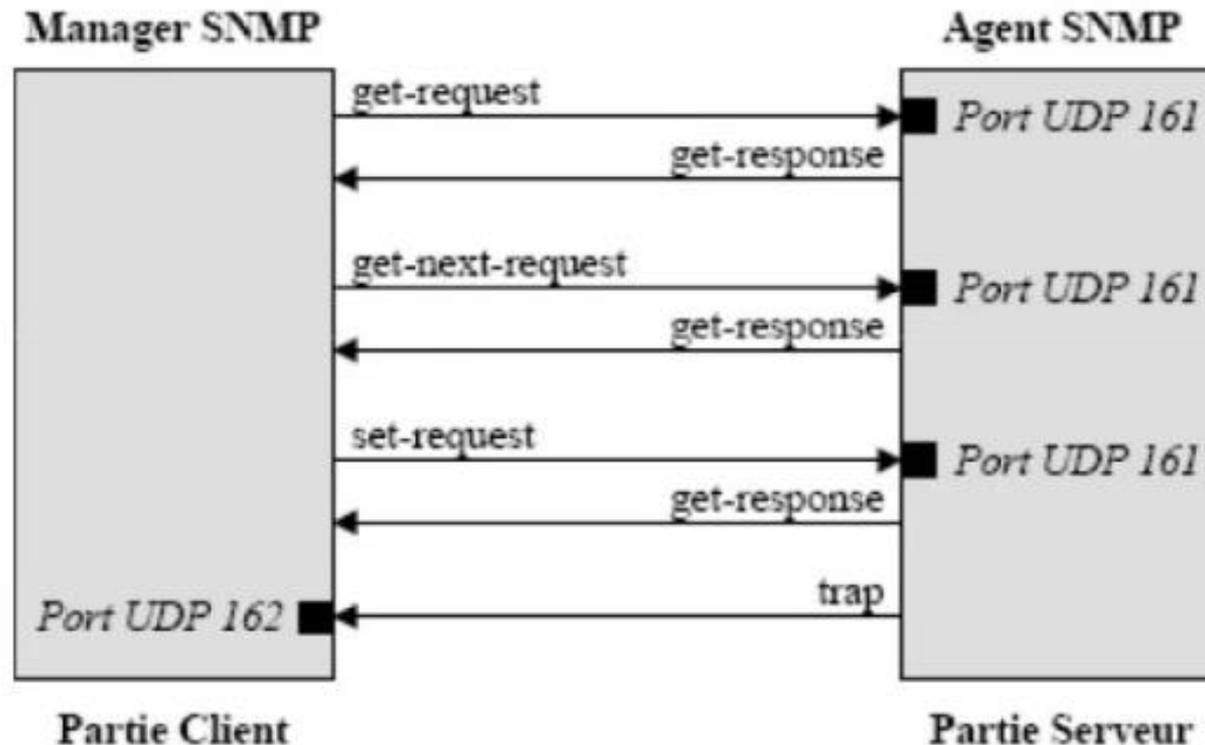
Implémentation du SNMP

Opérations

Opérations du protocole SNMP

- **LECTURE** : lit la valeur d'une variable
 - *get-request, get-response*
- **ECRITURE** : affecte une valeur à une variable
 - *set-request*
- **PARCOURS** : pour connaître les variables effectivement gérées par un noeud
 - *get-next-request, get-response*
- **NOTIFICATIONS** : pour signaler un événement extraordinaire à un gestionnaire
 - *trap*

Modèle client/serveur

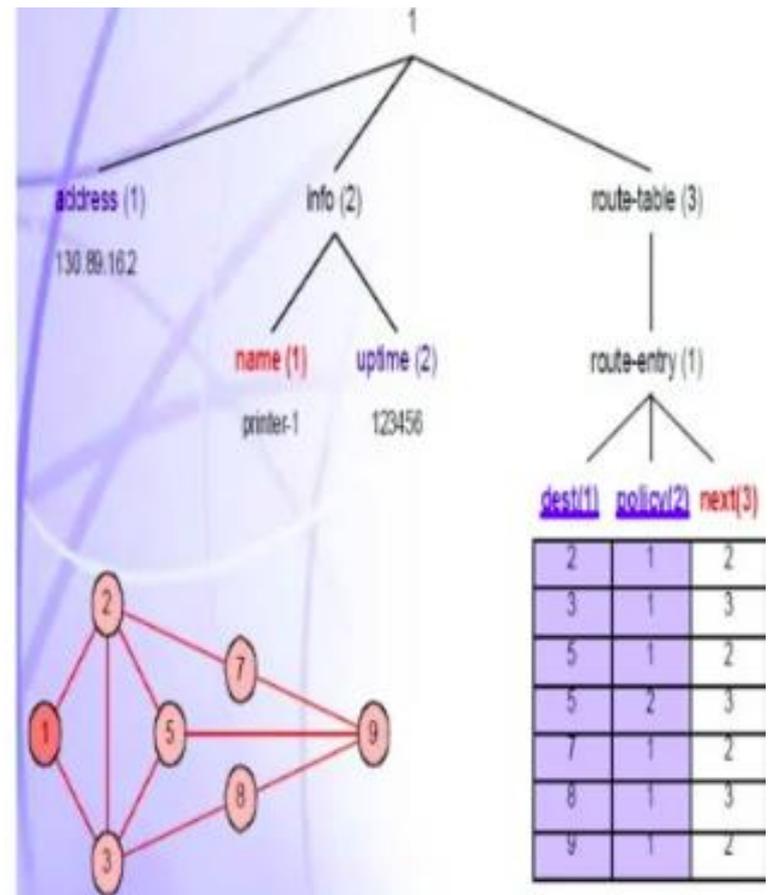


MIB

- **MIBs** sont des fichiers définissant les **objets** qui peuvent être demandés (queried), y compris :
 - *Nom de l'objet.*
 - *Description de l'objet.*
 - *Type de données.*
- Les MIBs sont des **textes structurés**.
- MIBs permettent également d'**interpréter** une valeur retournée par un agent.
- MIBs standard incluent **MIB-II**.

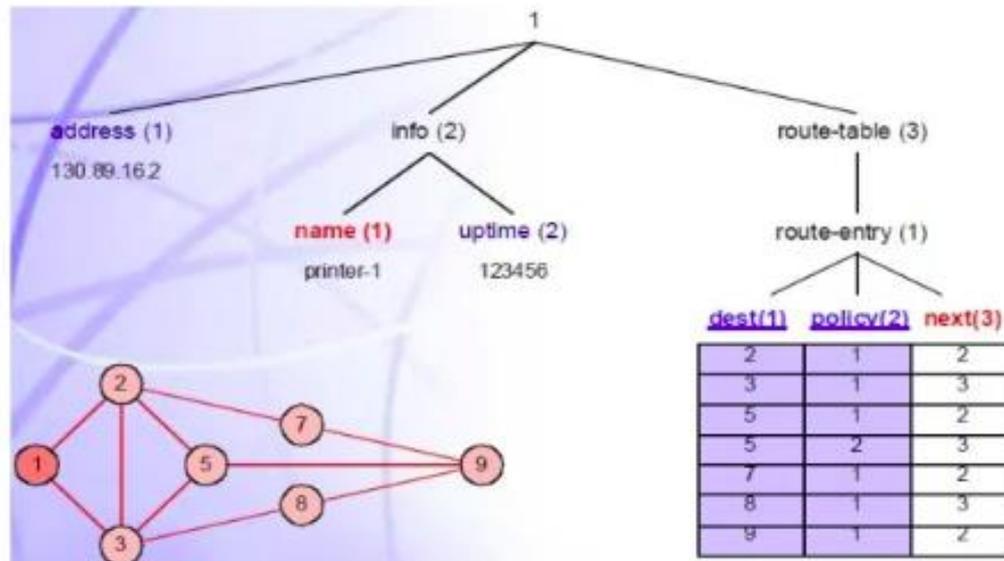
Exemple de MIB

- Get (1.1.0)
 - Response (1.1.0 => 130.89.16.2)
- Get (1.2.0)
 - Response (error-status = noSuchName)
- Get (1.1)
 - Response (error-status = noSuchName)
- Get (1.1.0; 1.2.2.0)
 - Response (1.1.0 => 130.89.16.2; 1.2.2.0 => 123456)
- Get (1.3.1.3.5.1)
 - Response (1.3.1.3.5.1 => 2)
- Get (1.3.1.1.5.1)
 - Response (1.3.1.1.5.1 => 5)
- Get (1.3.1.1.5.1, 1.3.1.2.5.1, 1.3.1.3.5.1)
 - Response (1.3.1.1.5.1 => 5, 1.3.1.2.5.1 => 1, 1.3.1.3.5.1 => 2)



Exemples de SET

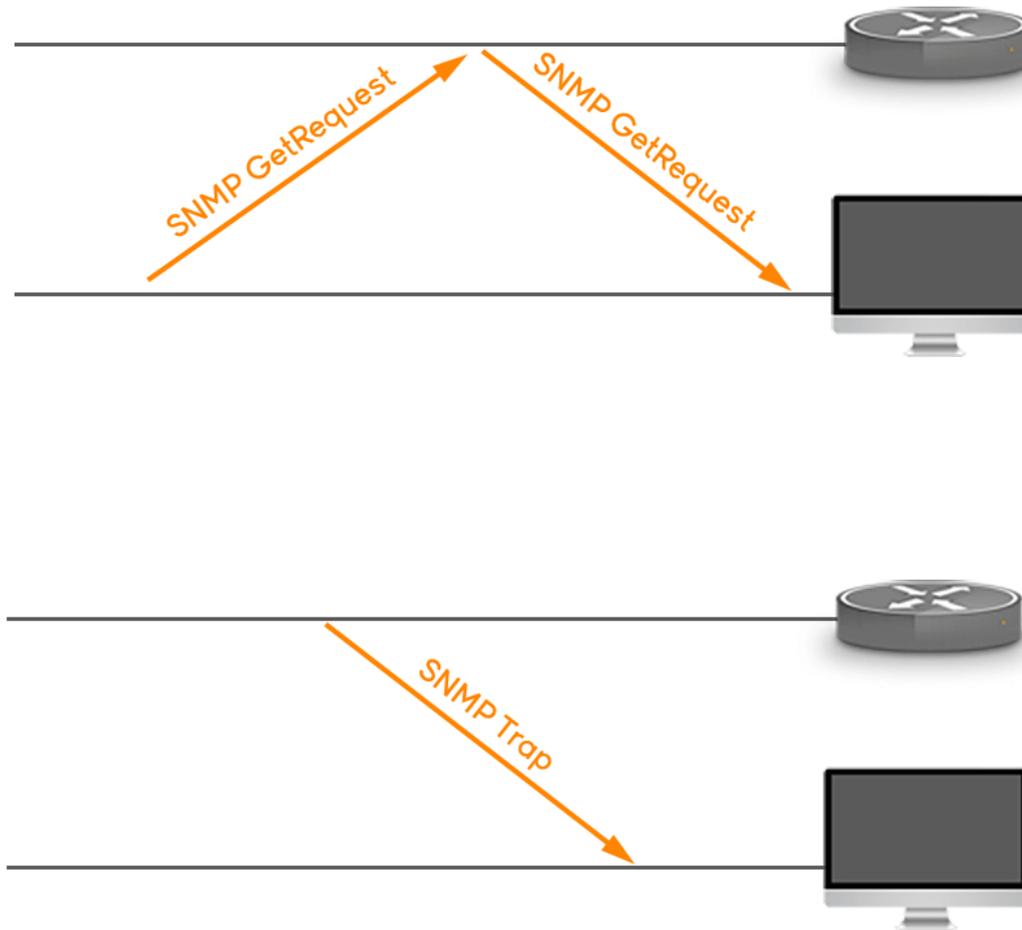
- `set(1.2.1.0 => my-printer)`
- `response(noError; 1.2.1.0 => my-printer)`
- `set(1.2.1.0 => my-printer, 1.2.3.0 => 0)`
- `response(error-status = noSuchName; error-index = 2)`



Trap notification du SNMP

- **Périphérique** entre dans un état **anormal** → Agent SNMP **prévient** le manager SNMP par le biais d'un **trap** SNMP.
- ***Generic traps***
 - Link **Up** ou Link **Down** (lorsque l'interface devient active ou au contraire passive).
 - **Cold start** (démarrage à froid) ou **warm start** (démarrage à chaud).
 - Authentication **failure** (échec d'authentification, lorsqu'un nom de communauté incorrect est spécifié dans une requête).

Trap notification du SNMP



Quelques outils de la supervision

Plusieurs outils:

- HP Open View
- Big Brother
- CiscoWorks 2000
- MRTG
- Nagios
- Zabbix

Objectif de ces outils :

1- Connaitre a tout instant l' **état** :

- des **noeuds** critiques (serveurs, switches, routeurs) et
- des **services** tournant sur les différents serveurs.

2- Analyser le **trafic** réseau afin de permettre une meilleure répartition des ressources réseaux

Logiciel de supervision: Nagios

The screenshot displays the Nagios XI web interface. The top navigation bar includes links for Home, Views, Dashboards, Reports, Configure, Tools, Help, and Admin. The left sidebar contains a 'Quick View' section with links to Service Detail, Host Detail, Hostgroup Summary, Hostgroup Overview, Hostgroup Grid, Servicegroup Summary, Servicegroup Overview, Servicegroup Grid, BPI, and Metrics. Below this are sections for Graphs (Performance Graphs, Graph Explorer), Maps (BEMap, Hypermap, Minemap, Nagvis, Network Status Map), Incident Management (Latest Alerts, Acknowledgements, Scheduled Downtime, Mass Acknowledge, Recurring Downtime, Notifications), and Monitoring Process (Process Info, Performance, Event Log).

The main content area is titled 'Nagios XI' and features a 'Status Grid' showing a list of hosts and their corresponding service status indicators. Below the status grid are several summary tables:

- Host Status Summary:**

Up	Down	Unreachable	Pending
2	5	0	0
Unhandled		Problems	All
5		5	7
- Service Status Summary:**

Ok	Warning	Unknown	Critical	Pending
24	1	7	25	0
Unhandled		Problems		All
34		34		58
- Status Summary For All Host Groups:**

Host Group	Hosts	Services
Linux Servers (linux-servers)	2 Up, 5 Down	24 Ok, 1 Warning, 7 Unknown, 17 Critical
Windows Servers (windows-servers)	1	1 Critical
- Status Summary For All Service Groups:**

Service Group	Hosts	Services
No status information found.		

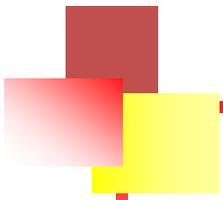
On the right side, there are 'Server Stats' and 'Server Statistics' sections. The 'Server Statistics' table shows various metrics and their values:

Metric	Value
Load	
1-min	0.48
5-min	0.19
15-min	0.11
CPU Stats	
User	8.23%
Nice	0.00%
System	0.80%
I/O Wait	0.20%
Steal	0.00%
Idle	90.76%
Memory	
Total	1838 MB
Used	647 MB
Free	408 MB
Shared	104 MB
Buffers	782 MB
Cached	909 MB
Swap	
Total	2047 MB
Used	0 MB
Free	2047 MB

At the bottom right, there is a 'Monitoring Engine Stats' section with 'Monitoring Engine Check Statistics' table:

Metric	Value
Active Host Checks	
1-min	6
5-min	7
15-min	7
Passive Host Checks	

The footer of the interface shows 'Nagios XI 5.2.5' and a 'Check for Updates' link. On the far right, there are links for 'About', 'Legal', and 'Copyright © 2008-2016 Nagios Enterprises, LLC'.



Fonctionnalités de Nagios

- Surveillance des **services réseaux** (*SMTP, POP3, http, NNTP, PING*, etc)
- Surveillance des **ressources** des stations (*serveur, routeur* ...) comme la **charge du processeur**, des informations sur l'**utilisation des disques durs**, les **processus en cours**, les fichiers de **log**, . . .
- Surveillance des données environnementales comme par exemple la **température**.

Logiciel de supervision: Zabbix

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

Dashboard

Favourite maps

Local network

Maps

Favourite graphs

New host: CPU load

Graphs

Favourite screens

Zabbix server

Screens Slide shows

Last 20 issues

HOST	ISSUE	LAST CHANGE	AGE	INFO	ACK	ACTIONS
Zabbix server 1	Version of zabbix-agent(d) was changed on Zabbix server 1	2016-01-11 22:36:06	1m 39s		No	1
Zabbix server 1	Lack of free swap space on Zabbix server 1	2015-08-11 23:29:28	5m 3d		Yes 4	

2 of 2 issues are shown Updated: 22:37:45

System status

HOST GROUP	DISASTER	HIGH	AVERAGE	WARNING	INFORMATION	NOT CLASSIFIED
Discovered hosts	0	0	0	1	1	0
Network devices	0	0	0	0	0	0
SNMP hosts	0	0	0	0	0	0
Zabbix servers	0	0	0	1	1	0

Updated: 22:37:45

Host status

HOST GROUP	WITHOUT PROBLEMS	WITH PROBLEMS	TOTAL
Discovered hosts	7	1	8
Network devices	1	0	1
SNMP hosts	2	0	2
Zabbix servers	0	1	1

Updated: 22:37:44

Discovery status

DISCOVERY RULE	UP	DOWN
Local network2	6	1

Updated: 22:37:44

Status of Zabbix

PARAMETER	VALUE	DETAILS
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled /templates)	54	10 / 1 / 43
Number of items (enabled/disabled/not supported)	356	350 / 0 / 6
Number of triggers (enabled/disabled [problem/ok])	95	94 / 1 [2 / 92]
Number of users (online)	3	2
Required server performance, new values per second	4.79	

Updated: 22:37:45

Web monitoring

HOST GROUP	OK	FAILED	UNKNOWN
Discovered hosts	1	0	0
Zabbix servers	1	0	0

Updated: 22:37:44

Debug

Références

- RFC: <http://www.rfc-editor.org>
 - RFC 1095 : CMOT
 - RFC 1213 : MIB-II
 - RFC 1212 : MIB
 - RFC 1189 : CMOT AND CMIP
 - RFC 1155,1157 : SNMPv1
 - RFC 1905 : SNMPv2

Références

- Réseaux, Andrew Tanenbaum, InterEditions
- Simple Network Management Protocol
Technology Overview, Cisco,
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55029.htm

Annexe

Format des PDU (1)

- Get, Get-next, Inform, Response, Set et Trap:

PDU Type	Request ID	Error status	Error index	Variable bindings
----------	------------	--------------	-------------	-------------------

PDU Type: Identification du message
Request ID: Correspondance requête/réponse
Error status: Type d'erreur (réponse)
Error index: Correspondance erreur/variable (réponse)
Variable bindings: Correspondance variable/valeur

Format des PDU (2)

- Get-bulk:

PDU Type	Request ID	Non-repeaters	Max-repetitions	Variable bindings
----------	------------	---------------	-----------------	-------------------

PDU Type, Request ID et Variable bindings: Mêmes fonctions

Non-repeaters: Nombre de variables demandées au travers de
Variable bindings devant être retournées sans
répétition

Max-repetitions: Nombre de répétitions des variables restantes dans
Variable bindings

Requête Get-bulk

- Requête:

Get-bulk	Request ID	3	4	A, B, C, D, E
----------	------------	---	---	---------------

- Réponse:

Response	Request ID	0	0	A, B, C, D ₀ , D ₁ , D ₂ , D ₃ , E ₀ , E ₁ , E ₂ , E ₃
----------	------------	---	---	--

Format des messages (1)

- Non sécurisé



- Authentifié mais non privé



- Privé et authentifié



← Crypté →

Format des messages (2)

- Context: Collection de ressources accessibles par une entité SNMPv2
- Digest: Résultat de l'algorithme de hachage
- Destination timestamp: Dernière horloge du récepteur connue de l'émetteur
- Source timestamp: Horloge de l'émetteur

SNMP v3

Avant de partir manger

- La structure ISO n'est utilisée que par les grandes compagnies (de façon propriétaire)
- Une très large utilisation de SNMP
 - Un protocole effectivement *Simple*
 - S'appuie sur le protocole TCP/IP
- Et le rôle de l'administrateur dans tout ça ?