Divers

- IPv6
- MPLS
- le futur de MPLS -> SD WAN
- SNMP

IPV6

- Pourquoi la migration Ipv4 -> Ipv6
- Fonctionnalités d'IPv6
- Adressage IPv6

Problèmes IPv4 (1)

- **Explosion des besoins en adresse**
  - Utilisation des services mobiles
  - Accroissement de la domotique
  - De plus en plus d'utilisateurs dans le monde
- Explosion un peu retardée grâce à :
  - Utilisation du DHCP
  - Utilisation du NAT et surtout du PAT
- Problème au niveau des tables de routage malgré le CIDR.

Caractéristiques d'IPv6

- Adressage sur 128 bits (c'est-à-dire 16 octets)
- Adressage hiérarchique pour optimiser le routage
- En-tête plus simple, utilisation de 8 champs au lieu de 13, et de taille fixe pour améliorer les performances
- Mécanisme plus évolué d'autoconfiguration
- Couche IPSec intégré au protocole
- Extension du multicast et abandon du broadcast
- Gestion de la mobilité

Format adresse IPv6

- Utilisation de la notation hexadécimale, en regroupant les chiffres par 4 et en les séparant par ‘:’
  ex : 2001:E323:A65A:95F5:63D4:08BB:76F5:A234

- Disparition des sous-réseaux, apparition de la taille du préfixe ‘/’ (nb de bits appartenant au préfixe)
  ex : 2F45:EE34:C23E::/48

- Elimination des 0 présents dans l’adresse:
  ex : 2001:0:0:0:0:342D:342F:FF45

  2001::342D:342F:FF45

En-tête IPv6

Format de l'en-tête du paquet: (min 40 octets)

Version (4 bits)	Priorité (8 bits)	Etiquette de flot (20 bits)	4 octets
Lg données (16 bits)	en-tête suivant (8 bits)	nb nœuds traversés (8 bits)	4 octets
Adresse émetteur (16 octets)			16 octets
Adresse récepteur (16 octets)			16 octets
Options			

Etiquette de flot : Pour s'assurer d'une QoS

lg données : taille des données utiles (max 65536)

en-tête suivant : protocole encapsulé (4, IP : 6, TCP : 17, UDP : 58,ICMPv6,..)

Nb nœuds traversés : remplace le TTL

Dans Option, on retrouve des informations nécessaires à en-tête suivant: 50, authentification : 44, fragmentation, etc…

Adresse unicast IPv6

- 1/8 de l'espace total d'adressage
- Utilisation du préfixe : 2000::/3
- 48 bits pour le réseau
  - - 23 bits affecté à chaque RIR (Regional Internet Registries) (fichier décrivant l'affectation)
  - - 9 bits FAI
  - - 16 bits pour le site
- 16 bits pour le sous-réseau
- 64 bits pour l'interface

Adresse lien local IPv6

- Adresse valide seulement sur un lien (elle ne traverse pas les routeurs)
- Fonctionnement identique à 169.254.0.0/16 en Ipv4
- Adresse donnée automatiquement à chaque système ce qui permet de découvrir les voisins.
  - Pour chaque interface, une adresse lien local.
- Utilisation du préfixe : FE80::/10 (voir /64 généralement)
- 64 bits pour l'interface en eui-64

Exemple : FE80::20C:29FF:FEF1:B52F / 64

Adresse site local IPv6

- Adresse utilisée sur un réseau privé
- Fonctionnement identique à la RFC 1918
- Utilisation du préfixe : FC00::/7

Adresse multicast IPv6

- Adresse qui désigne un ensemble d'interfaces
- Utilisation du préfixe : FFxy::/8
- Flag (x) : 3 premiers bits à 0,
  - dernier bit à 0 = validité permanente, sinon validité temporaire
- Scope (y): portée de la diffusion
  - 1 -> le nœud 2-> le lien 3-> sous-réseau 5-> site
- Identificateur de groupe
  - 1 -> toutes les machines
  - 2 -> tous les routeurs

Exemple : FF02:0:0:0:0:0:0:2

Gestion des adresses IPv6

- Attribution manuelle
  - On donne l'adresse Ipv6

- Auto-configuration (plug and play)
  - Mode "stateless" : on récupère automatiquement le préfixe du site et on rajoute la partie hôte via eui-64
  - Méthode SLAAC puis DHCPv6 stateless pour récupérer DNS, domain name, etc…
    (configuration par défaut actuellement)

  - Mode "statefull" : récupération de l'adresse via DHCPv6 (port 546 et 547 utilisé)
    - 4 transactions
      - 1) client envoie un paquet **Solicit** sur l'adresse : ff02::1:2 (547)
      - 2) DHCPv6 répond par **Advertise ,** via l'adresse lien local(546)
      - 3) client renvoie une **Request** sur l'adresse : ff02::1:2
      - 4) DHCPv6 finit par **Reply, ,** via l'adresse lien local.

Auto-configuration Stateless

- L'équipement prend son adresse lien local → FE80:….
- Vérification de l'unicité de cette adresse sur lien local
  - Envoi d'une trame ICMPv6 "sollicitation d'un voisin" (type 135) sur l'adresse multicast ff02::1
    - Si pas de réponse (attente 1 s), l'adresse est valide
    - Sinon, ICMPv6 "annonce d'un voisin" (type 136), adresse déjà utilisée
- Envoi d'une trame ICMPv6 "sollicitation d'un routeur" *(type 133 = RS)* sur l'adresse multicast FF02::2
- Réception d'une trame ICMPv6 "annonce d'un routeur" *(Type 124 =RA)* avec à l'intérieure le préfixe du réseau
- Par défaut un routeur envoie des RA régulièrement (200 secondes pour Cisco)

Transition IPv4 vers IPv6

- Utilisation de la double pile
  - On utilise en priorité IPv6
- Utilisation de tunnels
  - Pour aller de IPv4 vers IPv4 en passant sur un réseau IPv6 (4 to 6)
  - Pour aller de IPv6 vers IPv6 en passant sur un réseau IPv4 (6 to 4)
- Utilisation du NAT –PT (Protocol Translation)
  - De Ipv6 vers Ipv4
  - De Ipv4 vers IPv6

Exemple IPv6

- inet6num: 2001:660:5101::/48
  netname: FR-U-1-CLERMONTFERRAND
  descr: Universite de Clermont-Ferrand 1 - Auvergne
  country: FR
  admin-c: BT261-RIPE
  admin-c: JO1744-RIPE
  mnt-by: RENATER-MNT
  source: RIPE # Filtered

- inet6num: 2001:660:5102::/48
  netname: FR-U-2-CLERMONTFERRAND
  descr: Universite de Clermont-Ferrand 2 - Blaise Pascal
  country: FR
  admin-c: BT261-RIPE
  admin-c: JO1744-RIPE
  mnt-by: RENATER-MNT
  source: RIPE # Filtered

MPLS

Multi-protocol Label Switching

Introduction (1)

- Norme IETF : RFC 3031
  - But :
    - Accroitre la vitesse de traitement dans les équipements actifs du réseau

      Plus d'actualité du fait des progrès dans les routeurs
    - Enrichir les services de routage
  - MPLS se situe entre la couche 2 et 3, souvent traité comme un protocole de couche 2,5.

Introduction (2)

- Rôle principal
  - Combiner les concepts du routage IP de niveau 3, et les mécanismes de commutation de niveau 2
    - Permettre d'avoir un mode connecté à IP en évitant une surcharge au niveau entête
    - « Table de commutation plus rapide à lire… »
    - On élimine le concept de routage "next hop", pour avoir un routage global ➔ ATM, Frame relay,…
    - Mise en œuvre de services (Qos, VLSP,…)

Objectifs

- L'aspect "fonctionnalité" est plus important actuellement que l'aspect "performance "
  - Permettre une communication entre un ou plusieurs sites
  - Flexibilité sur le médium (ATM, SDH, Ethernet, PPP)
  - Création de VPN (réseau privé virtuel, mais non chiffré), VPLS (Virtual Private LAN Service)
  - Mise en place de Qos avec RSVP-TE
  - Traffic Engineering (gestion de trafic)
    - Découpage en classe suivant le trafic

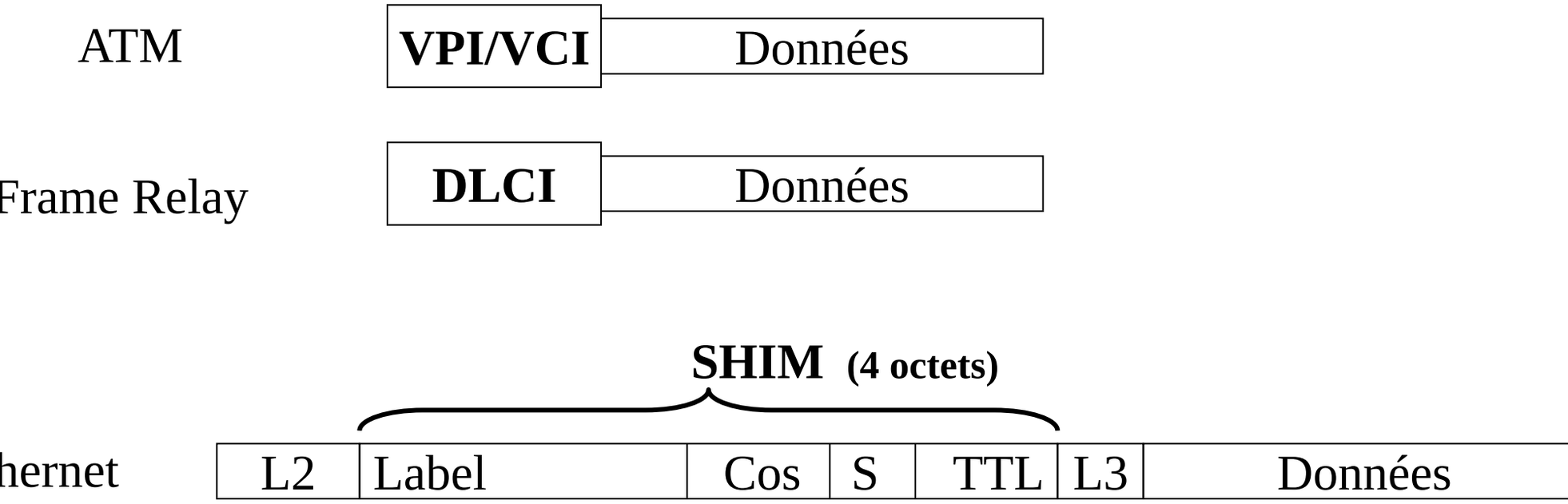
Fonctionnement

- Basé sur le label (étiquette)
  - A chaque paquet entrant sur le réseau MPLS, on lui associe un label ➔ un entier
  - L'acheminement des paquets **est basé sur l'analyse du label** et non plus sur l'analyse de l'adresse IP
  - MPLS utilise une technique de commutation
    - Chaque équipement MPLS (LSR : Label Switch Router) possède une table de commutation → échange de label entre l'entrée et la sortie

Principe (1)

- A l'entrée du réseau MPLS, équipement actif : E-LSR : Edge Label Switch Router (ou LER)
  - Décide de l'affectation d'un label à un paquet
    - Dépend des groupes ou des classes de flux FEC (Forwarding Equivalence Classes)
  - Tous les paquets d'une même FEC sont traités de la même manière (ils suivent le même chemin)
  - Le label est ajouté :
    - Entre la couche 2 et la couche 3 (environnement paquet)
    - Dans le champ VPI/VCI (identificateur de chemin virtuel/identificateur de canal virtuel pour ATM)

Label



Label : 20 bits :

ethertype : 0x8847

Cos : 3 bits : Class of service

S : 1 bit : empilement de label

TTL : 8 bits : Time To Live (identique au rôle en IP)

On ne regarde que le label et le TTL pour faire transiter le paquet

Principe (2)

- Le E-LSR (LER) est l'interface entre le monde MPLS et l'extérieur (interface IP traditionnelle)
  - 2 sortes de LER : ingress node ou egress node
  - Labellise le paquet ou enlève le label
- Les Paquets suivent le LSP (Label Switch Path)
  - Chemin composé par une suite de LSR
  - Configuré via le mécanisme de labels, pour une FEC donné
  - Peut-être configuré statiquement ou dynamiquement
  - Un label n'est utile que localement. A chaque LSR, changement de label pour suivre le LSP.

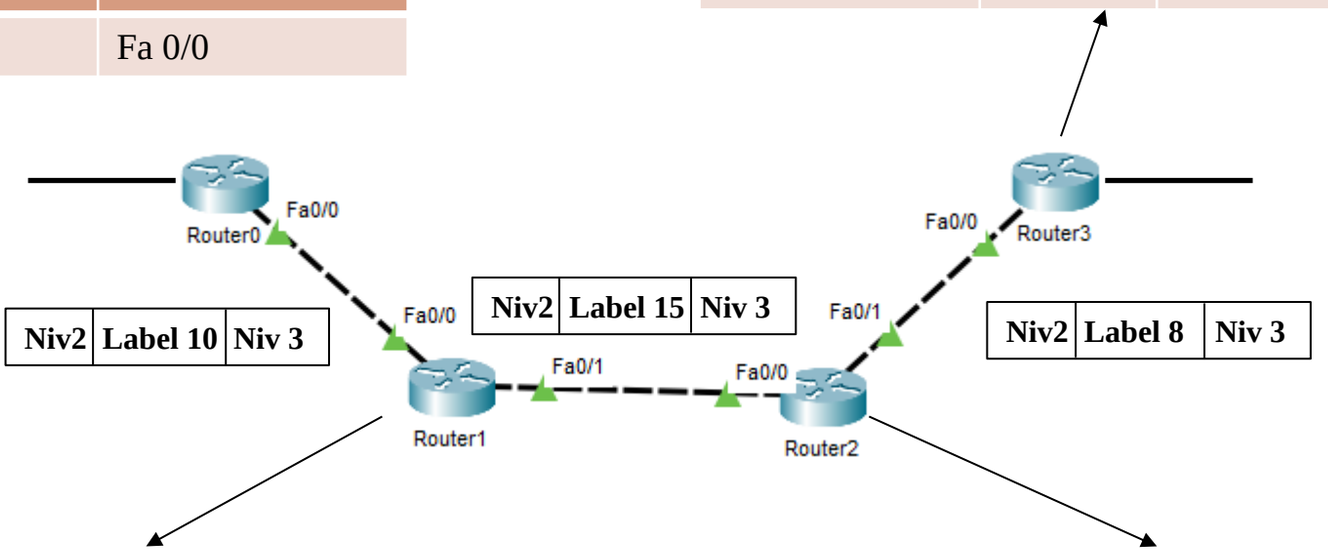
Protocole pour mettre en œuvre les LSP dynamique

➔ LDP (Label Distributed Protocol)

Principe (3)

Destination	Label Out	FastEthernet Out
195.10.5.0	10	Fa 0/0

FastEthernet IN	Label In	Label Out	FastEthernet Out
Fa 0/0	8	/	/



FastEthernet IN	Label In	Label Out	FastEthernet Out
Fa 0/0	10	15	Fa 0/1

FastEthernet IN	Label In	Label Out	FastEthernet Out
Fa 0/0	15	8	Fa 0/1

FEC

- FEC
  - Est la représentation d'un groupe de paquets qui ont en commun les mêmes besoins quant à leur transport
  - Sont basés sur les besoins en termes de service pour certains groupes de paquets, et plus généralement sur le même préfixe IP pour la destination
- A chaque paquet est associé une et une seule FEC à son entrée dans MPLS
- Les FEC sont partagés par tous les routeurs LSR du réseau, via le protocole LDP

Distribution de labels (1)

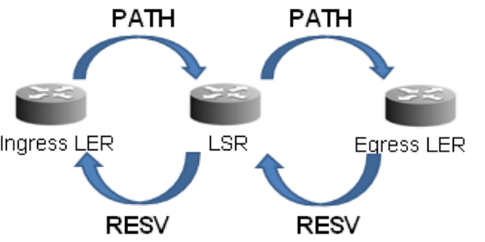
- Protocole LDP : Label Distribution Protocol
  - Mode indépendant et non sollicitée
    - Pour chaque route dans la table de routage, création d'un label
    - Annonce de chaque label à ses voisins, et donc diffusion des labels (utilisation de TCP, et de messages tel que Label request, et label mapping et aussi de paquets hello)

      → Création du LSP pour chaque route

    - Utilisation des routes déjà connues
      - Surcharge du réseau en certains points
    - Risque de création de boucles
      - Détection possible
      - On ne sait pas toutes les éviter

Distribution de labels (2)

- Mode de contrôle centralisé
  - 2 protocoles possibles :
    - **CR-LDP : Constraint Routing – LDP → extension de LDP**
    - **RSVP-TE : ReSerVation Protocol – Tunnel Extension**
  - But : choisir son chemin afin d'avoir une QoS
  - On impose le chemin d'une manière statique entre 2 E-LSR.
    - Entrée stricte : chemin directe entre 2 LSR
    - Entrée lâche : un chemin entre 2 LSR
  - Identification fixe du LSP tout au long du chemin (LSPId)
  - Champ présent dans la trame de création pour avoir une QoS définie
    - Pb si plus de places → notion de priorité de maintien
  - Pour rsvp-te, label mis en place via la réponse de la création du chemin et utilisation d'UDP.



Routage hiérarchique ou tunneling (1)

Utilisation du bit S de l'entête

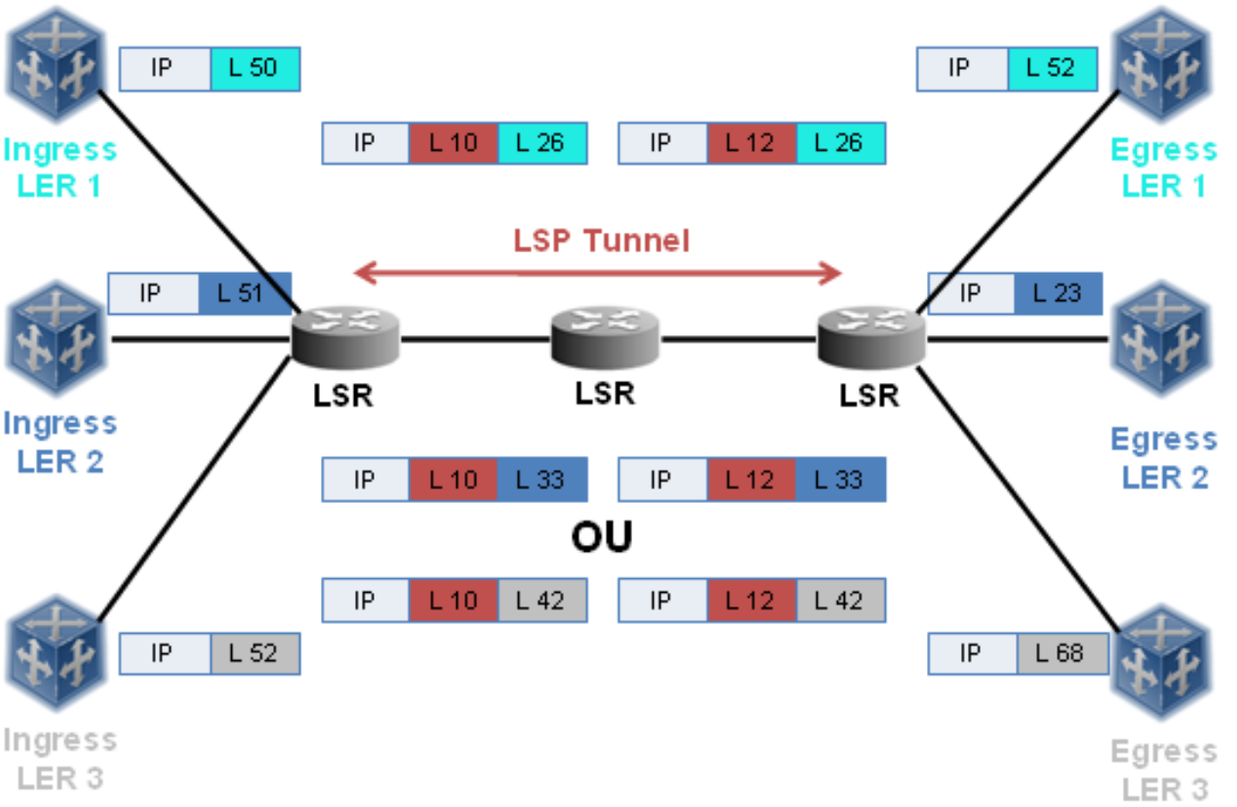
- Création de réseau virtuel à l'intérieur de MPLS (mise en place de tunnel)

- Un LSR peut faire 3 actions :
  - Replace : échange d'un label contre un autre label
  - Replace and push : modification d'un label et empilement d'un nouveau label (création du tunnel)
  - Pop : dépilement du premier label

Sauf ordre contraire, MPLS ne traite que le label supérieur

Permet l'agrégation de plusieurs flux

Routage hiérarchique ou tunneling (2)

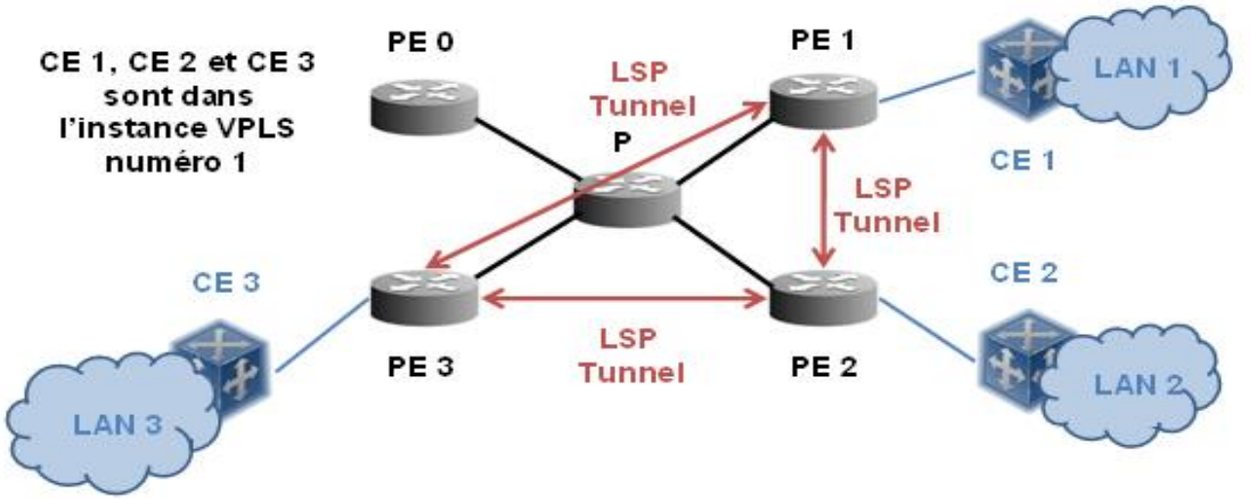


- 3 LSPs dans un seul backbone, tunneling
- Chaque label n'est que local

VPLS

- Vocabulaire :
  - P : provider Router ->routeur cœur de réseau <-> LSR
  - PE : provider edge : routeur d'extrémité
  - CE : Customer Edge : routeur appartenant aux client et connectés aux PE

- VPLS
  - VPN de niveaux 2
  - Utilisation du tunneling entre graphes complets des PE
  - Chaque PE possède une table d'adresses MAC



Conclusion MPLS

- Permet les Réseaux privés virtuels
- Gestion centralisée et simplifiée du réseau
- Mise en place de COS (Class Of Service)
- Très utilisé pour communiquer d'un site vers un autre site

MAIS

- Rigidité des communications (pas toujours simple de rajouter un chemin)
- Très cher -> passe par un opérateur
- Dépendance totale par rapport à l'opérateur
- De plus en plus utilisation du cloud, donc MPLS devient obsolète.

SD-WAN (1)

- Sotware-Defined Wide Area Network
  - Remplace le MPLS, car moins cher et plus évolutif
  - Utilisation d'un accès internet (choix entre différents opérateurs) -> diminution des coûts
  - Peut être utilisé sur différents supports (fibre, 4G, 5G,…)
  - Optimisation logicielle pour contrôler l'exploitation du réseau
    - Différents équipements
      - Boitier Client SD-WAN (permet étiqueter les paquets)
        - Aussi appelé CPE (Customer Provider Edge)
      - Contrôleur SD-WAN
        - Interface avec l'utilisateur
        - Envoie les infos aux Client SD-WAN

SD-WAN (2)

- En général, fourni et géré depuis le cloud
- Très orienté pour la communication entre cloud (cf applications multi-cloud)
- Chaque liaison SD-WAN peut être sécurisée.
- Pas de normes précises…. Géré par le fournisseur

- Réseaux hybrides : SD-Wan + MPLS
  - SD-WAN intègre MPLS dans ses choix possibles, en plus des liaisons internets.

SNMP

Simple Network Management Protocol

Introduction à SNMP

- Gestion d'un réseau
  - Gestion de la configuration des équipements
  - Gestion des problèmes du réseau
    - Pannes physiques, coupure, …
  - Gestion des performances, …

  - Les moyens utilisés :
    - Extraction des informations des éléments du réseau

    - Stockage de ces informations

      (avant ou après filtrage)
      -> de grandes quantités de données peuvent être présentes

    - Traitement et visualisation de ces données

Protocole snmp (1)

- Protocole de gestion de réseau proposé par l'IETF
  - SNMPv1 : première version, 1989 -> RFC 1065
  - SNMPv2 est divisé en :
    - Snmpv2c : amélioration de la version 1 sur le protocole
    - Snmpv2u : amélioration de la version 1 sur la sécurité
    - Snmpv2 : un mixte des deux versions
  - SNMPv3 : orienté vers la sécurité
  - Utilisation de toutes les versions de SNMP

Protocole snmp (2)

- SNMP est un protocole qui permet la gestion locale et à distante d'équipements tels que les routeurs, les switches, les serveurs,…

- Il permet :
  - De disposer d'une cartographie du réseau
  - De fournir un inventaire précis de chaque machine
  - De signaler les dysfonctionnements

Fonctionnement

- 3 éléments principaux :
  - **Agents :** chargés de superviser un équipement (agent SNMP)
  - **Stations de gestion** : capable de communiquer avec les agents et d'interpréter les données reçues (Manager)
  - **MIB :** Management Information Base

SNMP et le modele OSI

7	Application	Management et Agent APIs
		SNMP
6	Presentation	ASN.1 and BER
5	Session	RPC and NetBIOS
4	Transport	TCP and UDP
3	Réseau	IP and IPX
2	Data Link	Ethernet, Token Ring, FDDI
1	Physique	

SNMP est fait pour le protocole TCP/IP et fonctionne au-dessus d'**UDP** sur le **port 161** (SNMP message) et **162** (SNMP trap message)

SNMP

- SNMP peut se décomposer en 3 parties:
  - **Protocole SNMP**
    - Définit le format des messages entre les agents et les managers (primitives get, getnext, trap,…)
  - **Structure of Management Information (SMI)**
    - Règles spécifiant le format des données que peut récupérer SNMP (RFC 1155)
  - **MIB :**
    - Base de données qui contient les informations du système, codées en respectant le SMI

Les opérations

- *GetRequest* : recherche d'une variable de la MIB sur un agent
- *GetNextrequest* : recherche de la variable suivante
- *GetBulkRequest* : recherche d'un groupe de variables

- *SetRequest* : permet de changer la valeur d'une variable d'un agent

- *Trap* : détection d'un accident

- Une seule réponse : *GetResponse*, soit avec la valeur, soit avec *NoSuchObject*

LA MIB

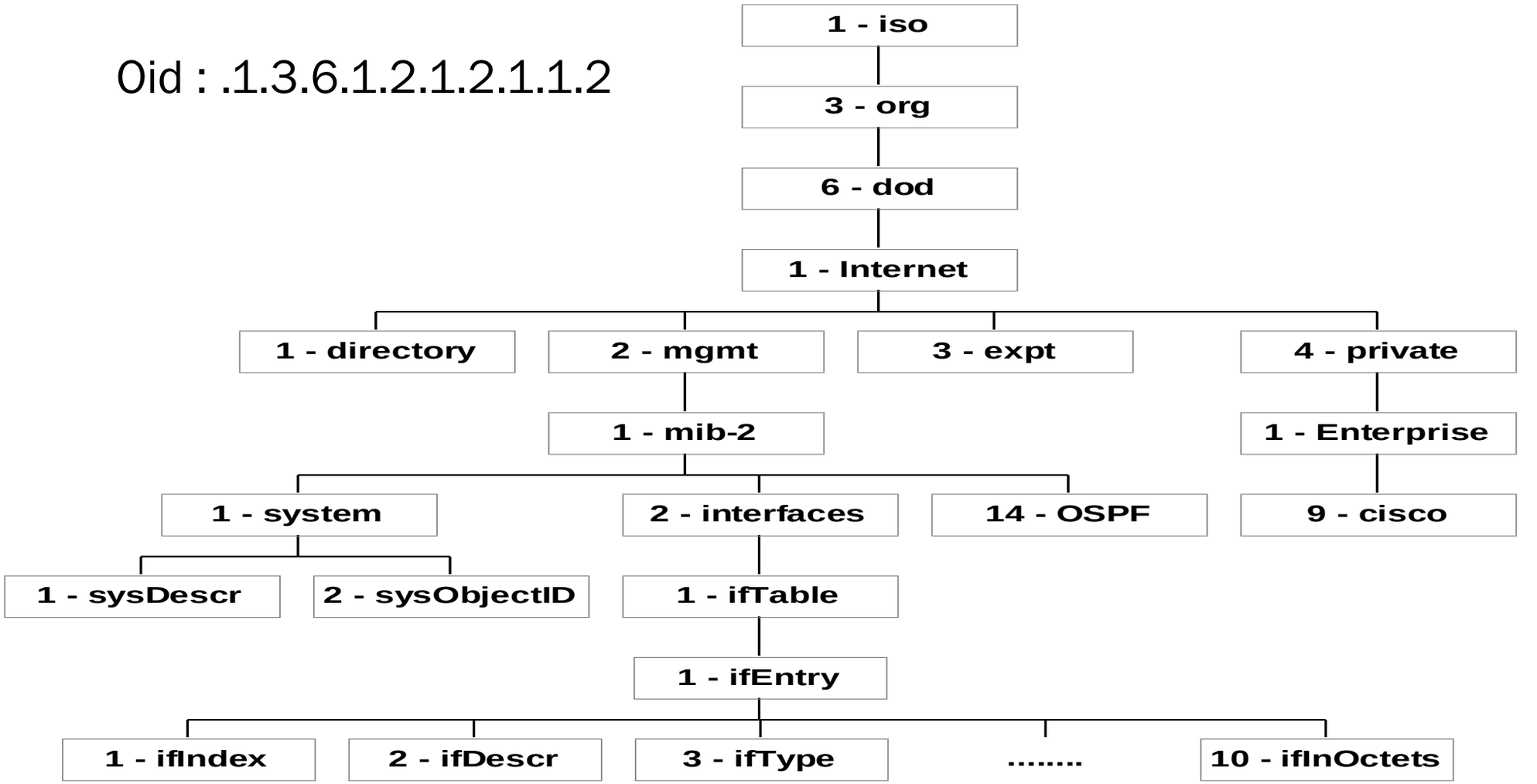
- Codé en respectant le SMI
  - Utilisation de ASN.1 pour définir les objets
  - Utilisation de BER, c'est-à-dire TLV pour encoder les messages

```
sysContact OBJECT-TYPE  -- OBJECT-TYPE décrit l'OID
    SYNTAX        DisplayString (SIZE (0..255))    -- champ qui décrit les infos
    ACCESS        read-write          -- ou read-write, write-only, not-accessible
    STATUS        mandatory           -- ou optional, deprecated, obsolete
    DESCRIPTION
          "Champ permettant de
           mettre l'information"
    ::= { system 4 }
```

OID (object identifier)

SNMP Name Structure

Oid : .1.3.6.1.2.1.2.1.1.2



Chaque entreprise va avoir sa MIB...

Récupération d'information

- Remontée d'information
  - Soit en utilisant le polling
  - Soit par émission de Trap
- Notion de communauté
  - Un agent n'envoie que vers sa communauté
    - Permet de mettre un peu de sécurité
    - Permet de distinguer les flux d'informations

Logiciels

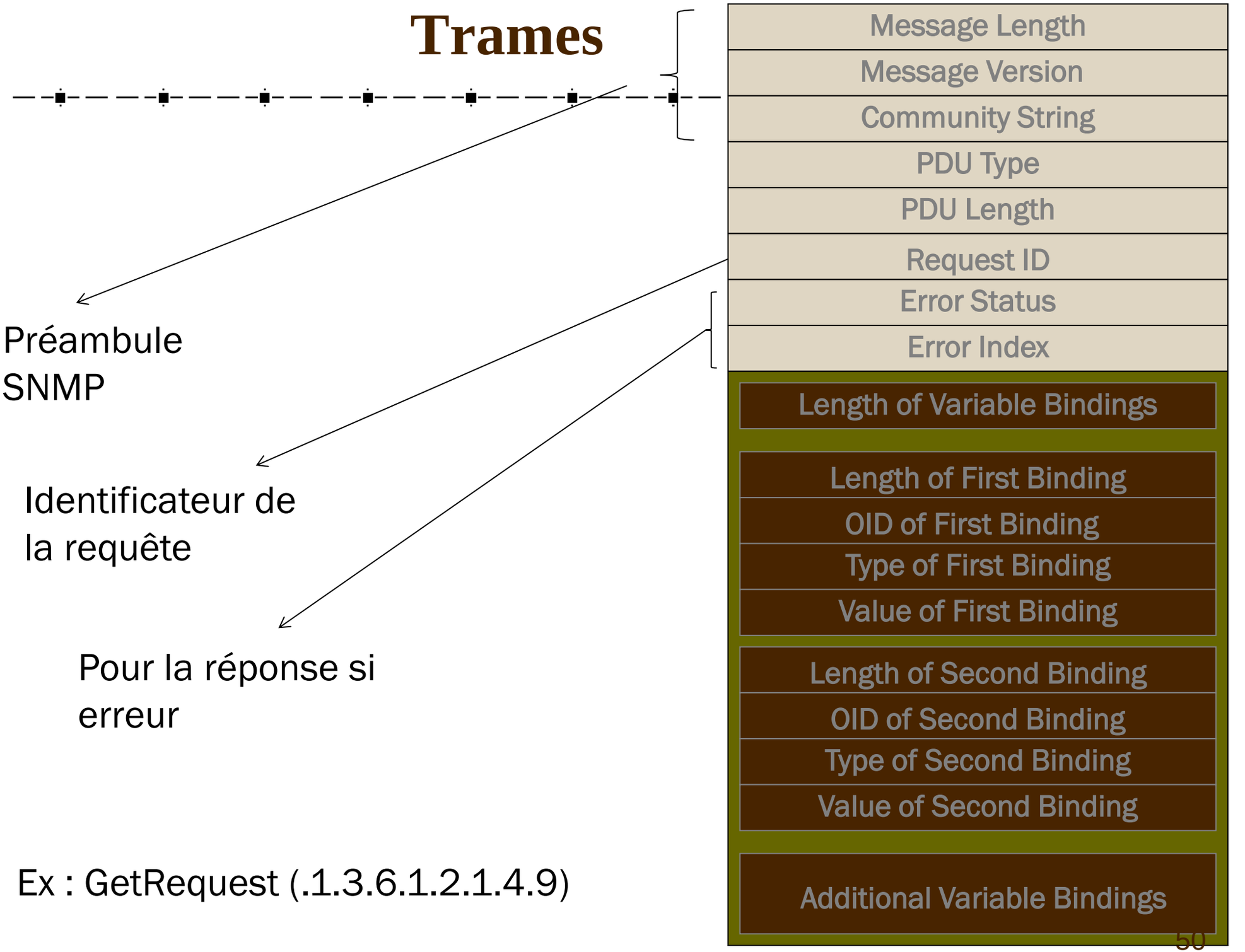
- De nombreux logiciels utilisent SNMP
  - HP OpenView
  - Centreon
  - Nagios
  - Cacti, Zabbix,
  - …

Autres manières de manager

- Au niveau programme,
  - Utilisation de log (log file, journal de bord, …)
  - Utilisation du protocole syslog
    - sur le port UDP 514
    - architecture client/serveur
    - Format : heure + hostname + processus + level + message
      - level 0= emergency, 1 = alert, …. , 6= info, 7= debug

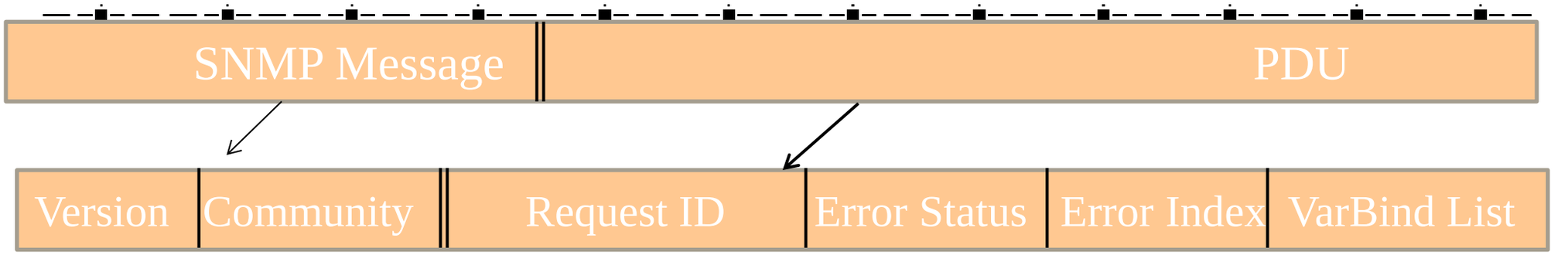
mais dans un réseau, tout vient d'un programme

Trames



Ex : GetRequest (.1.3.6.1.2.1.4.9)

Trames SNMP



Sur le port UDP 161, on obtient :

30 26 --> SNMP , longueur 0x26

02 01 00 → version

04 06 70 75 62 6C 69 63 → community

A0 19 → get-request + longueur

02 02 01 → request id

02 01 00 →

02 01 00 →

30 0E → varbind list + longueur

30 0C → var bind + longueur

06 08 →

2B 06 01 02 01 01 01 00

2B = 43 = 40*1 +3

```
PDU GET_request::=
        SEQUENCE {
          request-id   INTEGER,
          error-status       -- sometimes ignored
            INTEGER {
              noError(0),tooBig(1), noSuchName(2),
              badValue(3),readOnly(4),genErr(5) },
          error-index        -- sometimes ignored
            INTEGER,
          variable-bindings -- sometimes ignored
            VarBindList }
-- variable bindings
 VarBind ::=
        SEQUENCE {
          name ObjectName,
          value ObjectSyntax }
VarBindList ::=
        SEQUENCE OF VarBind
```