



Formation: Réseau avancé

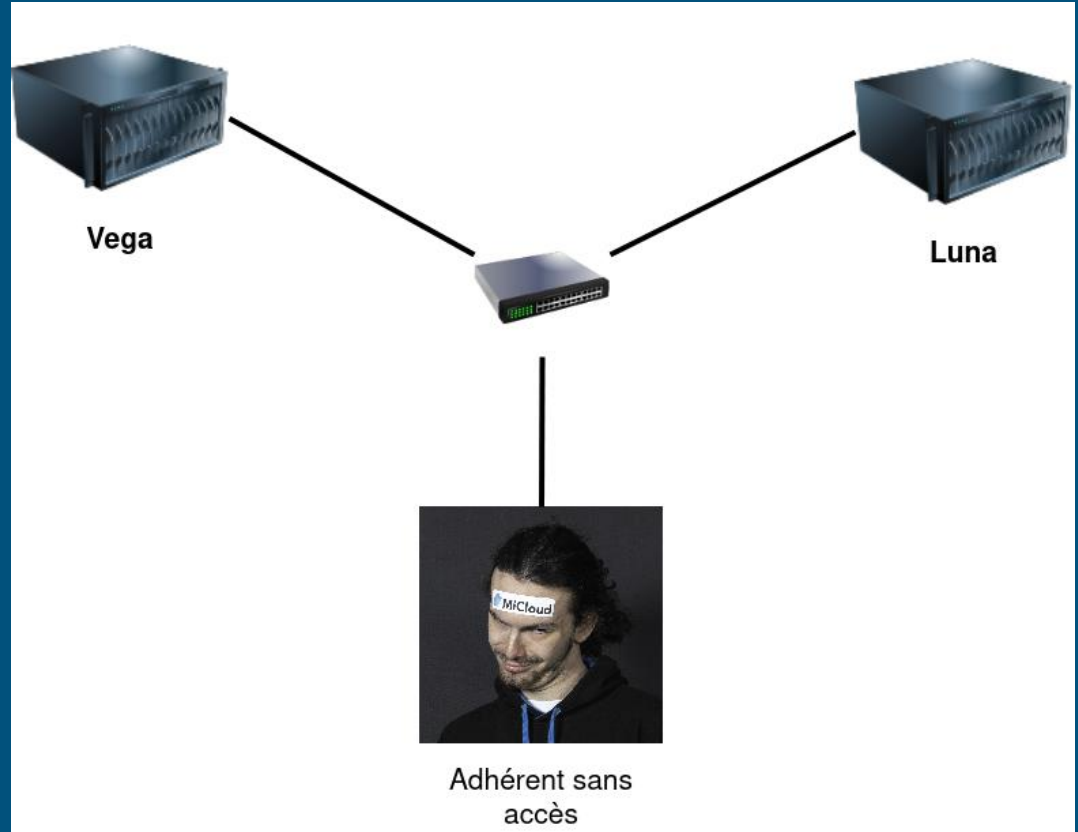
azurael & rustace

Sommaire

- Présentation
 - VLAN
 - Spanning Tree Protocol
 - ARP Inspection
 - Adressage et DHCP
 - DHCP Snooping
 - Routage
 - Filtrage
 - SNMP
- Kahoot

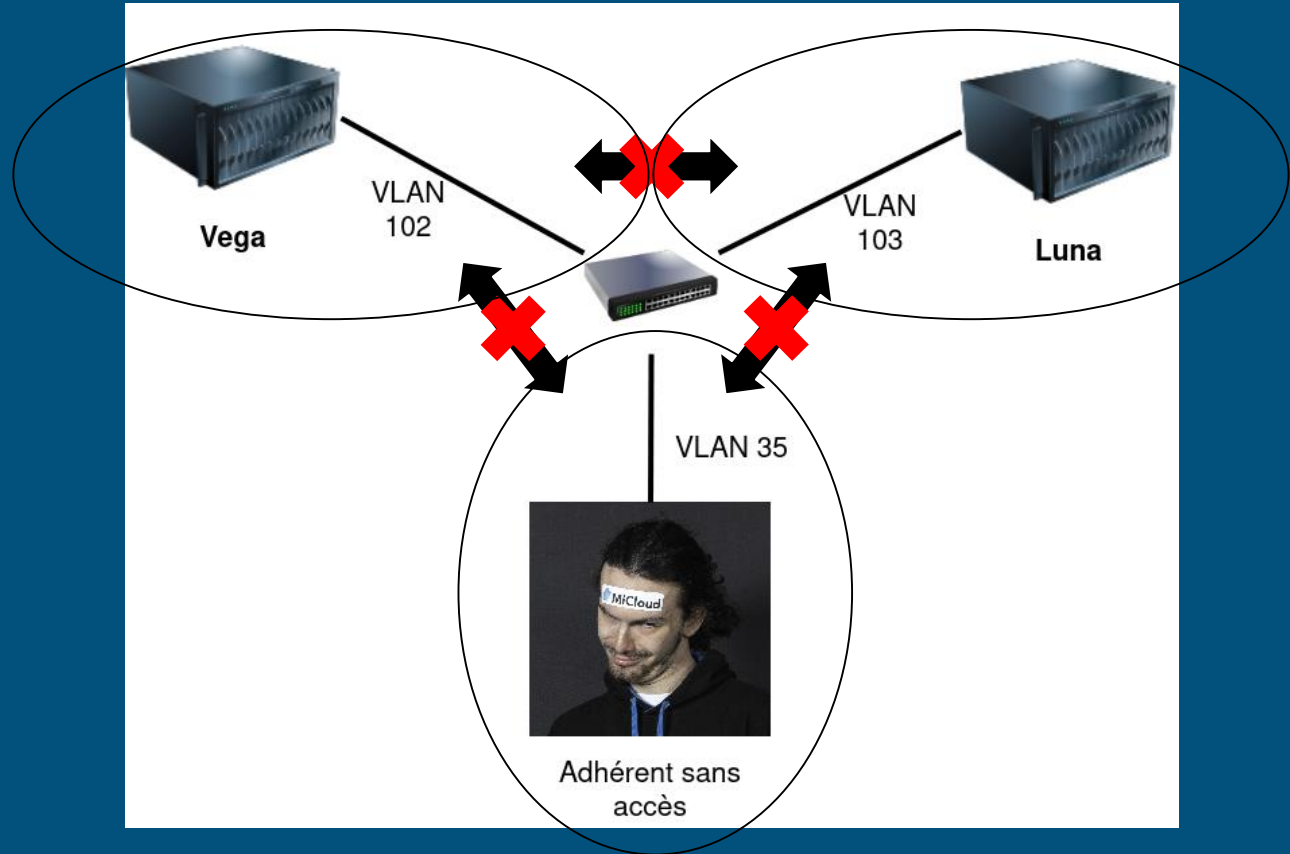
VLAN 1/4

Quand il y a pas de VLAN



VLAN 2/4

Quand il y a des VLAN



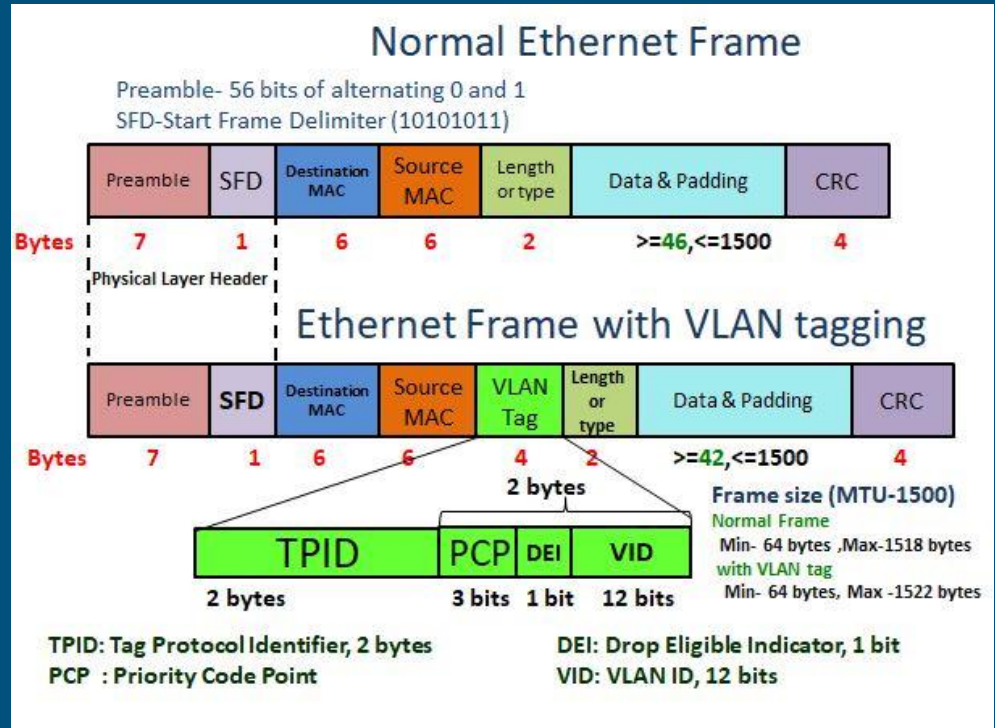
VLAN 3/4

Comment définir des VLANs ?

- Ports

Filtrage par

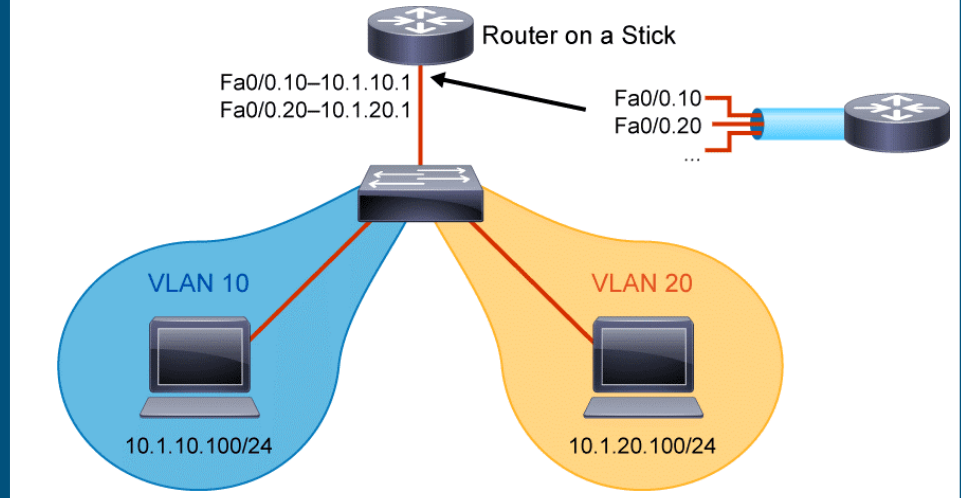
- Adresse MAC
- Sous réseau IP
- Protocole
- Politique



VLAN 4/4

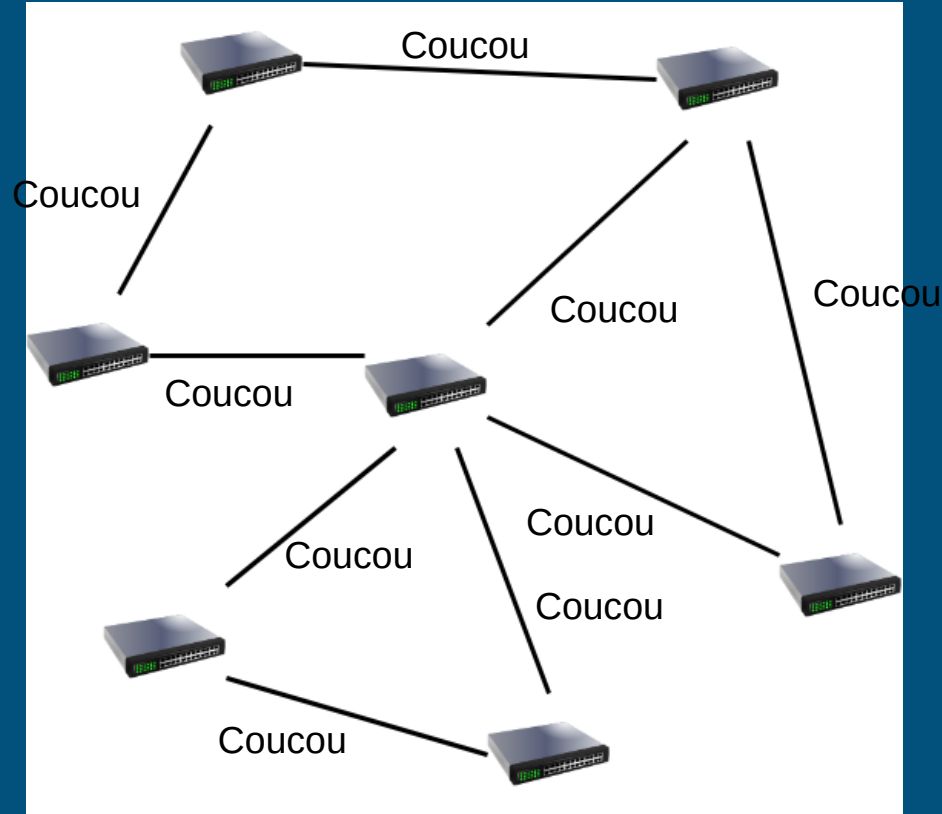
Mais dis moi Jamie, comment bébé peut quand même avoir accès aux serveurs prod ?

- Passer par la couche 3 (du modèle OSI)
 - Routeur
 - Switch de niveau 3
 - “Router on a stick”
 - SVI



Spanning Tree Protocol 1/4

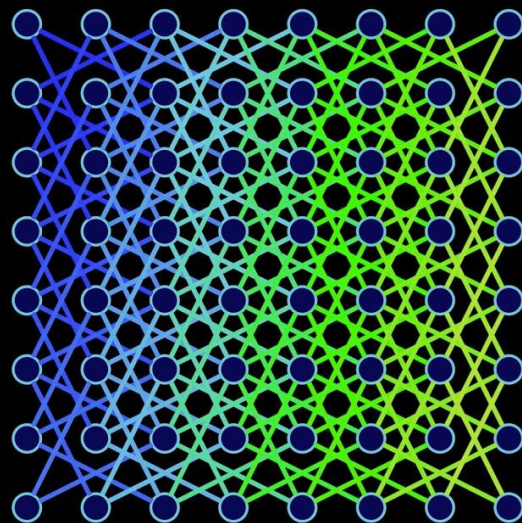
Qu'est-ce qu'un "packet storm" ?



Spanning Tree Protocol 2/4

La petite parenthèse club code :

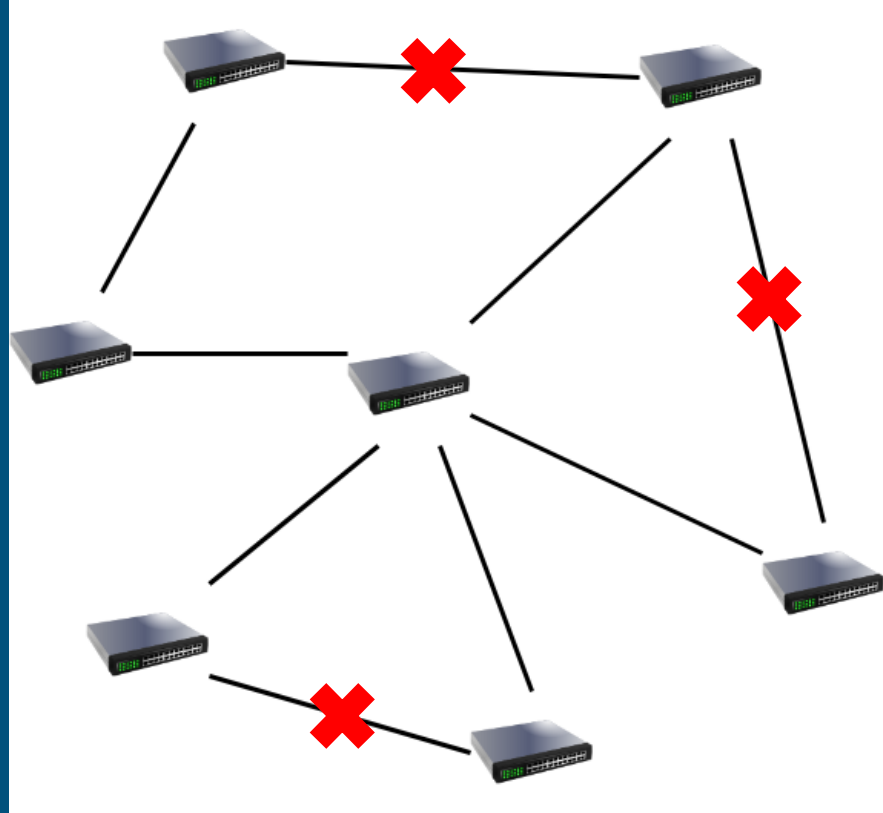
- Un graphe, c'est quoi ?
- C'est quoi un arbre ?
- C'est quoi un arbre couvrant (spanning tree) ?
- Pourquoi parler de ça ?



Graph
Theory

Spanning Tree Protocol 3/4

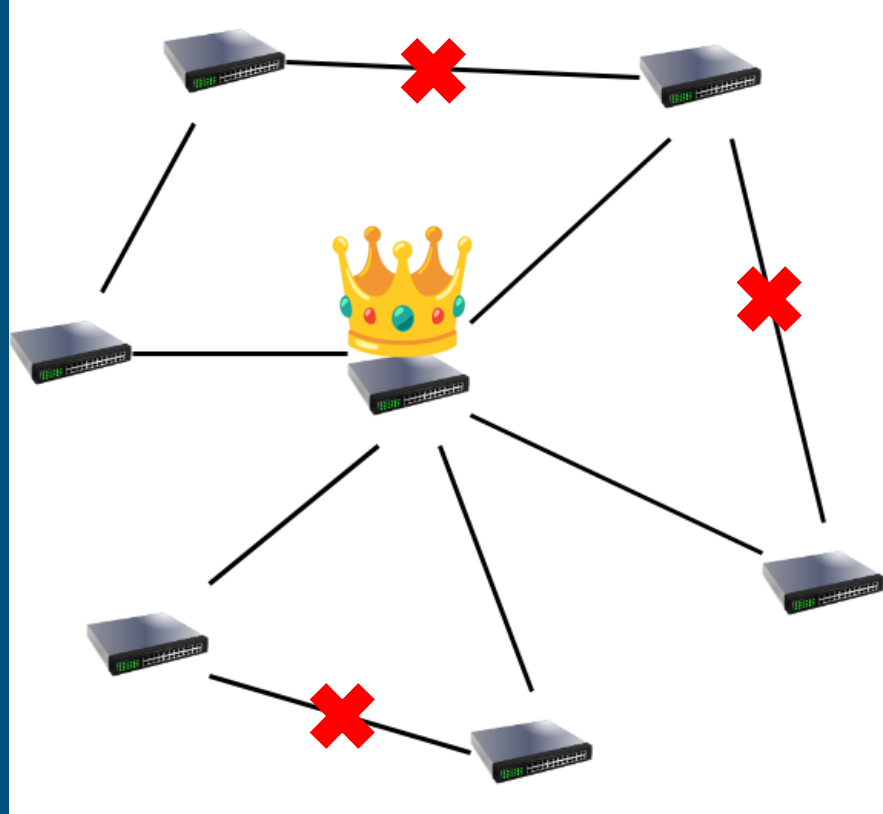
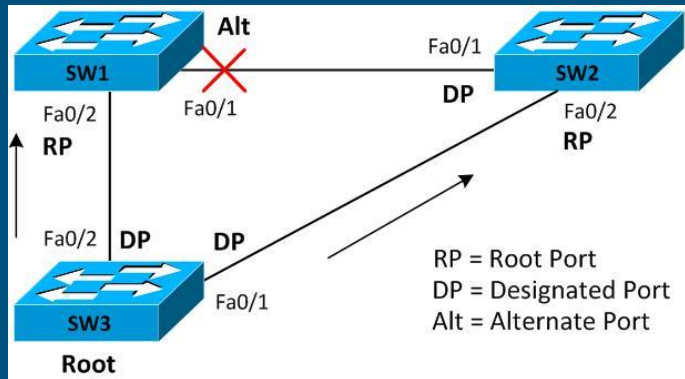
Pour remédier à ça : on fait un
arbre couvrant pour éviter les
boucles



Spanning Tree Protocol 4/4

Pour construire l'arbre couvrant minimum :

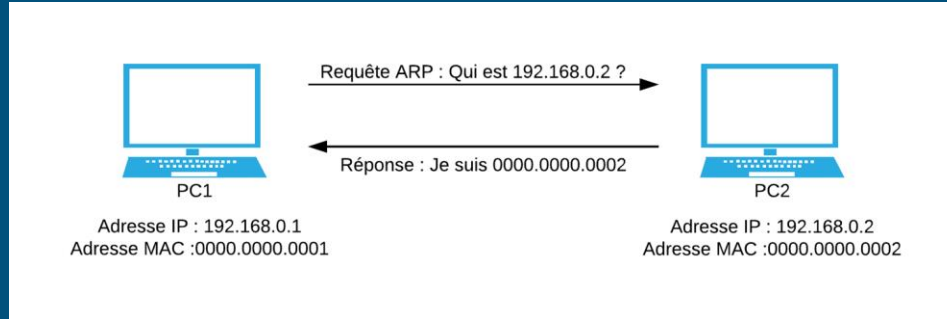
- Election d'un switch racine
- Détermination du chemin le plus court vers la racine



ARP Inspection 1/3

Address Resolution Protocol

- C'est quoi ARP déjà ?
 - a. Lien entre MAC et IP, donc couche 2 <--> couche 3
 - b. "Bonjour je dois envoyer cette trame à telle IP, c'est quoi sa MAC ?" (broadcast)
 - c. "Bonjour, c'est moi que tu cherches, voici mon IP et voici ma MAC" (unicast)
 - d. → Un broadcast + un unicast = une entrée dans le cache ARP



ARP Inspection 2/3

- Quel problème cela pose ?
 - Un attaquant peut voir et répondre à une requête ARP
 - Il peut associer sa MAC à l'IP demandée → interception de trafic (man in the middle)

ARP Inspection 3/3

- Comment y remédier ?
 - Le switch dispose d'une table de confiance
 - Réponse ARP correspond à la table → OK
 - Réponse ARP ne correspond pas à la table → suspicieux
- Et ensuite ?
 - Le trafic suspicieux peut être simplement loggé
 - On peut aussi prévenir l'administrateur (comment ?), voire couper le port

Faiblesse de ARP Inspection ?

Reboot du switch → table de confiance vide

Comment éviter une attaque à ce moment ?

Adressage et DHCP 1/3

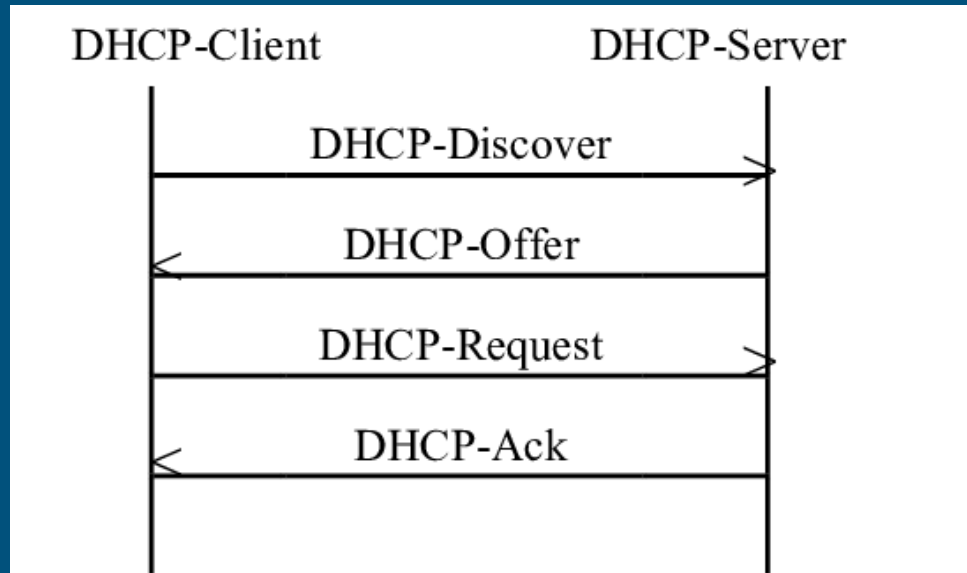
Les appareils communiquent entre eux grâce aux adresses IP
Mais d'où elle vient cette IP ?

- Attribution manuelle
 - C'est chiant
 - On a des conflits
- Automatisation
 - C'est cool et tout est pris en charge
 - C'est pas une bonne idée pour les équipements de l'administrateur
 - Sauf en cas de bail statique !

Adressage et DHCP 2/3

Fonctionnement de DHCP en pratique

Tip : DORA

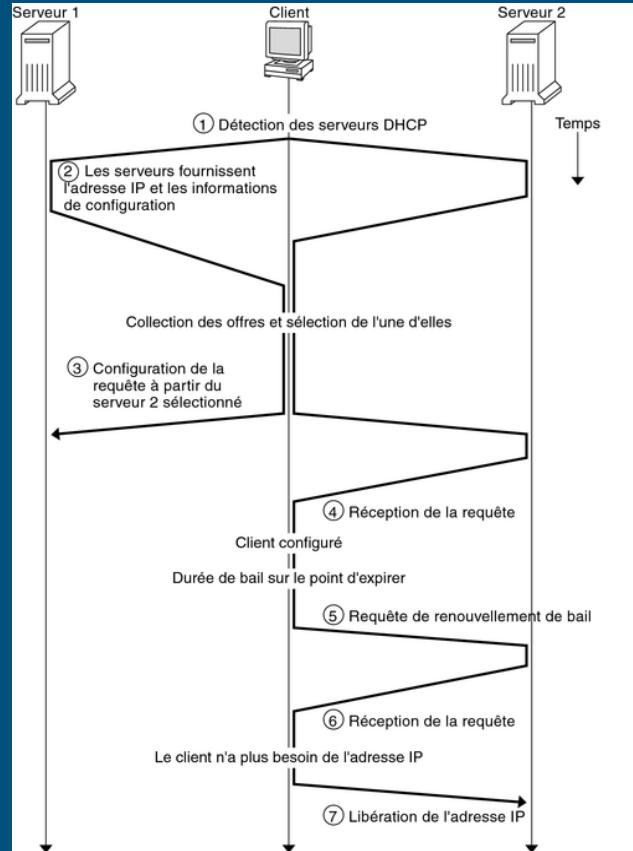


Adressage et DHCP 3/3

Éviter de tomber en
panne d'adresses

+

Ne pas être paumé si
le serveur DHCP
tombe en rade



DHCP Snooping 1/3

Comment peut-on abuser du DHCP ?

- Flood de requêtes DHCP pour épuiser les IP (DHCP Starvation)
- Quelqu'un s'interpose au milieu des requêtes DHCP et tente de se faire passer pour une gateway du serveur DHCP et faire une attaque type Man In The Middle (DHCP Spoofing)

Comment empêcher ça ?

- On paramètre simplement les ports qui ont le droit d'émettre des DHCP Offer
- Possibilité de log/prévenir un admin

DHCP Snooping 2/3

Les limites :

- Faut configurer les switchs (c'est pas grand chose mais faut le faire pour tous les switchs)
- Si on s'interpose sur un port "trusted", on peut quand même faire l'attaque

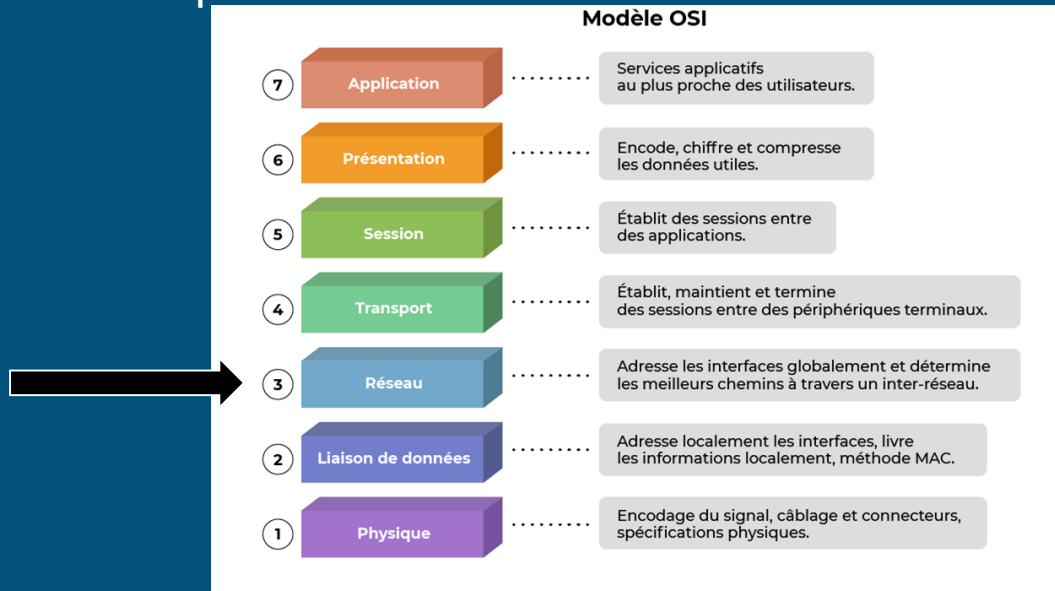
DHCP Snooping 3/3

DHCP Snooping crée une table DHCP. C'est elle que ARP Inspection utilise !

Routage 1/4

Quelques rappels rapides :

- Router c'est choisir un chemin
- Notamment utile quand on va de réseau en réseau



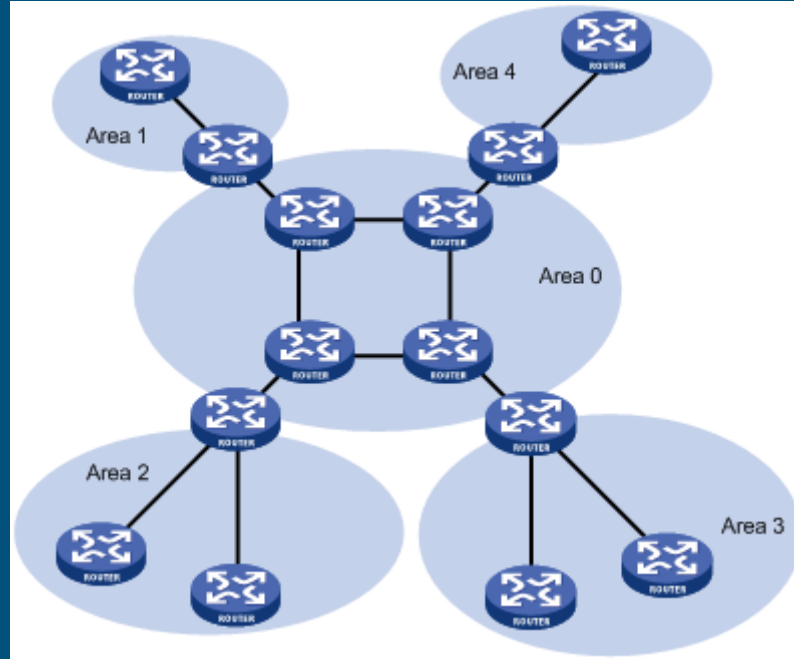
Routage 2/4

- Routage statique
 - Définition la route pour chaque réseau à atteindre
 - OK pour de petits réseaux Vierge Extra
 - Complicé en cas d'évolution
 - Devient très vite horrible
- Routage dynamique
 - Giga chads routeurs s'envoient les infos sur leurs tables de routage
 - Reconvergence automagique en cas de changement sur l'infra

Routing 3/4

IGP : OSPF

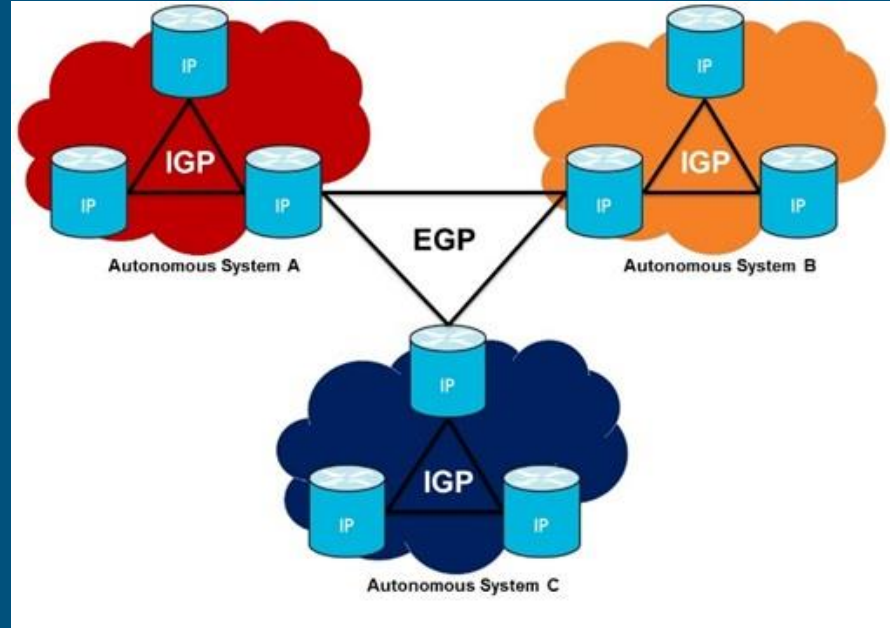
- Intérieur d'un AS
 - Réseau d'entreprise
 - Lier les routeurs d'un site
- Facile



Routeage 4/4

EGP: **BGP**

- Lie les AS entre eux
- Convergence lente
- Fragilité relative
- Super compliqué



Filtrage 1/3

Sacerakoi ?



Filtrage 2/3

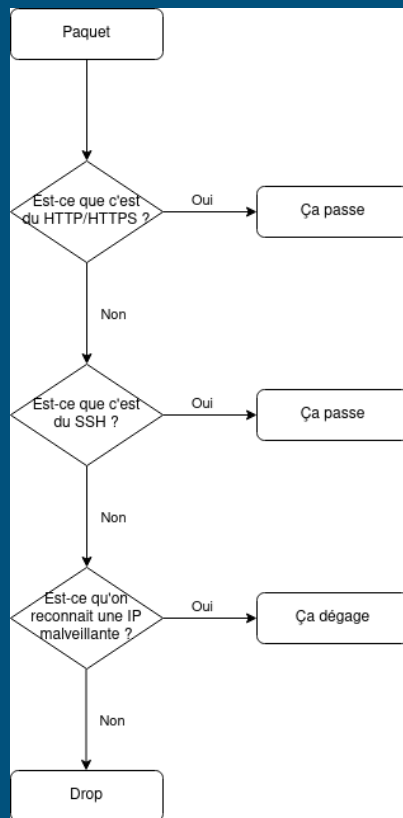
En pratique, on définit des “règles de filtrage” :

On regarde le paquet reçu et on le fait passer par toute les règles dans l'ordre

On peut ainsi choisir de :

- ALLOW/Permit : Laisser passer
- BLOCK/Deny : Ne pas laisser passer

Filtrage 3/3

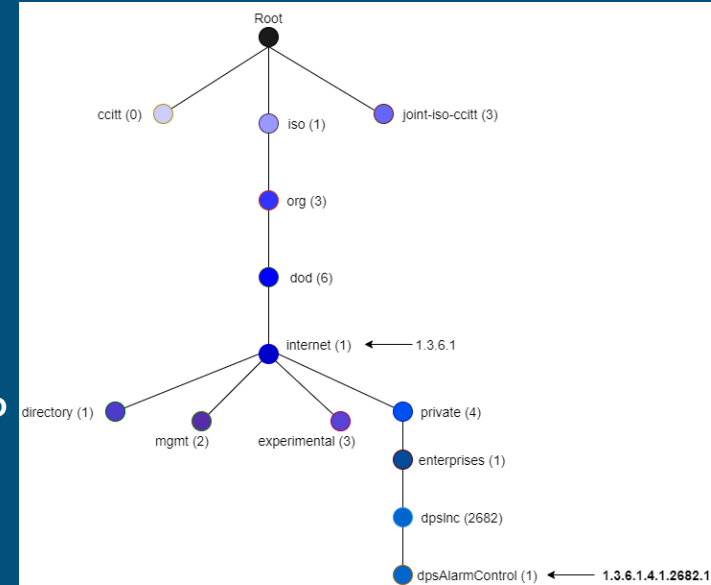


Simple Network Management Protocol

SNMP 1/4

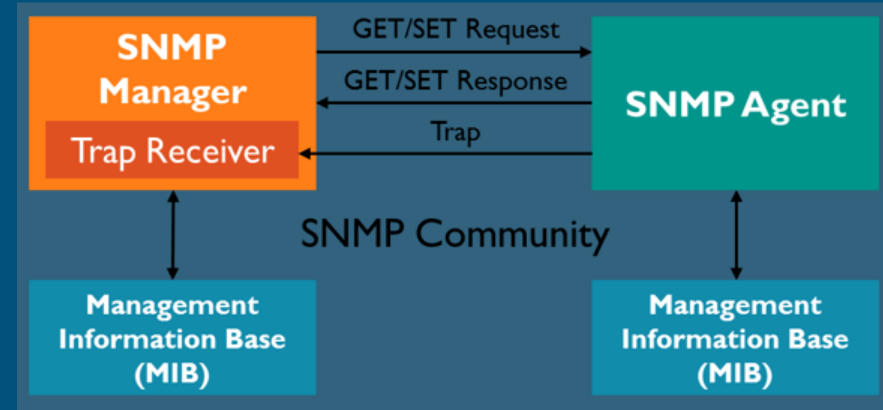
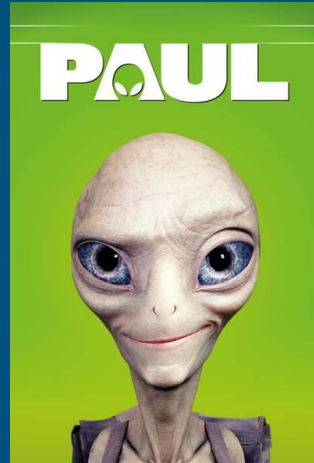
Presque tous les outils de supervision utilisent SNMP

- SNMP utilise des variables
- Ces variables sont réparties dans un arbre
- Les applications peuvent décider de la hiérarchie de leurs branches
- Un OID est une adresse qui remonte depuis la racine jusqu'aux variables
- Une MIB est une base de données permettant d'interpréter les OID



SNMP 2/4

- Les agents sont installés sur les éléments monitorés
- Les managers demandent et reçoivent les données des agents
- Les managers interprètent les données grâce à la MIB



SNMP 3/4

Un exemple :

1.3.6.1.2.1.1.3

→ vous donne l'uptime

The screenshot shows the SnmpB application window. The 'Remote SNMP Agent' is set to 'CISCO1940'. The 'MIB Tree' panel displays a hierarchical view of the MIB, with 'sysUpTime' selected under the 'system' node. The 'Query Results' panel shows the output of the query: '-----SNMP query started-----', '1: sysUpTime.0 14 days, 6:19:27.60', '-----SNMP query finished-----', 'Total # of Requests = 1', and 'Total # of Objects = 1'. The 'Node Info' panel provides detailed information about the selected 'sysUpTime' object.

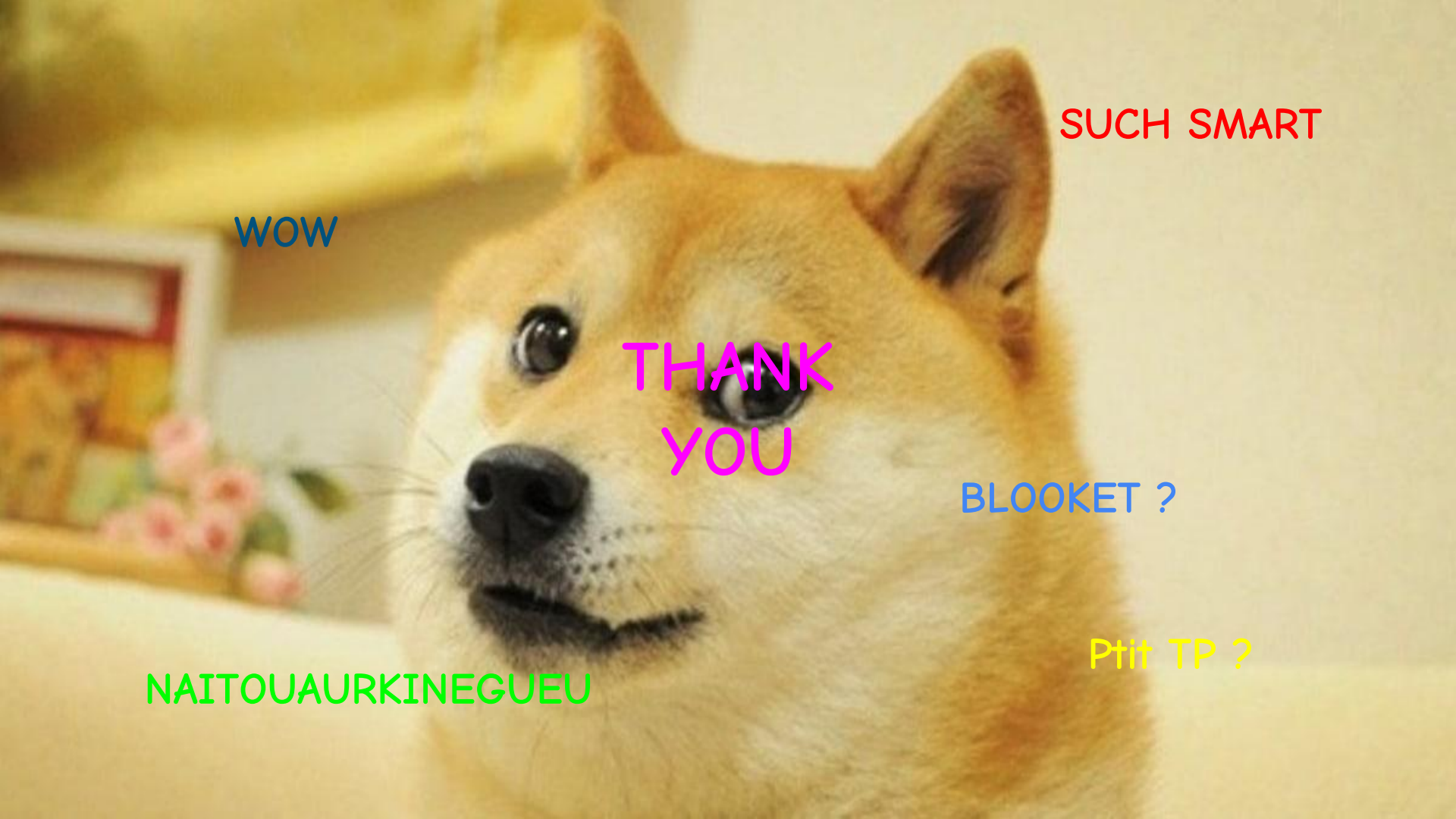
Node Info	
Name:	sysUpTime
Oid:	1.3.6.1.2.1.1.3
Composed Type:	TimeTicks
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 4294967295
Module:	SNMPv2-MIB
Description:	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

SNMP 4/4

Zabbix

Un manager
agençant les
données pour
les rendre plus
exploitables





SUCH SMART

WOW

THANK
YOU

BLOOKET ?

Ptit TP ?

NAITOUAURKINEGUEU