

## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

# **Interconnexion de réseaux locaux**

## **Objectifs**

Cette leçon a pour but de présenter les outils de base de l'interconnexion de réseaux locaux que sont les ponts et les switch Ethernet.

## **Prérequis**

Bonne connaissance des réseaux locaux, en particulier d'Ethernet.

## **Connaissances**

Objectifs et principes des ponts et switch Ethernet.

## **Compétences**





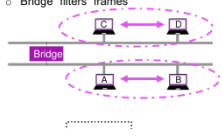

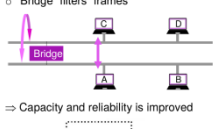
Définir une architecture réseau fondée sur des ponts ou des switch Ethernet.



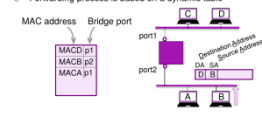

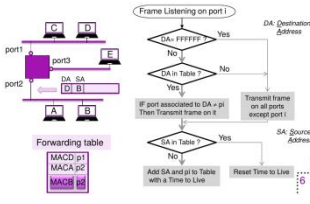
## **Évaluation des connaissances**


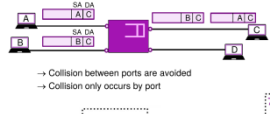




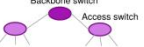

Description du fonctionnement d'un pont.

## **Évaluation des compétences**

Analyse d'une architecture réseau.

 <p><b>Enterprise networks</b> Local Area Network Interconnection</p> <p>Béatrice Paillassa</p>	<p>Cette leçon présente l'architecture des réseaux locaux utilisés en entreprise. Elle explique le concept de raccordement par pont et sa mise en œuvre par des switch.</p>
 <p>Some history of LAN architecture</p> <ul style="list-style-type: none"> <li>Deployment issues in enterprise <ul style="list-style-type: none"> <li>Distance issue</li> <li>Performance issue</li> </ul> </li> <li>Resolved by interconnection</li> </ul> <p>High speed backbone network</p> 	<p>Lorsqu'il a fallu passer du stade du laboratoire au déploiement en entreprise, les réseaux locaux ont dû faire face à des problèmes de déploiements liés à leur limitation en distance et en débit.</p> <p>Ces problèmes ont été résolus par un mécanisme d'interconnexion entre différents réseaux, recouvrant chacun un bâtiment à un débit à l'époque de 10 Mbps, qui étaient raccordés par un réseau de débit plus élevé, le réseau d'arrière-plan, par l'intermédiaire de ponts.</p>
 <p><b>BRIDGE Interconnection</b></p> <ul style="list-style-type: none"> <li>All elements of the bridge interconnection receive a broadcast frame → they are in the same LAN</li> <li>Bridge "filters" frames</li> </ul> 	<p>Tous les éléments qui appartiennent à l'interconnexion sont capables de recevoir les trames en diffusion, ils sont dans le même réseau local.</p> <p>En ce qui concerne les autres trames, le pont va effectuer un filtrage de telle sorte que les communications propres à un réseau local restent localisées sur ce réseau local.</p> <p>Sur l'illustration, les stations C et D peuvent échanger en même temps que les stations A et B.</p> <p>Si un échange doit avoir lieu entre la station C sur un réseau et la station A sur un autre réseau, le pont se chargera de relayer les trames</p> <p>Le pont augmente la capacité du réseau local. Il améliore également la sûreté de fonctionnement du système car si un réseau local tombe en panne, des communications peuvent continuer à fonctionner sur un autre réseau local.</p>
 <p><b>BRIDGE Interconnection</b></p> <ul style="list-style-type: none"> <li>All elements of the bridge interconnection receive a broadcast frame → they are in the same LAN</li> <li>Bridge "filters" frames</li> </ul>  <p>⇒ Capacity and reliability is improved</p>	<p>La fonction principale du pont est le relayage de trame</p> <p>Le pont écoute les trames qui circulent sur tous les réseaux qu'il raccorde. Pour chaque trame, le pont détermine s'il doit la relayer et sur quel réseau. Pour ce faire, il utilise l'algorithme standard 802.1d qui est l'algorithme de pont transparent.</p>

 <h3>BRIDGE functioning</h3> <ul style="list-style-type: none"> <li>Frame forwarding <ul style="list-style-type: none"> <li>Receive all MAC frames</li> <li>Filter frames to forward <ul style="list-style-type: none"> <li>→ IEEE 802.1D transparent bridging algorithm</li> </ul> </li> <li>Transmit the filtered frames with the MAC protocol</li> </ul> </li> <li>Heterogeneous MAC <ul style="list-style-type: none"> <li>Bridge adapt MAC frame format : header, frame length ...</li> </ul> </li> </ul>	<p>L'algorithme du pont transparent est le suivant.</p> <p>Le pont utilise un processus de relayage en se référant à une table remplie de façon dynamique.</p> <p>Dans cette table il y a une association entre les adresses destination des stations et les ports par lesquels le pont peut joindre une station.</p> <p>Sur l'illustration B transmet à D. Le pont écoute, il decode la trame. Grâce à la table il sait que D peut être atteinte par le port 1. Il relaie la trame sur ce port.</p> <p>Quand une trame est entendue et que l'adresse destination n'est pas connue, le pont transmet la trame sur tous les ports excepté celui sur lequel il a entendu la trame. Toutes les stations reçoivent la trame, y compris donc le destinataire.</p> <p>Pour remplir la table, le pont se débrouille tout seul, le processus est transparent d'où le nom de l'algorithme, grâce à un processus d'apprentissage simple : le pont qui entend une station source sur un port associe son adresse à ce port dans la table.</p>
 <h3>IEEE802.1D-Transparent bridging</h3> <ul style="list-style-type: none"> <li>Forwarding process is based on a dynamic table <div>  </div> </li> <li>Unknown frame are broadcasted on all ports except on reception port</li> <li>Learning process : table is filled up dynamically</li> </ul>	<p>Le pont raccorde 3 segments par 3 ports notés p1, p2, p3.</p> <p>B souhaite transmettre à D. B élabore une trame avec comme adresse destination D et comme adresse source B, et transmet sa trame.</p> <p>Le pont entend la trame. Il vérifie si la trame est en diffusion. Ce n'est pas le cas.</p> <p>Il cherche dans sa table de relayage s'il connaît l'adresse destination D. Il trouve que l'adresse destination est associée au port 1. Le pont va donc relayer la trame sur le port1.</p>
 <h3>Transparent bridging algorithm</h3> <div>  </div>	<p>Le pont va également effectuer son processus d'apprentissage. Il vérifie dans sa table si il connaît ou pas l'adresse source. Si ce n'est pas le cas il va mémoriser dans sa table l'adresse, en lui associant une durée de vie.</p> <p>Ainsi si une station change de port, l'entrée de la table va s'éliminer au bout d'un certain temps sans que le pont ait à faire quoi que ce soit.</p>

 <p>Beyond the bridge is the Ethernet switch</p> <ul style="list-style-type: none"> <li>o Ethernet switch forwards frame according to 802.1D algorithm</li> <li>o Switch schedules frames</li> </ul>  <p>→ Collision between ports are avoided → Collision only occurs by port</p>	<p>Au-delà du pont, le switch Ethernet</p> <p>Le switch Ethernet relaye les trames avec l’algorithme 802.1 d que nous venons de voir.</p> <p>Le switch ordonnance également les trames de façon à éviter les collisions</p> <p>Lorsque 2 stations, A et B sur l’illustration, transmettent à C, le switch détermine par l’algorithme de pont transparent sur quel port il doit relayer les trames, et il ordonnance les trames de façon à éviter les collisions sur le port de sortie.</p> <p>Avec un switch Ethernet on considère que les collisions sont par port.</p>
 <p>HUB –SWITCH What is the difference?</p> <ul style="list-style-type: none"> <li>o HUB acts as a IEEE Repeater Stations receive all frames</li> <li>o Switch acts as a IEEE bridge Stations receive: <ul style="list-style-type: none"> <li>• Destinated frames</li> <li>• Broadcast frames</li> <li>• Unknown frames</li> </ul> </li> </ul> 	<p>Quelle est la différence entre un équipement hub et un équipement switch ?</p> <p>Un Hub fonctionne comme un répéteur. Chaque station est capable de recevoir toutes les trames car un répéteur fait passer toutes les trames d’un segment à un autre segment.</p> <p>Par contre pour un switch c’est différent. Le switch fonctionne comme un pont. Les stations ne reçoivent que les trames qui leur sont destinées, les trames en diffusion, ainsi que les trames dont le switch ne connaît pas l’adresse destination.</p>
 <p>Enterprise network representations</p> <p>LAN logical view</p>  <p>LAN hierarchical view</p>  <p>LAN technical view</p> 	<p>Nous pouvons faire une synthèse des architectures de réseau d’entreprise en nous appuyant sur le schéma.</p> <p>Dans l’entreprise le réseau local peut être considéré comme un système à diffusion, donc on peut le représenter par une vue logique comme étant un bus</p> <p>En fait, ce bus est constitué par un ensemble de switch. Ces switch sont des switchs d’accès, localisés dans des bâtiments qui raccorderont des stations, et, ces switchs sont organisés de façon hiérarchique. Ils sont raccordés à un switch qui agit comme le réseau d’arrière-plan vu en début de cette leçon.</p> <p>Cette vue va être réalisée par un ensemble de matériels que l’on peut voir sur l’image. Il y manque les câbles, il devrait y avoir un peu partout des câbles reliant les ports de ces équipements.</p>



### Summary

- Ethernet networks are based on SWITCH elements
- Switch offers a bridge function
  - Frames are filtered with transparent bridging algorithm
- Enterprise networks are based on level 2, routing by destination

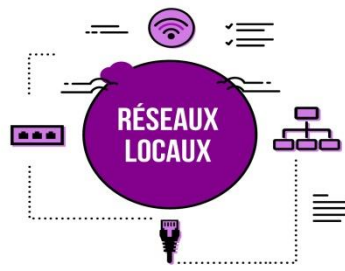


10

Les équipements Ethernet utilisés en entreprise sont des switches.

Leur fonctionnement est analogue à celui d'un pont. Le switch filtre les trames en utilisant l'algorithme de pont transparent.

Dans le réseau d'entreprise le routage est dit de niveau 2, il s'effectue sur les trames, et, c'est un routage par destination puisque les tables contiennent des adresses destination MAC.



## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

# **La problématique des réseaux locaux d'entreprise**

## **Objectifs**

Cette leçon a pour but de présenter les contraintes liées aux réseaux locaux intégrant de nombreuses machines sur une zone vaste.

## **Prérequis**

Connaissance des principes et fonctionnement des réseaux locaux tels qu'ethernet ou Wi-Fi.

## **Connaissances**

Identifier les difficultés de passage à l'échelle des réseaux locaux.

## **Compétences**



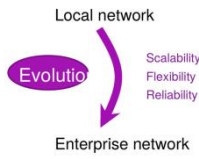


Savoir définir l'architecture d'un réseau local de grande ampleur.

## **Évaluation des connaissances**

Décrire les enjeux des réseaux locaux d'entreprise.

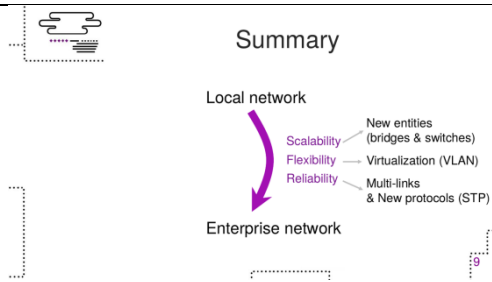
## **Évaluation des compétences**

Définir l'architecture d'un réseau local.

 <p><b>Enterprise networks</b> <i>Challenges</i></p> <p>Julien FASSON</p>	<p>Imaginons que l'on est des milliers d'utilisateurs sur plusieurs sites différents. On a vu l'Ethernet et le wifi. Mais ils ne vont pas être suffisants pour mettre en place de tel type de réseaux locaux, que l'on appelle des réseaux d'entreprise.</p> <p>L'objectif de cette leçon est donc de voir les besoins des réseaux locaux à évoluer vers les réseaux d'entreprise actuels.</p>
 <p><b>Objectives</b></p> 	<p>Ces trois besoins que je vous ai choisis sont le passage à l'échelle, la flexibilité et une certaine qualité de service.</p> <p>Commençons par le premier besoin : le passage à l'échelle.</p>
 <p><b>Scalability</b></p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>↗ AREA</p> <p><b>But</b></p> <ul style="list-style-type: none"> <li>• Wi-Fi coverage area is limited</li> <li>• Ethernet on twisted pair cables</li> <li>✓ Max length = 100m</li> <li>✓ Max number of repeaters = 4</li> </ul> <p>⇒ Limited to small buildings</p> </div> <div style="text-align: center;"> <p>↗ USERS &amp; DEVICES</p> <p><b>But</b></p> <ul style="list-style-type: none"> <li>• CSMA/CA &amp; CSMA/CD cannot scale</li> </ul> <p>⇒ Limited to few users</p> </div> </div>	<p>En fait, il y a deux problèmes de passage à l'échelle.</p> <p>D'abord, il y a le passage à l'échelle géographique. Les entreprises veulent être de plus en plus étendues et donc leurs réseaux aussi. Or, si l'on regarde les technologies comme Ethernet ou wifi, elles ont des limites en termes de portée ; wifi a une petite portée alors qu'Ethernet en utilisant de la paire de cuivre torsadée à une taille maximum de 100 mètres. Si on rajoute 4 répéteurs, cela fait une taille maximale de 500 mètres ce qui est très petit pour un réseau. Donc on est limité à de petits bâtiments. D'autre part, il y a un passage à l'échelle en nombre d'utilisateurs.</p> <p>Les réseaux d'entreprise ont de plus en plus d'équipements connectés. Or, si l'on regarde les deux méthodes d'accès qui sont CSMA/CA et CSMA/CD, elles sont très sensibles au nombre d'utilisateurs et risque de s'écrouler dans le cas d'un trop grand nombre d'utilisateurs sur le réseau.</p>
 <p><b>Solution for scalability</b></p> <ul style="list-style-type: none"> <li>○ Cut the network into pieces <ul style="list-style-type: none"> <li>• Large number of small pieces</li> <li>• Interconnected</li> </ul> </li> </ul> <p style="text-align: center;">↓</p> <ul style="list-style-type: none"> <li>○ New equipments <ul style="list-style-type: none"> <li>• Bridges</li> <li>• Switches</li> </ul> </li> </ul>	<p>La solution pour le passage à l'échelle est de couper le problème en morceau. On va couper le réseau en petits morceaux que l'on va devoir interconnecter les uns avec les autres, et pour cela il va falloir introduire de nouveaux équipements : les ponts et les commutateurs internet.</p>

 <h3>Flexibility</h3> <ul style="list-style-type: none"> <li>Users want to be in their LAN <ul style="list-style-type: none"> <li>✓ In the office</li> <li>✓ At home</li> </ul> </li> <li>Multi-sites</li> <li>Different LAN in a same site</li> </ul> <p><b>But</b></p> <p>Multiplication of networks &amp; equipments</p> <p>⇕</p> <p>One cable = One network</p> <p>5</p>	<p>Le second besoin, il est en termes de flexibilité.</p> <p>Un utilisateur qu'il soit chez lui en télétravail ou à son bureau, veut être dans son réseau d'entreprise. À côté de cela, une entreprise peut avoir plusieurs sites à travers le monde, elle voudrait que son réseau soit unique. Et encore, une même entreprise sur un même site peut avoir besoin d'avoir plusieurs réseaux par exemple un réseau pour la comptabilité et un autre pour l'exploitation. Donc, là, on va avoir un gros problème, car si l'on veut réussir à faire un réseau avec autant de flexibilité, on va devoir multiplier les câbles, multiplier les équipements, car, dans les réseaux que l'on vous a présenté, un câble égale un réseau, une borne wifi égale un réseau.</p>
 <h3>Solution for flexibility</h3> <p>Virtualization</p> <ul style="list-style-type: none"> <li>One cable = Several networks</li> <li>Virtual Local Area Network : VLAN</li> </ul> <p>6</p>	<p>Pour résoudre ce problème, la solution qui va être mise en place, c'est de la virtualisation : on va essayer de mettre sur une entité physique, un même câble par exemple, des réseaux différents. Cela va nous conduire à une notion, la notion de Virtual Local Area Network que l'on appelle les VLANs.</p>
 <h3>Reliability</h3> <ul style="list-style-type: none"> <li>LAN has to ensure <ul style="list-style-type: none"> <li>Heavy traffic load</li> <li>Hardware breaks down</li> </ul> </li> </ul> <p><b>But</b></p> <p>Ethernet &amp; Wi-Fi aren't redundant</p> <p>7</p>	<p>Enfin le troisième besoin, c'est d'apporter une certaine qualité de service. Cela signifie ici, pour un LAN, de pouvoir travailler avec un grand nombre d'utilisateurs et donc une grande charge en trafic. Mais il s'agit aussi de ne pas tomber dès qu'un seul équipement, qu'une seule carte, un seul câble est défaillant.</p> <p>Le problème, c'est que dans Ethernet et Wifi, tel que nous l'avons vu, il n'y a pas vraiment de redondance. Donc comment introduire cette redondance ?</p>
 <h3>Solution for reliability</h3> <ul style="list-style-type: none"> <li>Multiple links for the same destination <ul style="list-style-type: none"> <li>Need of equipments</li> <li>Issues: <ul style="list-style-type: none"> <li>✓ Manage multiple links (loops)</li> <li>✓ Detect hardware failures</li> </ul> </li> </ul> </li> </ul> <p>⇓</p> <ul style="list-style-type: none"> <li>A new protocol: STP Spanning Tree Protocol</li> </ul> <p>8</p>	<p>On va introduire des liens multiples dans le réseau. Ces liens multiples, bien sûr pour fonctionner, ont besoin d'équipements dont je vous ai déjà parlés : des commutateurs et des ponts. Ils présentent des problèmes, car dès qu'il y a des liens multiples, il y a des boucles dans le réseau. Le second problème est qu'il faudra être capable de détecter les pannes matérielles.</p> <p>Pour cela, on va mettre en place un nouveau protocole qui se nomme STP pour Spanning Tree Protocol.</p>





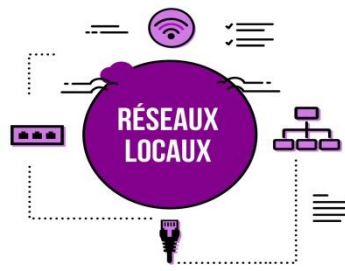
Pour conclure, nous avons vu trois enjeux principaux des réseaux locaux pour devenir des réseaux d'entreprises ; à savoir :

- le passage à l'échelle,
- la flexibilité et
- une certaine qualité de service.

Nous avons pointé du doigt les solutions qui sont :

- de mettre en place des nouvelles entités, des nouveaux équipements,
- d'utiliser de la virtualisation, avec les VLANS,
- d'utiliser plusieurs liens, des liens multiples et donc de mettre en place un protocole, le protocole STP pour gérer tout ça.

Au cours de cette semaine, vous allez voir en détail ces solutions.



## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

# **Les réseaux locaux virtuels dynamiques**

## Objectifs

Cette leçon a pour but de présenter les principes des réseaux locaux virtuels dynamiques.

## Prérequis

Bonne connaissance des réseaux locaux. Connaissance de la problématique des réseaux locaux d'entreprise, connaissance des réseaux privés virtuels.

## Connaissances

Principe de fonctionnement des réseaux privés virtuels dynamiques.

## Compétences




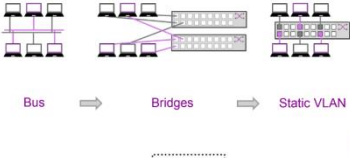

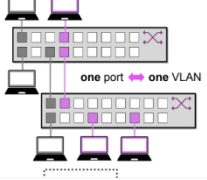
Définir une architecture réseau fondée sur la notion de réseaux locaux virtuels dynamiques.

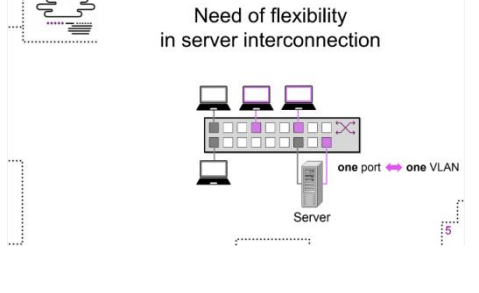
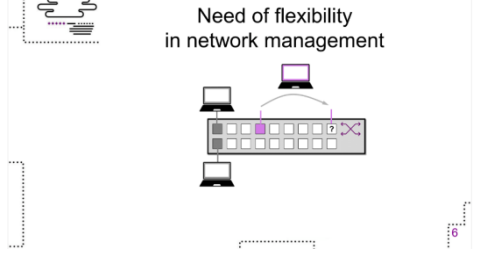
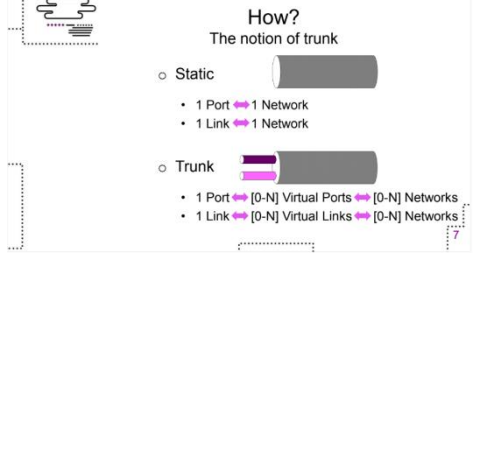
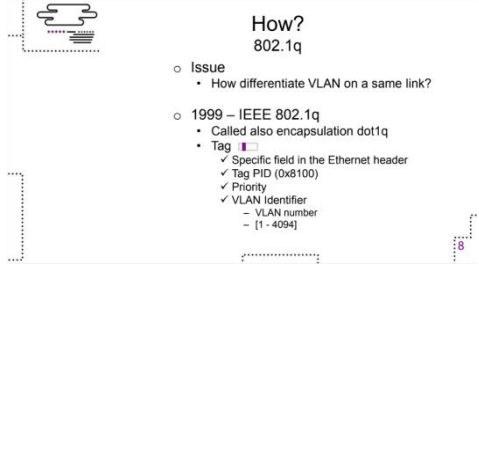
## Évaluation des connaissances

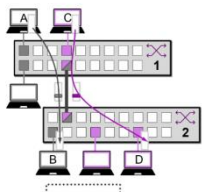
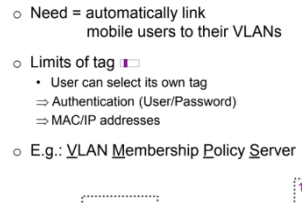
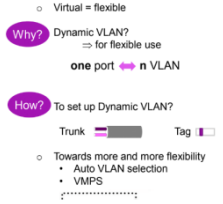
Décrire les principes d'un réseau local virtuel dynamique.

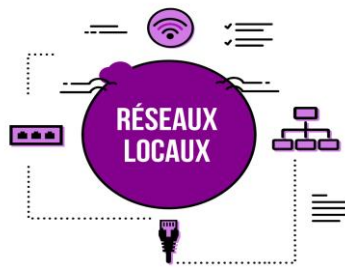
## Évaluation des compétences

Définir une architecture réseau fondée sur la notion de réseaux locaux virtuels dynamiques.

 <p><b>Enterprise Network</b> <i>Dynamic VLAN</i></p> <p>Julien FASSON</p>	<p>Dans cette leçon, nous allons introduire la « dynamicité » dans les VLANs.</p>
 <p><b>Objectives</b></p> <p>Dynamic VLAN...</p> <ul style="list-style-type: none"> <li>Why? Need of more flexibility</li> <li>How? Implementation</li> </ul>	<p>Je vous propose de voir pourquoi l'on a besoin de faire des VLANs dynamiques, à savoir le besoin de flexibilité. Déjà, les VLANs ont introduit de la flexibilité comme on va le voir, mais il y a un besoin supplémentaire. Et ensuite nous allons voir comment nous allons mettre en œuvre cette flexibilité.</p>
 <p><b>Evolution of LAN topology</b></p> 	<p>Donc, pour faire un petit récapitulatif de l'évolution des LANs :</p> <ul style="list-style-type: none"> <li>- Dans un premier temps, on avait les bus. Par exemple, là, j'avais besoin d'un réseau, je mets un bus pour faire un réseau. J'ai besoin d'un deuxième réseau dans mon entreprise, je mets un deuxième bus dans ce réseau. Le problème, c'est que j'ai besoin de câblage un peu partout.</li> <li>- Et du coup, on va inventer des équipements, par exemple les ponts ou les commutateurs, qui vont permettre de réduire le nombre de câbles nécessaires et d'avoir des équipements actifs dans le réseau.</li> <li>- Puis on va mettre en place des VLANs qui vont nous permettre au lieu d'avoir deux commutateurs différents pour avoir deux réseaux d'avoir un seul commutateur pour avoir deux réseaux.</li> </ul>
 <p><b>Need of flexibility in switch interconnection</b></p> 	<p>À partir de là voyons ce dont on a besoin en plus que simplement des VLANs statiques.</p> <p>Regardons d'abord un premier besoin : celui d'interconnecter un ou deux, ou trois, ou quatre commutateurs ensembles. Là, je vous ai mis deux commutateurs. Si, par exemple, sur les deux commutateurs, vous partagez deux VLANs différents, il va falloir pour interconnecter le VLAN gris : un port sur le commutateur du haut et un port sur le commutateur du bas puis un câble entre les deux. Et pour interconnecter le VLAN violet, un port sur le commutateur du haut et un port</p>

	<p>sur le commutateur du bas.</p> <p>Donc si vous avez dix VLANs, vous aurez dix liens et dix ports occupés en statiques sur chacun des commutateurs pour dire, j'appartiens VLAN 1, j'appartiens au VLAN 2 et ainsi de suite.</p>
	<p>De la même manière, si vous voulez mettre un équipement sur votre réseau qui appartient à deux réseaux différents : par exemple, vous avez un serveur d'authentification sur plusieurs VLANs car vous avez besoin d'authentifier vos utilisateurs sur plusieurs réseaux. Et bien, ce serveur va devoir être branché d'une part sur le VLAN 1, le gris et sur l'autre VLAN, le VLAN 2, le violet.</p>
	<p>Enfin, si un utilisateur décide de bouger, par exemple, il change d'endroit, de pièce ou de bureau. Et bien, il va se retrouver à un autre endroit, s'y brancher, et la question qui se pose est : comment je fais pour me retrouver dans mon VLAN, le VLAN violet ?</p>
	<p>Alors comment introduire cette virtualité dynamique ?</p> <p>On a besoin d'une notion, la notion de trunk.</p> <p>À la base sans trunk, un port va être statique, cela signifie que ce port équivaut à un réseau, de la même manière le lien branché sur ce port est dans un seul réseau, un VLAN.</p> <p>Si l'on rajoute la notion de trunk, on va dire que le port est découpé en plusieurs sous-ports qui sont des ports virtuels et ces ports virtuels vont correspondre à autant de réseaux que l'on a envie, de 0 à N. Bien sûr, il va falloir mettre un maximum. Et cela ne peut pas se faire tout seul.</p>
	<p>On a besoin d'une autre notion qui est la notion introduite par 802.1q que l'on appelle souvent dot1q. Si vous utilisez des équipements, des commutateurs par exemple, vous aurez besoin de ce mode d'encapsulation, dot1q. Et l'on va introduire une étiquette, un tag, que l'on va venir coller dans l'en-tête de la trame Ethernet pour dire « cette trame appartient à tel VLAN ». Cela signifie que cette couleur, ce VLAN que l'on va introduire, va directement être marqué à l'intérieur de la trame Ethernet. Cela passe par un petit champ que l'on appelle le champ VLAN identifier qui est lui-même dans un champ spécifique.</p>

 <p><b>Illustration</b> Switch interconnection</p>	<p>Pour comprendre ces principes, je vous propose de reprendre l'illustration précédente d'interconnexion entre deux switches, 1 et 2, qui partagent deux VLANs, le VLAN gris et le VLAN violet.</p> <p>On va transformer les deux liens qui permettent l'interconnexion des VLANs en un trunk, et, à partir de là, si la machine A veut communiquer avec la machine B, elle va envoyer sa trame au commutateur. Le commutateur va ajouter un tag et l'envoyer au commutateur 2 qui pourra savoir à quel VLAN appartient la trame, le gris, et l'envoyer à B.</p> <p>De la même façon quand la machine C envoie une trame vers D, elle va être taguée et le commutateur 2 pourra savoir que cette trame ne peut être envoyée qu'aux machine du VLAN violet, et donc à D.</p>
 <p><b>Towards more flexibility</b></p> <ul style="list-style-type: none"> <li>o Need = automatically link mobile users to their VLANs</li> <li>o Limits of tag <ul style="list-style-type: none"> <li>• User can select its own tag <ul style="list-style-type: none"> <li>⇒ Authentication (User/Password)</li> <li>⇒ MAC/IP addresses</li> </ul> </li> </ul> </li> <li>o E.g.: <u>VLAN Membership Policy Server</u></li> </ul>	<p>Bien sûr, ce n'est pas suffisant en soi. Le simple tag ne va pas permettre à un administrateur de réseau de configurer automatiquement les VLANs des utilisateurs lorsqu'ils bougent, ce qui était notre besoin précédent.</p> <p>Pourquoi ? Parce que notre utilisateur pourrait très bien décider tout seul du VLAN auquel il appartient, au lieu d'être dans le VLAN de production par exemple, il peut se mettre dans le VLAN administrateur s'il a à choisir et à tagger lui-même ses trames.</p> <p>Donc, ça demande d'autres technologies, d'autres mécanismes. Une solution consiste à authentifier de l'authentification des utilisateurs qui va être couplé au taggage pour lui permettre de rentrer dans son VLAN. On peut aussi un lien entre son adresse MAC et le VLAN auquel il appartient.</p> <p>Pour faire cela, un certain nombre de protocoles existe dont le plus commun est VLAN Membership Policy Server, VMPS, qui est un protocole utilisé par CISCO pour ses commutateurs.</p>
 <p><b>To summarize</b></p> <ul style="list-style-type: none"> <li>o Virtual = flexible</li> <li>Why? Dynamic VLAN? <ul style="list-style-type: none"> <li>⇒ for flexible use</li> <li>one port → n VLAN</li> </ul> </li> <li>How? To set up Dynamic VLAN? <ul style="list-style-type: none"> <li>Trunk → Tag</li> </ul> </li> <li>o Towards more and more flexibility <ul style="list-style-type: none"> <li>• Auto VLAN selection</li> <li>• VMPS</li> </ul> </li> </ul>	<p>La notion à retenir est que virtualisation rime avec flexibilité.</p> <p>Dans cette leçon, nous avons vu :</p> <ul style="list-style-type: none"> <li>- pourquoi on avait besoin de « dynamicité »</li> <li>- comment on mettait en place les VLANs dynamiques</li> <li>- et comment on allait plus loin avec l'affectation dynamique de port, par exemple avec VMPS.</li> </ul>



## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

## **Les réseaux locaux virtuels**

### Objectifs

Cette leçon a pour but de présenter le fonctionnement des réseaux locaux virtuels.

### Prérequis

Bonne connaissance des réseaux locaux, d'Ethernet et du fonctionnement des switch Ethernet.

### Connaissances

Principes et mise en œuvre des réseaux locaux virtuels.

### Compétences



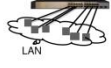




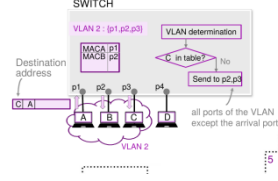
Analyse d'un réseau local à base de réseaux virtuels.

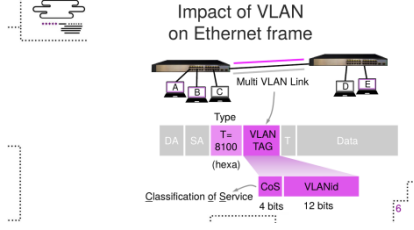
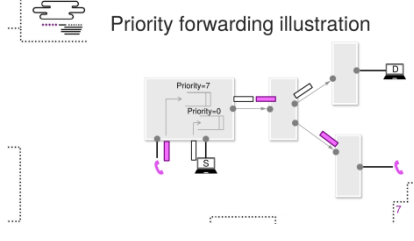
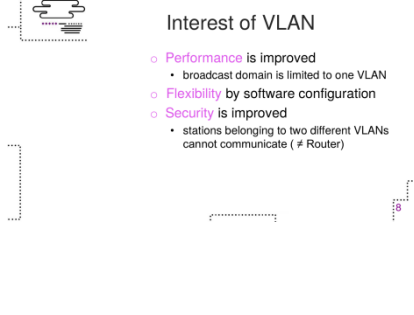
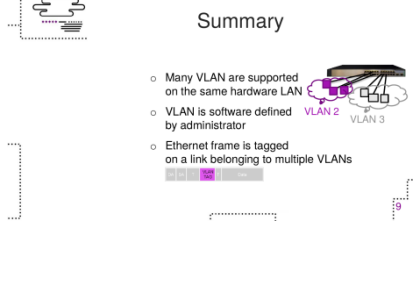
### Évaluation des connaissances

Description du principe des réseaux locaux virtuels.

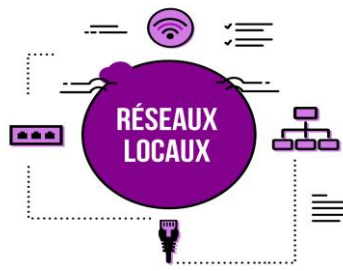
### Évaluation des compétences

Définir un réseau à base de réseaux locaux virtuels.

 <p><b>Enterprise networks</b> Virtual Local Area Networks</p> <p>Béatrice Paillassa</p>	<p>La notion développée dans cette leçon est celle de réseau virtuel qui correspond à un fonctionnement logiciel du réseau local. Ce qui permet d'avoir plusieurs instances de réseaux locaux sur le même matériel.</p>
 <p>What is a <u>Virtual Local Area Network</u>?</p> <p>LAN = Broadcast domain : all elements receiving broadcast frames</p> <div> <div> <p>Hardware LAN</p> <p>→ hardware connection</p>  <p>LAN</p> </div> <div> <p>Virtual LAN</p> <p>→ hardware connection ④ software rules</p>  <p>VLAN 2 VLAN 3</p> </div> </div>	<p>Pour définir la notion de réseau local virtuel nous nous référons au domaine de diffusion.</p> <p>Dans le réseau local matériel, le domaine de diffusion est constitué des éléments qui sont physiquement raccordés au réseau</p> <p>Par contre, dans le réseau local virtuel, il faut que les éléments soient matériellement raccordés au réseau mais également qu'ils satisfont à des règles logicielles. Grâce à ces règles il est possible de segmenter le réseau matériel en plusieurs réseaux virtuels.</p>
 <p>VLAN definition rule</p> <ul style="list-style-type: none"> <li>Depends on the administrator policy <ul style="list-style-type: none"> <li>Port policy <ul style="list-style-type: none"> <li>Port1 is in VLAN 2</li> </ul> </li> <li>Address policy <ul style="list-style-type: none"> <li>MAC 01:22:33:45:A6:E6 is in VLAN 2</li> <li>IP 10.0.0.0 is in VLAN 2</li> </ul> </li> <li>Application policy <ul style="list-style-type: none"> <li>VoIP is in VLAN 2</li> </ul> </li> </ul> </li> </ul>	<p>Qu'en est-il des règles logicielles qui permettent de définir les VLAN ?</p> <p>Elles vont dépendre du choix politique adopté par l'administrateur. Celui-ci peut adopter :</p> <ul style="list-style-type: none"> <li>Une politique par port, il configure chaque port avec le numéro de VLAN qui lui est associé. En cas de déplacement de station, cela peut conduire à une reconfiguration des ports.</li> <li>L'administrateur peut également choisir une politique par adressage que ce soit de niveau MAC ou de niveau IP</li> </ul> <p>Ou bien</p> <ul style="list-style-type: none"> <li>Un politique par application, en associant par exemple la téléphonie IP à un VLAN</li> </ul>
 <p>VLAN functioning</p> <ul style="list-style-type: none"> <li>Based on MAC forwarding table</li> <li>One forwarding table per VLAN</li> <li>Forwarding tables are managed by IEEE 802.1 algorithm</li> </ul>	<p>Le Fonctionnement d'un VLAN repose sur l'utilisation de tables de relaiage par adresse MAC</p> <p>On aura une table de relaiage par VLAN et ces tables sont gérées par l'algorithme IEEE802.1 de pont transparent.</p>
 <p>VLAN functioning - illustration</p> 	<p>Regardons une illustration du fonctionnement d'un VLAN.</p> <p>Nous avons représenté un switch qui raccorde 3 stations définies dans le VLAN2.</p> <p>Lorsque la station A transmet à la station C, le switch va tout d'abord identifier dans quel VLAN se situe la communication.</p>

	<p>Il va ensuite regarder le champ adresse destination et vérifier si cette adresse est connue, dans la table du VLAN qu'il vient d'identifier.</p> <p>Comme ce n'est pas le cas, il diffuse la trame sur tous les ports du VLAN à l'exception de celui d'entrée</p>
	<p>La notion de VLAN a un impact sur la trame Ethernet</p> <p>Lorsqu'un lien est multi-VLAN c'est-à-dire qu'il achemine des communications de plusieurs VLAN, une étiquette est rajoutée aux trames qui circulent sur ce lien.</p> <p>La présence de l'étiquette est reconnue dans la trame Ethernet, grâce à une valeur particulière du champ type, 8100 en hexa.</p> <p>En détaillant le format de la trame de l'étiquette on note qu'il y a la possibilité de faire de la classification de services.</p> <p>Il y a :</p> <ul style="list-style-type: none"> <li>• 4 positions pour la classification de services et</li> <li>• 12 positions pour identifier le VLAN.</li> </ul>
	<p>La notion de COS permet de traiter différemment les trames. Ainsi le switch peut relayer en priorité les trames de téléphonie comme indiqué sur l'illustration.</p>
	<p>Une fois expliqué le fonctionnement du VLAN nous pouvons mieux comprendre son intérêt.</p> <p>Le VLAN améliore la :</p> <ul style="list-style-type: none"> <li>• performance, car le domaine de diffusion est segmenté</li> <li>• flexibilité de la configuration, car elle s'effectue par logiciel</li> <li>• sécurité, car les communications restent localisées dans un VLAN et 2 stations situées dans 2 VLAN ne peuvent pas communiquer (sauf si elles utilisent un routeur).</li> </ul>
	<p>Nous retiendrons que :</p> <ul style="list-style-type: none"> <li>• plusieurs VLAN peuvent coexister sur une même infrastructure matérielle ;</li> <li>• le VLAN est configuré logiquement par l'administration</li> <li>• les trames Ethernet qui circulent sur un lien multi VLAN sont étiquetées.</li> </ul>





## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

## **La sécurité des réseaux locaux**

### Objectifs

Cette leçon a pour but de présenter les outils de base de la sécurité des réseaux locaux.

### Prérequis

Bonne connaissance des réseaux locaux

### Connaissances

Principales techniques utilisées pour assurer la sécurité des réseaux locaux.

### Compétences




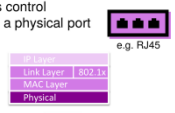

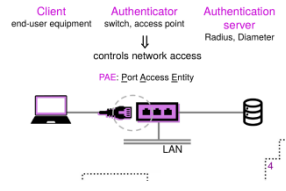
Analyser les outils de sécurisation des réseaux locaux.

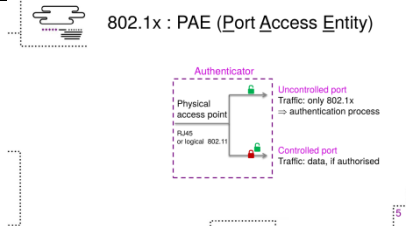
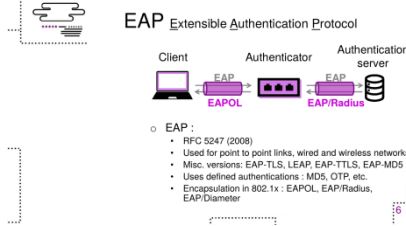
### Évaluation des connaissances

Décrire les techniques de sécurisation des réseaux locaux.

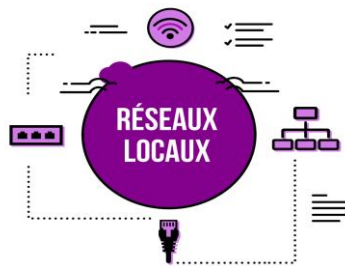
### Évaluation des compétences

Dérouler un scénario de sécurisation d'un réseau local.

 <p><b>Enterprise networks</b> <i>Lan security</i></p> <p>Samiha Ayed</p>	
 <p><b>Objectives</b></p> <ul style="list-style-type: none"> <li>802.1x standard <ul style="list-style-type: none"> <li>802.1x architecture</li> <li>EAP authentication protocol</li> </ul> </li> </ul>	<p>Dans cette vidéo, j'aborde avec vous la norme IEEE 802.1. Je vous présente les différents composants de l'architecture proposée par ce standard ainsi que le protocole d'authentification EAP.</p>
 <p><b>The 802.1x standard</b></p> <ul style="list-style-type: none"> <li>IEEE - June 2001</li> <li>Authentication before any auto-configuration (IP...)</li> <li>Access control through a physical port</li> </ul> 	<p>La norme 802.1x a été définie par l'IEEE en juin 2001. L'idée de base de ce standard est comment un utilisateur qui rejoint le réseau peut être authentifié et autorisé à rejoindre ce réseau avant même d'avoir une adresse IP.</p> <p>Ce contrôle d'accès est basé sur le port. Ici on parle de port de connectivité physique comme par exemple le RJ45 pour Ethernet. Pour ce contrôle d'accès lors de la phase d'authentification, nous nous plaçons au niveau de la couche 2.</p>
 <p><b>802.1x entities</b></p> 	<p>Le standard définit trois composants qui constituent son architecture :</p> <ul style="list-style-type: none"> <li>le client c'est le système à authentifier qui peut être un poste de travail ou un serveur</li> <li>l'authentificateur qui autorise l'accès au réseau mais n'a pas la capacité de déterminer si une machine est autorisée ou pas à joindre le réseau. Dans la plupart des implémentations actuelles, le système authentificateur est un équipement réseau par exemple un commutateur Ethernet une borne d'accès sans fil ou un commutateur routeur IP</li> <li>le troisième composant est le serveur d'authentification qui est l'entité qui décide si l'accès est permis ou pas et informe l'authentificateur de cette décision. Le serveur d'authentification est typiquement un serveur radius ou tout autre équipement capable de faire de l'authentification.</li> </ul> <p>Le système authentificateur contrôle l'accès au réseau via le point d'accès physique au réseau nommé PAE (Port Access Entity). C'est au niveau du PAE que portent l'essentiel des modifications introduites par le protocole 802.1x.</p>

 <p>802.1x : PAE (Port Access Entity)</p>	<p>La principale innovation amenée par le standard 802.1x consiste à scinder le port d'accès physique au réseau qui peut être matérialisée par un câble RJ45 ou le port logique 802.11 en deux ports logiques qui sont connectés en parallèle sur le port physique.</p> <p>Le premier port logique est toujours accessible et dit non contrôlé mais il ne gère que les trames spécifiques à 802.1x et c'est à travers lequel on assure le processus d'authentification.</p> <p>Le deuxième port est dit contrôlé et peut prendre deux états : ouvert ou fermé et c'est le port qu'on utilise pour le transfert des données, une fois le client authentifié et autorisé à accéder au réseau.</p>
 <p>EAP Extensible Authentication Protocol</p> <ul style="list-style-type: none"> <li>Client</li> <li>Authenticator</li> <li>Authentication server</li> </ul> <p>○ EAP :</p> <ul style="list-style-type: none"> <li>• RFC 5247 (2008)</li> <li>• Used for point to point links, wired and wireless networks</li> <li>• Misc. versions: EAP-TLS, LEAP, EAP-TTLS, EAP-MD5</li> <li>• Uses defined authentications : MD5, OTP, etc.</li> <li>• Encapsulation in 802.1x : EAPOL, EAP/RADIUS, EAP Diameter</li> </ul>	<p>Le standard 802.1x ne crée pas un nouveau protocole d'authentification mais s'appuie sur les standards existants. Le dialogue entre le client le système authentificateur et le serveur d'authentification se fait en utilisant le protocole EAP défini par la RFC 5247.</p> <p>Ce protocole a été défini pour être utilisé pour des liaisons point à point pour des réseaux filaires ou aussi pour des réseaux sans fil. Il existe plusieurs variantes du protocole EAP comme EAP-TLS, LEAP, EAP-TTLS pour EAP-MD5 qui assurent des différentes propriétés de sécurité.</p> <p>Concernant les méthodes d'authentification, EAP utilise des méthodes d'authentification prédéfinies comme le MD5 et le OTP. EAP est utilisable avec différents protocoles de niveau 2 (donc niveau liaison) grâce au mécanisme d'encapsulation.</p> <p>Par exemple dans le cas où le client et le système authentificateur sont connectés par Ethernet, les paquets EAP sont transportés dans des trames Ethernet spécifiques EAPOL (pour EAP Over Lan). Le dialogue entre le système authentificateur et le serveur d'authentification se fait par une simple ré-encapsulation des paquets EAP dans un format qui convient aux serveurs d'authentification par exemple le format RADIUS dans notre cas.</p>

<div data-bbox="183 190 598 414" data-label="Diagram"> </div>	<p>Pour assurer la communication entre les différents composants, l'EAP définit quatre types de paquets : request response, succes, et fail.</p> <p>Suivons un exemple de communication.</p> <ul style="list-style-type: none"> <li>- Alice branche son câble rj45 pour se connecter au réseau local donc une requête EAP start est envoyée à l'authentificateur qui lui pose la question sur l'identité d'Alice à travers un message EAP request.</li> <li>- Alice répond en envoyant son identité dans une EAP response.</li> <li>- Ayant reçu l'identité d'Alice, l'authentificateur informe le serveur d'authentification de la présence d'Alice et lui demande si elle est autorisée à accéder au réseau.</li> <li>- Le serveur radius demande si Alice peut fournir des informations privées comme son mot de passe par exemple.</li> <li>- L'authentificateur transfère la requête vers Alice qui envoie son mot de passe dans une EAP response.</li> <li>- L'authentificateur transfère la réponse au serveur radius et reçoit son autorisation pour que Alice accède au réseau.</li> <li>- L'authentificateur envoie finalement cette autorisation à Alice dans un EAP success. Dans ce cas d'authentification réussie, le système authentificateur débloquera le port contrôlé.</li> </ul>
<div data-bbox="183 1292 598 1534" data-label="Diagram"> </div>	<p>En conclusion le standard 802.1x existe principalement pour assurer l'authentification à travers les ports physiques. Cette norme est utile dans le cadre des réseaux filaires et elle a également montré son utilité pour la norme 802.11i, dédiée à la sécurité Wi-Fi.</p>



## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

## **Le spanning tree**

### Objectifs

Cette leçon a pour but de présenter le protocole du « Spanning Tree ».

### Prérequis

Bonne connaissance des réseaux locaux.

### Connaissances

Principes et fonctionnement du protocole du « Spanning Tree ».

### Compétences




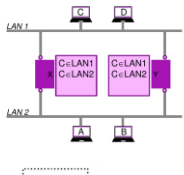
Savoir quand et comment utiliser le « Spanning Tree Protocol » dans un réseau local.



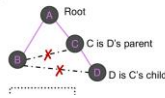


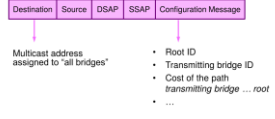
### Évaluation des connaissances


Décrire le problème et les solutions apportées par le « Spanning Tree ».

### Évaluation des compétences

Décrire le fonctionnement du « Spanning Tree Protocol » sur un exemple simple.


 <p><b>Enterprise networks</b> <i>Spanning Tree Protocol</i></p> <p>Gentian Jakllari</p>	<p>Cette leçon est consacrée au protocol Spanning Tree.</p>
 <p><b>Objectives</b></p> <ul style="list-style-type: none"> <li>Understanding topology loops</li> <li>How the spanning tree protocol avoids topology loops</li> </ul>	<p>Elle a deux objectifs:</p> <ul style="list-style-type: none"> <li>comprendre le problème créé par l'existence de boucles dans les réseaux Ethernet,</li> <li>comprendre comment le protocole Spanning Tree évite les boucles.</li> </ul>
 <p><b>What's with topology loops</b></p> 	<p>Tout d'abord, commençons par illustrer avec un exemple simple pourquoi les boucles sont si mauvaises pour les réseaux.</p> <p>Supposons que C envoie un paquet à A et que les tables de tous les ponts soient vides.</p> <p>Les ponts X et Y notent dans leurs tables que C réside dans le LAN 1 et mettent le paquet dans le buffer d'émission pour pouvoir le transférer sur le LAN 2. Une conséquence de cette action est que le réseau se retrouve avec deux copies du paquet d'origine.</p> <p>L'un des ponts, disons X, arrive à transmettre d'abord le paquet de C sur le LAN 2</p> <p>En conséquence, le pont Y note que maintenant C est dans le LAN 2 et met une nouvelle copie du paquet pour le transférer sur le LAN 1.</p> <p>Le point Y, à son tour, émet la premier copie sur le LAN 2. Cette copie arrive au pont X qui note que maintenant C est dans le LAN 2 et mets une nouvelle copie du paquet pour le transférer sur LAN 1. À ce stade, il existe déjà quatre copies du paquet d'origine dans le réseau.</p> <p>On peut continuer à faire cet exercice le reste de la journée et le paquet original continuera à faire des boucles et se multiplier. À la fin, ce seul paquet finira par submerger le réseau.</p>

 <h3>Avoiding loops</h3> <ul style="list-style-type: none"> <li>Tree: a graph without loops</li> <li>General principle <ul style="list-style-type: none"> <li>Create a virtual tree on top of the Ethernet topology including all bridges → <i>spanning tree</i></li> <li>Only ports on the virtual spanning tree are allowed to forward packets</li> </ul> </li> </ul>	<p>Il est clair que l'on doit éviter les boucles dans les réseaux Ethernet. Pour ce faire, on utilise une structure simple, un arbre qui, par définition, n'a pas de boucles.</p> <p>Le principe général de la solution consiste à créer d'abord un arbre virtuel sur la topologie du réseau qui couvre tous les ponts, nous appelons cela un arbre couvrant, « spanning tree » en anglais. Puis, d'autoriser uniquement les ports appartenant à l'arbre couvrant à transférer des paquets.</p>
 <h3>Creating a tree</h3> <ol style="list-style-type: none"> <li>Identify the root</li> <li>for every bridge identify parent &amp; children</li> </ol> <p>E.g.</p> 	<p>Maintenant, qu'est-ce que cela signifie de construire un arbre ? D'abord, on doit identifier le pont qui fonctionnera comme racine et ensuite, pour chaque pont, nous devons identifier son parent et ses enfants.</p> <p>Dans cette topologie simple, A est la racine et l'arbre se compose uniquement des liens parents-enfants. Les deux autres liens seront coupés.</p>
 <h3>Spanning tree protocol</h3> <ul style="list-style-type: none"> <li>Bridges need to <i>communicate</i> to agree on the tree structure</li> <li>packet exchange</li> <li>A new control frame: <i>BPDU</i></li> </ul>	<p>Nous présentons maintenant le protocole spanning tree. Évidemment, un tel protocole exige que les ponts se coordonnent et, dans un réseau, cela ne peut être effectué qu'en échangeant des paquets.</p> <p>Le protocole spanning tree, donc, introduit un nouveau paquet de contrôle appelé BPDU (Configuration Bridge Protocol Data Unit).</p>
 <h3>Configuration Bridge Protocol Data Unit (BPDU)</h3> 	<p>Le BPDU est une trame standard. La donnée est le message de configuration. Il contient entre autres :</p> <ul style="list-style-type: none"> <li>le Root ID (l'adresse du pont qui fonctionne comme racine),</li> <li>l'adresse du pont qui transmet ce paquet particulier,</li> <li>et le coût du chemin reliant le pont émetteur à la racine.</li> </ul> <p>La destination est une adresse spéciale multicast attribuée à tous les ponts.</p>



### Using BPDUs to establish a tree

- Bridges **transmit** BPDUs periodically
  - what they believe to be the root ID
  - the cost of the best path to the root
  - initially every bridge assumes it is the root
- Bridges **receive** BPDUs periodically
  - update the root ID
  - update the cost to the root
- After "enough" BPDUs have been exchanged every bridge will know:
  - the rootID: the bridge with the smallest ID
  - the cost of the path to the root
  - its parent and children



Les ponts transmettent les BPDU périodiquement et incluent dans la trame ce qu'ils croient être l'ID de la racine et le coût du meilleur chemin vers la racine. Initialement, chaque pont suppose qu'il est la racine.

Les ponts reçoivent des BPDU périodiquement et peuvent mettre à jour l'identité de la racine et le coût du meilleur chemin vers la racine. Une fois qu'un nombre "suffisant" de paquets ont été échangés, chaque pont connaîtra :

- la racine, c'est le pont avec la plus petite adresse du réseau,
- le coût du meilleur chemin vers la racine,
- son parent et ses enfants.



### Using BPDUs to establish a tree

— Upon receiving a BPDU —



Pour illustrer cela considérons un réseau Ethernet très simple avec 2 ponts seulement. Au début, les deux ponts supposent qu'ils sont la racine et chacun envoie une BPDU:




- le pont avec adresse 100 transmet une BPDU où la racine est définie comme 100 et le coût pour 0.
- de même pour le pont avec adresse 500.

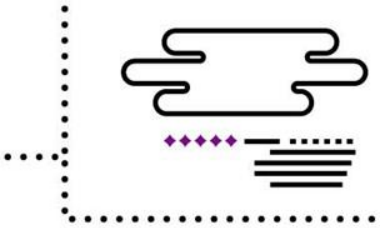
Après avoir reçu une BPDU, le pont avec l'adresse 500 compare la configuration qu'il a reçue avec la sienne et décide que la première est meilleure (pour les classer, on compare successivement l'ID de la racine, l'ID du pont et le port sur lequel le pont a transmis ce paquet). Il met à jour sa configuration de spanning tree et définit 100 comme la racine avec un coût de 8.

De l'autre côté, pour le pont 100, la configuration reçue est pire que la sienne et, par conséquent, il ne change rien.

Finalement, le pont 100 décide qu'il est la racine et le parent de 500. Dans le langage du protocole, le parent est appelé le pont désigné et le port respectif, un port désigné. De son côté, 500 décide que 100 est la racine et son parent. Le port sur lequel il reçoit les paquets BPDU de la racine s'appelle le port racine. Les ports désignés et les ports racine sont maintenus actifs tandis que le reste est bloqué.



 <h3>Dealing with failures</h3> <ul style="list-style-type: none"> <li>Age field is attached to the tree configuration</li> <li>The root bridge periodically transmits BPDUs with age set to 0</li> <li>When bridges receive BPDUs from the root, they reset the tree age &amp; transmit a BPDU with the new age</li> <li>The root or any part of the path between a bridge and the root fails? <ul style="list-style-type: none"> <li>The tree age on the bridge will keep increasing</li> </ul> </li> <li>The age reaches a threshold? <ul style="list-style-type: none"> <li>The bridge calculate a <i>new tree</i>.</li> </ul> </li> </ul>	<p>Maintenant, comment faire pour gérer les pannes dans le réseau ? Chaque pont attache une valeur d'âge à sa configuration d'arbre. Le pont racine transmet périodiquement des BPDU avec un âge réinitialisé à 0. Lorsque les ponts reçoivent des BPDU de la racine, ils réinitialisent l'âge de l'arbre à 0 et transmettent une BPDU avec ce nouvel âge sur tous leurs ports désignés. Si le pont racine ou une partie du chemin entre lui et le pont cible tombe en panne, l'âge de l'arbre sur le pont continuera à augmenter.</p> <p>Si l'âge atteint un certain seuil, le pont va calculer un nouvel arbre.</p>
 <h3>Important parameters</h3> <ul style="list-style-type: none"> <li><b>Forward delay</b> <ul style="list-style-type: none"> <li>Time for the spanning tree protocol to converge <ul style="list-style-type: none"> <li>No data packets are forwarded during this period</li> <li>Should be at least twice the maximum transit time across the network</li> </ul> </li> </ul> </li> <li><b>Hello time</b> <ul style="list-style-type: none"> <li>Frequency of BPDUs transmission</li> </ul> </li> <li><b>Max age</b> <ul style="list-style-type: none"> <li>The maximum time for which a tree configuration is considered valid</li> </ul> </li> </ul>	<p>Avant de terminer, nous présentons quelques paramètres importants pour l'exécution du protocole spanning tree :</p> <ul style="list-style-type: none"> <li>Forward delay <ul style="list-style-type: none"> <li>a) Le forward delay correspond au temps nécessaire pour que les ponts considèrent que le protocole spanning tree ait converge</li> <li>b) Pendant ce temps, aucun paquet de données ne peut être transmis par les ponts</li> <li>c) Ce temps doit être au moins deux fois le temps maximal de transit dans le réseau</li> </ul> </li> <li>Hello time <ul style="list-style-type: none"> <li>a) Le hello time correspond à la fréquence de transmission de BPDU</li> </ul> </li> <li>Max age <ul style="list-style-type: none"> <li>a) Le max age est le temps maximum pendant lequel la configuration de l'arbre est valide.</li> </ul> </li> </ul>
 <h3>Summary</h3> <ul style="list-style-type: none"> <li>Topology loops are highly likely in complex enterprise networks</li> <li>Bridge loops can have serious consequences (Packets can loop indefinitely and proliferate)</li> <li>The spanning tree algorithm is an elegant solution for identifying a loop-free subset of the topology (a tree)</li> </ul>	<p>Pour résumer, les boucles sont fréquentes dans les réseaux d'entreprises. Ces boucles, induites par les ponts, peuvent avoir des conséquences lourdes, car les trames sont alors dupliquées sans fin.</p> <p>Le spanning tree est une solution élégante pour supprimer ces boucles en créant un arbre sur la topologie du réseau.</p>



# Enterprise networks

## *Virtual Local Area Networks*

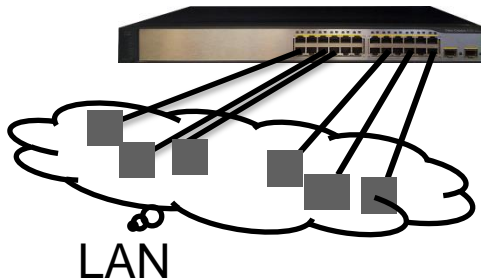
Béatrice Paillassa

# What is a Virtual Local Area Network?

LAN = Broadcast domain : all elements receiving broadcast frames

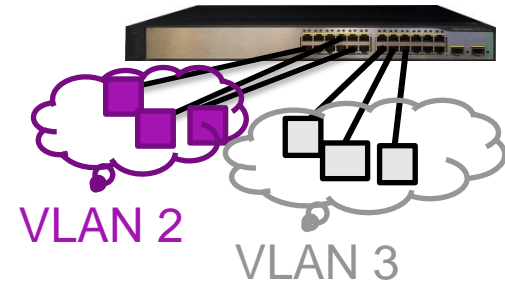
## Hardware LAN

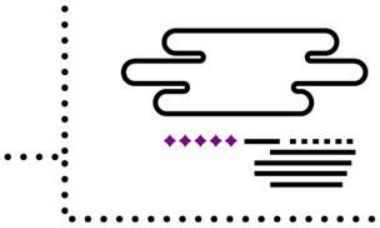
→ hardware connection



## Virtual LAN

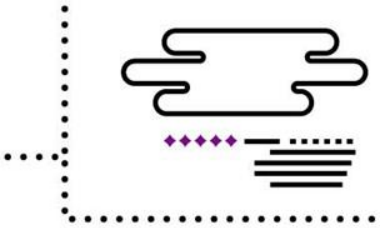
→ hardware connection  
⊕ software rules





# VLAN definition rule

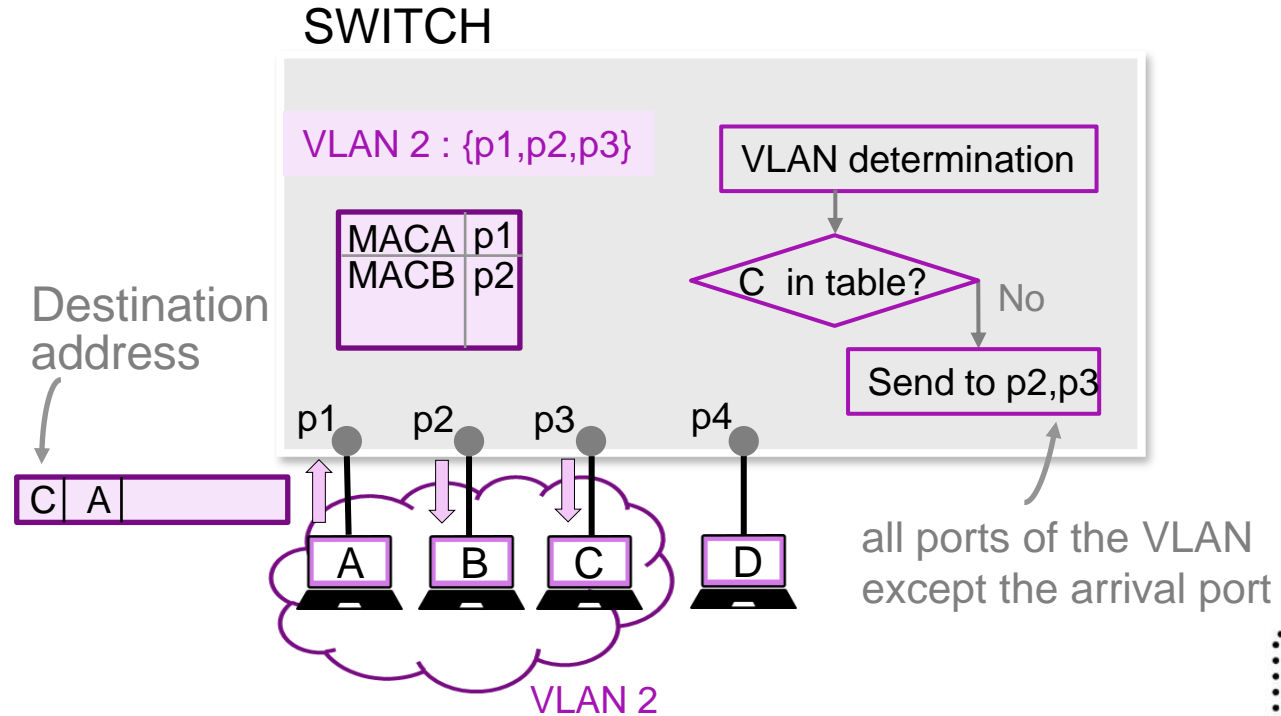
- Depends on the administrator policy
  - Port policy
    - > Port1 is in VLAN 2
  - Address policy
    - > MAC 01:22:33:45:A6:E6 is in VLAN 2
    - > IP 10.0.0.0 is in VLAN 2
  - Application policy
    - > VoIP is in VLAN 2



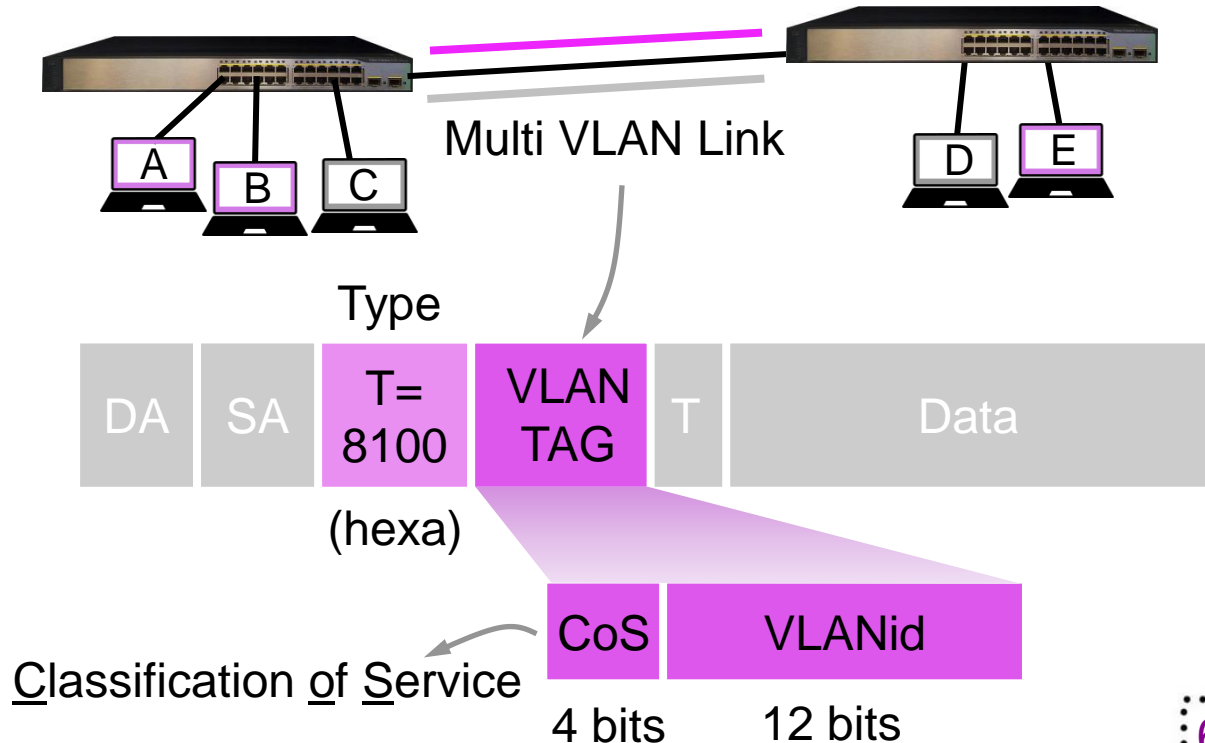
# VLAN functioning

- Based on MAC forwarding table
- One forwarding table per VLAN
- Forwarding tables are managed by IEEE 802.1 algorithm

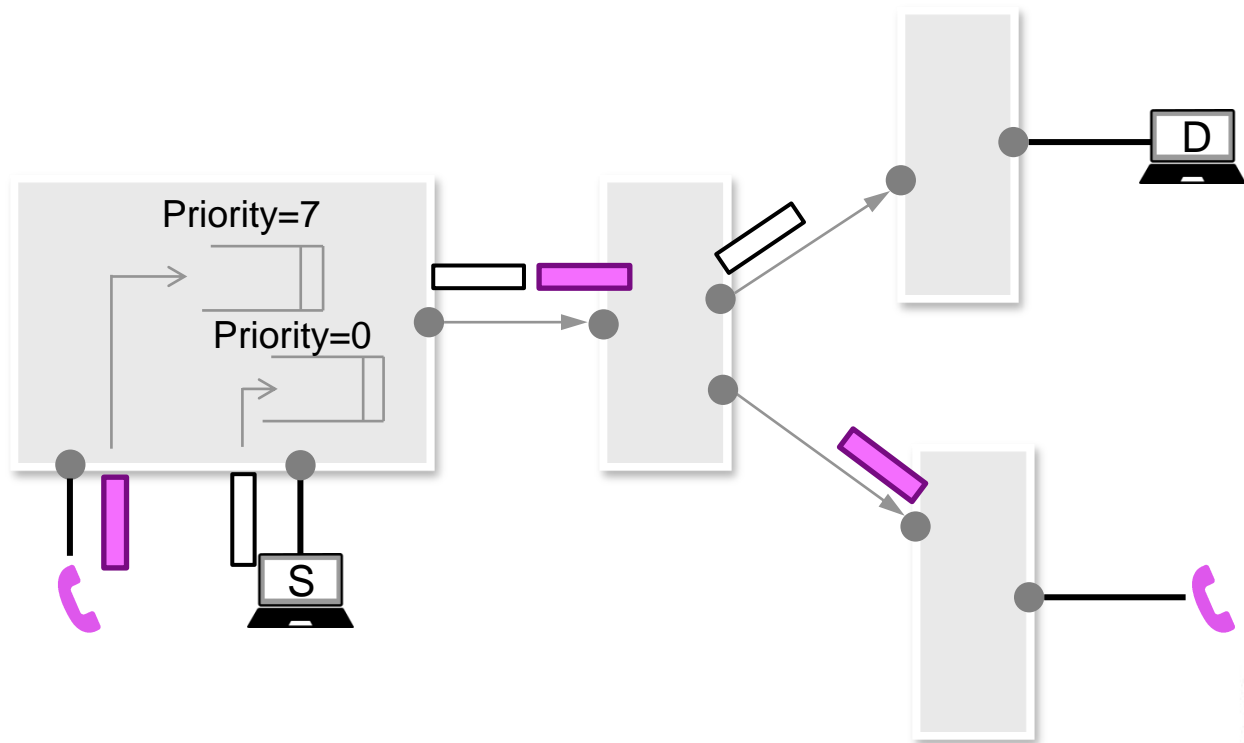
# VLAN functioning - illustration



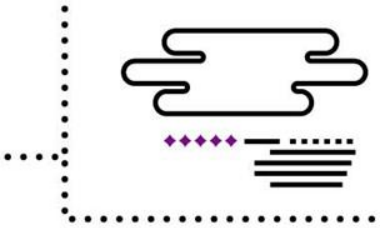
# Impact of VLAN on Ethernet frame



# Priority forwarding illustration







# Interest of VLAN

- **Performance** is improved
  - broadcast domain is limited to one VLAN
- **Flexibility** by software configuration
- **Security** is improved
  - stations belonging to two different VLANs cannot communicate (  $\neq$  Router)

# Summary

- Many VLAN are supported on the same hardware LAN
- VLAN is software defined by administrator
- Ethernet frame is tagged on a link belonging to multiple VLANs

