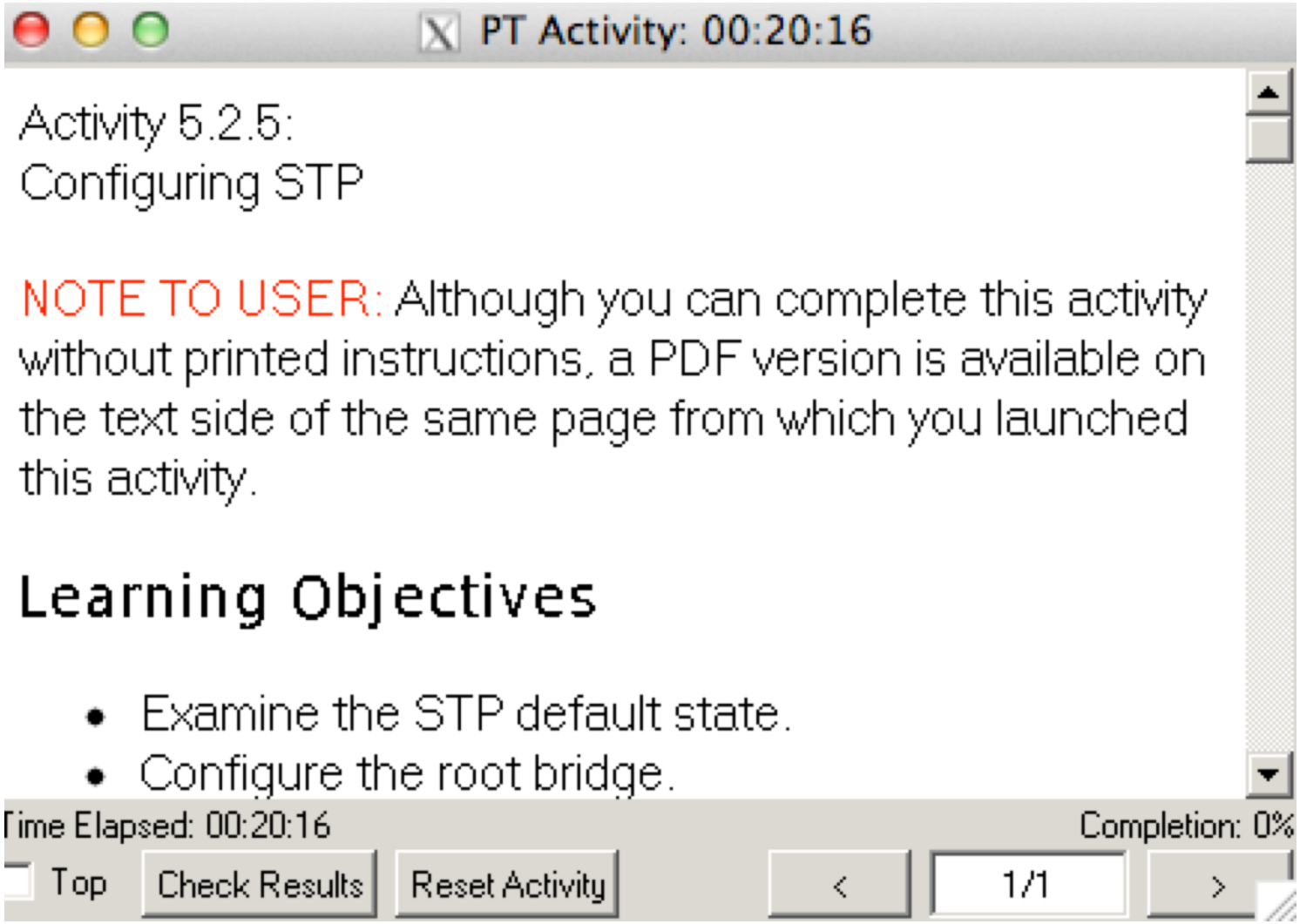
TP M1

Sondes Kallel

Objectif

- Consolidation des connaissances sur les réseaux avec des travaux pratiques
  - Packet tracer : un simulateur de matériel réseau Cisco (routeurs, commutateurs)
  - Salles réseaux : découverte et configuration de matériels Cisco
    - http://e-campus2.uvsq.fr : vérifier votre accès (login + mdp)

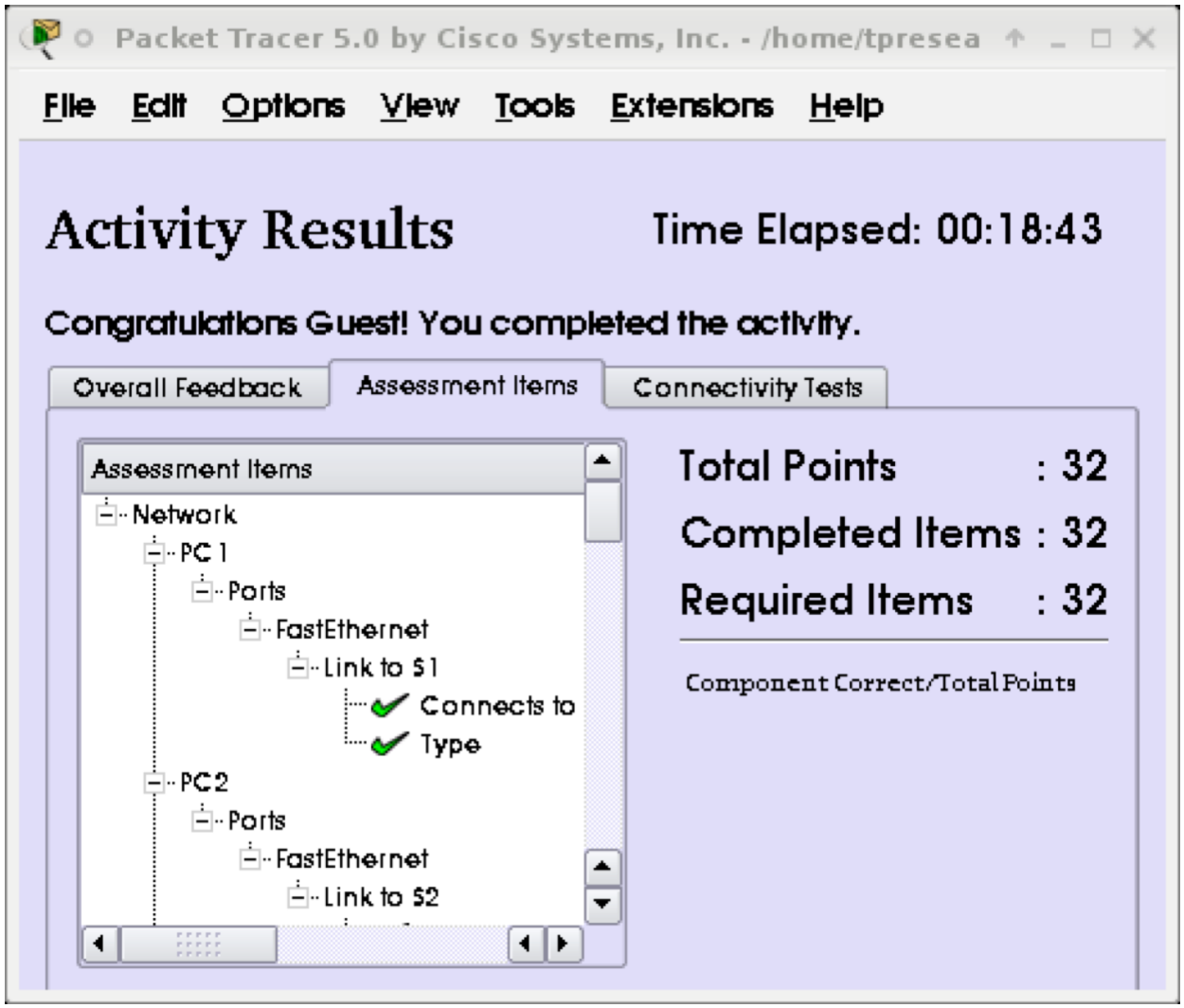
PT activity


PT Activity: 00:20:16
Activity 5.2.5:
Configuring STP
NOTE TO USER: Although you can complete this activity without printed instructions, a PDF version is available on the text side of the same page from which you launched this activity.
Learning Objectives
Examine the STP default state.
Configure the root bridge.
Time Elapsed: 00:20:16
Completion: 0%
Top
Check Results
Reset Activity
<
1/1
>

PT activity

- Le PT activity vous indique les étapes à suivre dans votre initiation Cisco, il permet même de s'assurer que le réseau fonctionne bien ou que vous avez bien répondu au question grâce au bouton Check Results du PT Activity. (croix rouge si c'est pas bon, check vert si c'est bon).
- Attention vous devez toujours enregistrer votre fichier .pka pour ne pas perdre la configuration que vous avez effectuée.
- Pour récupérer le fichiers .pka en effaçant toutes les configurations que vous avez effectuées depuis le début de l'exercice appuyer sur **Reset Activity**

PT activity


Packet Tracer 5.0 by Cisco Systems, Inc. - /home/tpresea
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:18:43
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Assessment Items
Network
PC 1
Ports
FastEthernet
Link to S1
Connects to
Type
PC2
Ports
FastEthernet
Link to S2
Total Points : 32
Completed Items : 32
Required Items : 32
Component Correct/Total Points

Que faire à la fin du TP

- A la fin du TP vous devez soumettre votre compte rendu (avec les fichiers .pka) dans la boite de dépôt qui se trouve dans le lien d'e-campus :
- ***http://e-campus2.uvsq.fr***
- N'Oubliez pas de mettre NOM, PRENOM, DPLOME (Master) et GROUPE dans la première ligne de votre compte rendu.
- **Toute omission de ces informations sera sanctionnée**

ATTENTION: manipulation des équipements Cisco

- Les cables, équipements et PCs doivent impérativement être RANGES en fin de journée
- Recpectez les mots de passe donnés dans l'énoncée :
  - Pensez à vos camarades qui vont récupérer le routeurs et qui ne connaissent pas le mdp !!!
- Sauvegarder vos configurations à chaque étape.

Rappel

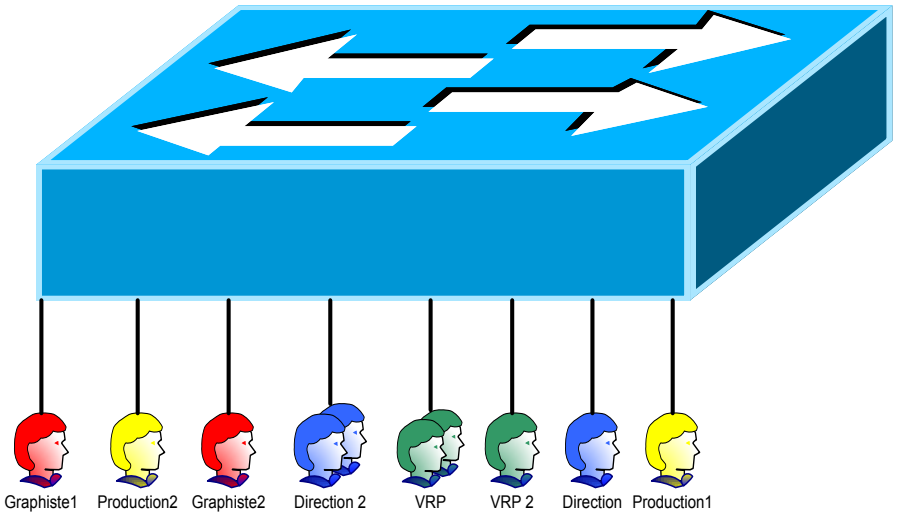
VLAN, routage, VTP, SPT, cables droits et croisés, commandes Cisco

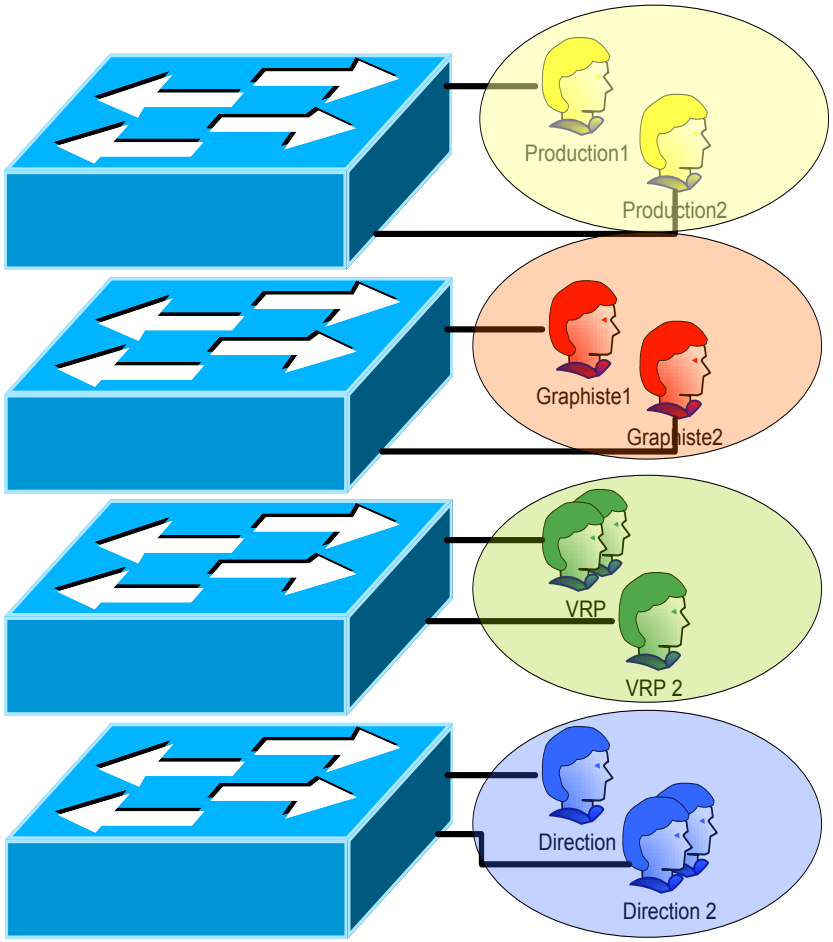
VLAN et VTP

Rappel

- VLANS
  - Ensemble logique d'unités ou d'utilisateurs pouvant être regroupé quelque soit leur emplacement physique
  - Est utilisé pour segmenter les domaines de diffusion
  - Avantages des VLANs
    - Réduction du coût, securité, meilleure performance, meilleure gestion

Rappel





Peuvent être regroupés par :

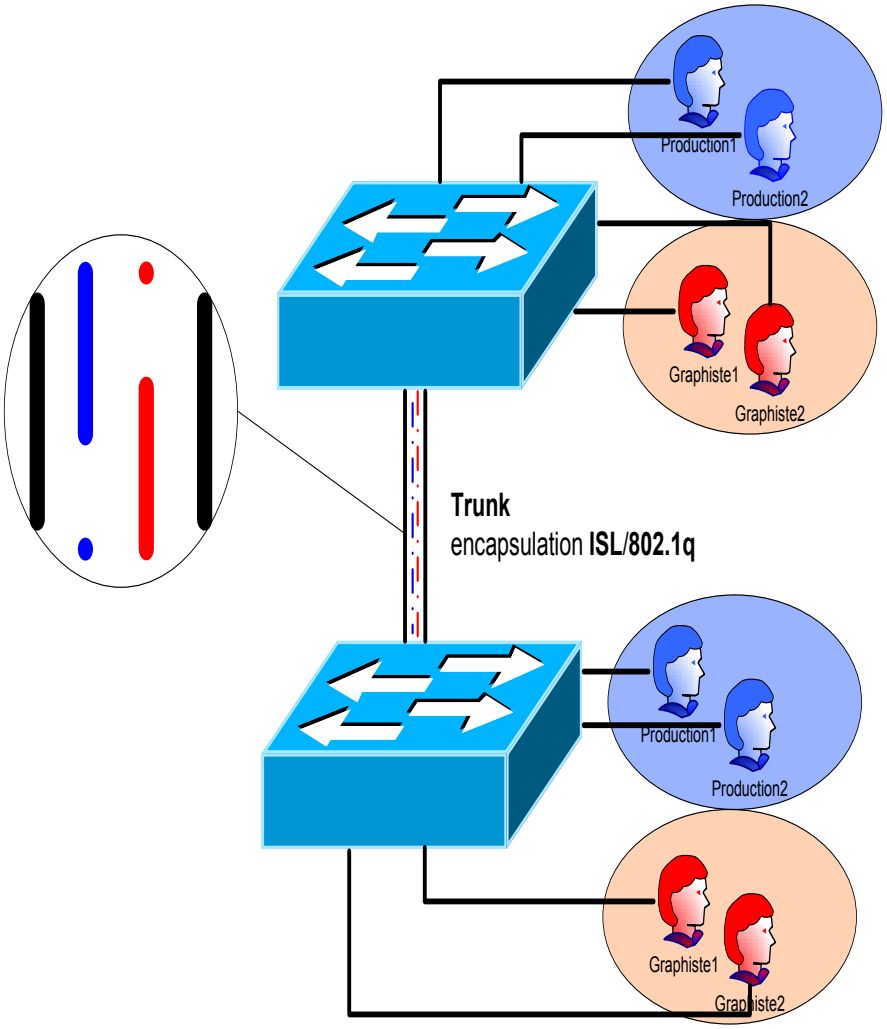
- Fonction (ex : même service dans l'entreprise)
- Application (ex : utilisation des même logiciels)
- Protocole (ex : protocoles de couches 3)
- Identifiant (ex : adresse MAC)
- etc.

Rappel

- Types de Trafic dans un VLAN
  - Données
  - Voix
  - Protocol de réseau
  - Gestion de réseau
- La communication entre différent VLANs requiert l'utilisation de
  - Routeurs

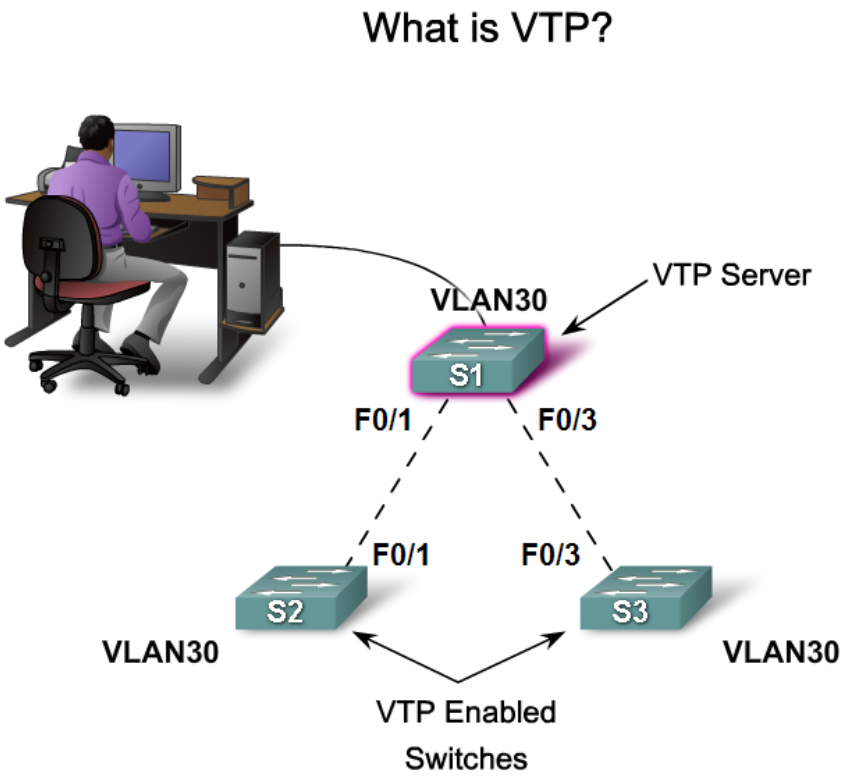
Rappel

- Les trunks
  - Un conduit commun utilisé par plusieurs VLANs pour une communication intra-VLAN
- IEEE 802.1Q
  - Le standard du protocole de trunking
  - Utilise le tagging des trames pour identifier le VLAN auquel appartient la trame



Problématique

- Pour ajouter un VLAN sur un réseau
  - L'administrateur doit l'ajouter sur chaque switch !
  - Necessite beaucoup de manipulation sur de grands réseaux
- Imaginons que nous avons un grand nombre de switch !!!
  - C'est pénible de faire la configuration sur tous les switchs un par un
    - Solution : administration des VLANs



Administration des VLAN ?

- Pour éviter cela, sur des switchs Cisco, la manipulation peut être faite sur un seul switch
  - La modification sera alors diffusée sur les autres via le protocole VTP : VLAN Trunking Protocol
  - Nous distinguons dans ce cas, des switchs VTP server et des VTP client
  - Le VTP server va diffuser la modification vers les autres switchs VTP client

VTP

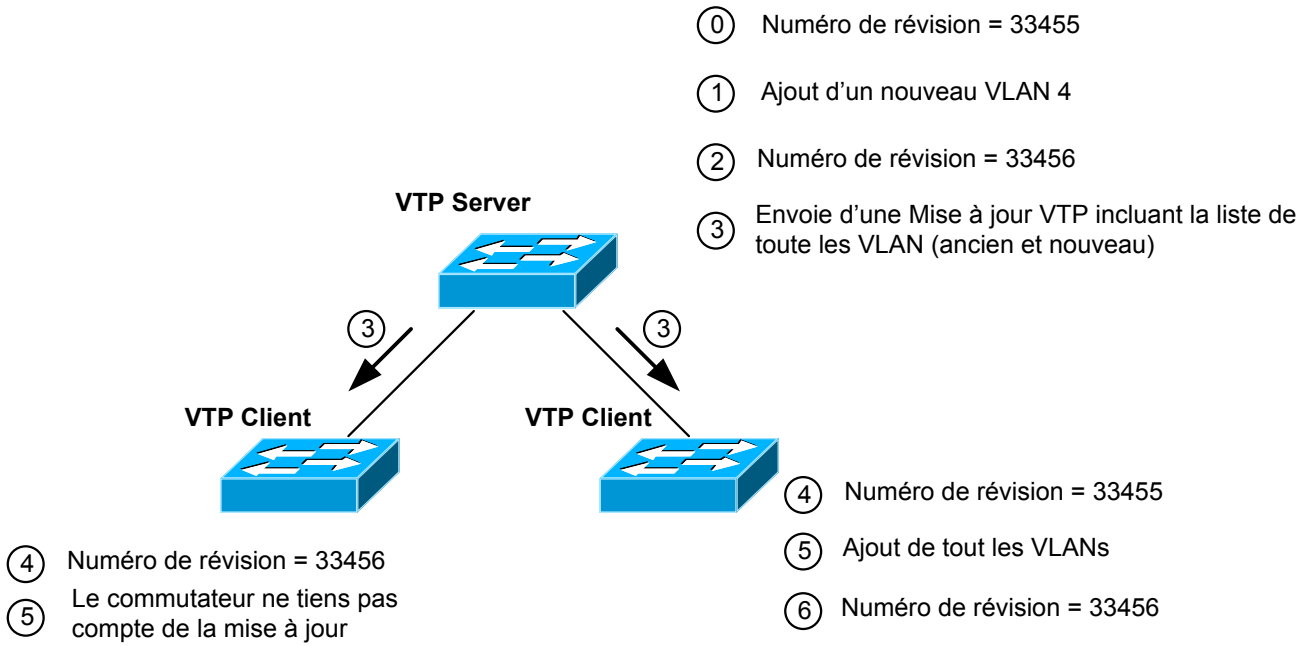
- Le protocole VTP (VLAN Trunk Protocol) a pour but de diffuser la création des VLAN à travers les commutateurs

- Réduction de la charge administrative en ne créant les VLAN que sur les commutateurs « servers »

- 3 états VTP possibles pour un commutateur :
  - Server
  - Client
  - Transparent (autonome)

VTP: Fonctionnement du protocole

- Quand il y a changement dans la création des VLAN, une mise à jour est envoyée avec un numéro de révision par les « VTP servers »
- Si un VTP client reçoit une mise à jour avec un numéro de révision supérieur au sien, il l'applique.



Le vocabulaire VTP

- Le VTP domain
  - Tous les switchs appartenant au même VTP domain échangeront leurs informations sur les VLANs
- Les VTP Mode
  - Un switch peut être en mode server
    - il diffuse ses informations sur les VLAN à tous les autres switchs appartenant au même VTP domain
    - ces informations sont stockées en NVRAM et sur un tel switch, il est possible de créer, modifier ou détruire un VLAN du VTP domain
  - en mode client
    - Il stocke uniquement les informations sur les VLAN, transmises par le switch en mode VTP server sur le même domaine.
  - ou bien en mode transparent
    - Il transmet les informations VTP aux autres switchs mais ne les traitent pas. Ces switchs sont autonomes et ne participent pas aux VTP
- Le VTP Pruning
    - Supprime la propagation des messages de broadcast, multicast et autres messages inconnu unicast sur les liens trunks afin d'optimiser la bande passante
- Le native vlan est utilisé sur les trunk pour permettre le transport de trames ethernet non taguées (certains trafic ne supportent pas de tag par exemple)

VTP: fonctions des modes

- Les modes VTP

Fonction	Mode Server	Mode Client	Mode Transparent
Envoie des MAJ VTP	OUI	NON	NON
Les instances reçoivent les MAJ et synchronise et se synchronise avec les autres Switch	OUI	OUI	NON
Fait suivre les MAJ VTP reçue par une liaison « trunk »	OUI	OUI	OUI
Sauvegarde la configuration des VLAN en NVRAM	OUI	NON	OUI
Peut créer, modifier ou supprimer des VLAN en utilisant les commandes de configurations	OUI	NON	OUI

Commandes Cisco

Commandes de création de domaine

- **vtp domain {nom} [password mdp | pruning | v2-mode]**
  - Donne un nom de domaine
- **vtp mode {server | client | transparent}**
  - Donne un mode VTP au switch

```
Switch>enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)# vtp domain LABO
Changing VTP domain from CISCO to LABO
Switch(config)# vtp mode transparent
Setting Device to VTP TRANSPARENT mode.
```

Commandes Cisco

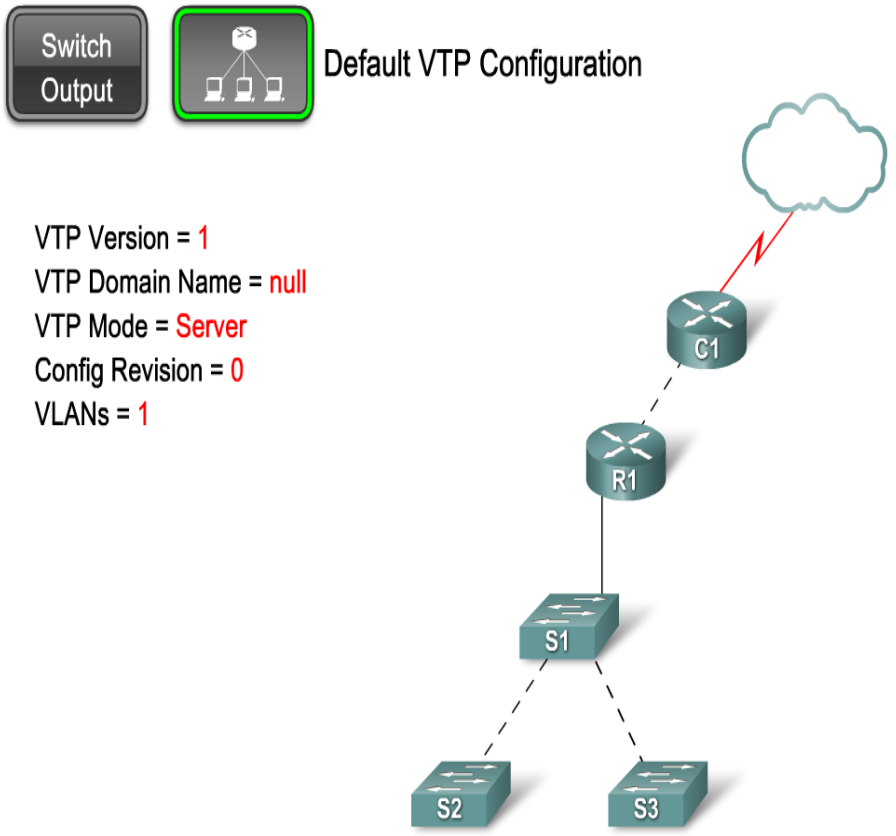
Commandes de visualisation de VLAN

- **show vlan [id {id} | name {nom de vlan}]**
  - Affiche des informations sur le VLAN

```
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
10   DRH                              active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
30   Admin                            active    Fa0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

La configuration par défaut

- Par défaut, un switch est en mode server
  - le VTP domain name = null
  - Tous les ports sont dans le VLAN 1
  - Le numéro de révision de la configuration VTP est 1
  - La version du protocole VTP est 1
    - Il existe 3 versions. Pour un VTP domain, tous les switchs doivent être dans la même version
- La commande show vtp status permet de visualiser la configuration d'un switch



Commandes Cisco

Commandes d'affichage d'état

- **show vtp status**
  - Affiche la configuration VTP et le statut du processus

```
Switch#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 250
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : LABO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x80 0x86 0x88 0xE7 0xB1 0x6E 0xBB 0xF8
Configuration last modified by 0.0.0.0 at 3-1-93 00:08:35
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

Configurer VTP dans les commutateurs

- Identifier les problèmes rencontrés dans la configuration

Common VTP Configuration Issues

- Incompatible VTP Versions
- VTP Password Issues
- Incorrect VTP Mode Name
- All Switches set to VTP Client Mode

Configurer VTP dans les commutateurs

- Gérer les VLANs dans un réseau implémentant VTP


```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name faculty
S1(config-vlan)#exit
S1(config)#interface FastEthernet 0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#exit
S1#
```

Le SPT

Conception d'un bon réseau

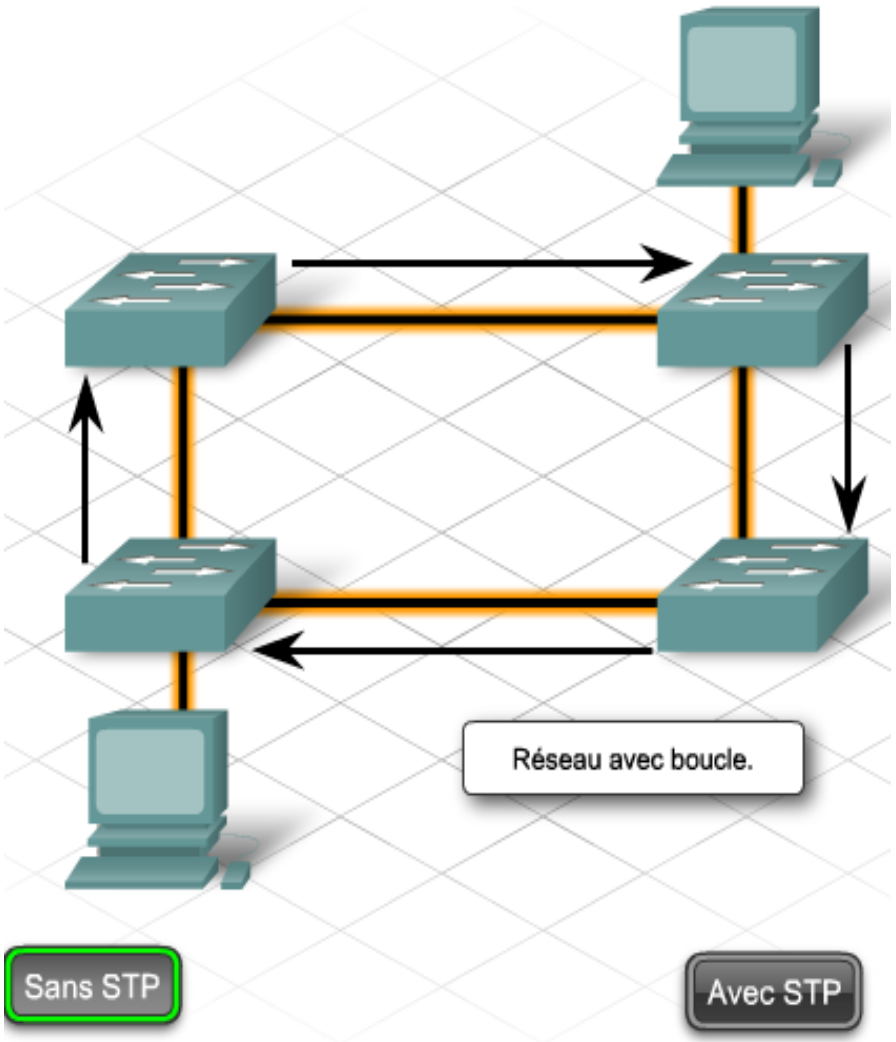
- Besoin de fiabilité, tolérance de pannes
  - Établissement de chemins redondants
- Conséquences
  - Boucles de commutations
  - Tempêtes de broadcast
  - Bande passante réduite
  - Congestion

Boucle de commutation

- Un bon réseau doit pouvoir proposer un chemin alternatif en cas de panne d'une liaison ou d'un commutateur. Le protocole Spanning-tree garantit un chemin unique entre deux nœuds du réseau.

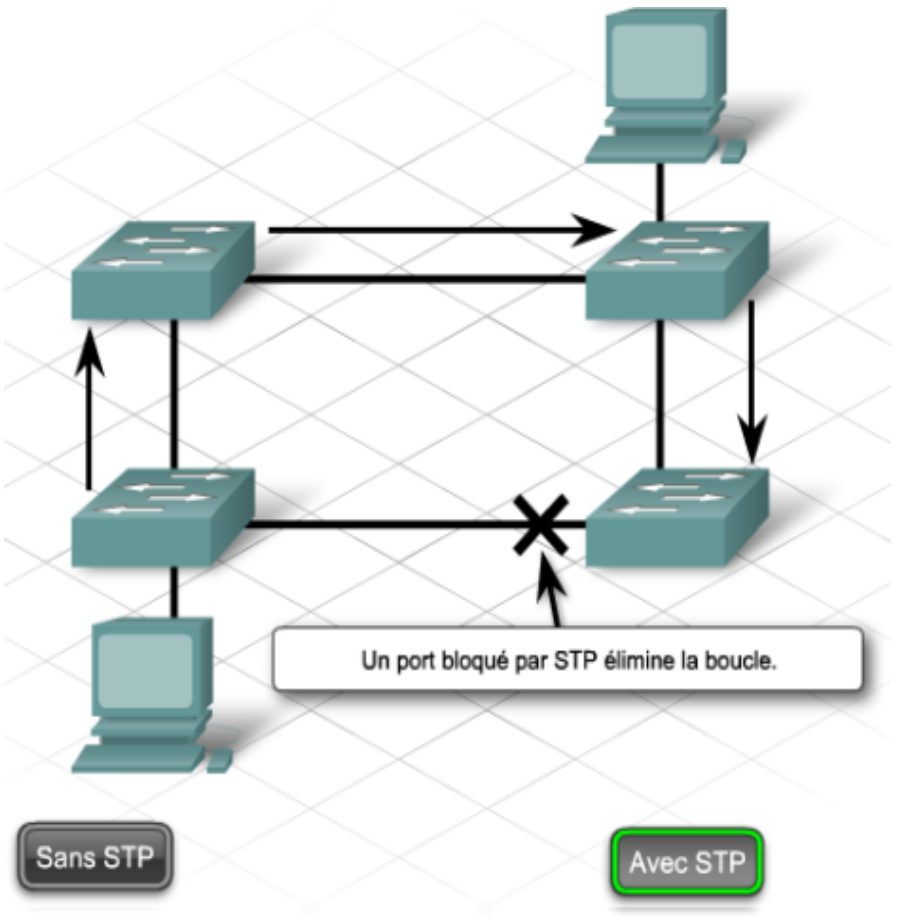
Boucle de commutation

- Bouclage dans un réseau maillé
- L'envoi d'une trame broadcast qui tourne indéfiniment. (tempête de broadcast)
  - Peut causr crash de l'ordinateur



Boucle de commutation : Solution

- Un bon réseau doit pouvoir proposer un chemin alternatif en cas de panne d'une liaison ou d'un commutateur.
- Le protocole **Spanning-tree** garantit un chemin unique entre deux nœuds du réseau.



Le protocole SPT

- But de STP
  - Éviter les boucles de commutations
  - Garder une tolérance de pannes

- Moyens utilisés
  - Établir un arbre unique de chemins
  - Supprimer les boucles de commutation
  - Garder des liens redondants (backup)

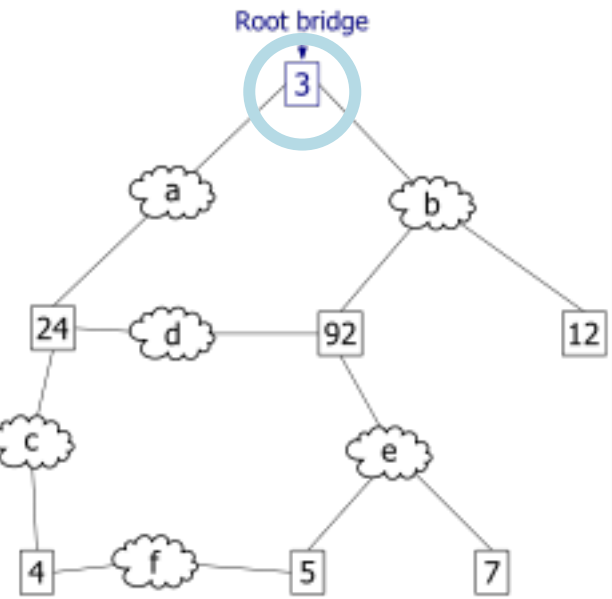
Le protocole SPT

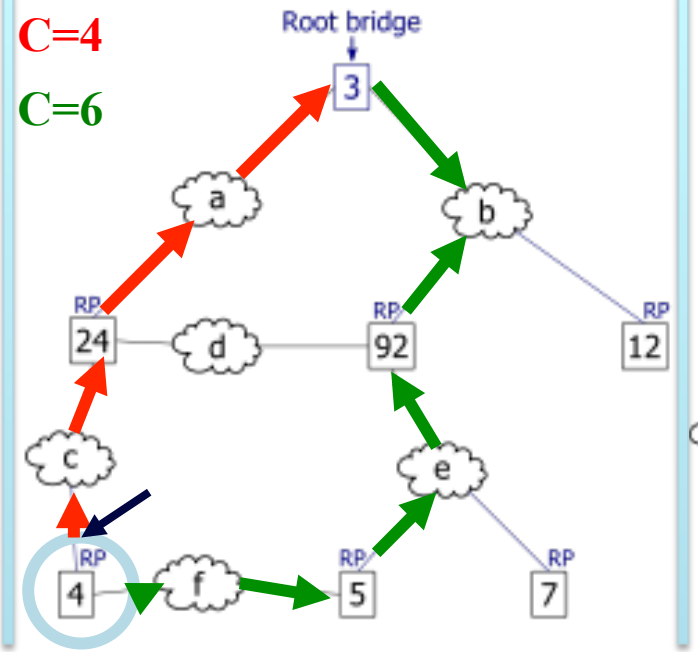
- Élection du pont racine → **root bridge**
  - fondé sur la priorité de pont et sur l'adresse MAC (Bridge ID)
  - priorité la plus faible est élu
  - sinon, adresse MAC la plus faible

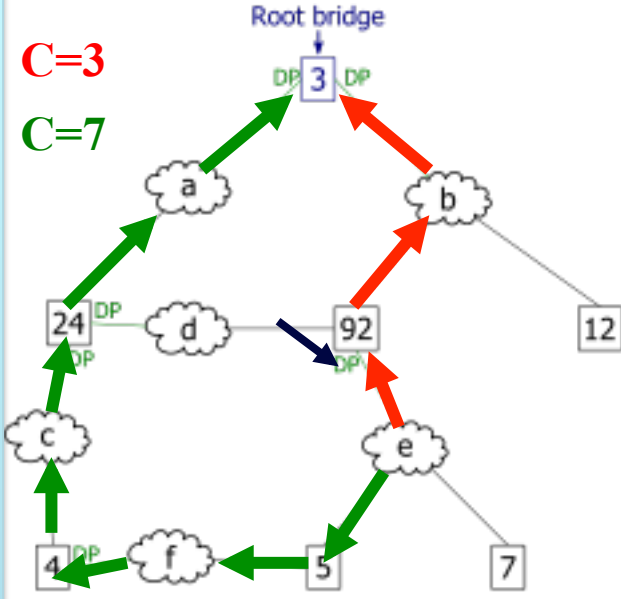
- Chaque commutateur calcule le coût vers le root bridge, élection du port racine → **root port**
  - coût le plus faible est élu
  - coût basé sur la bande passante

- Élections de ports désignés ou les ports bloqués → **designated port et blocked port**

Fonctionnement du SPT (1)







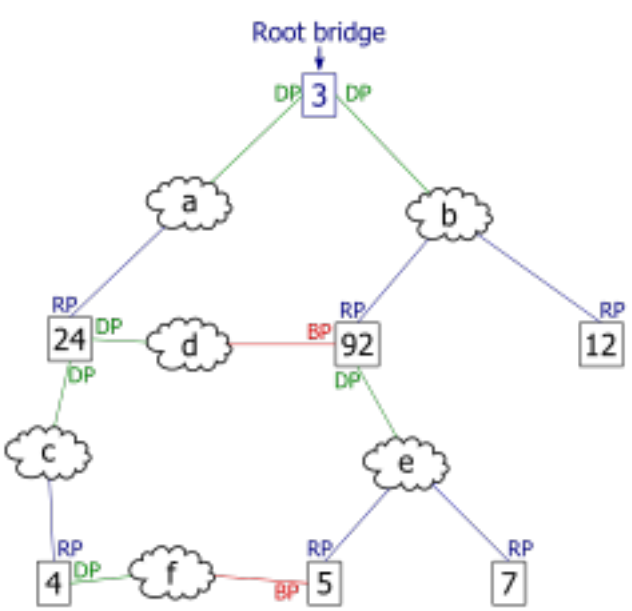
Pont racine :
Le plus petit *bridge ID* vaut 3. Par conséquent, le commutateur 3 devient le commutateur racine.

Port racine (RP)
En supposant que le coût de traversée de chaque segment réseau est 1, le chemin de moindre coût du commutateur 4 au com racine passe par le segment réseau c. Par conséquent, le port racine pour le com 4 est celui qui mène au segment réseau c.
Du switch x au switch racine

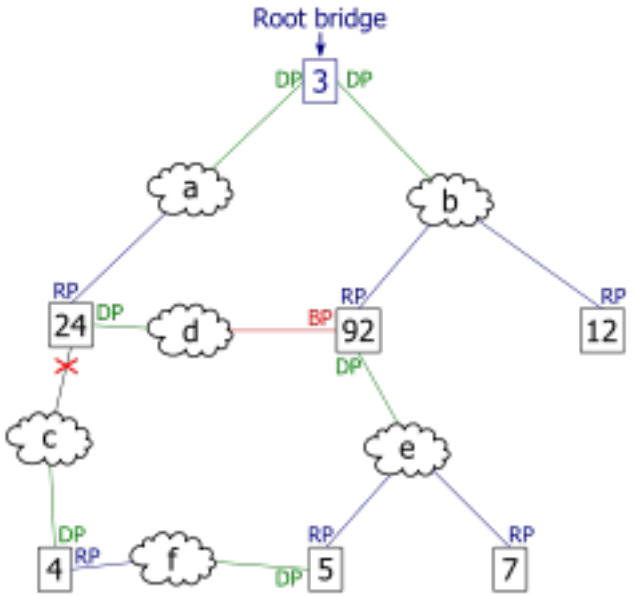
Port désignés (DP):
Le chemin de moindre coût depuis le segment réseau e passe par le com 92. Par conséquent, le port désigné pour le segment réseau e est le port qui le connecte au commutateur 92.
Du segment au switch racine

a,b,c,d,e et f : segment de réseau / 3,24,92,4,5,7,12 : switch

Fonctionnement du SPT (2)



Port bloqué :
Tout port qui n'est ni racine ni désigné devient un port bloqué.



Après la chute d'un lien (marquée par une croix), un nouvel arbre de moindre coût est calculé.

Commandes Cisco

Modification de la priorité d'un port :

- **Switch_A>enable**
- **Switch_A#configure terminal**
- **Switch_A(config)#interface Ethernet N°_d'interface**
- **Switch_A(config-if)#spanning-tree cost (0 -> 65535)**

- Par défaut : le « cost » est calculé en fonction de la bande passante du lien.

Commandes Cisco

Modification de la priorité d'un commutateur :

- **Switch_A>enable**
- **Switch_A#configure terminal**
- **Switch_A(config)#spanning-tree priority (0 -> 65535)**

- Par défaut : priority = 32768

Commandes Cisco

Information de Root ID, Brigde ID et interface :

- **Switch_A>enable**
- **Switch_A#show spanning-tree**

Information sur le coût de la liaison d'une interface sur un commutateur :

- **Switch_A>enable**
- **Switch_A#show spanning-tree interface fastEthernet 0/1**

Commandes Cisco

Information en temps réel :

- **Switch_A>enable**
- **Switch_A#debug spanning-tree**

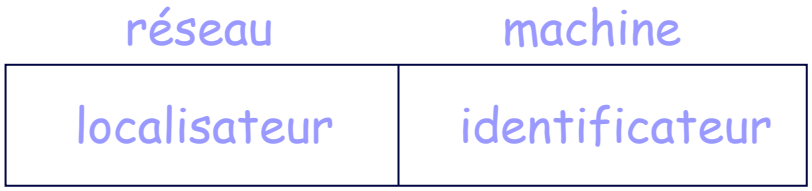
Pour stopper :

- **Switch_A#u all (undebug all)**

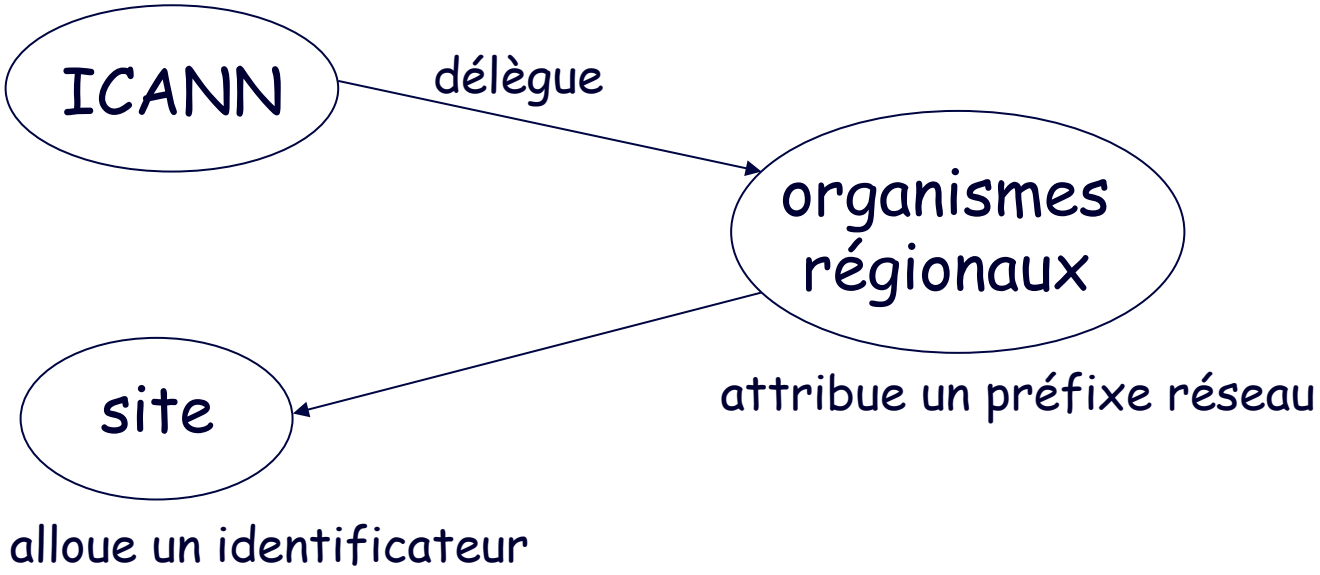
Adressage, routage, classes

Adressage IP

- adressage
  - pour l'identification d'un équipement réseau
  - pour le routage
- plan d'adressage homogène
  - format : 4 octets ➔ 4,3 milliards d'adresses ???
  - notation décimale pointée : x1.x2.x3.x4
- adresse globalement unique et hiérarchique
- format : <réseau> <machine>
  - localisateur ou préfixe réseau : identificateur de réseau
  - identificateur : identificateur de machine



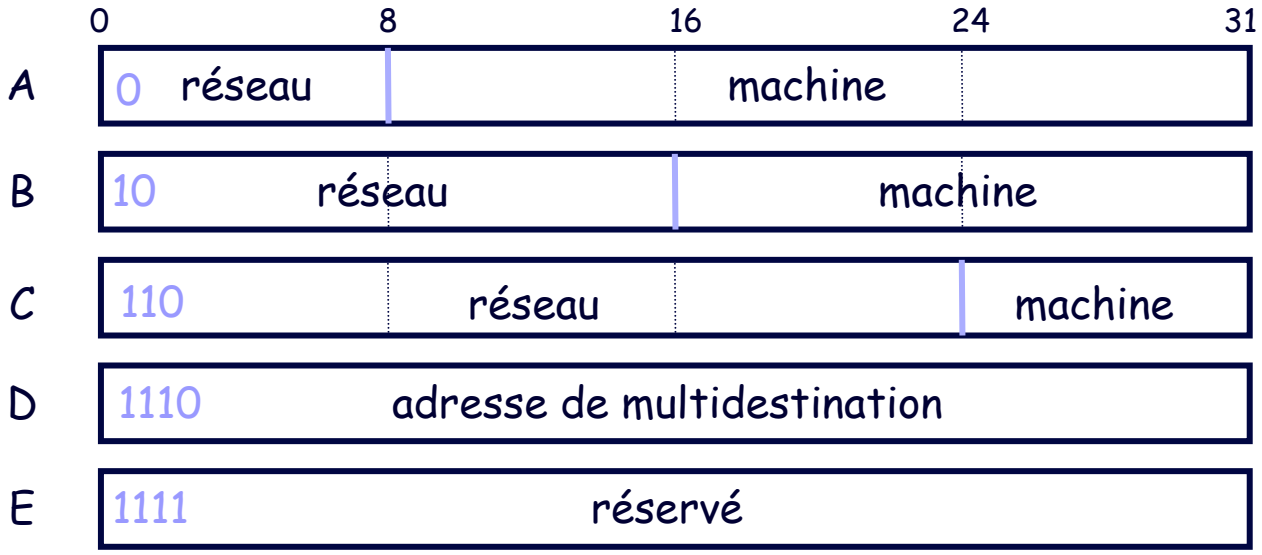
Attribution des adresses



ICANN : Internet Corporation for Assigned Names and Numbers

Classes d'adresses

- le découpage <réseau> / <machine> n'est pas fixe
- 5 classes d'adresses

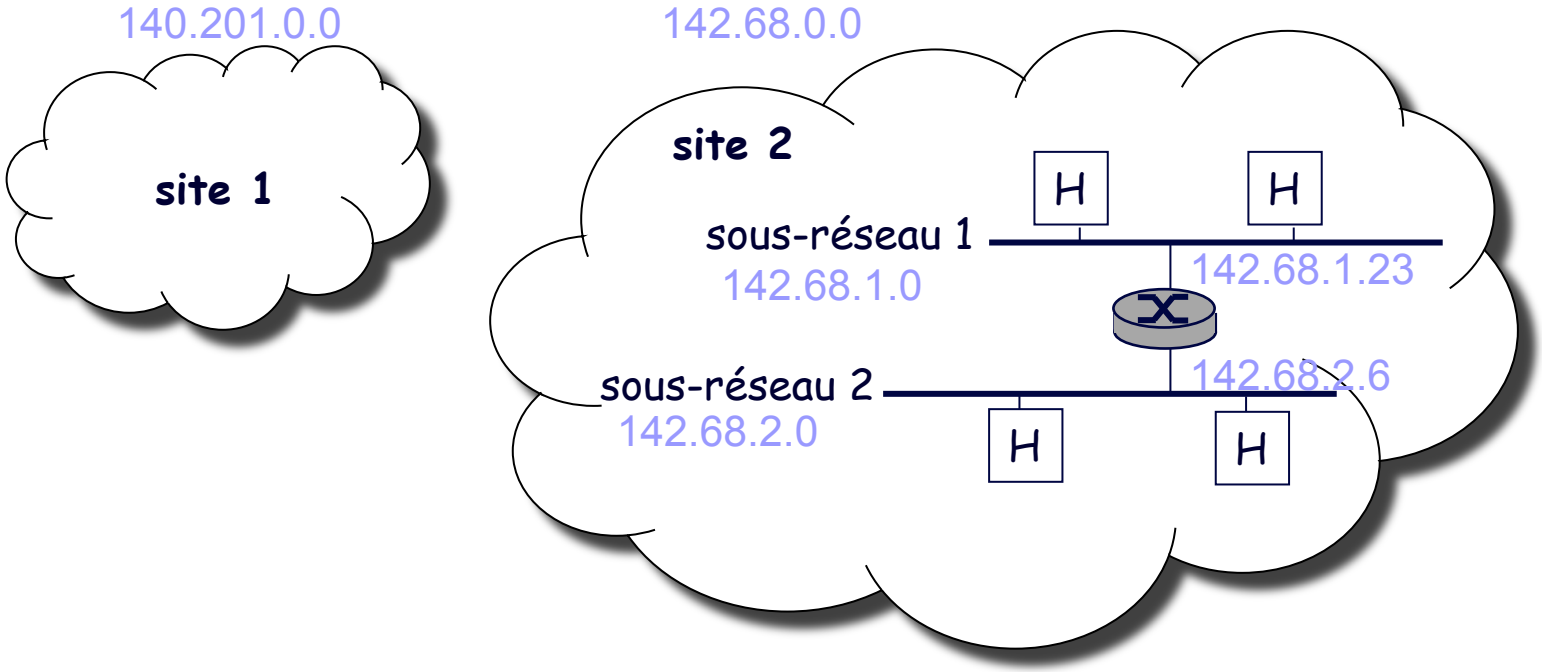


Classes d'adresses

- classe A : 2^7 réseaux (128)
  - réservé: 0.0.0.0 et 127.0.0.0
  - disponible: 1.0.0.0 à 126.0.0.0
    - 126 réseaux classe A et 16 777 214 machines/réseau
- classe B : 2^{14} réseaux (16 384)
  - réservé: 128.0.0.0 et 191.255.0.0
  - disponible 128.1.0.0 à 191.254.0.0
    - 16 382 réseaux classe B et 65 534 machines/réseau
- classe C : 2^{21} réseaux (2 097 152)
  - réservé 192.0.0.0 et 223.255.255.0
  - disponible 192.0.1.0 à 223.255.254.0
    - 2 097 150 réseaux classe C et 254 machines/réseau

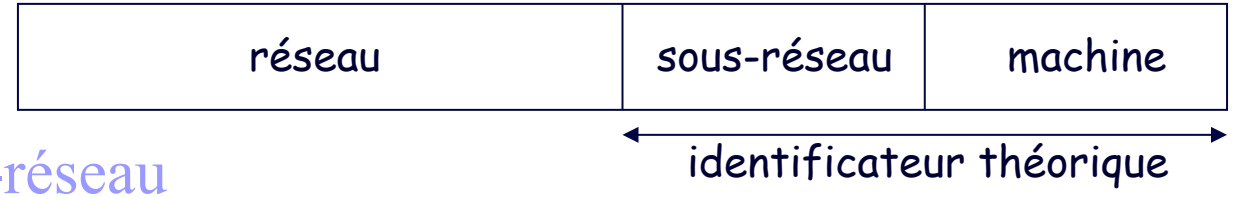
Subnetting

- Problème
  - distinction <réseau> / <hôte> insuffisante en pratique



Sous-adressage

- Principe
  - ajout d'un niveau hiérarchique dans l'adressage
    - adresse de sous-réseau
  - subdivision de la partie <hôte>



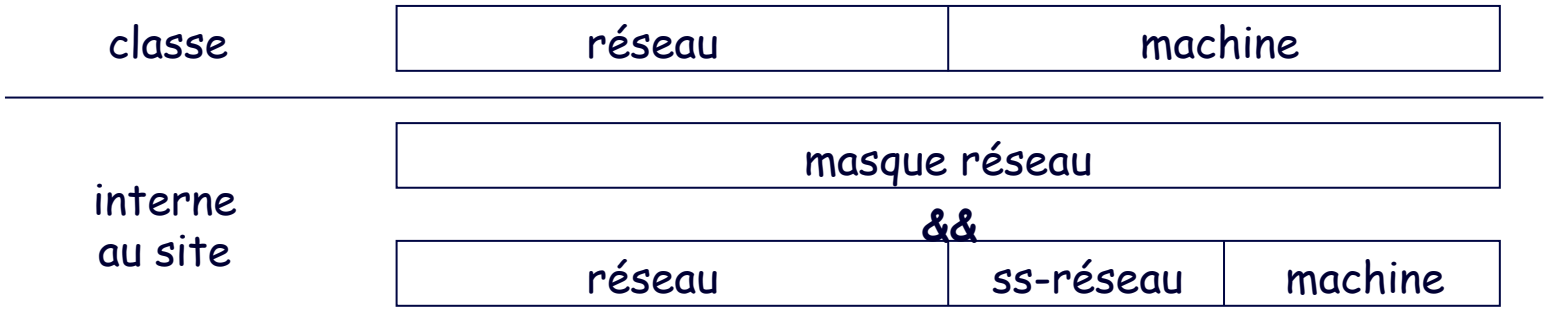
- le sous-réseau
  - est un réseau physique (i.e. un réseau IP connexe) du réseau de site
  - a une visibilité purement interne (transparent vis à vis de l'extérieur).

Le masque de sous-réseau

- Le masque indique la frontière entre la partie <sous-réseau> et la partie <machine>
- Le masque est propre au site et il est de 32 bits
- Bits du masque de sous-réseau (*subnet mask*)
  - positionnés à 1 ➔ partie réseau
  - positionnés à 0 ➔ partie machine
- Exemple
  - `11111111 11111111 11111111 00000000`
  - 3 octets pour le champ réseau, 1 octet pour le champ machine
- Notations
  - décimale pointée
    - exemple : 255.255.255.0
  - adresse réseau/masque
    - exemple : 193.49.60.0/27 (27 = nombre de bits contigus du masque)

Masque de sous-réseau

- Utilisation :



- Exemple :
  - le réseau 142.68.0.0 (classe B!) a comme masque 255.255.255.0
  - soit l'hôte d'@IP 142.68.2.6

	10001110.01000100.00000010.00000110	142.68.2.6
&&	11111111.11111111.11111111.000000	255.255.255.0
=	10001110.01000100.00000010.00000000	142.68.2.0

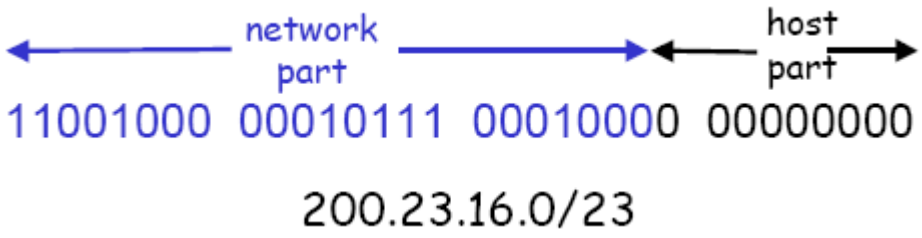
  - ↳ l'hôte est sur le sous-réseau numéro 2, et a comme identificateur 6
  - Le netmask permet de savoir si la machine source et destination sont sur le même sous-réseau.

Le masque de sous-réseau

- Le choix du découpage <réseau> / <hôte> dépend des perspectives d'évolution du site
  - exemple classe B :
    - 8 bits pour la partie sous réseau ➔ 256 sous réseaux de 254 machines
    - 3 bits pour la partie sous réseau ➔ 8 sous-réseaux de 8190 machines
  - exemple classe C :
    - 4 bits pour la partie sous-réseau ➔ 16 sous-réseaux de 14 machines

Adresse IP : CIDR

- Adressage par classe :
  - utilisation inefficace de l'espace d'adressage
  - Ex : une adresse de classe B a assez de place pour pour 65K hôtes, même si il n'y a que 2K hôtes dans ce réseau
- CIDR : Classless InterDomain Routing
  - La taille de la partie réseau est arbitraire
  - Format de l'adresse : a.b.c.d/x, où x est le # de bits dans la partie réseau de l'adresse
  - Ex: 128.96.0.0/16 : regroupe les numéros de 128.96.0.0 à 128.96.255.255
    => équivalent d'une classe B en notation classique



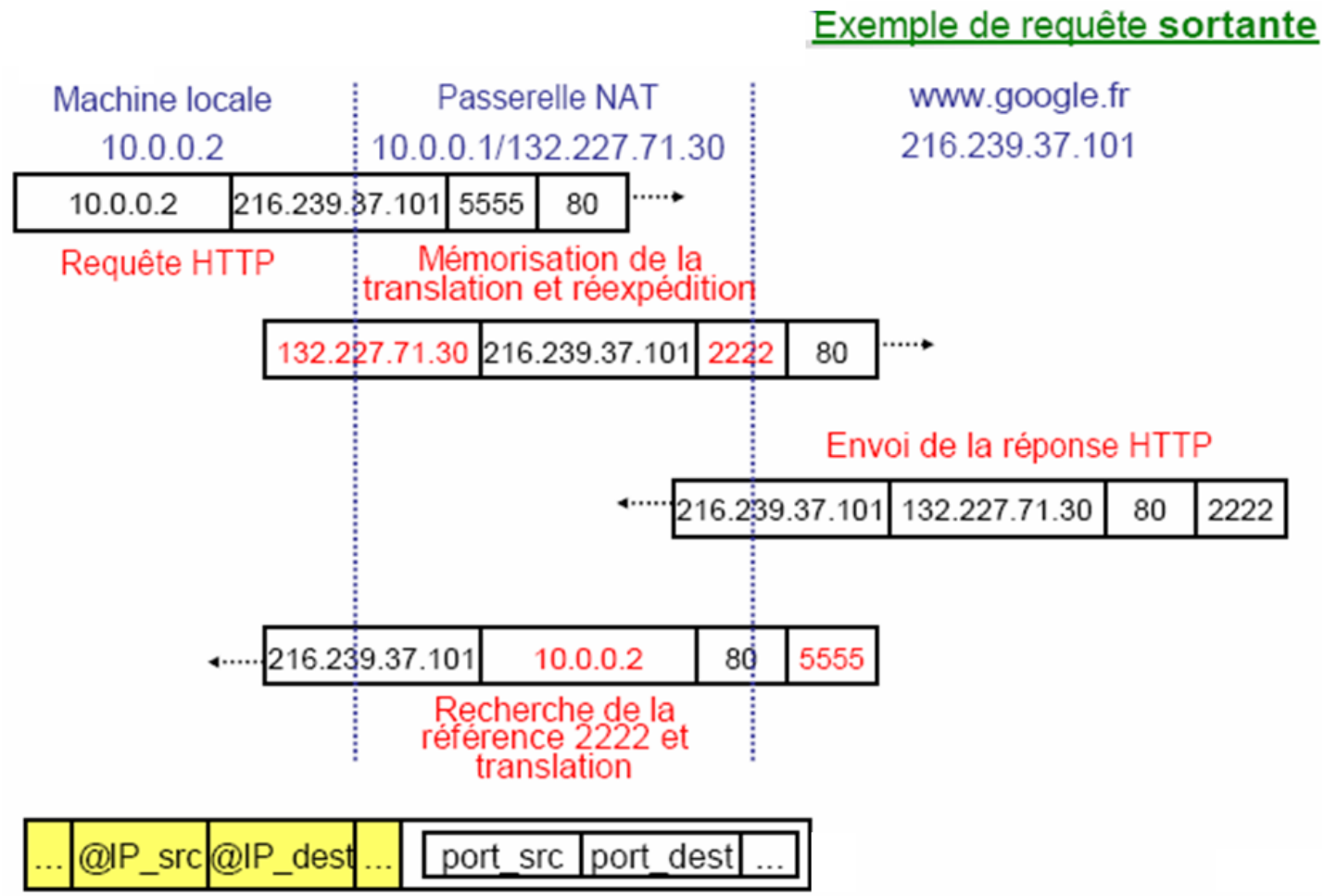
Les adresses privées et le NAT

- Adresses privées (RFC 1918)
  - des adresses qui ne seront jamais attribuées (adresses illégales) et qui ne sont pas routables sur l'Internet
  - classe A : de 10.0.0.0 à 10.255.255.255
  - classe B : de 172.16.0.0 à 172.31.255.255
  - classe C : de 192.168.0.0 à 192.168.255.255
- Si une entreprise qui utilise des adresses privées souhaitent tout de même disposer d'une connexion à l'Internet, il faut
  - demander une adresse publique
  - faire des conversions adresse privée <--> adresse publique

Les adresses privées et le NAT

- NAT (RFC 3022) - Network Address Translator
  - mise en correspondance d'une adresse privée et d'une adresse publique
  - traduction statique ou dynamique (lors de la connexion)
  - une solution au manque d'adresses IP publiques : quelques adresses IP publiques pour beaucoup d'adresses IP privées mais le NAT est coûteux en perf.
- Fonctionnement du NAT
  - une table stockée dans le NAT fait la correspondance entre (@IP_src privée, port_src) et une @IP_publique
  - quand le paquet part : @IP_src devient @IP_publique, port_src devient la référence de l'entrée dans la table
  - quand la réponse revient : port_dest du paquet permet de retrouver dans la table @IP et port src

NAT


Exemple de requête sortante
Machine locale
10.0.0.2
Passerelle NAT
10.0.0.1/132.227.71.30
www.google.fr
216.239.37.101
10.0.0.2
216.239.37.101
5555
80
Requête HTTP
Mémorisation de la translation et réexpédition
132.227.71.30
216.239.37.101
2222
80
Envoi de la réponse HTTP
216.239.37.101
132.227.71.30
80
2222
216.239.37.101
10.0.0.2
80
5555
Recherche de la référence 2222 et translation
...
@IP_src
@IP_dest
...
port_src
port_dest
...

Protocole ICMP

- Internet Control Message Protocol), RFC 792
- Objectif
  - Rapport d'erreurs de la couche Réseau
- Exemple
  - Au cours d'une session HTTP, un message d'erreur « Réseau de destination inaccessible » est affiché
  - Quand un routeur ne peut pas trouver le chemin spécifié par l'application, il génère un message d'erreur à la source
  - Le terminal reçoit le message ICMP et renvoie le code d'erreur à la couche TCP qui à son tour le renvoie à l'application

CABLES DROITS CROISES

Sondes Kallel

Droits ou croisés

- **Quand utiliser du câble droit ou du câble croisé avec un réseau Ethernet ?**
- La technologie Ethernet supporte le câble à paire torsadée à huit fils.
- 10BASE-T IEEE 802.3
- 100BASE-TX IEEE 802.3u
- 1000BASE-T IEEE 802.3ab
- 10GBASE-T IEEE 802.3an

Droit ou croisés

- On utilise ce câble en catégories récentes avec une prise modulaire RJ45 (8P8C). Les schémas de brochage répondent aux normes de câblage structuré T568A et T568B.

Droits ou croisés

- Les commutateurs (switches) et concentrateurs (hubs) sont identifiés comme étant des DCE (Data Connexion Equipement)
- alors que les stations terminales et les routeurs sont des périphériques DTE (Data Terminal Equipment).
- Les équipement identique DTE/DTE ou DCE/DCE se connectent avec un câble croisé (qui croise les paires d'émission et de réception).
- Les équipements de type différents se connectent avec un câble droit car la position émission réception sur leur interfaces est déjà inversée.

Droit ou croisés

- Outre le fait que les nouvelles gammes de matériel actif s'adaptent automatiquement aux câbles en reconnaissant les positions du signal, on utilisera soit du câble croisé ou droit selon le type de matériel que l'on connecte :

DROIT OU CROISES

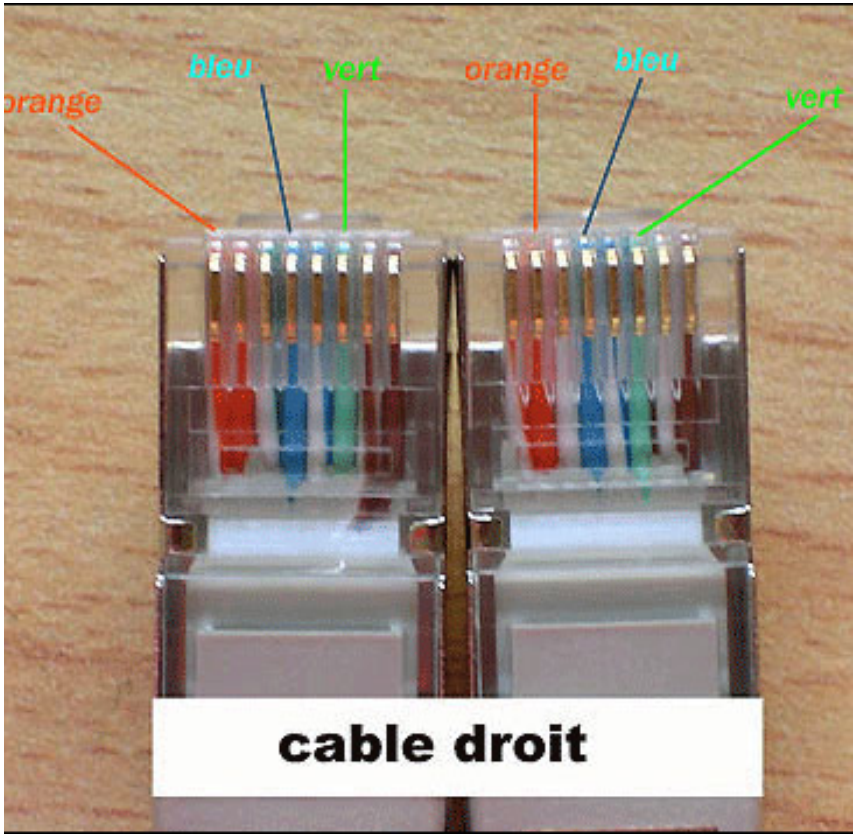
- **Câbles droits :**
- PC à Hub
- PC à Switch
- Switch à Routeur

- **Câbles croisés :**
- Switch à Switch
- Hub à Hub
- Routeur à Routeur
- PC à PC
- Hub à Switch
- PC à Routeur

Comment reconnaitre un cable droit et cable croisé

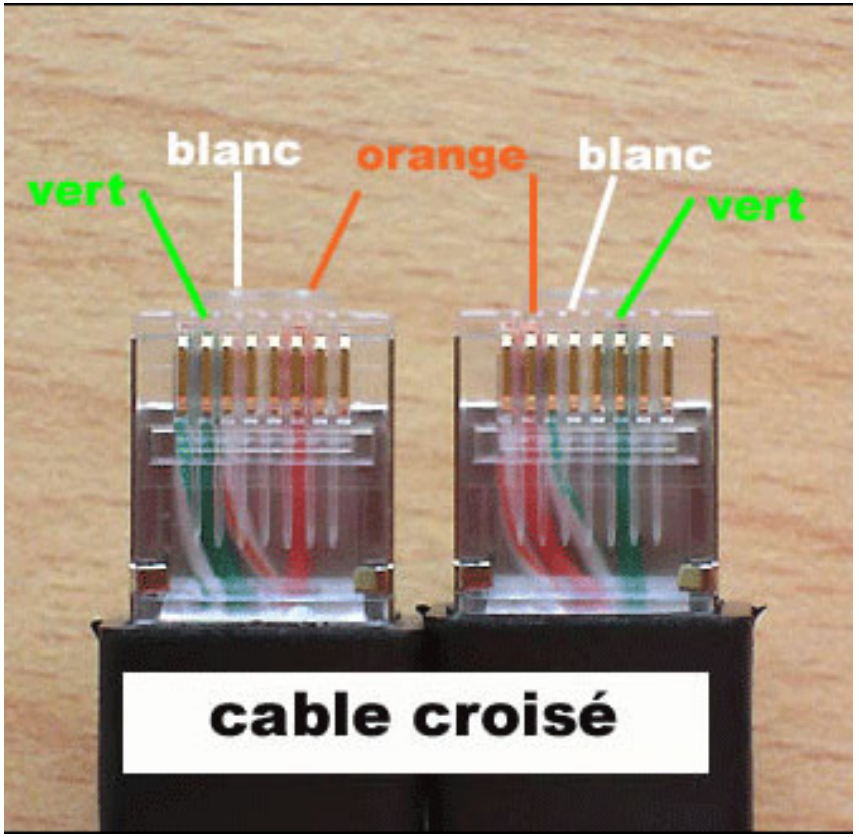
- Vous avez des cables **ethernet** a la maison mais comment reconnaitre un cable croisé d'un cable droit ?

- Prenez les 2 extrémités du câble et tournez les "bitonios" vers le bas. En mettant les **extrémités des câbles cote à cote** vous remarquerez le sens des fils. Si ceux-ci sont arrangés de la meme façon c'est un câble droit, a l'inverse si les fils apparaissent "désordonnés" c'est un câble croisé.



Comment reconnaitre un cable droit et cable croisé

- **Comment reconnaitre un cable droit et cable croisé**
- Vous avez des cables **ethernet** a la maison mais comment reconnaitre un cable croisé d'un cable droit ?
- Prenez les 2 extrémités du câble et tournez les "bitonios" vers le bas. En mettant les **extrémités des câbles cote à cote** vous remarquerez le sens des fils. Si ceux-ci sont arrangés de la meme façon c'est un câble droit, a l'inverse si les fils apparaissent "désordonnés" c'est un câble croisé.

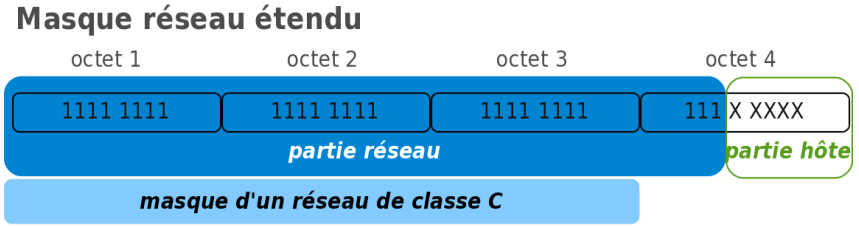


Découpage en sous-réseaux : Exemple

- On reprend l'exemple de la classe C 192.168.1.0 dont le masque réseau est par définition 255.255.255.0.
- Sans découpage, le nombre d'hôtes maximum de ce réseau est de 254.
- Considérant qu'un domaine de diffusion unique pour 254 hôtes est trop important, on choisit de diviser l'espace d'adressage de cette adresse de classe C.

Découpage en sous-réseaux : Exemple

- On réserve 3 bits supplémentaires du 4ème octet en complétant le masque réseau.
  - De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte.



Découpage en sous-réseaux : Exemple

Adresse réseau	192.168. 1. 0	Plage d'adresses utilisables	Adresse de diffusion
Masque de réseau	255.255.255.224		
Sous-réseau 0	192.168. 1. 0	192.168.1. 1 - 192.168.1. 30	192.168.1. 31
Sous-réseau 1	192.168. 1. 32	192.168.1. 33 - 192.168.1. 62	192.168.1. 63
Sous-réseau 2	192.168. 1. 64	192.168.1. 65 - 192.168.1. 94	192.168.1. 95
Sous-réseau 3	192.168. 1. 96	192.168.1. 97 - 192.168.1.126	192.168.1.127
Sous-réseau 4	192.168. 1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
Sous-réseau 5	192.168. 1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
Sous-réseau 6	192.168. 1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
Sous-réseau 7	192.168. 1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Découpage en sous-réseaux : Remarques

- Selon les termes du document RFC950, les sous-réseaux dont les bits de masque sont tous à 0 ou tous à 1 ne devaient pas être utilisés pour éviter les erreurs d'interprétation par les protocoles de routage dits classful comme RIPv1. En effet, ces protocoles de routages de «première génération» ne véhiculaient aucune information sur le masque sachant que celui-ci était déterminé à partir de l'octet le plus à gauche. Dans notre exemple ci-dessus, il y avait confusion aux niveaux de l'adresse de réseau et de diffusion.
  - L'adresse du sous-réseau 192.168.1.0 peut être considérée comme l'adresse réseau de 2 réseaux différents : celui avec le masque de classe C (255.255.255.0) et celui avec le masque complet après découpage en sous-réseaux (255.255.255.224).
  - De la même façon, l'adresse de diffusion 192.168.1.255 est la même pour 2 réseaux différents : 192.168.1.0 ou 192.168.100.224.
- Depuis la publication du document RFC950, en 1985, les protocoles de routage qui servent à échanger les tables d'adresses de réseaux connectés entre routeurs ont évolué.
- Tous les protocoles contemporains sont conformes aux règles de routage inter-domaine sans classe (CIDR). Les protocoles tels que RIPv2, OSPF et BGP intègrent le traitement des masques de sous-réseaux.
- Ils peuvent même regrouper ces sous-réseaux pour optimiser le nombre des entrées des tables de routage. Pour appuyer cet argument, le document RFC1878 de 1995 spécifie clairement que la pratique d'exclusion des sous-réseaux all-zeros et all-ones est obsolète.

Commandes switch et routeur

Commandes Cisco

Commandes sur routeur

Objectif	Commande
Passer en mode de configuration globale	**configure terminal** Exemple : Router> **enable** Router# configure terminal Router(config)#
Indiquer le nom du routeur	**hostname** *name* Exemple : Router(config)# **hostname Router1** Router(config)#
Définir un mot de passe chiffré pour empêcher tout accès non autorisé au mode d'exécution privilégié	**enable secret** *password* Exemple : Router(config)# **enable secret cisco** Router(config)#
Définir un mot de passe pour empêcher tout accès non autorisé à la console	**password** *password* **login** Exemple : Router(config)# **line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#

Commandes Cisco

Commandes sur routeur

Définir un mot de passe pour empêcher tout accès Telnet non autorisé. Lignes vty du routeur : 0 4 Lignes vty du commutateur : 0 15	**password** *password* **login** Exemple : Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** Router(config-line)#
Configurer la bannière MOTD.	**Banner motd %** Exemple : Router(config)# **banner motd %** Router(config)#
Configurer une interface. L'interface du routeur est désactivée par défaut L'interface du commutateur est activée par défaut	Exemple : Router(config)# **interface fa0/0** Router(config-if)# **description** *description* Router(config-if)# **ip address** *masque d'adresse* Router(config-if)# **no shutdown** Router(config-if)#
Enregistrer la configuration en mémoire NVRAM.	**copy running-config startup-config** Exemple : Router# **copy running-config startup-config** Router#