Identifiez les domaines de collision et de diffusion

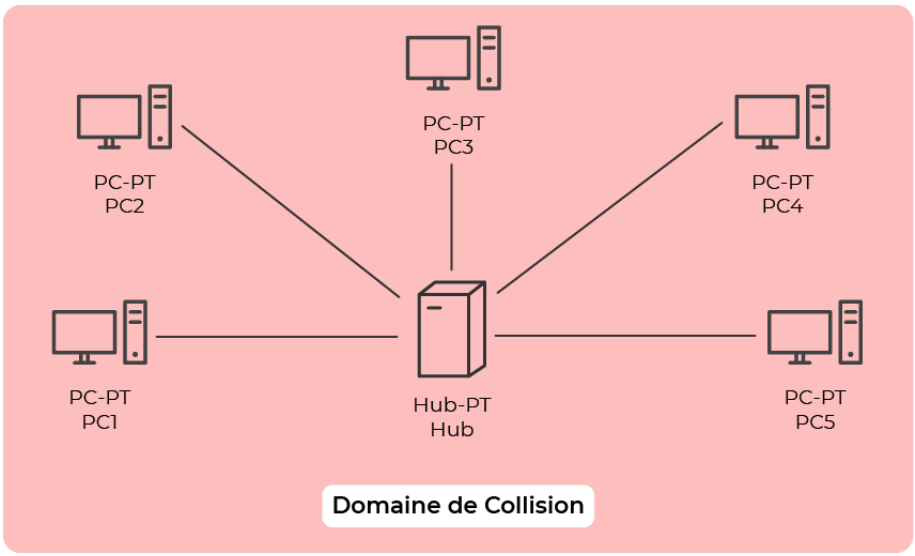
Identifiez les domaines de collision

Dans les chapitres précédents, vous avez acquis une meilleure compréhension de ce que sont un commutateur et son fonctionnement. Allons ici un peu plus loin.

Les commutateurs fonctionnent les uns avec les autres mais également avec d'autres équipements, pour éliminer les **collisions** et réduire la **congestion** du réseau :

- Une collision est quand deux paquets sont émis en même temps sur un segment de réseau.
- La congestion du réseau (ou augmentation du trafic) arrive quand le réseau est très fortement ralenti.

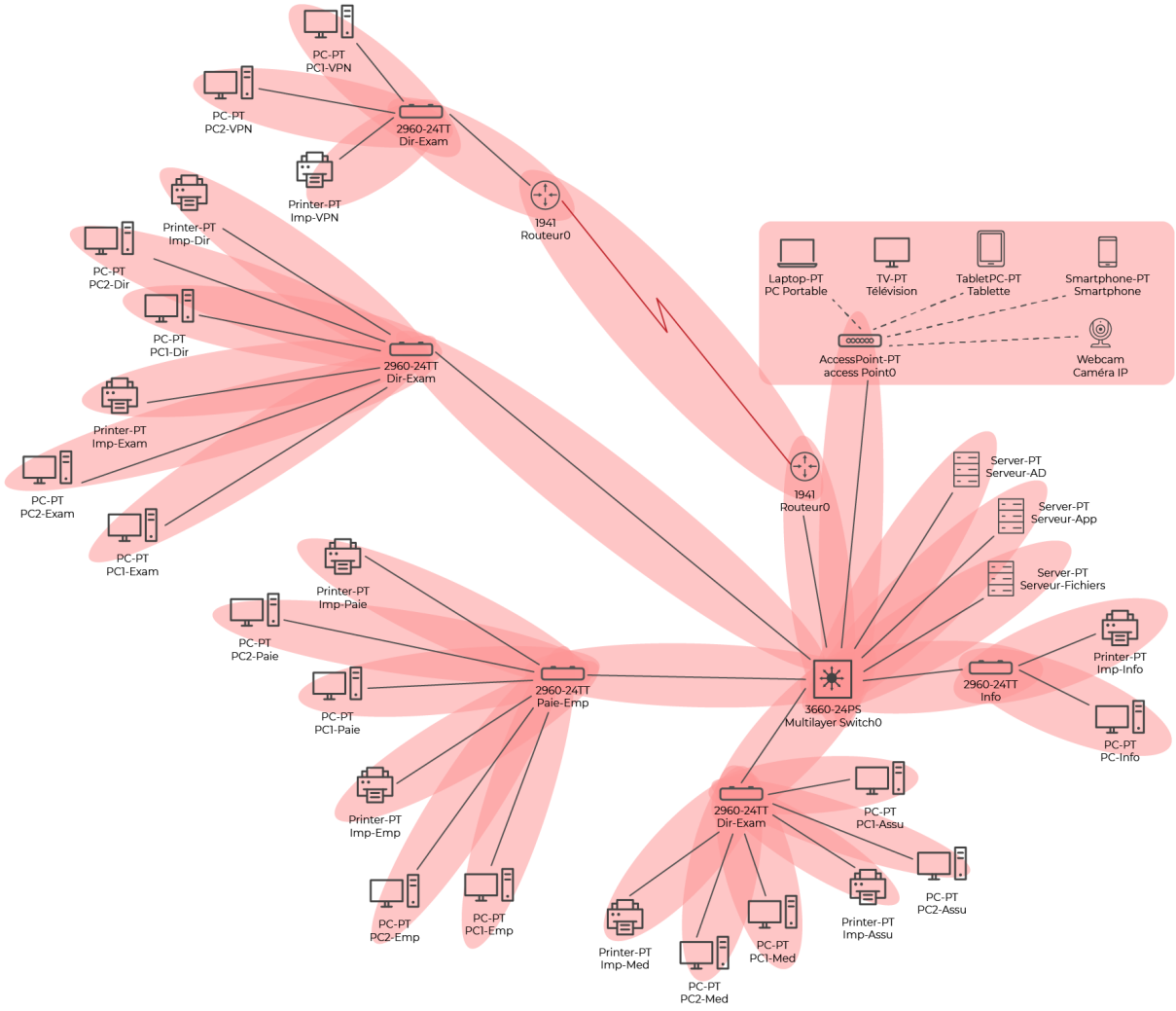
Dans les segments **Ethernet** traditionnels basés sur le **concentrateur**, les périphériques réseau étaient en concurrence pour le support partagé. Ces segments de réseau qui partagent **la même bande passante** entre les périphériques sont appelés ***domaines de collision***. Lorsque deux ou plusieurs dispositifs dans le même domaine de **collision** tentent de communiquer en même temps, une collision se produit. C'est ce qui se passait avant avec l'utilisation des concentrateurs, plus communément appelé ***hubs***.



Domaine de collision avec un hub
Cet équipement n'est plus utilisé car il génère des domaines de collision trop importants, et le réseau devient très vite congestionné.

Si un port de commutateur fonctionne en **mode bidirectionnel** non simultané, chaque segment est dans son **propre domaine de collision**.

Si je reprends le schéma de réseau de la métropole, vous pouvez définir les domaines de collision comme ceci :

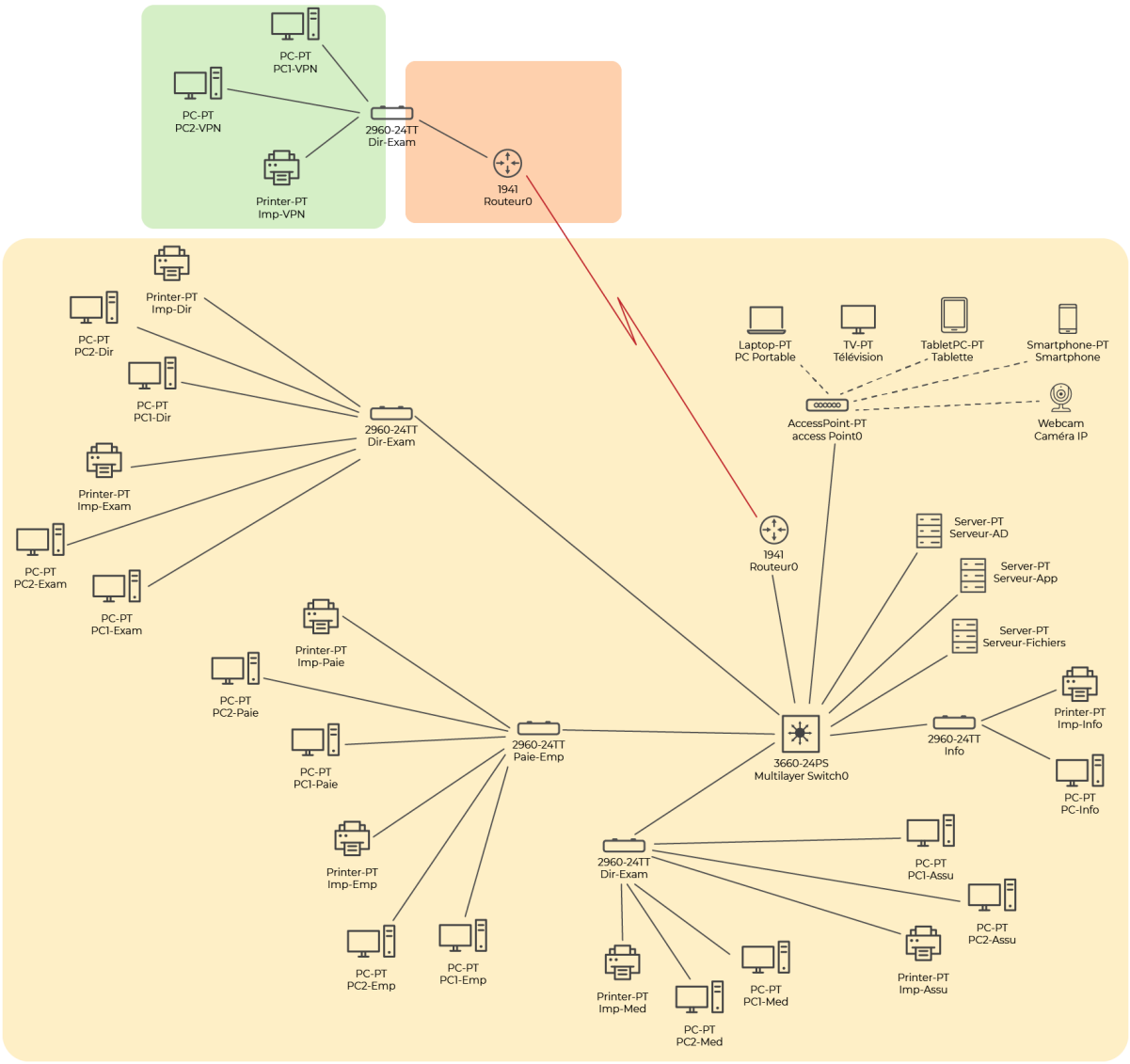


Chaque cercle rouge est un domaine de collision dans le réseau de l'entreprise.
Plus vos domaines de collision sont petits, meilleur sera votre réseau !

Identifiez les domaines de diffusion

Un ensemble de commutateurs interconnectés constitue **un domaine de diffusion unique**. Seul un périphérique de couche réseau, tel qu'un **routeur**, peut diviser un domaine de diffusion de couche 2. Les routeurs sont utilisés pour segmenter les domaines de diffusion, mais ils segmentent également les domaines de collision.

Si je reprends mon schéma de réseau, vous pouvez définir les domaines de diffusion comme ceci :



Domaines de diffusion dans le réseau de l'entreprise
Nos domaines de diffusion sont assez gros. Surtout celui du domaine de diffusion qui correspond au réseau de l'entreprise ; ce n'est pas bon signe !

Lorsqu'un commutateur reçoit une trame de diffusion, il la transfère à tous ses ports, sauf au port d'entrée où elle a été reçue. Chaque périphérique connecté au commutateur reçoit un exemplaire de la trame de diffusion, et la traite.

Les diffusions **réduisent l'efficacité** du réseau. Aussi, la **bande passante** du réseau est utilisée pour transmettre le trafic de diffusion ! Un nombre de diffusions et une charge trop élevés sur un réseau peuvent entraîner un encombrement qui **ralentit** les performances réseau. Vous devez bien vous rendre compte que notre domaine de diffusion est bien trop gros, il faut donc trouver une solution !

En résumé

Vous avez vu dans ce chapitre :

- Les domaines de collision sont des paquets entrant en conflit sur un segment réseau.

- Les domaines de diffusion sont un segment réseau où n'importe quel ordinateur connecté au réseau peut directement communiquer avec tous les autres ordinateurs du même LAN, sans devoir passer par un routeur.

Utilisez les VLAN pour réduire vos domaines de diffusion

Découvrez les avantages des VLAN

Vous avez vu précédemment que pour limiter le domaine de diffusion, il fallait utiliser des routeurs car ils **segmentent** les domaines de diffusion. Il serait envisageable de segmenter chaque service avec des routeurs, mais cela coûterait très cher et serait complexe à mettre en œuvre.

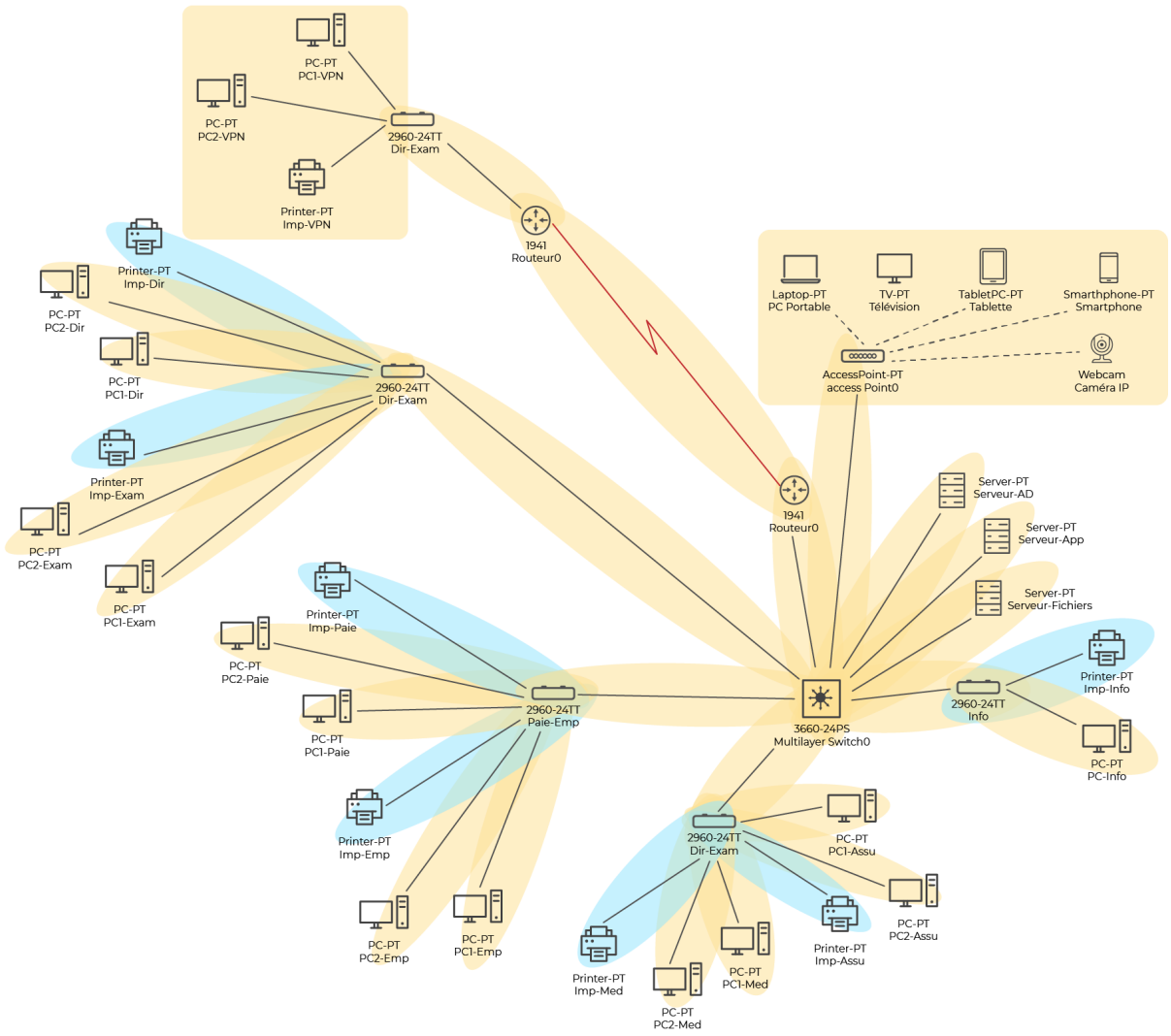
Dans un réseau commuté, on utilisera plutôt des **VLAN** qui assurent la **segmentation** et favorisent la flexibilité de l'entreprise. Les VLAN (**VitualLAN**) reposent sur des **connexions logiques** et non sur des connexions physiques.

Rappelez-vous : au début du cours, je vous demandais de vous intéresser aux services de l'entreprise en tant qu'administrateur réseau. C'est indispensable, car dans la très grande majorité des réseaux informatiques, les **VLAN** sont créés en fonction des **services** dans l'entreprise, et ils sont une représentation logique de ces services !

Les VLAN permettent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application.

Chaque VLAN est considéré comme un **réseau logique distinct**. Les appareils d'un VLAN se comportent comme s'ils se trouvaient sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLAN. N'importe quel port du commutateur peut appartenir à un VLAN.

Les VLAN améliorent les **performances réseau** en divisant de vastes domaines de diffusion en domaines plus petits. Si un périphérique VLAN envoie une trame Ethernet de diffusion, tous les périphériques du VLAN la reçoivent, mais pas les périphériques d'autres VLAN.



Chaque cercle représente un domaine de diffusion dans le réseau de l'entreprise (les imprimantes, en bleu, sont sur le même domaine de diffusion)

Les domaines de diffusion sont maintenant plus petits, mais aussi plus nombreux 😅 !

Grâce aux VLAN, les administrateurs de réseau peuvent mettre en œuvre des politiques d'accès et de sécurité en fonction de groupes d'utilisateurs spécifiques. Chaque port de commutateur peut être attribué à un seul VLAN (à l'exception des ports connectés à un téléphone IP ou à un autre commutateur).

Chaque VLAN d'un réseau commuté correspond à un réseau IP. Par conséquent, la conception d'un VLAN doit tenir compte de la mise en œuvre d'un modèle d'adressage hiérarchique.

L'adressage hiérarchique du réseau signifie que les numéros de réseau IP sont appliqués à des segments de réseau ou à des VLAN. Cette segmentation prend en considération le réseau dans son ensemble. Les blocs d'adresses réseau contiguës sont réservés et configurés sur les périphériques situés dans une zone spécifique de réseau. Voici le plan d'adressage **un peu simplifié** avec les VLAN que vous allez mettre en œuvre dans Cisco Packet Tracer :

Groupes	VLAN ID	Adresse réseau	Première adresse disponible	Dernière adresse disponible	Passerelle réseau

Direction	20	192.168.20.0 /24	192.168.20.1	192.168.20.253	192.168.20.254
Examen Concours	21	192.168.21.0 /24	192.168.21.1	192.168.21.253	192.168.21.254
Paie/DRH	22	192.168.22.0 /24	192.168.22.1	192.168.22.253	192.168.22.254
Emploi	23	192.168.23.0 /24	192.168.23.1	192.168.23.253	192.168.23.254
Médecine	24	192.168.24.0 /24	192.168.24.1	192.168.24.253	192.168.24.254
Assurance	25	192.168.25.0 /24	192.168.25.1	192.168.25.253	192.168.25.254
Info/RGPD	27	192.168.27.0 /24	192.168.27.1	192.168.27.253	192.168.27.254
Serveurs	30	192.168.30.0 /24	192.168.30.1	192.168.30.253	192.168.30.254
Impression	40	192.168.40.0 /24	192.168.40.1	192.168.40.253	192.168.40.254
Téléphones	50	192.168.50.0 /24	192.168.50.1	192.168.50.253	192.168.50.254
WIFI	60	192.168.60.0 /24	192.168.60.1	192.168.60.253	192.168.60.254
Administration	100	192.168.100.0/24	192.168.100.1	192.168.100.253	192.168.100.254

Le tableau suivant répertorie les **avantages** de la conception d'un réseau avec des VLAN :

Bénéfice	**Description**
Domaines de diffusion plus petits	La division d'un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion.
Sécurité optimisée	Seuls les utilisateurs du même VLAN peuvent communiquer ensemble.
Amélioration de l'efficacité des ressources IT	Les VLAN simplifient la gestion du réseau car les utilisateurs ayant des besoins similaires peuvent être configurés sur le même VLAN, et les VLAN peuvent être nommés pour les rendre plus faciles à identifier.
Coût réduit	Les VLAN réduisent la nécessité de mises à niveau coûteuses du réseau et utilisent plus efficacement la largeur de bande et les liaisons montantes existantes, ce qui permet de réaliser des économies.
Meilleures performances	Les domaines de diffusion plus petits réduisent le trafic inutile sur le réseau, et améliorent les performances.
Une gestion simplifiée des projets et des applications	Les VLAN regroupent les utilisateurs et les périphériques réseau pour prendre en charge l'entreprise ou les exigences géographiques ; cela permet d'avoir des fonctions distinctes qui rendent la gestion d'un projet ou l'utilisation d'une application spécialisée plus facile.

Identifiez les types de VLAN

1. VLAN par défaut

Le VLAN par défaut sur un commutateur Cisco est le VLAN 1. Par conséquent, tous les ports du commutateur sont sur le VLAN 1. Ce qu'il faut savoir :

- Tous les ports sont attribués à VLAN 1 par défaut.
- Le VLAN natif est le VLAN 1 par défaut.
- Le VLAN de gestion est le VLAN 1 par défaut.
- Le VLAN 1 ne peut être renommé ni supprimé.

La commande **show vlan brief** permet de connaître l'appartenance des VLAN en fonction des interfaces. Tous les ports sont actuellement attribués au VLAN 1 par défaut. Aucun VLAN natif n'est explicitement attribué et aucun autre VLAN n'est actif ; par conséquent, le VLAN natif est défini comme VLAN de gestion. Il s'agit d'un risque de sécurité.

```
Switch# show vlan brief
VLAN    Name                             Status  Ports
----  -------------------- ---------
-------------------------------
1  default                       active        Fa0/1, Fa0/2,
Fa0/3,
Fa0/4
                                             Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                             Fa0/9, Fa0/10, 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
                                             Gig0/1, Gig0/2
1002    fddi-default                 active
1003    token-ring-default  active
1004    fddinet-default              active
1005    trnet-default        active
Switch#
```

2. VLAN de données

Les VLAN de données sont des VLAN configurés pour séparer le trafic généré par l'utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.

3. VLAN natif

Le trafic utilisateur à partir d'un VLAN doit être marqué avec son **ID VLAN** lorsqu'il est envoyé à un autre commutateur. Les ports de **Trunk** sont utilisés entre les commutateurs pour prendre en charge la transmission du **trafic balisé**.

Le VLAN natif sur un commutateur Cisco est le VLAN 1 (VLAN par défaut). Il est généralement recommandé de configurer le VLAN natif en tant que VLAN inutilisé, distinct du VLAN 1 et des autres VLAN. En fait, il n'est pas rare de dédier un VLAN fixe jouant le rôle de VLAN natif pour tous les ports Trunk du domaine commuté.

3. VLAN de gestion

Un VLAN de gestion est un VLAN de données configuré spécifiquement pour le trafic de gestion réseau, y compris SSH, Telnet, HTTPS, HTTP et SNMP. Par défaut, le VLAN 1 est configuré comme VLAN de gestion sur un commutateur de couche 2.

4. VLAN voix

Un VLAN distinct est nécessaire pour prendre en charge la voix sur IP (VoIP). Le trafic VoIP requiert les éléments suivants :

- Bande passante consolidée pour garantir la qualité de la voix.
- Priorité de transmission par rapport aux autres types de trafic réseau.
- Possibilité de routage autour des zones encombrées du réseau.
- Délai (ping) inférieur à 150 ms sur tout le réseau.

Vous reviendrez sur ce concept de VLAN voix plus loin dans le cours.

En résumé

Vous avez vu dans ce chapitre :

- Les VLAN regroupent de façon logique et indépendante un ensemble de machines informatiques. L'avantage d'une conception d'un réseau avec des VLAN est qu'elle permet de réduire les domaines de diffusion, et donc de réduire la congestion du réseau.
- Les différents types de VLAN :
    - VLAN par défaut ;
    - VLAN de données ;
    - VLAN natif ;
    - VLAN de gestion ;
    - VLAN voix.

Paramétrez les VLAN

Créez des VLAN

Vous allez à présent créer vos premiers VLAN. Travaillez dans un premier temps sur le commutateur **Dir-Exam**. Et, je suis sympathique avec vous, je vous donne le schéma avec le nom des interfaces :

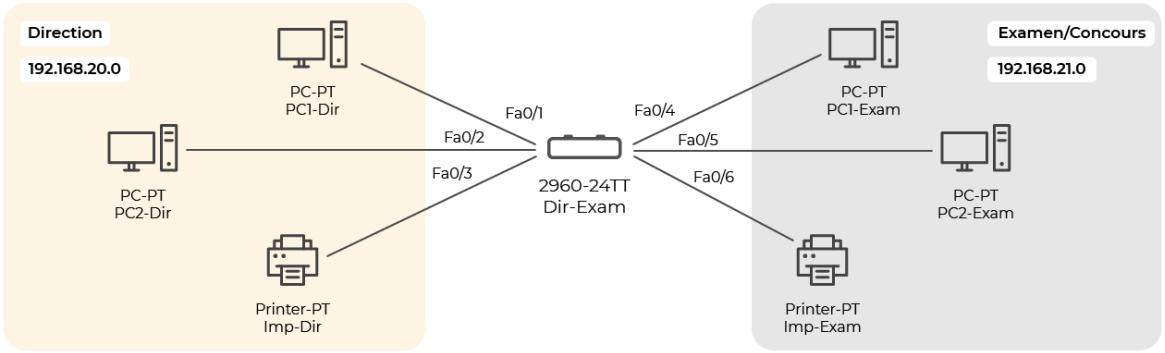


Schéma du commutateur Dir-Exam
Pour le commutateur Dir-Exam, il faudra créer 5 VLAN :

Dir-Exam	
VLAN ID	**Nom VLAN**
20	Direction
21	Examen/ Concours
40	Impression
50	Téléphonie
100	Administration

Pour créer les VLAN, il faut taper les commandes suivantes :

Tâche	**Commande IOS**
Passez en mode de configuration globale	Dir-Exam# **configure terminal**
Créez un VLAN avec un numéro d'identité valide	Dir-Exam(config)# **vlan 20**
Indiquez un nom unique pour identifier le VLAN	Dir-Exam(config-vlan)# **name Direction**
Repassez en mode d'exécution privilégié	Dir-Exam(config-vlan)# **end**

En règle générale, les numéros de VLAN correspondent aux identifiants **sous-réseaux IP**. De plus, pour les réseaux de petite taille et de taille moyenne, la plage acceptée pour l'identifiant VLAN (VLAN ID) est de 1 à 1 000.

Allez, je vous montre la configuration complète pour le commutateur **Dir-Exam** :

```
Dir-Exam# configure terminal
Dir-Exam(config)# vlan 20
Dir-Exam(config-vlan)# name Direction
Dir-Exam(config-vlan)# exit
Dir-Exam(config)# vlan 21
Dir-Exam(config-vlan)# name Examen/Concours
Dir-Exam(config-vlan)# exit
Dir-Exam(config)# vlan 40
Dir-Exam(config-vlan)# name Impression
Dir-Exam(config-vlan)# exit
Dir-Exam(config)# vlan 50
Dir-Exam(config-vlan)# name Telephonie
Dir-Exam(config-vlan)# exit
Dir-Exam(config)# vlan 100
Dir-Exam(config-vlan)# name Administration
Dir-Exam(config-vlan)# end
```

Votre VLAN Administration doit se mettre en "**up**" juste après avoir entré la commande **vlan 100** ; c'est normal, vous aviez déjà configuré une adresse **IP** sur ce vlan 100, et je vous avais dit qu'elle serait active dès le VLAN créé. C'est ce que vous venez de faire 😉 !

Bon, vous êtes autonome maintenant, je vais vous laisser faire les autres commutateurs. Mais je vous aide un peu en vous donnant la liste des VLAN présents dans chaque commutateur :

Paie-Emp	
VLAN ID	**Nom VLAN**
22	Paie/DRH
23	Emploi
40	Impression
50	Téléphonie
100	Administration

Med-Assu	
VLAN ID	**Nom VLAN**
24	Médecine
25	Assurance
40	Impression

50	Téléphonie
100	Administration

Info	
VLAN ID	**Nom VLAN**
27	Info
40	Impression
50	Téléphonie
100	Administration

Attribuez des VLAN

Pour attribuer un VLAN à une interface, il faut taper les commandes suivantes :

Tâche	**Commande IOS**
Passez en mode de configuration globale	Dir-Exam# **configure terminal**
Allez dans l'interface	Dir-Exam(config)# **int fa0/1**
Configurez le mode d'accès du VLAN	Dir-Exam(config-if)# **switchport mode access**
Attribuez le VLAN à l'interface	Dir-Exam(config-if)# **switchport access vlan 20**
Repassez en mode d'exécution privilégié	Dir-Exam(config-if)# **end**

Allez, je vous montre la configuration complète pour le commutateur **Dir-Exam** :

```
Dir-Exam(config)# interface fa0/1
Dir-Exam(config-if)# switchport mode access
Dir-Exam(config-if)# switchport access vlan 20
Dir-Exam(config-if)# exit
Dir-Exam(config)# interface fa0/2
Dir-Exam(config-if)# switchport mode access
Dir-Exam(config-if)# switchport access vlan 20
Dir-Exam(config-if)# exit
Dir-Exam(config)# interface fa0/3
Dir-Exam(config-if)# switchport mode access
Dir-Exam(config-if)# switchport access vlan 40
Dir-Exam(config-if)# exit
Dir-Exam(config)# interface fa0/4
Dir-Exam(config-if)# switchport mode access
Dir-Exam(config-if)# switchport access vlan 21
Dir-Exam(config-if)# exit
Dir-Exam(config)# interface fa0/5
```

```
Dir-Exam(config-if)# switchport mode access
Dir-Exam(config-if)# switchport access vlan 21
Dir-Exam(config-if)# exit
Dir-Exam(config)# interface fa0/6
Dir-Exam(config-if)# switchport mode access
Dir-Exam(config-if)# switchport access vlan 40
Dir-Exam(config-if)# exit
```

Attribuez les VLAN aux différentes interfaces des commutateurs **Paie-Emp**, **Med-Assu** et **Info** en respectant le schéma suivant :

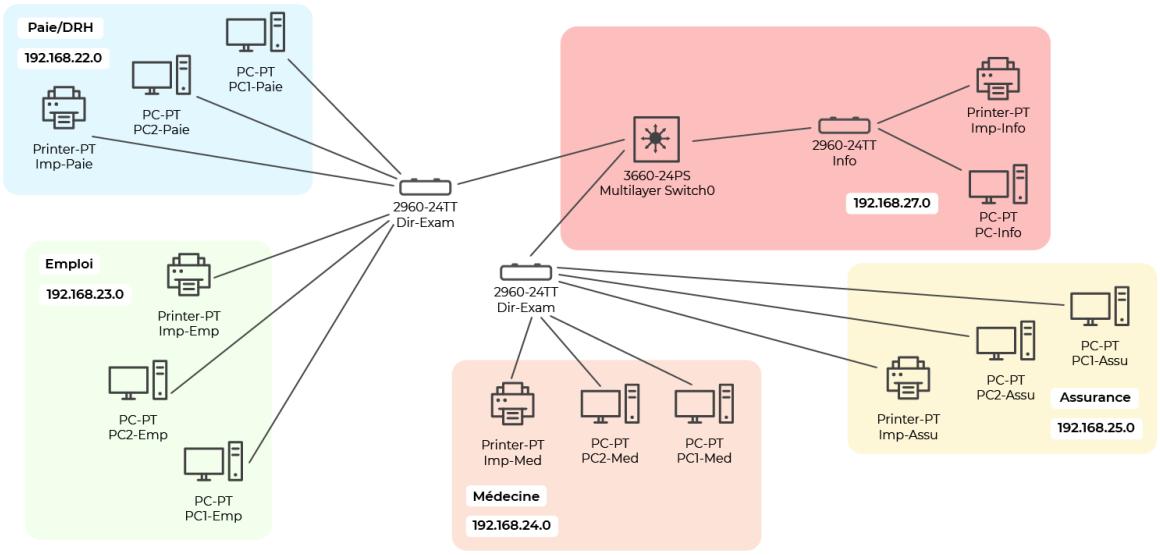


Schéma du réseau de l'entreprise avec les commutateurs à configurer et le nom des interfaces affiché

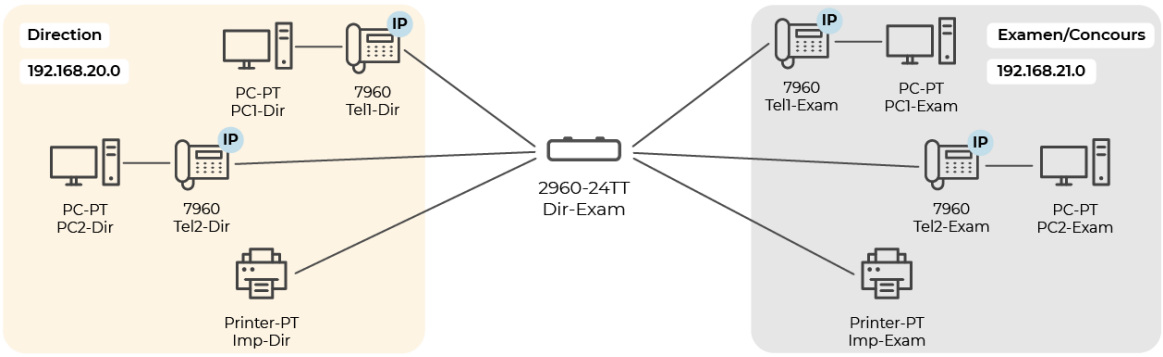
Ajoutez la téléphonie sur IP dans votre entreprise

Ajoutez des téléphones sur IP dans Cisco Packet Tracer

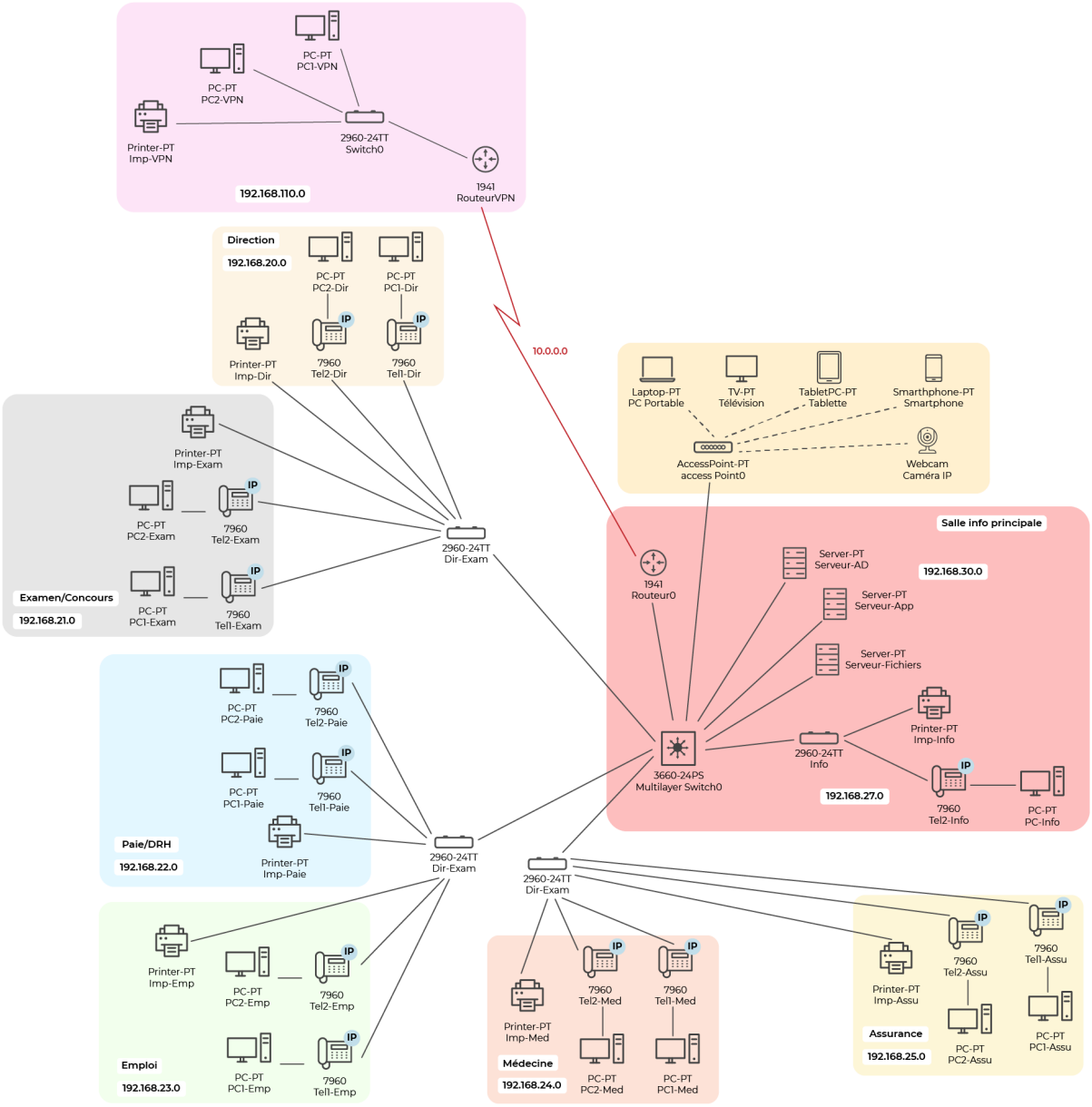
Vous allez rajouter la téléphonie sur IP dans votre entreprise mais vous allez me maudire car il va falloir revoir un petit peu le schéma du réseau 😡 ! Vous allez devoir ajouter des IP Phones entre vos ordinateurs et votre interface du commutateur.

Vous essayez de votre côté ?

Voilà à quoi doivent ressembler les périphériques finaux connectés au commutateur **Dir-Exam** :



Les périphériques finaux connectés au commutateur Dir-Exam
Donc à la fin, votre schéma réseau doit ressembler à ceci :



Le schéma de réseau de la métropole Chantilly-Grenade

C’est promis, ce schéma réseau final sous Cisco Packet Tracer ne bougera plus 🙏 !

Configurez la téléphonie sur IP sur les commutateurs

Bon, c’est cool, j’ai rajouté mes téléphones IP mais si je lance des tests de communication (pings), plus rien ne marche, même entre des postes situés sur le même sous-réseau 🤬 !

Pas d’inquiétude ! Il vous faut configurer les commutateurs pour indiquer que des VLAN voix doivent être configurés sur les ports où sont connectés des téléphones sur IP.

Pour rappel, il n’est pas possible de configurer plusieurs VLAN sur une interface sauf si l’on ajoute :

- un VLAN voix ;
- des ports Trunk, où plusieurs VLAN peuvent être “autorisés” sur un port. Vous verrez juste après dans le cours ce que c’est.

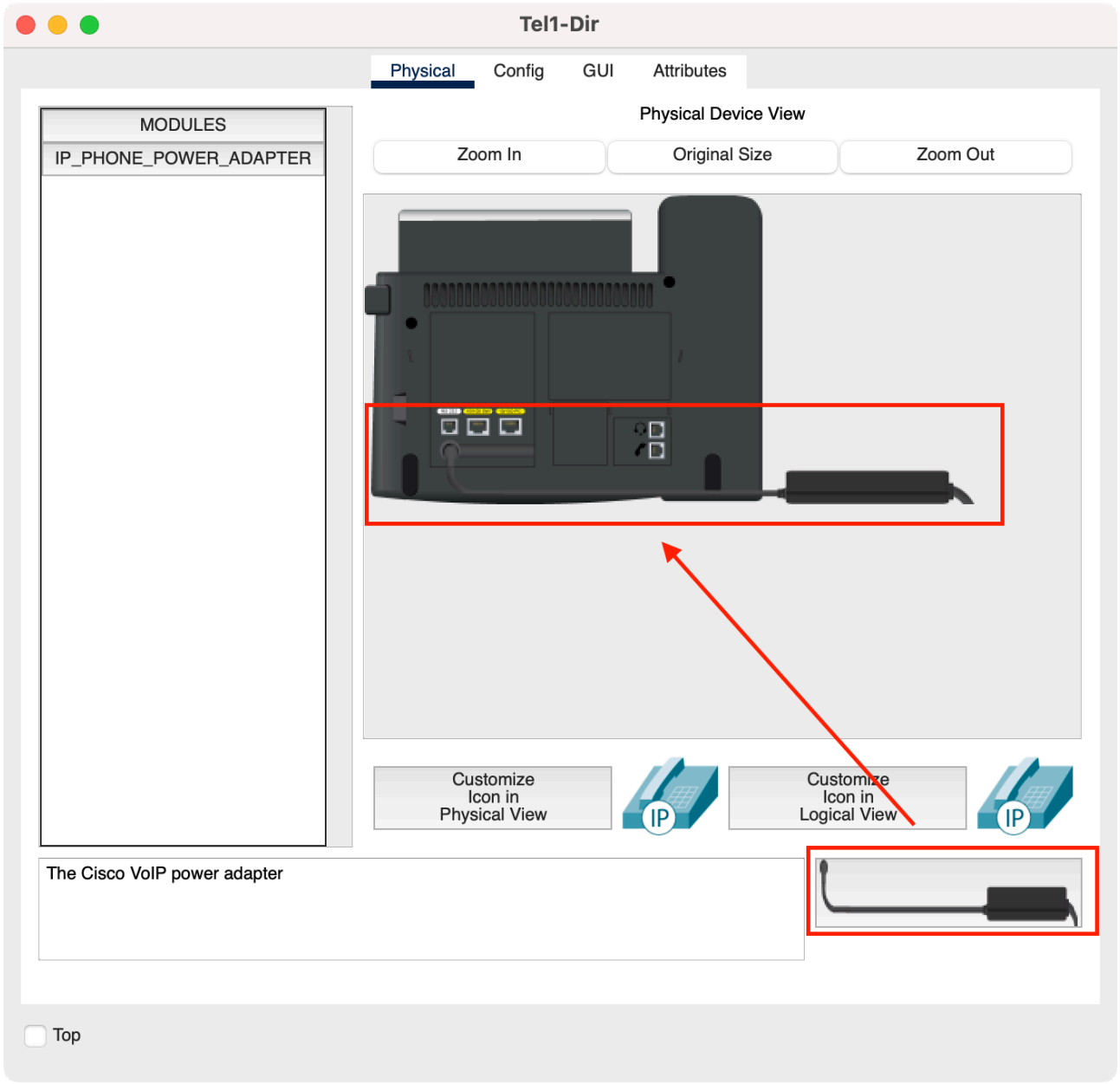
Comme vous avez déjà créé le VLAN **Téléphonie**, vous devez à présent :

- activer la qualité de service (ou Quality of Service) sur les interfaces. Elle assure les bonnes conditions à un type de trafic donné ;
- ajouter l’appartenance d’un VLAN voix à chaque interface où un IP Phone est connecté.

Voici la configuration complète pour le commutateur **Dir-Exam** :

```
Dir-Exam(config)# int f0/1
Dir-Exam(config-if)# mls qos trust cos
Dir-Exam(config-if)# switchport voice vlan 50
Dir-Exam(config-if)# exit
Dir-Exam(config)# int f0/2
Dir-Exam(config-if)# mls qos trust cos
Dir-Exam(config-if)# switchport voice vlan 50
Dir-Exam(config-if)# exit
Dir-Exam(config)# int f0/4
Dir-Exam(config-if)# mls qos trust cos
Dir-Exam(config-if)# switchport voice vlan 50
Dir-Exam(config-if)# exit
Dir-Exam(config)# int f0/5
Dir-Exam(config-if)# mls qos trust cos
Dir-Exam(config-if)# switchport voice vlan 50
Dir-Exam(config-if)# exit
```

Lorsque vous ajoutez des téléphones sur IP, et nous ne l’avons pas fait avant, n’oubliez pas de les **alimenter**. Pour cela, sélectionnez le bloc d’alimentation en le faisant glisser jusqu’à la broche d’alimentation.



Le bloc d'alimentation sélectionné puis raccordé à la broche d'alimentation

En résumé

Vous avez vu dans ce chapitre :

- La commande vlan *Numéro_de_VLAN* permet de créer des VLAN, et la commande switchport access vlan *Numéro_de_VLAN* permet d'attribuer les VLAN à des ports.
- La commande switchport voice vlan *Numéro_de_VLAN* permet d'ajouter des téléphones IP et de configurer des commutateurs pour y intégrer le VLAN téléphonie.

Terminez le paramétrage des VLAN

Vérifiez des informations sur les VLAN

Une fois qu'un VLAN est configuré, les configurations VLAN peuvent être validées à l'aide des commandes IOS de Cisco **show**. La commande **show vlan** affiche une liste de tous les VLAN configurés :

```
Dir-Exam> show vlan
VLAN Name                    Status      Ports
---- --------------------- ---------
   -------------------------------
1   default                  active          Fa0/7, Fa0/8,
Fa0/9,
Fa0/10
                                             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,
Gig0/2
20   Direction               active          Fa0/1, Fa0/2
21   Examen/Concours         active          Fa0/4, Fa0/5
40   Impression                   active         Fa0/3, Fa0/6
50   Telephonie                   active         Fa0/1,
Fa0/2, Fa0/4,
Fa0/5
100  Administration               active
1002  fddi-default                active
1003  token-ring-default     active
1004  fddinet-default              active
1005  trnet-default          active

VLAN      Type SAID    MTU Parent    RingNo   BridgeNo  Stp
BrdgMode Trans1 Trans2
---- ----- ------ ----- ------ ------ -------- ---- --------
------ ------
1    enet 100001  1500 -  -  -    -  -    0  0
20   enet 100020  1500 -  -  -    -  -    0  0
21   enet 100021  1500 -  -  -    -  -    0  0
40   enet 100040  1500 -  -  -    -  -    0  0
50   enet 100050  1500 -  -  -    -  -    0  0
100  enet 100100  1500 -  -  -    -  -    0  0
```

```
1002 fddi 101002  1500 -  -  -    -  -    0  0
1003 tr   101003  1500 -  -  -    -  -    0  0
1004 fdnet     101004  1500 -  -  -    ieee - 0   0
1005 trnet101005  1500      -  -  -    ibm  -  0   0

VLAN Type  SAID   MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
---- ----- ------ ----- ------ ------ -------- ---- --------
------ ------
Remote SPAN VLANs
------------------------------------------------------------
----------------
Primary Secondary Type      Ports
------- --------- -----------------
------------------------------------------
Dir-Exam>
```

On utilisera plutôt la commande **show vlan brief** qui n'affiche qu'un **résumé** des VLAN associés aux interfaces. Il n'affichera que les premières lignes de la commande précédente.

On peut également afficher des précisions sur les VLAN en affichant des informations sur les interfaces, en utilisant la commande **show interfaces** :

```
Dir-Exam> show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (Direction)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 50
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
```

```
Unknown multicast blocked: disabled
Appliance trust: none

Dir-Exam>
```

Modifiez l'appartenance d'un VLAN

Il existe plusieurs façons de modifier l'appartenance des ports aux VLAN. Si le port d'accès au commutateur a été attribué de manière incorrecte à un VLAN, il vous suffit de saisir à nouveau la commande de configuration de l'interface **switchport access vlan** *vlan-id* avec l'ID VLAN correct.

Pour modifier l'appartenance d'un port à un VLAN, utilisez la commande **no switchport access vlan**.

Si vous enlevez l'appartenance d'un VLAN à un port, le VLAN est toujours actif bien qu'il ne soit plus associé à l'interface.

Supprimez le VLAN

La commande **no vlan** *vlan-id* est utilisée pour supprimer un VLAN du fichier **vlan.dat**, c'est ce fichier qui contient la liste des VLAN créés.

Avant de supprimer un VLAN, réattribuez d'abord tous les ports membres à un VLAN différent. Tous les ports qui ne sont pas déplacés vers un VLAN actif sont incapables de communiquer avec d'autres hôtes après la suppression du VLAN. La communication ne pourra se faire qu'une fois les ports attribués à un VLAN actif.

L'ensemble du fichier vlan.dat peut être supprimé à l'aide de la commande **delete flash:vlan.dat** en mode d'accès privilégié. La version abrégée de la commande (**delete vlan.dat**) peut être utilisée si le fichier vlan.dat n'a pas été déplacé de son emplacement par défaut.

Après l'exécution de cette commande et le redémarrage du commutateur, les VLAN précédemment configurés ne sont plus présents. Cette commande rétablit les paramètres d'usine par défaut du commutateur, en ce qui concerne les configurations de VLAN.

Pour rétablir l'état par défaut d'un commutateur Catalyst :

- débranchez tous les câbles, à l'exception de la console et du câble d'alimentation du commutateur ;
- entrez la commande **erase startup-config** suivie de la commande **delete vlan.dat** dans le mode d'exécution privilégié.

Effectuez un Trunk de VLAN

Maintenant que vous avez configuré et vérifié les VLAN, il est temps de configurer et de vérifier les Trunks VLAN.

Un **Trunk de VLAN** est un lien de couche 2 entre deux commutateurs, qui achemine le trafic **pour tous les VLAN** (à moins que la liste des VLAN autorisés ne soit restreinte manuellement ou dynamiquement).

Pour activer la liaison Trunk du commutateur Dir-Exam, configurez le port d'interconnexion avec l'ensemble des commandes de configuration d'interface indiquées dans ce tableau :

Tâche	**Commande IOS**
Passer en mode de configuration globale	Dir-Exam# **configure terminal**
Passer en mode de configuration d'interface	Dir-Exam(config)# **interface g0/1**
Régler le port en mode de trunking permanent	Dir-Exam(config-if)# **switchport mode trunk**
Choisir un VLAN natif autre que le VLAN 1	Dir-Exam(config-if)# **switchport trunk native vlan 100**
Indiquer la liste des VLAN autorisés sur la liaison Trunk	Dir-Exam(config-if)# **switchport trunk allowed vlan 20,21,40,50,100**
Repasser en mode d'exécution privilégié	Dir-Exam(config-vlan)# **end**

Il faut que vous fassiez de même sur le lien Trunk des commutateurs **Paie-Emp**, **Med-Assu** et **Info**, je vous laisse le faire tout seul ! 😎

Pour vérifier que le lien Trunk est bien configuré, utilisez la commande **show interfaces** vue précédemment, mais cette fois-ci sur l'interface où est configuré le Trunk :

```
Dir-Exam# show interface g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 100 (Administration)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 20-21,40,100
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
```

```
Appliance trust: none

Dir-Exam#
```

Pour réinitialiser le port Trunk à l'état par défaut, utilisez les commandes **no switchport allowed vlan** et **no switchport trunk native vlan** pour supprimer les VLAN autorisés et réinitialiser le VLAN natif du Trunk.

Lorsqu'il est remis à l'état par défaut, le Trunk autorise tous les VLAN, et utilise le VLAN 1 comme VLAN natif.

En résumé

Vous avez vu dans ce chapitre :

- Les commandes **show vlan brief** et **show interfaces *Nom_Interface* switchport** affichent des informations sur les VLAN.
- La commande **no vlan** pour modifier l'appartenance à un VLAN en reconfigurant le VLAN, et le supprimer.
- Un lien Trunk permet de relier plusieurs commutateurs ensemble et de faire passer les VLAN.
- Les commandes switchport mode trunk et **switchport native vlan *Numéro du VLAN*** configurent un lien Trunk sur un commutateur Cisco Catalyst.

Réalisez le routage inter-vlan

Faites le routage inter-vlan

Dernière étape de notre périple : la configuration de notre cœur de réseau. Eh bien en fait, la configuration d'un commutateur de niveau 3 diffère très peu de la configuration d'un commutateur de niveau 2. Vous allez réaliser les mêmes étapes que précédemment, à savoir :

1. Créer les VLAN dans le commutateur de niveau 3.
2. Affecter les VLAN dans les différentes interfaces.
3. Créer les liaisons Trunks et autoriser les VLAN sur ces liaisons Trunks.

Allez, vous cherchez un peu tout seul ?

Voici la réponse :

```
SwitchL3(config)# vlan 20
SwitchL3(config-vlan)# name Direction
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 21
SwitchL3(config-vlan)# name Examen/Concours
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 22
SwitchL3(config-vlan)# name Paie/DRH
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 23
SwitchL3(config-vlan)# name Emploi
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 24
SwitchL3(config-vlan)# name Medecine
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 25
SwitchL3(config-vlan)# name Assurance
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 27
SwitchL3(config-vlan)# name Info/RGPD
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 30
SwitchL3(config-vlan)# name Serveurs
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 40
SwitchL3(config-vlan)# name Impression
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 50
SwitchL3(config-vlan)# name Telephonie
```

```
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 60
SwitchL3(config-vlan)# name Wifi
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 100
SwitchL3(config-vlan)# name Administration
SwitchL3(config-vlan)# exit
SwitchL3(config)# interface g1/0/2
SwitchL3(config-if)# switchport trunk encapsulation dot1q
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan
20,21,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# interface g1/0/3
SwitchL3(config-if)# switchport trunk encapsulation dot1q
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan
22,23,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# interface g1/0/4
SwitchL3(config-if)# switchport trunk encapsulation dot1q
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan
24,25,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/5
SwitchL3(config-if)# switchport trunk encapsulation dot1q
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan
27,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/6
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 30
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/7
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 30
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/8
SwitchL3(config-if)# switchport mode access
```

```
SwitchL3(config-if)# switchport access vlan 30
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/9
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 60
SwitchL3(config-if)# exit
```

Il faut bien spécifier l'utilisation des trames en **dot1q** sur les liaisons **Trunks** sur un commutateur de niveau 3 en utilisant la commande **switchport trunk encapsulation dot1q**.

Bon c'est super tout cela, mais le but d'un commutateur de niveau 3, c'est de faire du routage, non ?

Certes, vous avez configuré précédemment votre table de routage, mais il reste une configuration importante : il faut créer une passerelle pour tous les VLAN afin qu'ils puissent communiquer ensemble !

Vous allez procéder de la même manière que pour les commutateurs de niveau 2. C'est-à-dire : **créer des interfaces virtuelles** (**SVI**). Comme vous l'avez déjà fait avant, je vous donne les commandes à rentrer pour créer toutes les passerelles sur les interfaces virtuelles SVI :

```
SwitchL3(config)# interface vlan 20
SwitchL3(config-if)# description Passerelle SVI Direction
SwitchL3(config-if)# ip address 192.168.20.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:20::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 21
SwitchL3(config-if)# description Passerelle SVI
Examen/Concours
SwitchL3(config-if)# ip address 192.168.21.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:21::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 22
SwitchL3(config-if)# description Passerelle SVI Paie/DRH
SwitchL3(config-if)# ip address 192.168.22.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:22::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 23
SwitchL3(config-if)# description Passerelle SVI Emploi
SwitchL3(config-if)# ip address 192.168.23.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:23::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 24
SwitchL3(config-if)# description Passerelle SVI Medecine
SwitchL3(config-if)# ip address 192.168.24.254 255.255.255.0
```

```
SwitchL3(config-if)# ipv6 address 2001:db8:acad:24::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 25
SwitchL3(config-if)# description Passerelle SVI Assurance
SwitchL3(config-if)# ip address 192.168.25.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:25::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 27
SwitchL3(config-if)# description Passerelle SVI Info/RGPD
SwitchL3(config-if)# ip address 192.168.27.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:27::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 30
SwitchL3(config-if)# description Passerelle SVI Serveurs
SwitchL3(config-if)# ip address 192.168.30.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:30::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 40
SwitchL3(config-if)# description Passerelle SVI Impression
SwitchL3(config-if)# ip address 192.168.40.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:40::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 50
SwitchL3(config-if)# description Passerelle SVI Telephonie
SwitchL3(config-if)# ip address 192.168.50.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:50::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# interface vlan 60
SwitchL3(config-if)# description Passerelle SVI Wifi
SwitchL3(config-if)# ip address 192.168.60.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:60::254/64
SwitchL3(config-if)# no shutdown
SwitchL3(config-if)# exit
SwitchL3(config)# int vlan 100
SwitchL3(config-if)# description Passerelle SVI
Administration
SwitchL3(config-if)# ip address 192.168.100.254 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:100::254/64
SwitchL3(config-if)# no shutdown
```

```
SwitchL3(config-if)# exit
```
C’est bon, votre maquette sous Cisco Packet Tracer doit être totalement **fonctionnelle**. Pour cela il va falloir faire des **tests**.

Vous pouvez avoir une certaine latence (ou lenteur) concernant le bon fonctionnement de vos tests de communication (pings). C’est-à-dire qu’il est fort possible que vos premiers pings n’aient pas de réponse ! Soyez patient !

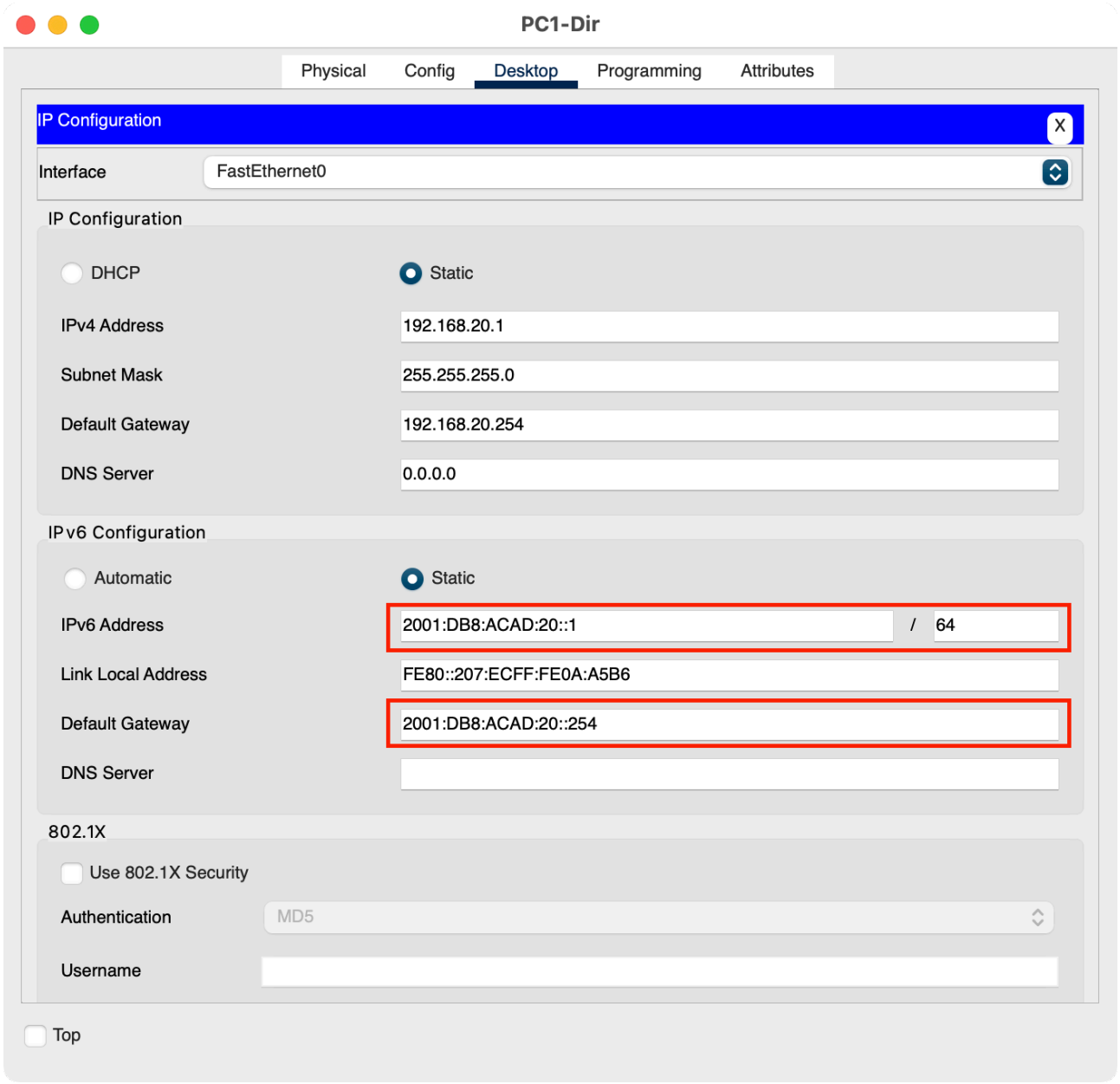
En effet, Cisco Packet Tracer simule également les protocoles réseaux pour se rapprocher au maximum du fonctionnement réel des équipements d’interconnexion !

Configurez votre réseau avec l’IPv6

Vous avez configuré tous les équipements d’interconnexion avec l’adressage IPv6, c’est super mais ce serait bien de s’en servir. Il faut donc maintenant configurer tous les périphériques finaux en utilisant le **protocole IPv6**. Il faudra donc configurer les périphériques finaux comme ceci :

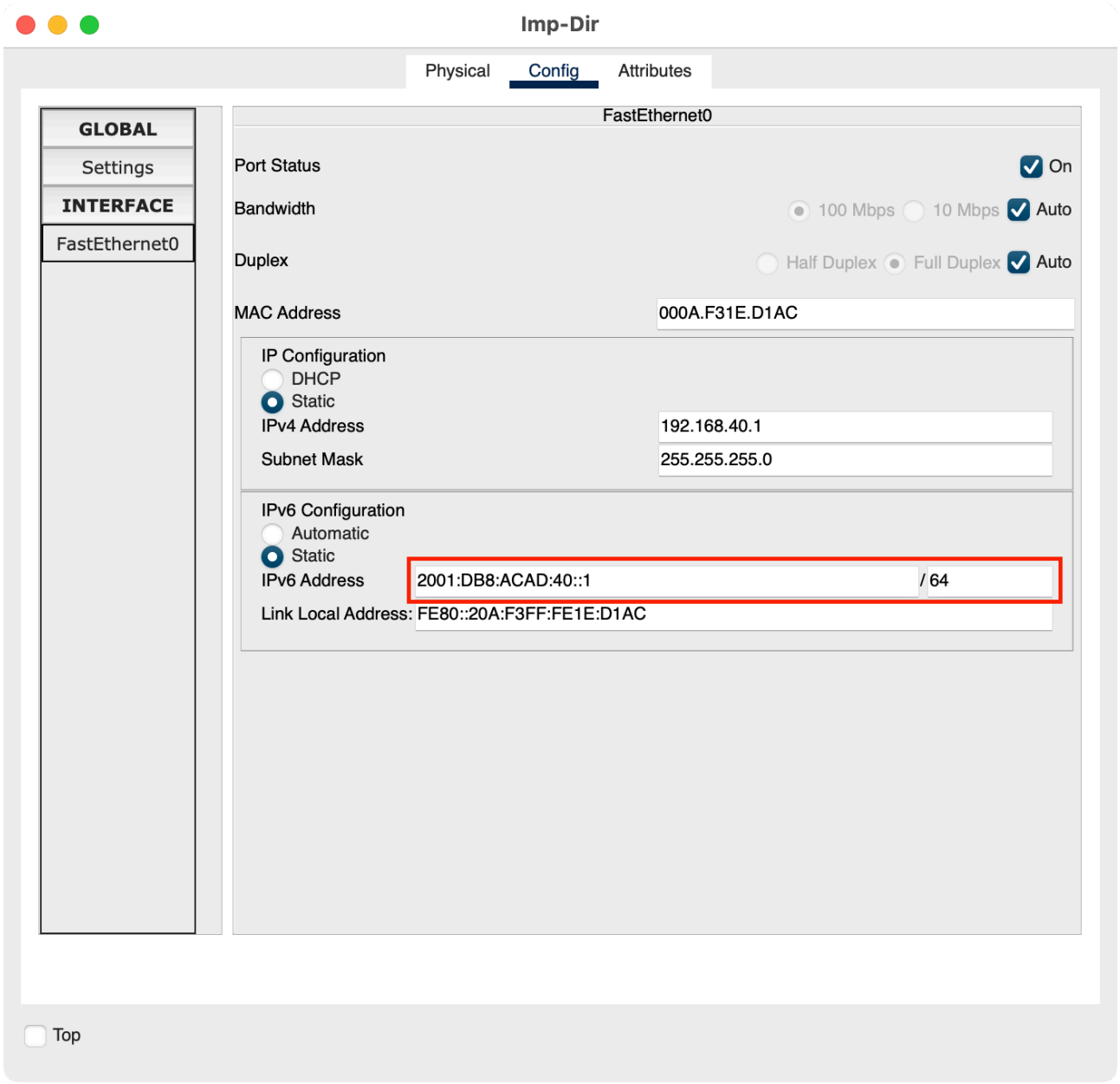
- **Adresse IPv6** : **2001:db8:acad:*Numéro_Sous_Réseau*::*NuméroPoste***.
- **Préfixe IPv6** : Cela correspond au masque de sous-réseau IPv4, vous mettrez toujours le même : **/64**.
- **Passerelle IPv6** : Cela correspond à la passerelle par défaut IPv6.

Allez, je suis gentil, je vous montre la configuration IP complète du **PC1-Dir**. Vous devriez ensuite arriver à faire tout seul cette configuration sur tous les autres postes. 😉

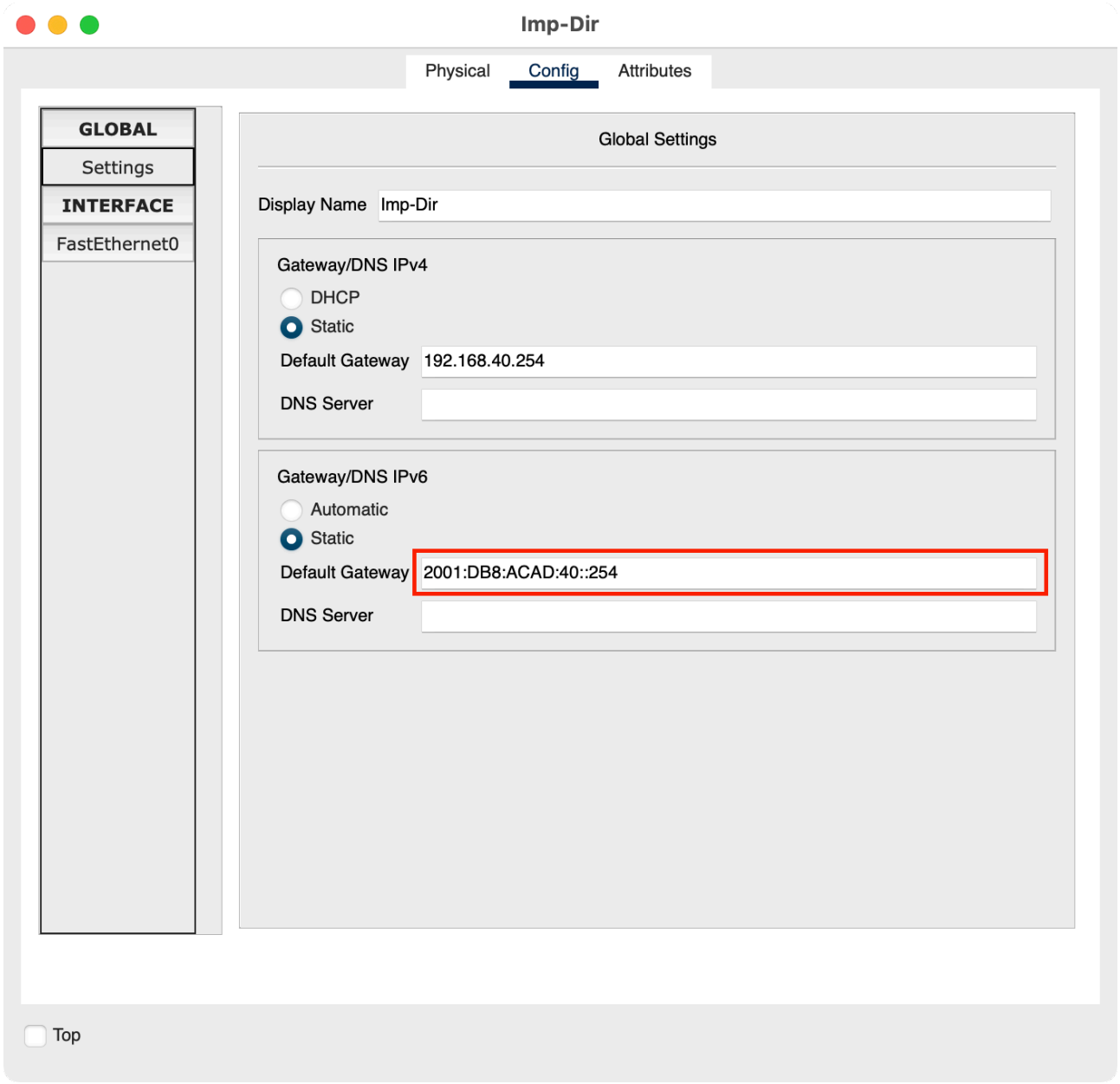


Configuration IP complète avec les paramètres IPv6 à Configurer. Ne touchez pas à l'adresse IPv6 Link Local (Link Local Address)

Pour l'imprimante **Imp-Dir**, comme pour l'**IPv4**, les configurations se réalisent dans 2 menus différents :



Configuration de l'Adresse IPv6 et du Préfixe pour une Imprimante dans Cisco Packet Tracer Menu Config → Interface → FastEthernet0



Configuration de la Passerelle par Défaut IPv6 pour une Imprimante dans Cisco Packet Tracer
Menu Config → Global → Settings
Quand vous avez réalisé les configurations de tous les postes (et de tous les périphériques finaux WiFi), de tous les serveurs et de toutes les imprimantes, vous pouvez réaliser les **tests de communication en IPv6**.

En résumé

Vous avez vu dans ce chapitre :

- Le routage inter-vlans en créant
    - des VLANs dans le commutateur de niveau 3,
    - en affectant les VLANs dans le commutateur de niveau 3,
    - en créant des liaisons Trunks et en autorisant les VLANs sur ces liaisons Trunks.

- La configuration de l’adressage IPv6 des différents postes informatiques et des différentes imprimantes (Adresses IPv6, Préfixes IPv6 et Passerelles IPv6).

Sauvegardez vos configurations

Configurez le système de fichiers du routeur

Dans un grand réseau, vous avez beaucoup d'équipements d'interconnexion et il n'est pas possible de configurer manuellement, commande par commande, ces équipements.

Heureusement, il existe plusieurs façons de **copier** ou de **mettre à jour** vos configurations. Le **Cisco IFS** (**IOS File Systems**) permet à l'administrateur de naviguer dans différents répertoires et d'établir la liste des fichiers d'un répertoire. L'administrateur peut également créer des sous-répertoires en mémoire Flash ou sur un disque.

Les répertoires disponibles dépendent du périphérique. La commande **`show file systems`** répertorie tous les systèmes de fichiers disponibles sur un routeur Cisco 1941 ou sur un commutateur de niveau 3.

```
RouteurVPN# show file systems
File Systems:

         Size(b)        Free(b)     Type  FlagsPrefixes

*     255744000      221896413      disk     rw     flash0:
flash:#
         262136         255005     nvram     rwnvram:
RouteurVPN#
```

Cette commande fournit des informations utiles telles que :

- la quantité de mémoire totale et libre ;
- le type de système de fichiers ;
- les autorisations des fichiers.

Les autorisations comprennent la lecture seule (**ro** : **read only**), l'écriture seule (**wo** : **write only**) et la lecture et l'écriture (**rw** : **read write**). Notez que l'astérisque**`*`** devant le système de fichiers **Flash** indique qu'il s'agit du système de fichiers par défaut actuel, l'IOS amorçable se trouve dans la mémoire Flash, par conséquent, le symbole**`#`**est ajouté à la liste Flash pour indiquer qu'il s'agit d'un disque amorçable.

Le système de fichiers **Flash** étant le système de fichiers utilisé par défaut, la commande**`dir`**répertorie le contenu de Flash.

```
RouteurVPN# dir
Directory of flash0:/

 3    -rw-     33591768    <no date>
c1900-universalk9-mz.SPA.151-4.M4.bin
 2    -rw-        28282    <no date>    sigdef-category.xml
```

```
 1    -rw-      227537     <no date>    sigdef-default.xml

255744000 bytes total (221896413 bytes free)
RouteurVPN#
```

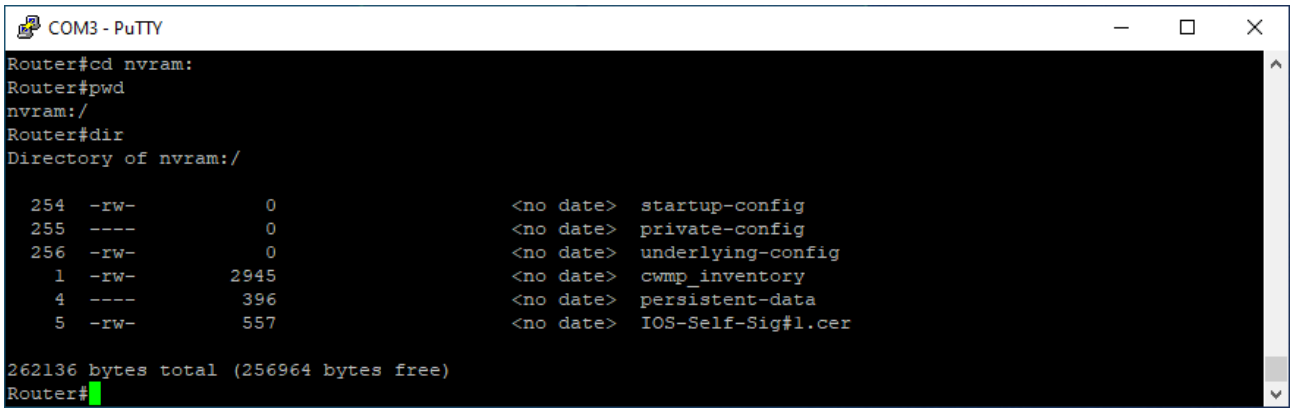
Plusieurs fichiers figurent en mémoire Flash mais seul le premier nous intéresse, il s'agit du nom de l'image en cours des fichiers Cisco IOS qui s'exécute dans la mémoire vive.

Sauvegardez dans la mémoire non volatile (NVRAM)

La mémoire non volatile (**NVRAM**) est une mémoire qui stocke les données **même lorsqu'elle n'est plus alimentée**. Pour afficher le contenu de la mémoire vive non volatile, utilisez :

- la commande**`cd`**(**change directory**), pour modifier le système de fichiers par défaut ;
- la commande**`pwd`**, pour afficher le répertoire actuel et vérifier que vous affichez le répertoire **NVRAM** ;
- la commande**`dir`**, pour afficher la liste du contenu de la mémoire non volatile NVRAM.

Parmi les différents fichiers affichés, le seul qui présente un intérêt pour nous est le fichier nommé "**startup-config**" qui définit la configuration au démarrage.



Commandes tapées sur un réel routeur Cisco 1941 avec prise en main à distance via le port console Cisco Packet Tracer ne donne malheureusement pas encore la possibilité d'utiliser ces commandes, mais elles fonctionnent sur un routeur Cisco 1941. Eh oui, c'est là que l'on touche les limites de la simulation ! 😞

Très bien, donc si vous voulez que vos configurations soient sauvegardées après le redémarrage de votre équipement réseau, vous devez les copier dans la mémoire non volatile.

Vous connaissez cette commande car vous l'avez déjà utilisée plusieurs fois :**`copy running-config startup-config`**. Il est possible de réaliser l'opération inverse si vous voulez recharger votre configuration initiale sans avoir à redémarrer l'équipement réseau :

```
RouteurVPN# copy running-config startup-config
Destination filename [startup-config]?

Building configuration...
```

```
[OK]
RouteurVPN# copy startup-config running-config
Destination filename [running-config]?

950 bytes copied in 0.416 secs (2283 bytes/sec)
RouteurVPN#
%SYS-5-CONFIG_I: Configured from console by console

RouteurVPN#
```

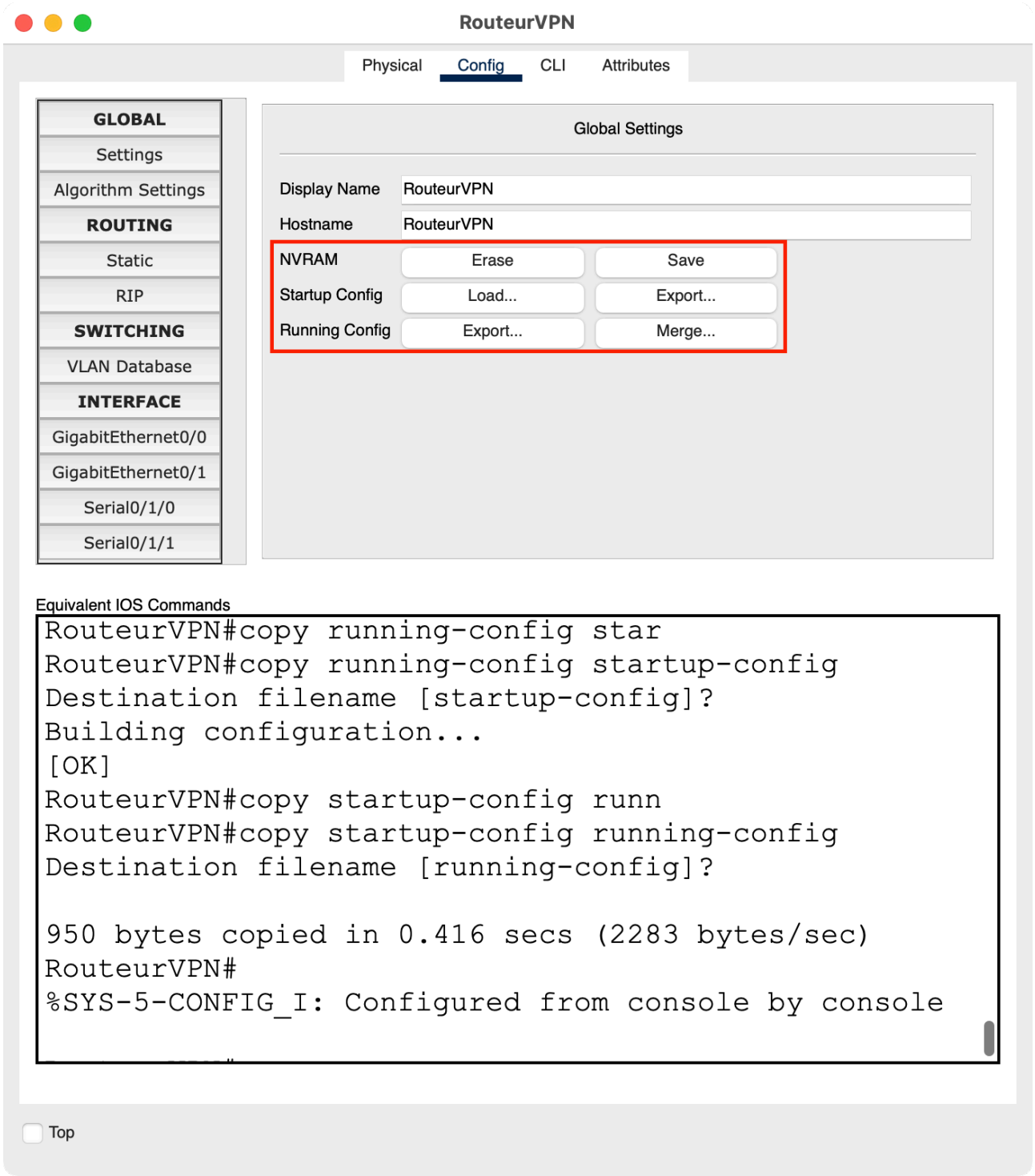
À retenir :

Running-Config : C'est la configuration que vous êtes en train de taper lorsque vous rentrez des lignes de commande, mais cette mémoire est effacée après le redémarrage du routeur.

Startup-Config : C'est la configuration qui est sauvegardée même lorsque le routeur est éteint ; cette configuration "écrase" la running-config après le redémarrage de l'équipement réseau.

Sauvegardez vos configurations dans Cisco Packet Tracer

Il est possible de **sauvegarder** et de **restaurer** vos configurations dans Cisco Packet Tracer. Il suffit d'aller dans l'équipement d'interconnexion et de choisir le menu **Config**.

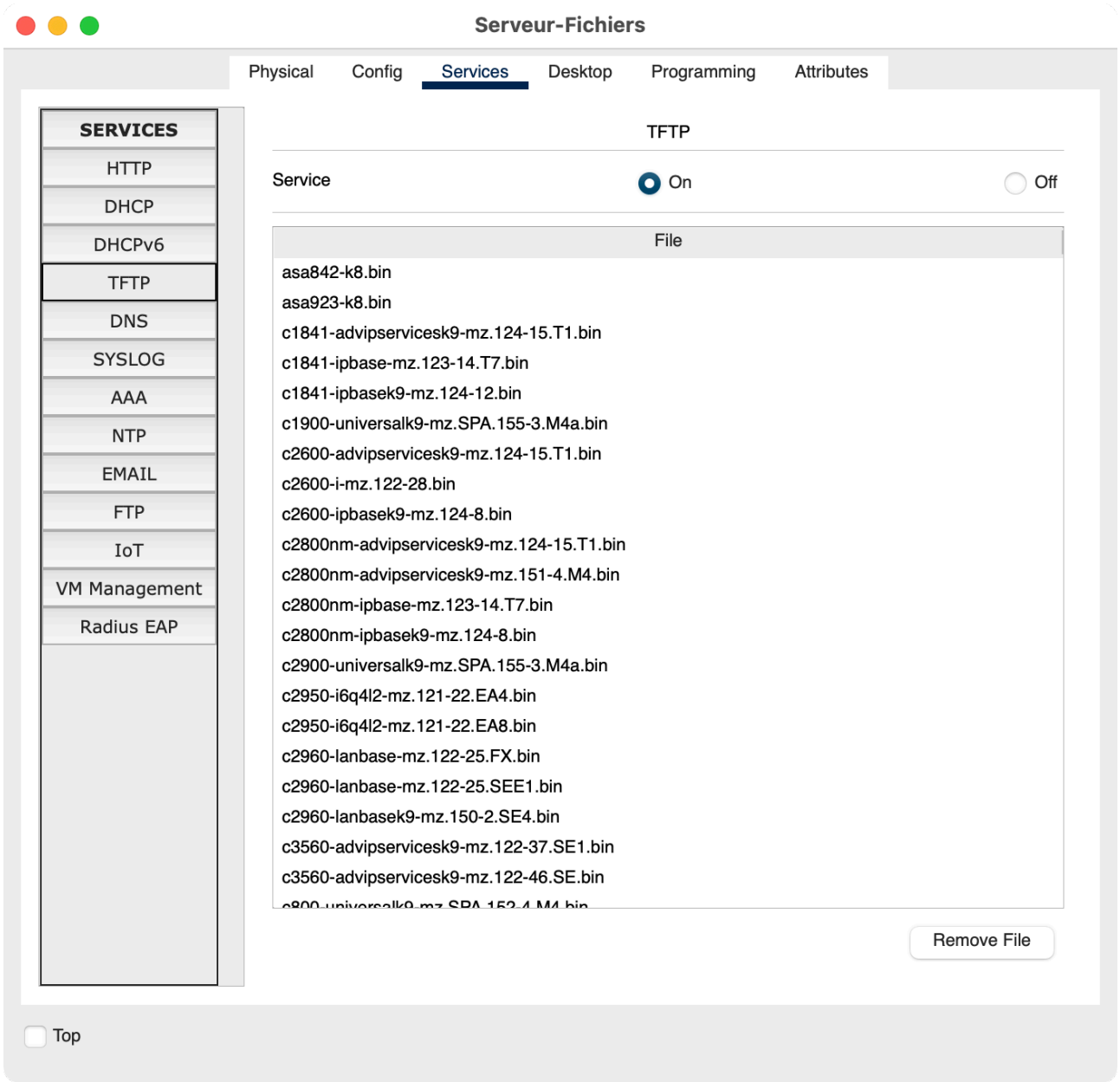


Le menu Config permet de tout sauvegarder et restaurer : NVRAM, Startup Config et Running Config 😋
Si vous avez suivi le cours “Concevez votre réseau TCP-IP”, vous avez utilisé ce menu car il vous permet aussi de configurer vos équipements réseau de manière très intuitive. Il faut le voir comme un assistant de configuration.

Bon maintenant, vous êtes grand, vous n’avez plus besoin de ce menu (sauf pour sauvegarder vos configurations 😉) mais il est intéressant de voir que lorsque vous utilisez les fonctions de cet assistant, les commandes équivalentes s’affichent dans la fenêtre, pratique pour apprendre les commandes Cisco IOS 😜 !

Sauvegardez vos configurations sur un serveur TFTP

Il est également possible de **sauvegarder** et de **restaurer** vos configurations en utilisant un serveur **TFTP**. Cela tombe bien, il existe ce service dans Cisco Packet Tracer !



Le service TFTP dans Cisco Packet Tracer. Magique, ce service est déjà activé !
Pour **copier** vos configurations vers un **serveur TFTP**, utilisez la commande**`copy running-config tftp`**et spécifiez l'adresse IP du serveur :

```
RouteurVPN# copy running-config tftp
Address or name of remote host []? 192.168.30.3
Destination filename [RouteurVPN-confg]?

Writing running-config.....!!
[OK - 950 bytes]

950 bytes copied in 7.047 secs (134 bytes/sec)
```

```
RouteurVPN#
```

Il est possible bien évidemment d'échanger des données entre le serveur TFTP et la mémoire non volatile (**startup-config**) !

Il suffit de taper la commande**`copy tftp running-config`**pour **restaurer** la configuration sur la mémoire en cours d'utilisation (**running-config**) depuis un **serveur TFTP** :

```
RouteurVPN# copy tftp running-config
Address or name of remote host []? 192.168.30.3
Source filename []? RouteurVPN-confg
Destination filename [running-config]?

Accessing tftp://192.168.30.3/RouteurVPN-confg...
Loading RouteurVPN-confg from 192.168.30.3: !
[OK - 950 bytes]

950 bytes copied in 0 secs
RouteurVPN#
```

En résumé

Vous avez vu dans ce chapitre :

- Le système de fichiers d'un routeur avec la commande `show file systems` qui permet d'afficher les différents systèmes de fichiers.
- La sauvegarde de vos configurations dans la mémoire non volatile avec la commande `copy running-config startup-config` .
- La sauvegarde de vos configurations dans Cisco Packet Tracer avec le menu Config des différents équipements d'interconnexion.
- La sauvegarde de vos configurations dans un serveur TFTP avec la commande `running-config startup-config` .

Vous êtes arrivé au bout de ce cours et félicitations à vous, vous venez de franchir un pas dans le vaste monde des réseaux. Cisco Packet Tracer est un outil formidable pour apprendre le fonctionnement des réseaux, mais surtout pour simuler des réseaux d'entreprise afin de configurer des équipements d'interconnexion.