Echange de Données de Surveillance

Support de Formation
TCP/IP

Application au routeur Mikrotik

Janvier 2020
Niamey, Niger

Programme

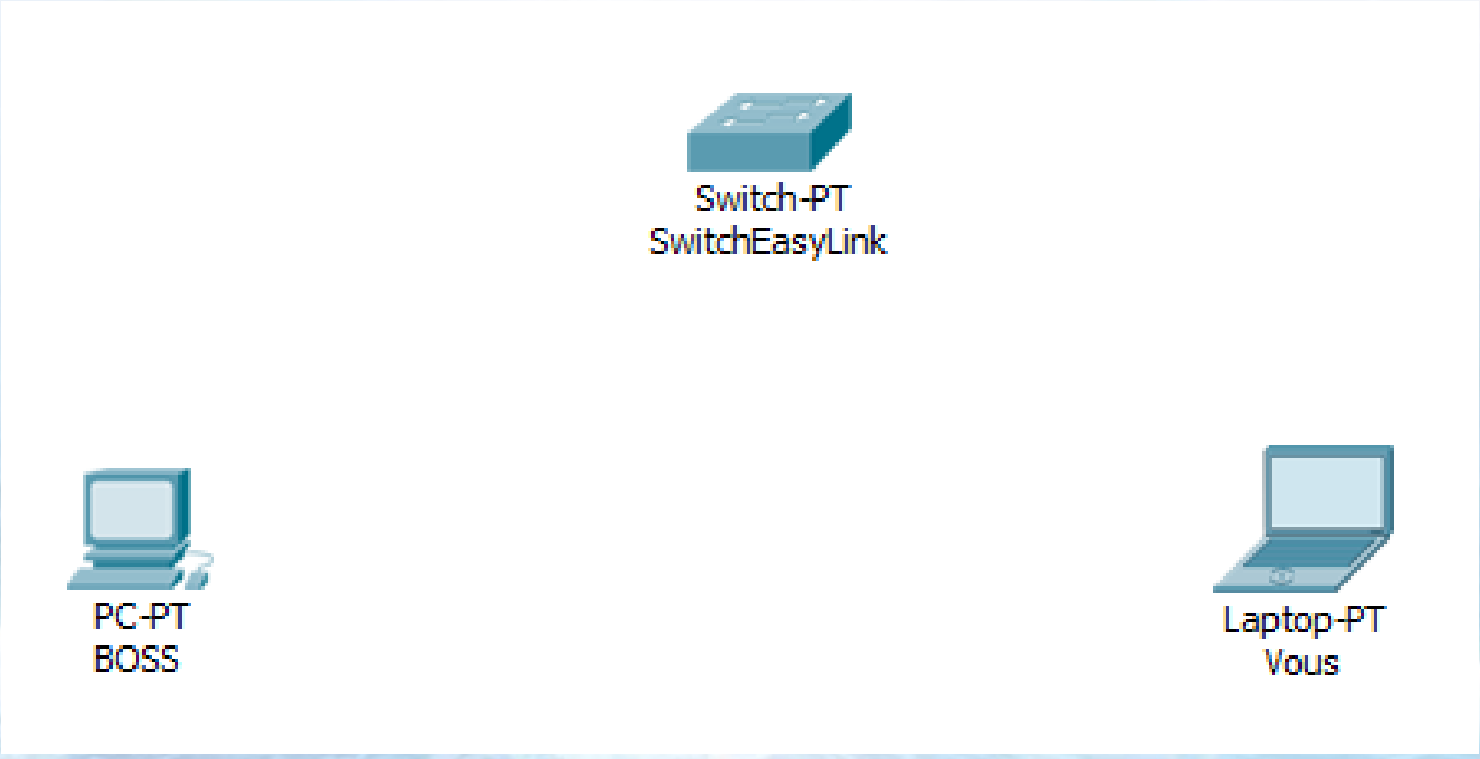
- Nous allons ici faire quelques exercices permettant de rappeler quelques notions importantes du protocole TCP/IP qui nous serviront dans la suite
- A l'issue de ces rappels, les notions d'adresses réseaux, de masque de sous réseaux, de VLAN et de routage statique auront été vues, l'idée est d'y revenir autant de fois que nécessaire
- Après une mise en application de ces notions nous augmenterons la complexité en abordant la notion de bridge, le transfert de flux multicast ainsi que le routage dynamique via RIP et OSPF

Les couches OSI qui nous intéressent

- Dans notre cas, seulement les 3 premières couches OSI nous intéressent:
  - La couche 1: La couche PHYSIQUE
    - Les câbles de transmission (ETH, Fibre, ligne téléphonique, coax, etc)
    - C'est la couche à vérifier en PREMIER
  - La couche 2: La couche LIAISON
    - Les machines présentes sur votre réseau
    - Les Switchs
    - Les Hub si vous en avez encore
    - Pour vérifier cette couche on procède généralement par un PING
  - La couche 3: La couche RESEAU
    - Un routeur
    - Un firewall
    - Un modem de FAI (qui est ni plus ni moins qu'un routeur)
    - Pour vérifier la couche 3, on procède généralement par un PING éventuellement suivi d'un trace route pour connaitre le chemin vers notre destination

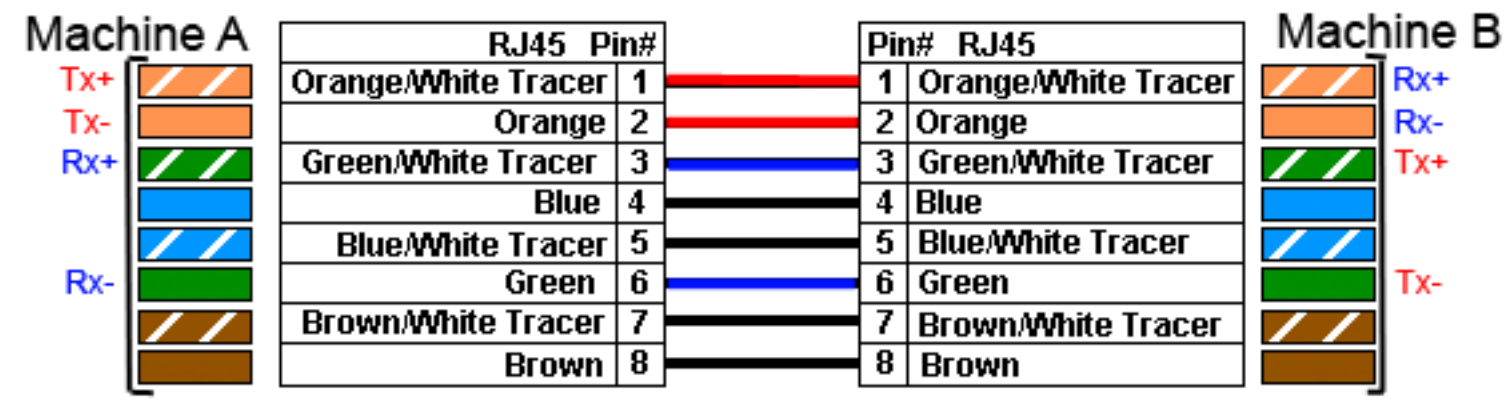
Partie 1: l’adressage réseau

- Mise en situation :



Première étape: la couche PHYSIQUE

- Ici il nous manque juste des câbles
- Nous allons utiliser des câbles FTP :



- Il y a plusieurs normes: la T568A et la T568B => couleurs différentes
- Dans tous les cas une paire TX et une paire RX

Câbles croisés ou droits?

- Il y eu une époque où le sens de transmission réception était figé sur les cartes réseaux. Donc certains vieux équipements fonctionnent toujours comme cela.
- Vérifier les datasheets en cas de problème, encore une fois la couche physique est à vérifier en premier.
- Attention: Un câble FTP CAT.5 raccordé par deux connecteurs RJ45 n'est pas forcément un câble Ethernet, c'est un câble qui peut faire transiter tout type de signaux et même du courant parfois (Power Over Ethernet).
- Ainsi il ne faut pas se fier aux apparences, un câble est juste un moyen de connecter deux appareils, ensuite le protocole de communication dépend des appareils en question.

Connexion d’un équipement à un switch

- Lors de la connexion d’un équipement à un switch:
  - Une négociation a lieu entre les deux équipement (LED orange puis verte dès que c’est terminé)
- Que se passe-t-il dans le switch à ce moment là :
  - Détection activité électrique
  - Initiation de dialogue
  - Négociation
  - Etablissement de la communication
  - Lien associé à l’adresse MAC de la machine

Première notion d'adresse: l'adresse MAC

- C'est une adresse unique associée à une machine
- Un PC en a une, un switch, un routeur, votre téléphone, etc
- Elle est unique
- Modifier son adresse MAC est possible et nécessaire pour certaines applications, cela ne nous concerne pas ici
- L'adresse MAC est généralement présentée en hexadécimal sous cette forme : XX:XX:XX:XX:XX:XX, sur 6 octets
- Certaines adresses sont réservées pour certaines marques, certains protocoles,…

Premier Bilan

- Tout semble réuni pour pouvoir communiquer:
  - Un média (Les câbles et le commutateur)
  - Des adresses (MAC)
- Il nous manque néanmoins un protocole de communication
  - Ce protocole sera le protocole TCP/IP
- Ce protocole aura besoin d'autres adresses pour fonctionner:
  - Les fameuses Adresses IP

Seconde notion d'adresses: L'adresse IP

- Une adresse IP est composée de deux choses:
  - Une adresse sur 4 octets
  - Un masque sur 4 octets également
- Représentation en binaire d'une l'adresse et d'un masque:
  - @host: 10000000.00001000.01000010.10000010
  - Mask: 11111111.11111111.11111110.00000000
- Et en décimal ça donne quoi ?

Conversion Décimal/Binaire

- Tableau de conversion décimal binaire:

Poids	128	64	32	16	8	4	2	1
Nombre Binaire	0	0	1	0	1	1	1	0
Conversion	0	0	32	0	8	4	2	0
Somme	46							

Poids	128	64	32	16	8	4	2	1
Nombre Binaire	1	1	1	1	1	1	1	1
Conversion	128	64	32	16	8	4	2	1
Somme	255							

- Sur Excel existe les fonctions DECBIN et BINDEC pour les conversions

Qu’est-ce qu’un masque ?

- Nous l’avons vu, un masque a la même forme qu’une adresse
- Un masque sert à déterminer le sous réseau dans lequel la machine se trouve
- L’apprentissage par l’exemple, reprenons notre adresse du début:
  - @host: 10000000.00001000.01000010.10000010
  - soit 128.8.66.130 en binaire
  - Mask: 11111111.11111111.11111110.00000000
  - soit 255.255.254.0 en binaire
- Quel est le sous réseau auquel cette adresse IP appartient ?

Adresse ET Masque = Sous Réseau

- Règles du ET logique :
  - 0 et 0 = 0
  - 0 et 1 = 0
  - 1 et 1 = 1

	128	64	32	16	8	4	2	1
Adresse	1	1	1	1	0	1	0	1
Masque	1	1	1	1	1	1	1	0
Sous réseau	1	1	1	1	0	1	0	0
Consersion	128	64	32	16	0	4	0	0
Somme	244							

- Ainsi dans notre exemple, nous aurons pour sous réseau ?

Autre représentation

- Nous avons le sous réseau suivant:
  - 128.8.66.0/23
  - /23 ???
- L'homme est généralement flémard, donc il cherche par tous les moyens à se simplifier la vie.
- Les masques sont limités à des 1 contigus, ainsi nous ne pouvons pas avoir 10101100 comme masque. Les masques sont de cette forme 11110000, ou 10000000. C'est-à-dire qu'à gauche d'un bit à 1 il ne peut y avoir que des 1.
- On parle de bits significatifs. Si l'on a un masque du type 255.255.255.0, en convertissant en binaire on s'aperçois que 24 bits sont à 1. On a donc décidé de le représenter /24
- Dans notre exemple nous avons 23 bits significatifs, donc /23.

Dimensionnement du réseau

- Grâce au sous réseau nous pouvons
  - Calculer le nombre de machines que le sous réseau pourra accueillir
  - Déterminer l'adresse de broadcast
- Autrement dit nous sommes capables de dimensionner notre réseau!
- Reprenons notre exemple parce qu'on l'aime bien quand même:
  - 128.8.66.0/23
- Notre première adresse possible sera: 128.8.66.1/23, facile
- Notre dernière adresse possible sera: 128.8.67.255/23,
  - hummmm, ok pourquoi??

Dernière adresse ?

- Pour déterminer la dernière adresse possible on reprend le binaire, super!

Poids	128	64	32	16	8	4	2	1
Adresse	0	1	0	0	0	0	1	0
Masque	1	1	1	1	1	1	1	0
Masque\	0	0	0	0	0	0	0	1
Last Adresse	0	1	0	0	0	0	1	1
Consersion	0	64	0	0	0	0	2	1
Somme	67							

- Opération logique inverse : X = 0 => X\ = 1 et vise versa
- Pour avoir la dernière adresse, on inverse le masque et l'on fait un OU logique avec l'adresse.
- Cette adresse sera l'adresse de broadcast du sous réseau considéré

L’adresse de broadcast

- To Broadcast signifie diffuser en bon français
- Ainsi un adresse de broadcast a été définie comme la dernière adresse de chaque sous réseau afin de permettre la diffusion de messages à toutes les machines présentes dans ce sous réseau.
- Cela peut être intéressant pour tous les messages utiles au réseaux, mais aussi pour certaines applications qui souhaitent diffuser des informations à plusieurs destinataires
- Un streaming vidéo n’est ni plus ni moins qu’un broadcast limité aux personnes visionnant la vidéo, ce que l’on appelle du multicast
- Un multicast ne s’adresse que aux personnes qui s’abonnent alors que le broadcast est général

En résumé

- Une adresse IP est composée d'une adresse ET d'un masque
- Le masque nous permet de déterminer le sous réseau et le nombre de d'adresses possible dans mon sous réseau
- Au sein de ces adresses, une adresse, la première, est celle du sous réseau et la dernière est celle du broadcast.
- En conclusion, grâce à ce sous réseau nous pouvons calculer le nombre de machines administrables au sein de notre sous réseau.
- Allez y!

Exercice de dimensionnement

- L'ASECNA va inaugurer un nouveau bâtiment aux Almadies
- Dans ce bâtiment 1000 personnes vont travailler et seront équipées d'un PC
- Globalement 1200 équipements seront à connecter en réseau local

  - Quel masque proposez vous et pourquoi ?
  - Proposez un sous réseau et donnez :
    - La première adresse utilisable
    - La dernière adresse utilisable
    - Le nombre de machines administrables
    - L'adresse de broadcast

Avez-vous des questions ?

Que se passe-t-il dans un switch ?

- Dès que l'on donne une adresse IP à notre PC, il mettra son adresse dans son entête de message, message que l'on appellera maintenant: trame Ethernet
- En plus de la sienne il va indiquer aussi à qui il souhaite l'envoyer, l'adresse du destinataire. C'est mieux d'écrire l'adresse quand on souhaite envoyer un message!
- Ainsi le switch reçoit la trame Ethernet et la décortique pour déterminer les adresses source et destination
- Il envoie alors une requête dite requête ARP. En langage humain c'est « Bonjour à tous, qui a l'adresse X.X.X.X ?
- Dans « Bonjour à tous », si on écoute bien on entend « Broadcast », si, si je vous assure, écoutez mieux
- Ainsi le switch envoie sur l'adresse de broadcast sa requête et s'il y a quelqu'un qui répond alors le switch enregistre que l'adresse MAC sur son lien X possède l'adresse IP Y. Et il met ça dans une table que l'on appelle donc, la table ARP!

Intérêt de la table ARP

- La Table ARP permet au switch d'aller plus vite pour la prochaine conversation
- En effet il n'enverra pas de nouvelle requête ARP, en tout cas pas tout de suite
- La table ARP est mise à jour régulièrement
- Le paramètre de mise à jour est paramétrable
- Parfois ce mécanisme buggue et pour mettre à jour la table ARP il est nécessaire de passer par un reboot
- Cette table ARP devient intéressante dans les configurations redondées pour lesquelles l'adresse IP est partagée par deux équipements dont un est actif et l'autre en backup.

Est-ce que l'on peut voir tout ça?

- La réponse est oui!
- Et ce n'est pas aussi simple que cela en a l'air
- Dans un petit réseau il est assez simple de s'y retrouver si l'on sait ce que l'on cherche
- Mais dans un réseau compliqué, avec de la redondance dans tous les sens, cela devient rapidement très complexe
- Un des outils utilisé pour sniffer un réseau est WIRESHARK
- Je suis loin, très loin d'être un expert WIRESHARK, mais encore une fois le principal est de savoir de quoi l'on parle et ce que l'on cherche. Vu qu'en général, c'est vous qui avez créé le réseau, les paramètres se limitent d'eux mêmes
- Par exemple si l'on recherche un ping on pourra filtrer sur le protocole ICMP

Adresses particulières

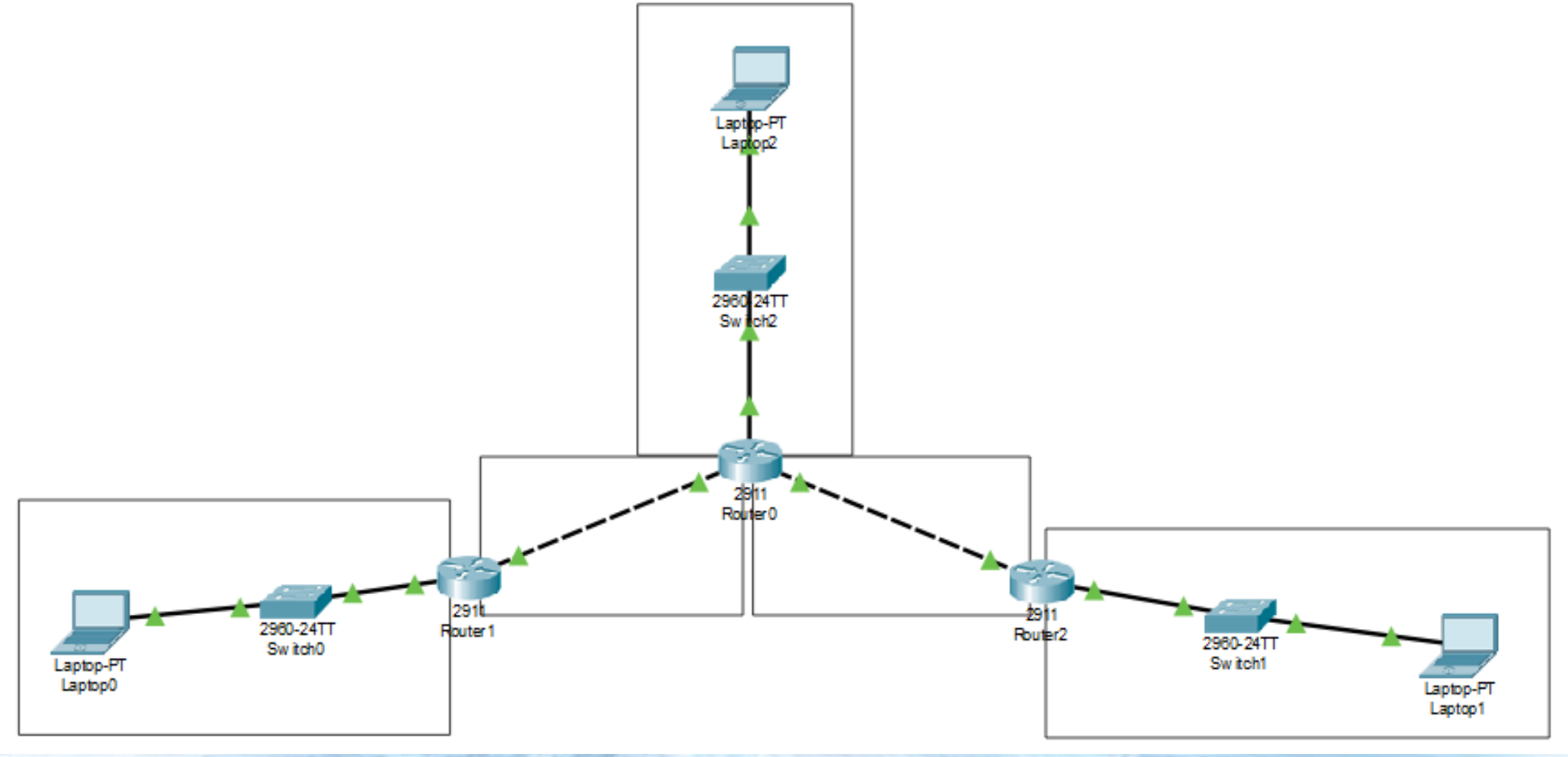
- Certaines adresses sont réservées, vous les trouverez sur internet sans problème
- Celles qui nous intéressent sont les adresses réservées aux réseaux privés:
  - 10.0.0.0/8 => plus de 16 millions d'adresses possibles
  - 172.16.0.0/12 => plus d'un million
  - 192.168.0.0/16 => plus de 65 000
- Ce sont des adresses non routables sur internet
- Nous administrerons tous nos réseaux dans ces plages d'adresses
- Par voie de conséquence, pour naviguer sur internet nous avons besoin d'une adresse publique

Passage au routage

- Tout ce que nous venons de voir s'intéresse au Niveau 2
- Passons la tête au niveau 3 pour voir
- Ainsi donc nous allons parler de routage, statique pour commencer

- Le mieux est de travailler sur un exemple:

Exercice de routage statique



Exercice de routage statique

- Exemple avec une topologie en étoile:
  - Réseau du site HUB: 10.220.0.0/16
  - Réseau du site 1: 10.221.0.0/16
  - Réseau du site 2: 10.222.0.0/16
  - Réseau du site X: 10.22X.0.0/16
- Proposez une architecture pour que les PC puissent communiquer avec le site central
- Que doit-on ajouter pour que tous les PC puissent communiquer ?

Notion utilisée: La passerelle

- Analogie avec les déplacements:
  - Je suis dans mon quartier, je peux y marcher sans problème
  - Si je souhaite aller dans le quartier adjacent séparé de mon quartier par une voie rapide j'ai besoin d'un outil pour traverser
  - Cet outil est une passerelle
- C'est la même chose en réseau, pour pouvoir aller au-delà de mon sous réseau j'ai besoin d'une passerelle
- Et comment ça marche ?

Notion de Route Statique

- Une Route déjà est un chemin qui permet d'aller quelque part: encore une analogie au déplacement !
- Une route statique est un chemin fixe qui permet d'aller vers cette destination, il n'y a pas d'autre chemin connu pour y aller
- Ainsi, si la route est coupée, je ne peux plus y aller
- Une route coupée et une route qui n'existe pas c'est la même chose en réseau, on ne peux pas passer par la jungle, il faut une route
- Exemple: Pour aller à Paris en avion depuis Dakar je sais que je dois passer par l'aéroport.
- En réseau cela revient à écrire une route statique qui dit que pour atteindre Paris, je dois d'abord atteindre l'aéroport qui est accessible

Notion de route statique

- Ecriture de la route statique dans le cas où nous voudrions atteindre le sous réseau X.Y.Z.0/24 via notre routeur:
  - static route add X.Y.Z.0/24 @passerelle

- Nous précisons donc d'abord le sous réseau visé et ensuite la porte d'accès
- Notre PC a une passerelle de renseignée, cette passerelle se traduit par la commande suivante:
  - static route add 0.0.0.0/0 @passerelle
- C'est une route par défaut, tout ce qui a pour destination autre chose que mon réseau sera envoyé à ma passerelle

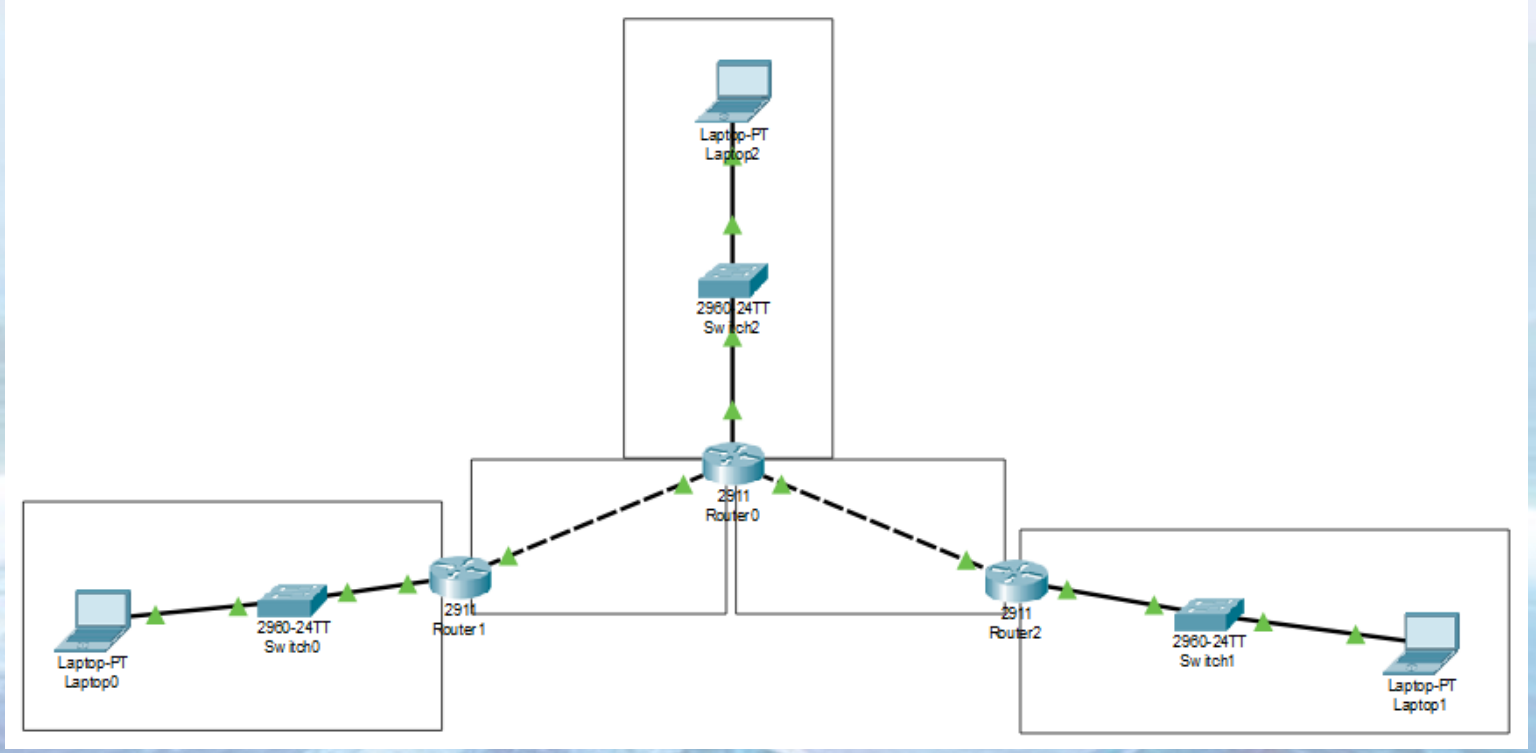
Avez-vous des questions ?

Routeurs Mikrotik

- Les routeurs Mikrotik, comme vous allez le constater, sont des routeurs assez intuitifs et simples de configuration
- Ils ont l'avantage de pouvoir être mis à jour gratuitement
- Ils offrent également la possibilité d'installer des fonctionnalités en fonction du besoin final (exemple avec le PIM) sans avoir besoin d'acheter de licence
- Important: une aide complète est disponible en ligne pour aider à la configuration du routeur, des exemples sont également proposés
- Les routeurs Mikrotik peuvent également réaliser des fonctions de firewall

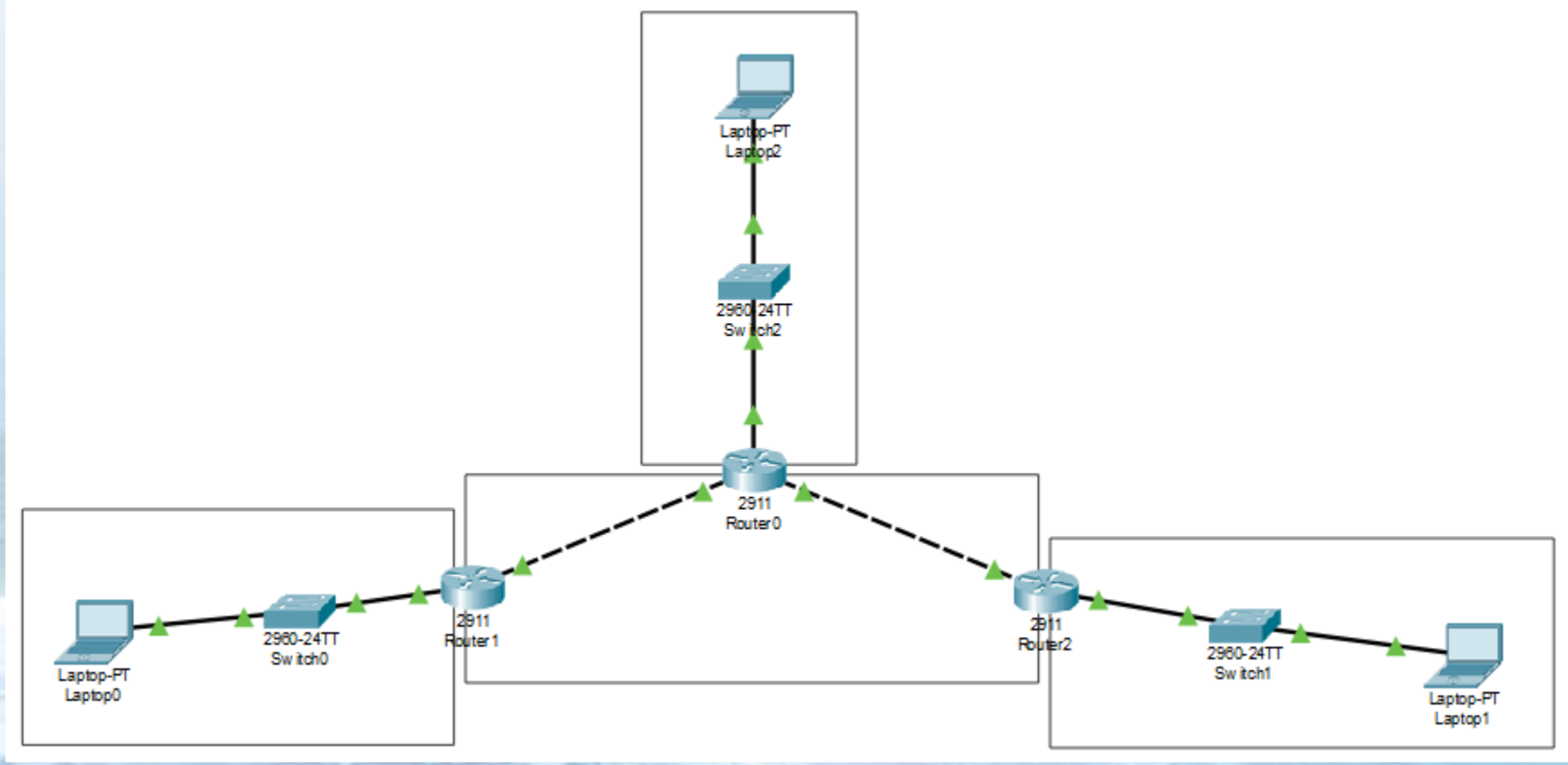
Mise en pratique

- Il est grand temps de pratiquer et d'appliquer les notions déjà vues
- Nous avons 5 routeurs à disposition, l'idée est, dans un premier temps, de créer le réseau de notre exercice appliqué à 5 sites :



Mise en pratique

- Léger changement: comment faire pour réaliser cette configuration ?



Notion de bridge

- Un routeur ne peut pas avoir deux interfaces configurées dans le même sous réseau
- Pour pouvoir profiter des avantages du niveau 2, il est nécessaire de créer ce que l'on appelle un bridge
- Le bridge est une association d'interfaces que l'on va regrouper dans un même sous réseau
- Ainsi, dans notre exemple l'idée est que la « transmission » se fasse dans le sous réseau 192.168.10.0/28
- Allez y!

Transfert de flux unicast

- Avec notre réseau routé ainsi constitué, nous sommes capable de faire transiter des flux unicast entre les différents sites
- Les données de surveillances sont généralement des flux multicast
- Les flux multicasts fonctionnent avec :
  - Un serveur Multicast
  - Des abonnés au serveur Multicast
- Or le multicast nativement est bloqué par les routeurs afin de limiter la propagation de messages inutiles et ainsi sauver de la bande passante pour les données utiles

Transferts de flux multicast

- S'il l'on souhaite faire transiter des flux multicast via un réseau routé il faut alors utiliser un protocole de routage multicast
- Ici encore plusieurs solutions existent
- Nous choisirons le PIM pour Protocol Independent Multicast
- Comme son nom l'indique, il est indépendant des protocoles de routage utilisés dans le réseau, il est donc utilisable partout à condition que les routeurs soient compatibles au PIM

Transferts de flux multicast

- Encore une fois ce protocole fonctionne grâce à la coopération des routeurs de proche en proche
- PIM fonctionne avec la déclaration d'interfaces PIM sur des adresses de flux multicast et à l'envoi de requête d'abonnement aux flux multicast
- Le PIM est indépendant du protocole de routage utilisé pour la transmission des informations
- Pour éviter une charge réseau inutile, un routeur est désigné pour recevoir les requêtes IGMP et les envoyer aux serveurs multicast correspondant, ce routeur doit donc être joignable par tous les routeurs participant au PIM
- Ce routeur est nommé le Rendez-Vous Point
- Nous allons mettre en place un transfert de flux multicast au sein de notre réseau

Avez-vous des questions ?

Un peu de dynamisme maintenant ?

Avant d'aller plus loin

- Avec ces notions vous êtes armés pour administrer le réseau d'échange de données de surveillance
- Ce qu'il y a de bien avec l'IP c'est que plein de choses peuvent se trouver sur Internet
- Regardez du côté de l'aide en ligne des Mikrotik qui est très bien faite mais également du côté de la communauté CISCO
- L'idée étant, comme cela a été réalisé dans cette formation, de connaitre les notions pour pouvoir ensuite les appliquer sur n'importe quel routeur
- Important: Lorsque vous administrez un réseau, tentez le plus possible d'utiliser des protocoles standardisés, cela permet ensuite d'avoir un réseau compatible avec d'autres équipements. Sachant que la technologie évolue très vite, cela permet de rallonger la durée de vie du réseau en utilisant des équipements COTS

Pour aller plus loin…

- Nous allons maintenant sortir de notre zone de confort et aller voir du côté des protocoles dynamiques

Le DHCP c’est quoi ?

- Un serveur DHCP permet de configurer automatiquement l’adresse et potentiellement la passerelle des machines clientes du DHCP
- Cela permet par exemple d’éviter les conflits d’adresses IP mais ce n’est pas toujours intéressant
- Une configuration statique sans route par défaut est tout à fait acceptable dans un petit réseau
- Pour configurer un serveur DHCP, il faudra déterminer les interfaces impactées, et la plage d’adresses voulues

Introduction au routage dynamique

- Lorsque nos architectures deviennent complexes il devient nécessaire de fonctionner en dynamique, notamment en topologie maillée
- Nous passons alors sur du routage dynamique qui permet
  - De la redondance en cas de perte d'un nœud dans le réseau
  - De configurer le réseau plus rapidement et avec moins de source d'erreur qu'en statique (si l'on oublie une route par exemple)
- Les protocoles que nous allons voir sont RIP et OSPF

Protocole RIP

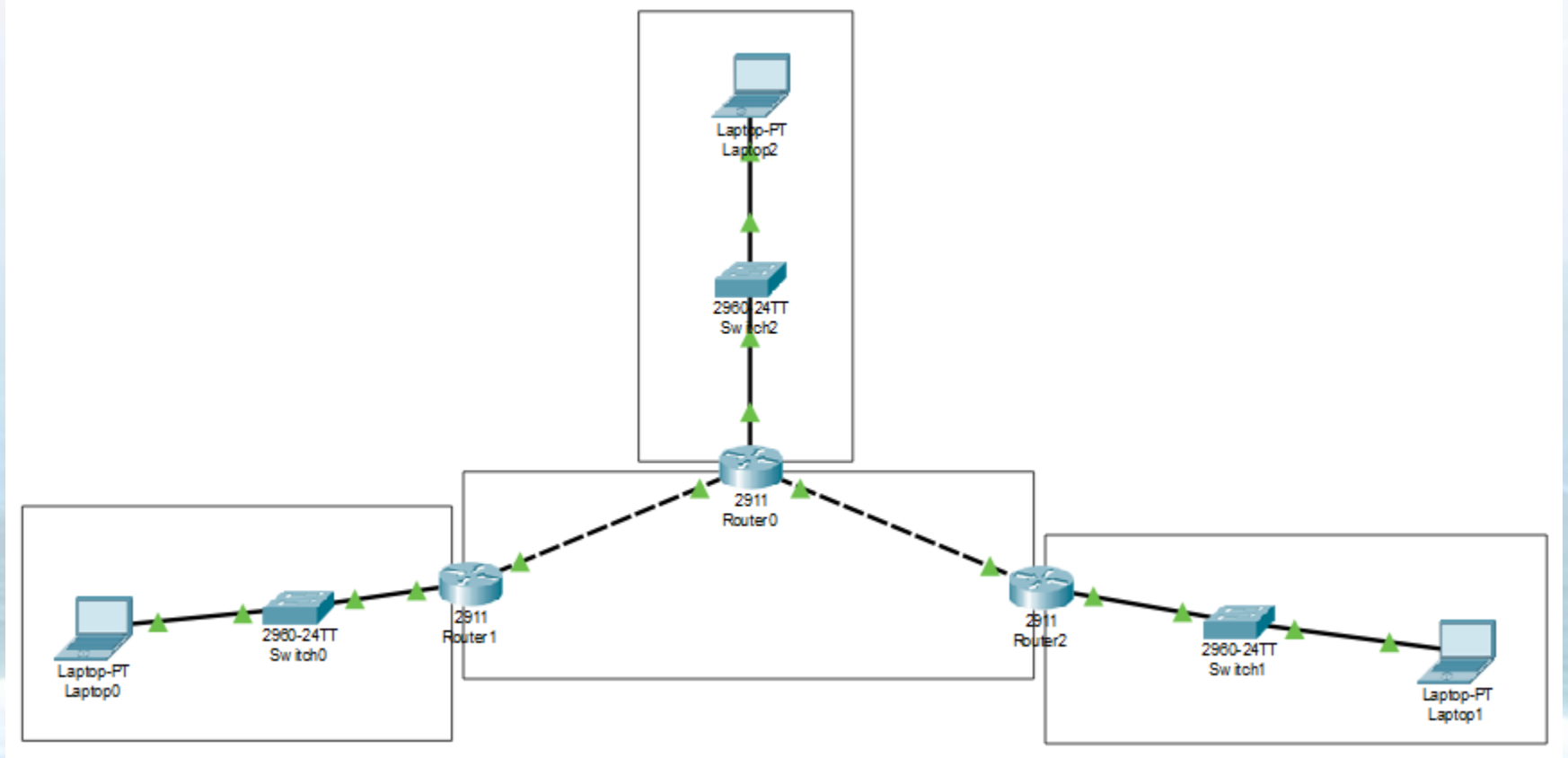
- RIP est le premier protocole inventé pour le routage dynamique
- Il n'est plus beaucoup utilisé mais il est une bonne porte d'entrée au routage dynamique
- Le principe de RIP est de faire collaborer les routeurs au sein du réseau, c'est-à-dire que chaque routeur déclaré RIP va indiquer sa table de routage à ses voisins
- Ainsi chaque routeur aura une vision de l'ensemble des réseaux joignables via ses voisins
- Une notion de poids est appliquée en fonction du nombre de sauts à réaliser pour atteindre une destination, les routes de faible poids seront utilisées en priorité
- Si une route n'est plus utilisable suite à la perte d'une interface par exemple, la seconde route la plus courte sera utilisée (si elle existe)

Protocole RIP

- Nous allons mettre en place le protocole RIP sur notre plateforme
- Avant cela il est donc nécessaire de supprimer les routes statiques que nous avions configuré

- Il va donc falloir déclarer le protocole et ensuite référencer dans chaque routeur les réseaux qui sont directement atteignables
- Ainsi, dans notre cas, les réseaux qui vont être indiqué dans chaque routeur seront :
  - Le réseau local d'une part
  - Et le réseau de transmission d'autre part
- Une fois la connexion réalisée, chaque routeur va partager sa table de routage et ainsi permettre l'interconnexion des réseaux

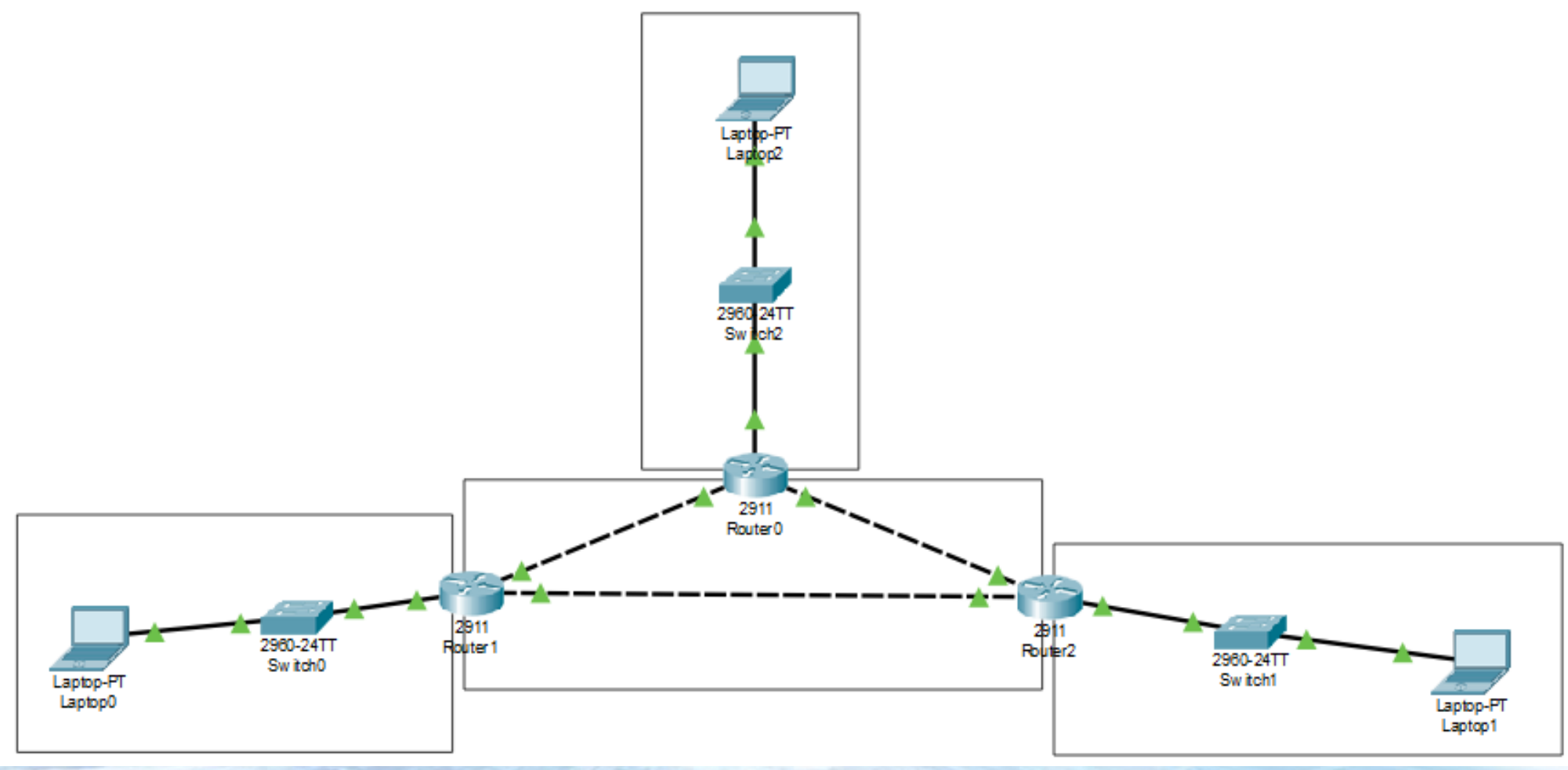
Application RIP



Protocole RIP

- Nous voyons ici que la configuration est plus rapide
- Au vue de notre topologie, l'intérêt s'arrête là
- L'idée est maintenant de mettre en place un réseau maillé
- C'est-à-dire que les sites déportés seront également connectés les uns aux autres

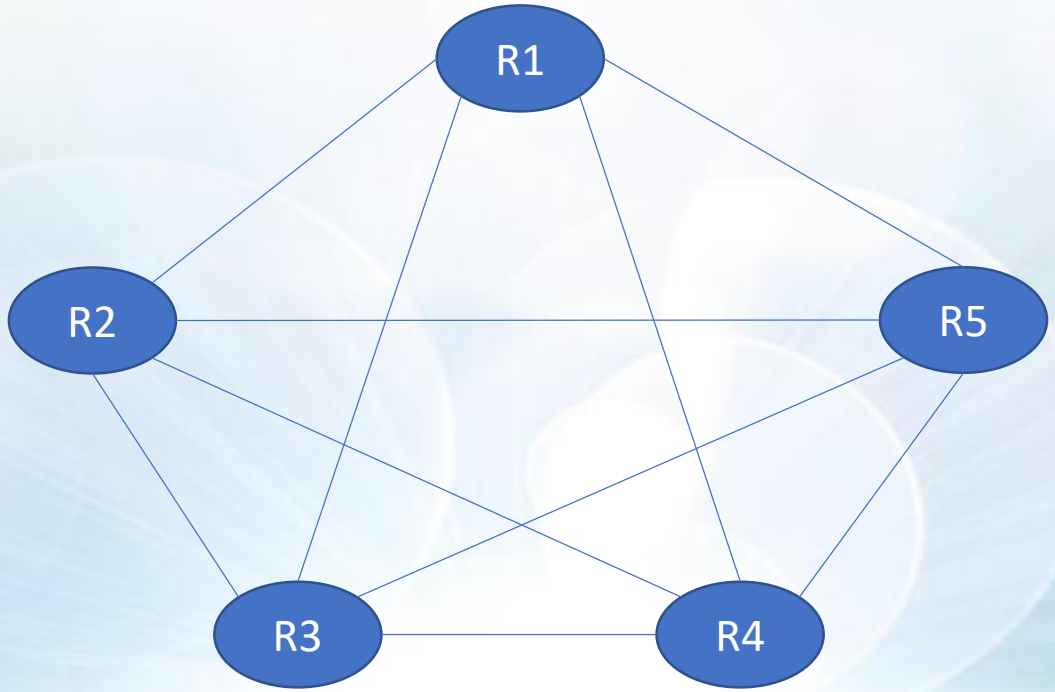
Application RIP



Application RIP

- Après avoir fait toutes les configurations nécessaires au changement de topologie, l'idée est de faire des tests de coupure de lien (comme si une liaison satellite était tombée par exemple
- Est-ce que nous avons bien une redondance des communications?
- Quel est le principal paramètre qui varie en cas de coupure?
- Avons-nous une perte de trafic à la coupure du lien ?
- Existe-t-il des protocole de redondance permettant de ne pas avoir de perte de trafic?

Topologie Full maillée avec 5 noeuds



Protocole OSPF

- Le protocole OSPF (Open Shortest Path First) fonctionne également grâce à la coopération des routeurs au sein du réseau
- Les différences résident principalement dans la performance de l'algorithme permettant de déterminer le plus court chemin
- En effet, en OSPF, l'algorithme prend en compte également l'état des liaisons et ne se limite pas au nombre de saut
- Analogie avec les déplacements:
  - En fonction du trafic et/ou de la topologie de la route, l'itinéraire le plus court entre un point A et un point B n'est pas forcément la route la plus courte en distance
  - Il en est de même en réseau, il est parfois préférable de faire un détour via un routeur si cela nous permet d'éviter une liaison satellite qui rajoute nécessairement du délai, mais cette route ne sera peut être pas toujours la plus rapide

Protocole OSPF

- Comme PIM, le protocole OSPF fait également appel à un routeur particulier qui va rassembler les données des autres routeurs et jouer le rôle de chef d'orchestre du réseau
- Ce routeur est le Designated Router
- Si le Designated Router n'est pas déterminé par l'administrateur réseau, le protocole en élira un
- C'est également ce qui peu se passer si le Designated Router tombe en panne
- Dans un réseau constitué, préparer une redondance pour le DR permet de limiter les pertes de données en cas de panne

Protocole OSPF

- Nous allons replacer RIP par OSPF dans notre réseau et faire les mêmes tests de redondance que nous avions fait avec RIP

- Il existe également des protocoles qui permettent d'utiliser plusieurs routes simultanément pour envoyer des flux, les flux passent alors par des chemins dont les paramètres de transmission (délai, jiggue, …) sont différents

- Un protocole est choisi en fonction du besoin. Pour un petit réseau simple, l'OSPF ne serait pas forcément le plus adapté
- La mise en place de protocole implique également une charge réseau qui est à prendre en compte lorsque la bande passante est limitée

Avez-vous des questions ?

Introduction au VLAN

- Repassons rapidement au N2 pour parler des VLAN
- VLAN stand for Virtual Local Area Network
- C’est un outil qui permet de séparer des réseaux par l’ajout d’une entête
- L’entête VLAN en question va être vérifiée à l’entrée et à la sortie d’un équipement pour filtrer les communications
- Ainsi, si une trame ne possède pas la bonne entête VLAN elle sera rejetée

Exemple sur le réseau Météo

- Etudions le cas de ce qui a été réalisé sur le réseau Météo de l'ASECNA
- Les notions qui seront abordées dans cet exemple:
  - Native VLAN
  - Access Mode
  - Trunk Mode
  - VLAN Membership

Exemple de configuration VLAN

Avez-vous des questions ?

Que souhaitez vous voir maintenant ?