IUT Béziers
Département Réseaux et Télécoms
Bachelor R&T

2021/2022
R103
F.C.

R103 – Réseaux locaux et équipements actifs

Concevoir le réseau d'"adopte un RT"

TP 3

Consignes

L'objectif de ce TP est de réaliser la configuration des équipements actifs et de l'ensemble des machines du réseau de notre entreprise fictive préférée : adopte un RT. Pour cela il faudra prévoir un plan d'adressage, configurer les routeurs et les switchs d'un montage packet tracer fourni.

1 La situation

Suite à votre précédente prestation, tout le câblage des machines a été réalisé, les armoires techniques ont été achetées et tout le matériel a été installé, voir même un peu plus que ce qui avait été initialement prévu. On retrouvera en effet dans le répartiteur général au rez-de-chaussée deux serveurs (DNS et WEB) qui viennent parfaire votre installation réseau. Mais il reste encore pas mal de choses à faire...

Pour l'instant seuls le rez-de-chaussée et le premier étage sont occupés. Le second étage servira plus tard quand l'entreprise se sera suffisamment étendue.

2 Le plan d'adressage

On souhaite réaliser le plan d'adressage des machines du réseau, c'est-à-dire trouver une structure logique d'adresse IP pour les machines fournissant le maximum d'informations possible. Voici ce que l'on souhaite faire :

- ▷ On utilisera l'adresse privée de réseau 10.0.0.0/8 pour les adresses.
- ▷ On souhaite que la salle dans laquelle se trouve la machine figure dans l'adresse.
- ▷ On souhaite que le numéro de la machine figure également dans l'adresse.
- ▷ On souhaite finalement que l'étage (0 pour le rez-de-chaussée et 1 pour le premier étage) figure dans l'adresse.
- ▷ On choisira pour l'adresse de la passerelle la dernière adresse disponible.

Exercice 1 Proposez un plan d'adressage qui satisfasse toutes ces conditions. Quel sera le masque de réseau qu'il faudra utiliser et pourquoi ?

Attention !

Le numéro de salle du labo est le 6, celui de l'accueil 7 et les salles techniques (sous répartiteurs) 0.

Exercice 2 On retiendra le format suivant pour l'adresse : 10.étage.salle.machine/8. Récupérez le

Version du document
1er janvier 2022

Nom du VLAN	Numéro du VLAN	Couleur sur le plan
secretariat	100	bleu
technique	101	vert
commercial	102	jaune
compta-dir	103	rose et orange
serveurs	104	sans couleur

Table 1 – Déclaration des VLANs.

fichier AdopteBase.pka et configurez l'ensemble des machines en respectant cette configuration.

Exercice 3 Pour les serveurs on remplacera le numéro de la machine par le port correspondant au service. Trouvez sur internet le port pour le service DNS ainsi que le port pour le service HTTP. Quelles seront les adresses des 2 serveurs ? Toujours sur le même montage, configurez les avec les adresses précédemment trouvées. Les services sont déjà configurés. Profitez en pour regarder les informations données dans la configuration des serveur DNS et web.

Exercice 4 Concernant le câblage des machines, la partie câblage fixe a déjà été réalisée (celle allant des prises murales jusque aux panneaux de brassage). Il vous reste à relier les prises murales aux PCs. Pour procéder au câblage des postes vous utiliserez des câbles droits allant des PCs (prise Ethernet) aux côté "Jack" des prises murales. La partie "PunchLine" correspond à l'arrière de la prise. Elle est reliée à l'arrière de la prise des panneaux de brassage. Sur l'interface quand la partie "PunchLine" est reliée elle apparaît grisée. Si elle ne l'est pas elle apparaît en noir.

Exercice 5 Donnez une procédure pour vérifier le bon fonctionnement de tous les services. Effectuez cette vérification et demandez à l'encadrant de venir valider.

La configuration du routeur de la société adopte un RT ne peut être effectuée que par l'intermédiaire du CLI (Command Line Interface) depuis un PC. Comme pour la configuration du switch lors du précédent TP, vous êtes encouragés à utiliser la touche tabulation pour compléter vos commandes et la touche " ?" pour connaître la liste des commandes disponibles ou la suite de la syntaxe d'une commande (paramètres à saisir).

Exercice 6 Reliez le PC pour pouvoir configurer le routeur. Votre réseau est relié au réseau de votre opérateur (petite icône de building dans le plan en mode "physical" au niveau "home city". En fonction des éléments que vous relèverez sur cette partie du schéma, configurez la liaison avec votre opérateur dans votre répartiteur général (type de câbles, adresses, masque, etc.). Vous configurerez les équipements actifs en mode CLI à l'aide du portable présent dans le local technique.

Exercice 7 Lorsque vous testez le fonctionnement de votre montage, lors de l'envoi d'un message ARP quels sont les équipements impactés ? Est-ce que cela est tenable si l'entreprise grossit (par exemple si on meuble le second étage) ?

3 Un peu plus de sécurité

On souhaite maintenant isoler les services de l'entreprise afin d'éviter l'envoi de messages en diffusion partout dans le réseau. Pour cela on va mettre en place des VLANs pour chaque service de l'entreprise. Voici la liste des VLAN à mettre en place et les code de couleurs des services correspondant sur le plan de l'entreprise 1.

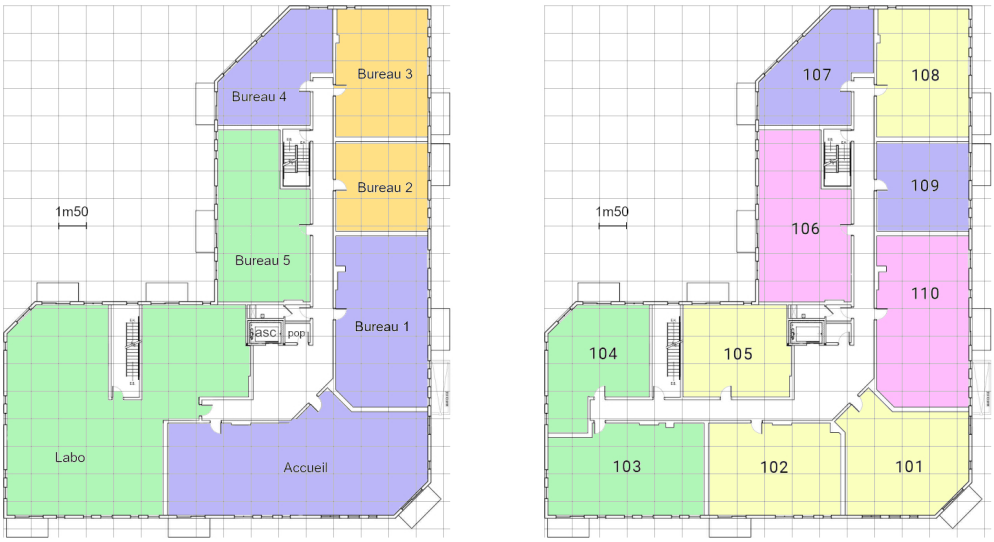

FIGURE 1 – Code de couleurs de la répartition des bureaux par services. Bleu : secrétariat, vert : technique, jaune : commercial, rose : comptabilité + direction. Les sous-répartiteurs/salle de serveurs n'ont pas de couleur.

Pour configurer les VLANs il existe plusieurs méthodes : le menu graphique ou le CLI. Pour la méthode graphique il suffit de cliquer sur le switch et d'aller dans l'onglet "config", ensuite, sous le menu **SWITCHING**, allez dans l'onglet "VLAN Database" et renseignez les VLANs.

L'autre méthode utilise le CLI. Pour cela utilisez les commandes suivantes avec XXX le numéro du VLAN et NomDuVLAN son nom :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan XXX
Switch(config-vlan)#name NomDuVLAN
```

Exercice 8 Récupérez le montage AdopteVLAN.pka. Mettez en place les VLANs sur les différents switchs.

Pour affecter un port à un VLAN il y a aussi 2 méthodes l'une utilisant l'interface graphique, l'autre le CLI. Pour l'interface graphique il suffit de sélectionner une interface dans l'onglet "config", puis de sélectionner son mode de fonctionnement : Access ou Trunk et enfin en mode access sélectionner le VLAN associé dans le menu déroulant. En CLI il faut utiliser les commandes suivantes :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch#interface FastEthernet0/X
Switch(config-if)#switchport mode <trunk/access>
Switch(config-if)#switchport access vlan X %si en mode access
```

Exercice 9 Configurez les ports des switchs en fonction des VLANs qui leurs sont associés. Comment configurer les liens entre les switchs ? Quel doit être le mode de fonctionnement des deux extrémités ?

Exercice 10 Est il possible de communiquer entre 2 machines sur des VLANs différents ? Que faudrait-

il pour que les machines puissent communiquer correctement ? Peut-on garder le plan d'adressage que nous utilisions précédemment ?

Exercice 11 Nous allons quand même changer le plan d'adressage pour faire apparaître le VLAN dans l'adresse des machines. On choisi de passer en 10.VLAN.SALLE.MACHINE/16. Appliquez ces changements sur le précédent montage. Que se passe-t-il au niveau de la passerelle ?

Pour permettre d'utiliser un passerelle par VLAN on va déclarer des interfaces virtuelles sur le routeur : une par VLAN (par exemple FastEthernet 0/0.100 pour la sous-interface appartenant au VLAN 100 sur l'interface physique FastEthernet 0/0. Ainsi chaque VLAN aura sa voie de sortie. Pour cela on utilise obligatoirement le CLI et les commandes suivantes, où X est le numéro du VLAN, @adresse l'adresse que l'on souhaite affecter à l'interface et @masque le masque associé :

```
Router#configure terminal
Router(config)#interface GigabitEthernet0/0/0.X
Router(config-subif)#encapsulation Dot1Q X
Router(config-subif)#ip address @adresse @masque
Router(config-subif)#no shut
Router(config-subif)#exit
```

Exercice 12 Configurez le routeur pour que tous les PCs puissent discuter ensembles et testez votre montage. Vous devriez pouvoir avoir accès au site web de l'opérateur, au site web d'"adopte un RT". Les machines devraient pouvoir toutes parler ensemble.

Exercice 13 Vérifiez que les requêtes ARP ne passent plus d'un VLAN à l'autre.

4 Un peu plus de sécurité

On souhaite maintenant que les VLAN ne puissent pas communiquer entre eux complètement. On souhaite que :

- ▷ Le VLAN direction/compta puisse communiquer avec tout le monde
- ▷ Que tous les VLANs puissent avoir accès aux serveurs
- ▷ Que tous les VLANs puissent avoir accès à l'extérieur de l'entreprise (réseau de l'opérateur)
- ▷ Que toutes les autres communications soient interdites.

Pour cela on va utiliser les ACLs (ACcess List) prévues à cet effet. Ce sont des règles qui vont permettre de filtrer le trafic entrant et sortant du routeur. (Sur les versions plus récentes des équipements CISCO il est possible de le faire sur les switchs layer 3, mais pas sur packet tracer). Appliquer une règle consiste en 2 étapes : définir les règles de filtrage, puis l'appliquer sur une interface.

Exercice 14 Pourquoi à votre avis est il plus intéressant de placer les ACLs sur les switchs que sur les routeurs ?

Pour tester les ACLs et leur fonctionnement avant de passer au montage final téléchargez le montage ACL.pka. Il est composé de 2 VLAN 10 et 20 comprenant chacun 2 PCs (en haut pour le VLAN10 et en bas pour le VLAN20). La passerelle a été configurée avec 2 sous-interfaces GigabitEthernet0/0/0.10 et .20 appartenant chacune à son réseau (192.168.10.0 et 192.168.20.0). Le but est d'interdire la communication inter-vlan tout en laissant passer les messages à destination du PC extérieur.

4.1 Définir les règles des ACLs

Le format de déclaration d'une ACL est le suivant : on la nomme et ensuite on définit ce qu'elle doit filtrer. A tout moment sur l'interface CLI vous pourrez regarder les autres options qui vous sont offertes pour toutes les commandes avec la touche " ?".

```
Router(config)#ip access-list extended NOM_DE_LA_REGLE
Router(config-ext-nacl)#deny ip @IPsource Wilcard @IP_destination Wildcard
Router(config-ext-nacl)#permit ip any any
```

Attention les "Wildcards" correspondent à la partie de l'adresse correspondante qu'il faut considérer dans la règle. Leur notation est l'inverse des masque de réseau. Par exemple si je donne comme adresse source l'adresse 192.168.1.0 et que je donne comme wildcard 0.0.0.255, la règle concernera toutes les adresses commençant par 192.168.1 (la partie correspondante aux 0 de la wildcard).

Exercice 15 A votre avis à quoi sert la dernière règle ? Est ce que l'ordre des règles à une importance ?

4.2 Appliquer la règle

Pour appliquer la règle sur une interface on utilise la syntaxe suivante :

```
Router(config)#interface NomDeLInterface
Router(config-subif)#ip access-group NOM_DE_LA_REGLE in/out
```

Le choix in ou out permet de filtrer sur les paquets entrants ou sortants.

Exercice 16 Utilisez ces commandes pour tester les ACL sur le montage acl.pka en fonction de ce qui est demandé plus haut. Le nom des règles à utiliser dans l'exercice sera "10vers20" et "20vers10".

Exercice 17 On passe au concret ... mettez ça en pratique sur le réseau de l'entreprise adopte un RT et testez son bon fonctionnement.

Fin