Atelier 10 : Routage & Adressage IP

Table des matières

[1 Topologie de routeur en IPv4 et Ipv6 1](#_Toc125304092)

[1.1 Fichier à utiliser, table d’adressage, topologie 1](#_Toc125304093)

[1.2 Objectifs 2](#_Toc125304094)

[1.3 Contexte/scénario 2](#_Toc125304095)

[1.4 Configurer la topologie et initialiser les périphériques 2](#_Toc125304096)

[1.4.1 Câblez le réseau conformément à la topologie indiquée. 2](#_Toc125304097)

[1.5 Configurer les périphériques et vérifier la connectivité 2](#_Toc125304098)

[1.5.1 Configurer les interfaces des ordinateurs. 3](#_Toc125304099)

[1.5.2 Configurez le routeur 3](#_Toc125304100)

[1.5.3 Vérifiez la connectivité du réseau. 3](#_Toc125304101)

[1.6 Afficher les informations du routeur 4](#_Toc125304102)

[1.6.1 Établissez une session SSH vers R1. 4](#_Toc125304103)

[1.6.2 Récupérez les informations matérielles et logicielles importantes. 4](#_Toc125304104)

[1.6.3 Affichez la configuration initiale. 4](#_Toc125304105)

[1.6.4 Affichez la table de routage sur le routeur. 5](#_Toc125304106)

[1.6.5 Affichez la liste récapitulative des interfaces sur le routeur. 5](#_Toc125304107)

[Questions de réflexion 6](#_Toc125304108)

[2 Routage statique, on le décline 6](#_Toc125304109)

[2.1 Cas ALPHA 6](#_Toc125304110)

[2.1.1 Présentation du cas 6](#_Toc125304111)

[2.2 Répondre aux questions 6](#_Toc125304112)

[2.3 Cas BETA 7](#_Toc125304113)

[2.3.1 Présentation du cas 7](#_Toc125304114)

[2.3.2 Répondre aux questions 7](#_Toc125304115)

[2.4 Cas GAMMA 8](#_Toc125304116)

[2.4.1 Présentation du cas 8](#_Toc125304117)

[2.4.2 Répondez aux questions suivantes : 8](#_Toc125304118)

[2.5 Cas DELTA 9](#_Toc125304119)

[2.5.1 Présentation du cas 9](#_Toc125304120)

[2.5.2 Répondre à la question suivante. 9](#_Toc125304121)

[2.6 Cas FARMHEROES 10](#_Toc125304122)

[2.6.1 Présentation du cas 10](#_Toc125304123)

[2.6.2 Répondre à la question suivante : 10](#_Toc125304124)

[2.7 Cas ÉMERAUDE 11](#_Toc125304125)

[2.7.1 Présentation du cas 11](#_Toc125304126)

[2.7.2 Trouvez et corrigez les erreurs présentées dans les 3 scénarii suivants. 11](#_Toc125304127)

# Introduction :

* Dans cet atelier, à partir des topologies qui nous sont fournie, aborderons le concept de routage. La première partie de ce document ce concentre sur une topologie physique packet tracert dans laquelle nous configurerons les éléments qui la compose afin de tester leur connectivité aussi bien avec l’IPV4 que l’IPV6. Afin d’activer le routage IPV6 nous manipulerons les commandes nécessaires et nous apprendrons également à manipuler la commande show afin de pouvoir afficher des informations concernant le routeur. Enfin dans le reste de cette activité nous seront confronté à différentes maquet packet tracert comportant chacune un ou plusieurs problèmes que nous devrons résoudre, il nous faudra donc mettre en application nos connaissance sur le routage.

# Topologie de routeur en IPv4 et Ipv6

## Fichier à utiliser, table d’adressage, topologie

Voici le fichier à utiliser : <Bloc2_sem2_Atelier_08_configuration_basique_de_routeur_02.pka>

**Table d’adressage**

|  |  |  |  |
| --- | --- | --- | --- |
| Appareil | Interface | Adresse IP / Préfixe | Passerelle par défaut |
| R1 | G0/0/0 | 192.168.0.1 /24 | S/O |
|  |  | 2001:db8:acad::1 /64 |  |
|  |  | fe80::1 |  |
|  | G0/0/1 | 192.168.1.1 /24 |  |
|  |  | 2001:db8:acad:1::1 /64 |  |
|  |  | fe80::1 |  |
|  | Loopback0 | 10.0.0.1 /24 |  |
|  |  | 2001:db8:acad:2::1 /64 |  |
|  |  | fe80::1 |  |
| PC-A | Carte réseau (NIC) | 192.168.1.10 /24 | 192.168.1.1 |
|  |  | 2001:db8:acad:1::10 /64 | fe80::1 |
| Serveur | Carte réseau (NIC) | 192.168.0.10 /24 | 192.168.0.1 |
|  |  | 2001:db8:acad::10 /64 | fe80::1 |

Ligne vierge - aucune information supplémentaire

## Objectifs

Partie 1 : Configuration de la topologie et initialisation des appareils

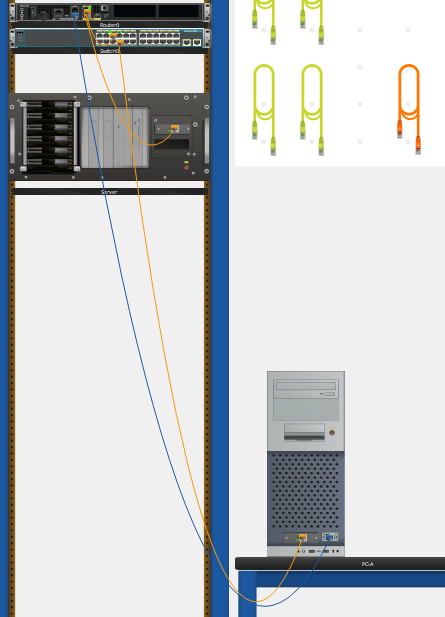
Partie 2 : Configuration des périphériques et vérification de la connectivité

Partie 3 : afficher les informations du routeur

## Configurer la topologie et initialiser les périphériques

### Câblez le réseau conformément à la topologie indiquée.

* Une fois le câblage de la topologie terminé, nous arrivons au résultat suivant :



## Configurer les périphériques et vérifier la connectivité

### Configurer les interfaces des ordinateurs.

* Il nous faut maintenant configurer les périphérique tel que l’adressage IP, le masque de sous-réseau et la passerelle par défaut sur le PC-A et l’adresse IP, le masque de sous-réseau et la passerelle par défaut sur le Serveur comme le montre les figures ci-dessous :
* Configuration PCA :

Une image contenant texte

Description générée automatiquement

* Configuration serveur :

Une image contenant texte

Description générée automatiquement

### Configurez le routeur

* Concernant la configuration du routeur, la capture d'écran ci-dessous montre les étapes pour accéder au routeur par la console, passer en mode de configuration, attribuer un nom de périphérique, définir le nom de domaine, crypter les mots de passe et configurer le système pour exiger un mot de passe d'au moins 12 caractères :

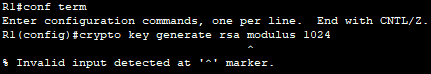
Une image contenant texte

Description générée automatiquement

* Voici la commande permettant de configurer le nom d’utilisateur SSHadmin avec le mot de passe voulu :



* Pour générer un ensemble de clés de crypto avec un module de 1024 bits voici comment faire :



Une image contenant texte

Description générée automatiquement

* Générer un ensemble de clés de cryptographie avec un module de 1024 bits permet de renforcer la sécurité des communications en utilisant des algorithmes de chiffrement plus robustes.
* La command « show crypto key mypubkey rsa » permet de montrer que cet ensemble de clés à bien été créé :

Une image contenant texte

Description générée automatiquement

Une image contenant texte, intérieur, capture d’écran

Description générée automatiquement

* + - 1. Attribuez $cisco!PRIV\* comme mot de passe d’exécution privilégié.

Une image contenant texte, intérieur, écran, orange

Description générée automatiquement

* + - 1. Attribuez $cisco!!CON\* comme un mot de passe de console. Configurez les sessions pour qu’elles se déconnectent après quatre minutes d’inactivité et activez la connexion.

Une image contenant texte

Description générée automatiquement

* La première ligne "line console 0" indique que nous configurons la console du routeur.
* La commande "password $cisco!!CON\*" définit le mot de passe de la console.
* La commande "exec-timeout 4" configure la session pour se déconnecter automatiquement après quatre minutes d'inactivité.
* La commande "logging synchronous" permet de supprimer les messages de journalisation qui peuvent interférer avec ma saisie.
* Enfin, la commande "login" active la connexion et demande un nom d'utilisateur et un mot de passe pour accéder à la console.
* Il faut s’assurer de sauvegarder la configuration en utilisant la commande "copy running-config startup-config" pour éviter de perdre les modifications en cas de redémarrage du routeur :

Une image contenant texte, intérieur, capture d’écran

Description générée automatiquement

* + - 1. Attribuez $cisco!!VTY\* comme mot de passe vty. Configurer les lignes VTY de sorte qu’elles acceptent uniquement les connexions SSH Configurez les sessions pour qu’elles se déconnectent après quatre minutes d’inactivité et activez la connexion à l’aide de la base de données locale.

Une image contenant texte

Description générée automatiquement

* La première ligne "line vty 0 4" indique que nous configurons les lignes VTY du 0 au 4.
* La commande "transport input ssh" configure les lignes VTY pour n'accepter que les connexions SSH.
* La commande "password $cisco!!VTY\*" définit le mot de passe vty.
* La commande "exec-timeout 4" configure la session pour se déconnecter automatiquement après quatre minutes d'inactivité.
* La commande "login local" active la connexion et utilise la base de données locale pour l'authentification.
* En core une fois on prend soin de sauvegarder la configuration en utilisant la commande "copy running-config startup-config" pour éviter de perdre les modifications en cas de redémarrage du routeur :

Une image contenant texte, intérieur, capture d’écran

Description générée automatiquement

* + - 1. Créez une bannière qui avertit quiconque d’accéder à l’appareil que tout accès non autorisé est interdit.
* Voici la commande à utiliser :



* + - 1. Activez le routage IPv6
* Pour activer le routage IPV6, on utilise la commande « IPV6 unicast-routing » :



* Cette commande active le routage IPv6 sur le routeur en activant le traitement des paquets IPv6 unicast. Le routeur peut ainsi échanger des paquets IPv6 avec d'autres réseaux.
  + - 1. Configurez les trois interfaces du routeur avec les informations d’adressage IPv4 et IPv6 de la table d’adressage ci-dessus. Configurez les trois interfaces avec des descriptions. Activez les trois interfaces.
* Interface G0/0/0 :





* Interface G0/0/1 :

Une image contenant texte

Description générée automatiquement

* Interface Loopback0 :

Une image contenant texte

Description générée automatiquement

* Le routeur ne doit pas autoriser les connexions vty pendant deux minutes si trois tentatives de connexion échouées se produisent dans une minute.
  + - 1. Réglez l’horloge sur le routeur.
* Voici un réglage de l’horloge qui pourrait convenir :



* + - 1. Enregistrez la configuration en cours dans le fichier de configuration initiale.
* Voici la commande permettant l’enregistrement de la configuration en cours dans le fichier de configuration initiale.

Une image contenant texte, intérieur, noir, sombre

Description générée automatiquement

* Si je n'avais pas enregistré la configuration dans le fichier initial (startup-config) et que j’aurais procédé au redémarrage du routeur, celui-ci va utiliser la configuration en mémoire volatile (running-config) qui est en cours d'exécution. Cela signifie que toute modification de configuration que vous avez effectuée depuis le dernier enregistrement de la configuration sera perdue après le redémarrage du routeur.

Fermez la fenêtre de configuration.

### Vérifiez la connectivité du réseau.

* Pour tester la connectivité du réseau, on peut utiliser l’outil ping sur l’IPV4 et l’IPV6 afin de voir si le tes abouti. On peut voir ici que tous cette passe bien :

Une image contenant texte

Description générée automatiquement

* En utilisant le client telnet / SSH, nous allons établir une connexion distante sur le PCA vers le routeur grâce à l’interface de bouclage du routeur, l’interface de bouclage est l’interface loopback0 :

Une image contenant texte, intérieur, orange, sombre

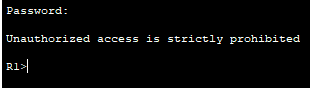
Description générée automatiquement

* Nous testerons ce moyen de connexion via l’IPV4 et l’IPV6 ( la mot de passe à utiliser est celui précédemment configuré : « 55Hadm!n2020 »).
* Test de connexion IPV4 :

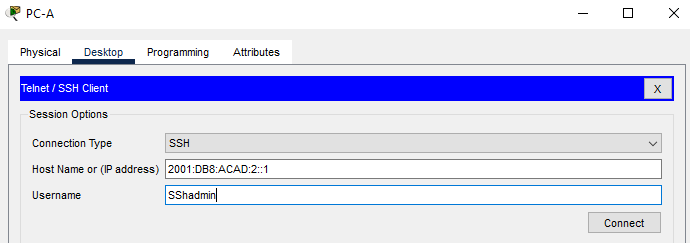
Une image contenant texte

Description générée automatiquement

* Ici on peut voir que le test de connexion abouti :



* Test de connexion adresse IPV6 :



* Ici aussi la connexion abouti :

Une image contenant texte

Description générée automatiquement

* Cependant, le protocole Telnet est considéré comme un risque de sécurité pour plusieurs raisons :
* Confidentialité des données : Telnet transmet les informations en clair, ce qui signifie que toute personne qui intercepte le trafic peut facilement lire les informations sensibles telles que les noms d'utilisateur et les mots de passe.
* Manque d'authentification forte : Telnet utilise une simple authentification de nom d'utilisateur et de mot de passe, qui peut facilement être contournée par des attaquants expérimentés.
* Vulnérabilités de sécurité connues : Telnet a plusieurs vulnérabilités de sécurité connues qui ont été exploitées par des pirates informatiques pour accéder à des systèmes distants.
* Manque de cryptage : Telnet ne prend pas en charge le cryptage des données, ce qui facilite la tâche aux pirates informatiques qui cherchent à intercepter le trafic.
* Pour pallier ce problème, il est recommandé d'utiliser des protocoles de connexion distants plus sécurisés tels que SSH (Secure Shell) pour se connecter à des systèmes distants, qui prennent en charge l'authentification forte, le cryptage des données et la confidentialité des données. La capture ci-dessous présente une connexion SSH grâce à l’outil vmrc que j’ai réalisé sur un server Ubuntu que j’ai créé :

Une image contenant texte

Description générée automatiquement

* La commande à saisir dans le terminal pour effectuer cette connexion SSH est la suivante :

***vmrc vmrc://root@172.31.1.1(1)/?moid= le moid de la machine virtuelle faisant ofice de server***

## Afficher les informations du routeur

* Nous allons maintenant voir que à l’aide de cette connexion telnet / ssh il est possible de recueillir des information sur le routeur.

### Établissez une session SSH vers R1.

### Récupérez les informations matérielles et logicielles importantes.

* + - 1. Utilisez la commande show version pour répondre aux questions sur le routeur.

Quel est le nom de l’image IOS exécutée par le routeur ?

* Aperçu de la commande show version :

Une image contenant texte

Description générée automatiquement

* Le nom de l'image IOS exécutée par le routeur est "bootflash:/isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin". Cela peut être vu dans la sortie de la commande "show version" dans la ligne "System image file".

Quelle quantité de mémoire vive non volatile (NVRAM) le routeur possède-t-il ?

* Le routeur dispose de 32768K bytes de mémoire vive non volatile (NVRAM). Cela peut être vu dans la sortie de la commande "show version" dans la ligne "32768K bytes of non-volatile configuration memory".

Quelle quantité de mémoire Flash le routeur possède-t-il ?

* Le routeur dispose de 3223551K bytes de mémoire Flash à bootflash:. Cela peut être vu dans la sortie de la commande "show version" dans la ligne "3223551K bytes of flash memory at bootflash:".
* La commande "show version | include register" affiche la valeur actuelle du registre de configuration du routeur Cisco. Le registre de configuration est un octet de mémoire non volatile qui stocke des paramètres de configuration importants, tels que le mode de démarrage du routeur, la source de la configuration de démarrage et les paramètres de mot de passe. La commande "include register" filtre la sortie pour ne montrer que la ligne contenant l'information sur le registre de configuration.



* Si le registre de configuration était 0x2142, lors du prochain rechargement du routeur, il démarrerait avec la configuration par défaut et sans tenir compte de la configuration stockée dans la mémoire NVRAM. Cela signifie que le routeur ne chargerait pas la configuration actuelle et le mot de passe d'enable serait également réinitialisé.

### Affichez la configuration initiale.

* + - 1. Utilisez la commande show startup-config sur le routeur pour répondre aux questions ci-dessous.

Comment les mots de passe sont-ils présentés dans les résultats ?

* Aperçu de la commande « show startup-config » :

Une image contenant texte

Description générée automatiquement

* Les mots de passe sont présentés sous forme chiffrée à l'aide d'un algorithme de hachage. Dans ce cas, les mots de passe sont chiffrés avec l'algorithme "Type 7". Par exemple, "password" est chiffré en "08654F471A1A0A56524A2F2B0461" et "enable secret" est chiffré en "$1$mERr$2q6B19eTeuK92k7m8Bhgz/". Il est important de noter que le chiffrement de type 7 est relativement faible et facilement cassable, il est donc recommandé d'utiliser d'autres méthodes de chiffrement plus sécurisée.
  + - 1. Use the show running-config | section vty command.

Quel est le résultat de l’exécution de cette commande ?

* La commande "show running-config | section vty" affiche la partie de la configuration en cours d'exécution du routeur Cisco qui concerne les lignes de terminal virtuel (VTY). Cette commande filtre la configuration pour ne montrer que les lignes VTY configurées sur le routeur :

Une image contenant texte

Description générée automatiquement

### Affichez la table de routage sur le routeur.

Utilisez la commande show ip route sur le routeur pour répondre aux questions ci-dessous.

* Résultat de la commande « show ip route » :

Une image contenant texte

Description générée automatiquement

* + - 1. Quel code est utilisé dans la table de routage pour indiquer un réseau connecté directement ?
* Le code utilisé dans la table de routage pour indiquer un réseau connecté directement est "C".
  + - 1. Combien d’entrées de route sont codées avec un code C dans la table de routage ?
* Il y a trois entrées de route codées avec le code C dans la table de routage :

=> 10.0.0.0/24 pour la Loopback0

=> 192.168.0.0/24 pour la GigabitEthernet0/0/0

=> 192.168.1.0/24 pour la GigabitEthernet0/0/1

### Affichez la liste récapitulative des interfaces sur le routeur.

* + - 1. Utilisez la commande show ip interface brief sur le routeur pour répondre à la question ci-dessous.
* Résultat de la commande « show ip interface brief » :

Une image contenant texte

Description générée automatiquement

Quelle commande a modifié l’état des ports Gigabit Ethernet depuis administratively « down » à « up » ?

* La commande qui a modifié l'état des ports Gigabit Ethernet de "administratively down" à "up" n'est pas claire à partir de la sortie de la commande "show ip interface brief". Il est possible que cela ait été fait avec la commande "no shutdown" pour activer les interfaces en mode administratif.
  + - 1. Exécutez la commande show ipv6 int brief afin de vérifier les paramètres IPv6 sur R1.
* Résultat de la commande « show ipv6 int brief » :

Une image contenant texte

Description générée automatiquement

Quelle est la signification de la partie [up/up] de la sortie ?

* La partie [up/up] dans la sortie de la commande "show ipv6 interface brief" indique l'état de la couche physique et de la couche liaison de données pour l'interface IPv6. Le premier "up" indique que la couche physique est activée et que l'interface est connectée. Le deuxième "up" indique que la couche liaison de données est activée et que l'interface est prête à transmettre des données IPv6. Si l'un des "up" était "down", cela indiquerait un problème avec la couche physique ou la couche liaison de données de l'interface IPv6.
  + - 1. Sur le serveur, modifiez sa configuration afin qu’il n’ait plus d’adresse IPv6 statique. Puis, exécutez la commande ipconfig sur Serveur afin d’examiner la configuration IPv6.

Quelle est l’adresse IPv6 affectée à Serveur ?

* Voici les modifications effectuée :

Une image contenant texte

Description générée automatiquement

Quelle est la passerelle par défaut attribuée à Serveur ?

* La capture ci-dessous montre que la passerelle par défaut est disponible en ipv6 et 4 :

Une image contenant texte

Description générée automatiquement

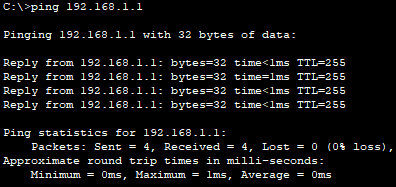
À partir du PC-A, envoyez une requête ping à l’adresse locale de la passerelle par défaut R1. A-t-elle abouti ?

* Ici il nous ai demandé d’effectué un ping sur la passerelle par défaut du routeur, la passerelle par défaut est l’interface G0/0/1 que l’on peut voir sur la capture ci-dessous :

Une image contenant diagramme

Description générée automatiquement

* Voici le résultat concluant du ping :



À partir du Serveur, envoyez une requête ping à R1 à l’adresse de monodiffusion IPv6 2001:db8:acad::1. A-t-elle abouti ?

* On peut voir ici que le ping fonctionne :

Une image contenant texte, intérieur

Description générée automatiquement

# Questions de réflexion

1. Lors de la recherche d’un problème de connectivité réseau, un technicien suspecte qu’une interface n’a pas été activée. Quelle commande show le technicien pourrait-il utiliser pour dépanner ce problème ?

* Le technicien pourrait utiliser la commande "show interfaces" pour dépanner le problème de connectivité réseau et vérifier si l'interface suspectée est activée ou non. Cette commande affiche l'état des interfaces réseau sur le périphérique et peut indiquer si une interface est activée ou désactivée :

Une image contenant texte

Description générée automatiquement

1. Lors de la recherche d’un problème de connectivité réseau, un technicien suspecte qu’un masque de sous-réseau incorrect a été attribué à une interface. Quelle commande **show** le technicien pourrait-il utiliser pour dépanner ce problème ?

* Le technicien pourrait utiliser la commande "show interfaces [nom de l'interface]" pour dépanner le problème de connectivité réseau et vérifier si le masque de sous-réseau est correctement configuré sur l'interface :

Une image contenant texte

Description générée automatiquement



# Routage statique, on le décline

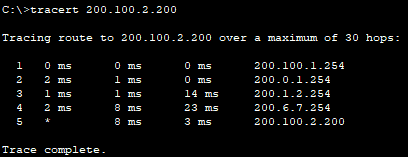
## Cas ALPHA

### Présentation du cas

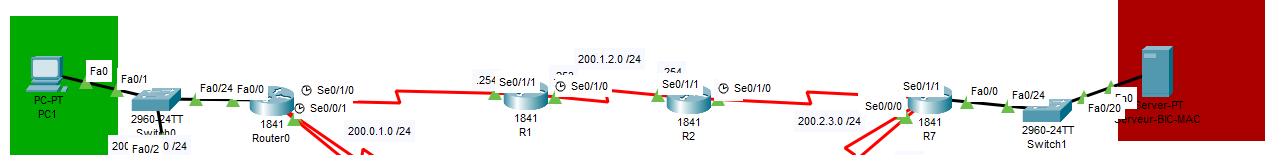
Examinez la maquette fournie : <Bloc2_sem2_Atelier_08_routage-ALPHA.pkt>

## Répondre aux questions

* 1. Donner la liste des routeurs traversés.



* Cette commande enverra des paquets de test à la destination spécifiée en utilisant le protocole ICMP ou UDP, et affiche une liste ordonnée des routeurs traversés par les paquets sur le chemin vers la destination. La liste des routeurs est généralement affichée avec leur adresse IP et leur nom d'hôte, ainsi que le temps nécessaire pour atteindre chaque routeur sur le chemin vers la destination.
* La figure ci-dessous présente la liste des routeurs traversé, à savoir : [R0 ; R1 ; R2 ; R7] :



* 1. Quel est, en nombre de sauts, le chemin le plus court entre PC1 et Serveur-BIC-MAC ? Donner la liste des routeurs traversés.
* Cette question n’a pas vraiment de sens, de plus elle est mal formulée. Il faudrait plus-tôt dire quel est le chemin avec le moins de latence.
* La capture ci-dessous démontre que le nombre de saut minimum est de 3 car le TTL de base est de 128, il est ici de de 125 :

Une image contenant texte

Description générée automatiquement

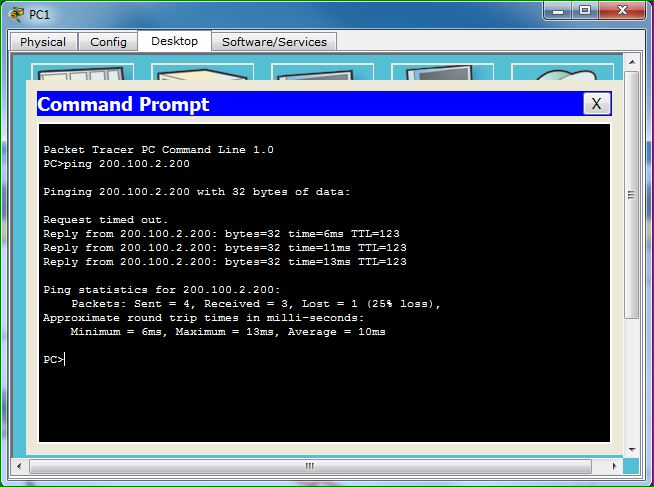
* Cependant, le nombre de saut ne représente pas le chemin le plus cour. Le chemin le plus court ce matérialise par la bande passante disponible sur le chemin emprunté, ou bien le temps que prendra le routeur à traiter l’information. Pour connaitre le chemin le plus court, il faudrait disposer de certaines informations tel que la bande passante disponible sur chaque itinéraire.
* En somme, le chemin le plus court entre le PC et le serveur n'est pas toujours le plus efficace en termes d'utilisation du réseau. En effet le choix du chemin dépend de plusieurs facteurs tels que la congestion du réseau, la qualité de service, la bande passante, la latence et la fiabilité des connexions. Car on peut avoir un chemin plus court mais avec plus de latence qu’n chemin plus long.
  1. Quel est le cheminement effectif d’un ping aller et retour de PC1 vers Serveur-BIC-MAC ?
     + - Le chemin qui correspond au ping de pc1 vers le serveur est le suivant :
* **PC1** > Router0 > R1 > R2 > R7 > **Serveur-BIC-MAC** > R7 > R2 > R1 > Router0 > **PC1**
  + - * **On peut collecter ces informations grâce à l’outil « tracert » qui nous fournit l’ip des interfaces des routeurs traversé :**

Une image contenant texte, noir, Appareils électroniques, écran

Description générée automatiquement

## Cas BETA

### Présentation du cas



On souhaite comprendre la valeur du TTL.

Vous disposez du fichier Packet Tracer correspondant à la maquette complète à laquelle sont intégrés PC1 et BIC-MAC. (<Bloc2_sem2_Atelier_08_routage-BETA.pkt>)

### Répondre aux questions

* 1. Sélectionner la réponse correcte parmi les suivantes :
     + - L’affirmation exact est la suivante :
* La valeur du TTL indique que le paquet a traversé 5 routeurs pour atteindre sa destination
  + - * En effet dans la commande ping, le TTL (Time to Live) est un paramètre qui spécifie le nombre maximum de routeurs (ou "sauts") que les paquets ICMP (Internet Control Message Protocol) peuvent traverser avant d'être abandonnés. Le TTL est définit avec une valeur par défaut de 128. Ici on peut voir que le TTL est de 123 donc 128-123 = 5.
  1. Sélectionnez la réponse correcte parmi les suivantes :
     + - L’affirmation correcte est la suivante :
* La valeur du TTL correspond à *l’echo response* (le retour)
  + - * Lorsque l'echo request est envoyé avec un TTL initial, chaque routeur sur le chemin de l'aller décrémente la valeur du TTL de 1 avant de transmettre le paquet au routeur suivant. Si le TTL atteint 0, le routeur abandonne le paquet et renvoie un message d'erreur à l'émetteur.
      * Lorsque l'echo request atteint la destination finale, celle-ci répond en générant une echo response qui inclut un champ de TTL. La valeur de ce champ de TTL dans l'echo response correspond au nombre de sauts que le paquet a effectués pour atteindre la destination finale et revenir.

La question 3 peut vous aider à répondre à la question 2 si vous manquez de certitudes.

* 1. Quels routeurs sont traversés [à l’aller] lorsque PC1 (repéré en vert sur la maquette) tente de joindre Serveur-BIC-MAC (repéré en rouge sur la maquette) ?
     + - Les routeurs traversés l’ord du ping de PC1 vers le serveur sont les suivants :
* R0
* R1
* R2
* R7
  + - * L’outil tracert permet de justifier cette réponse :

Une image contenant texte, Appareils électroniques, noir, écran

Description générée automatiquement

* + - * On obtient ici la liste des ip traversé l’ors du ping.

## Cas GAMMA

### Présentation du cas

Examinez la maquette Packet Tracer proposée : <Bloc2_sem2_Atelier_08_routage-GAMMA.pkt>

Le travail demandé porte sur un *ping* émis par PC0 (repérable par le carré vert) vers PC5 (repérable par le carré rouge)

### Répondez aux questions suivantes :

Si PC0 émet un *ping* vers PC5 :

* 1. Quelle sera l’adresse MAC destination de la trame - correspondant à l’echo request - qui partira de PC0 ?
     + - Grace à l’outil de simulation sur packet tracert, on peut obtenir le chemin suivant :

Une image contenant table

Description générée automatiquement

Adresse MAC interface d’entré routeur

Adresse MAC interface de sortie du routeur.

Adresse MAC PC5.

Adresse MAC PC0

* + - * **L’adresse MAC correspondant à un « echo request » est donc la « 0002.163d.b501 »**
  1. Quelle sera l’adresse IP destination du paquet - correspondant à l’echo request - qui partira de PC0 ?
     + - Le principe n’est pas le même que pour les adresses MAC, en effet nous avons pu voir que les adresse MAC corresponde à la couche 2 et que la communication ce passe au niveau de la couche 2. Cependant les adressent IP appartiennent à la couche 3 aussi appelé couche réseau elle est utilisé pour décrire les communication réseau, c’est pour cette raison que l’IP qui correspond à « echo request » est la « 10.5.5.10 ».

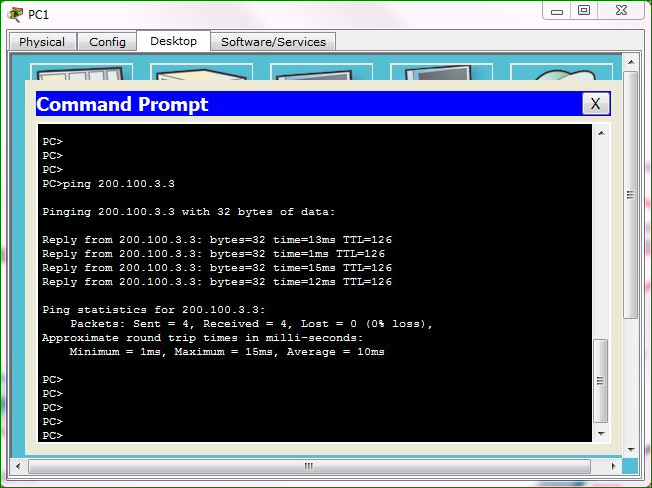


* 1. Quelle sera l’adresse MAC source de la trame reçue par PC5 ?
     + - L’adresse MAC source de la trame reçu par PC5 est « 0060.70E1.CC01 ».
  2. Quelle sera l’adresse IP source du paquet reçu par PC5 ?
     + - L’adresse IP source du paquet reçu par PC5 sera 192.168.3.5.

## Cas DELTA

### Présentation du cas

Examinez la copie d’écran ci-dessous : elle montre le résultat d’un *ping* depuis un poste PC1 et vers un autre poste (PC3).



Vous disposez de la maquette Packet Tracer correspondante : <Bloc2_sem2_Atelier_08_routage-DELTA.pkt>.

### Répondre à la question suivante.

Sélectionner les réponses correctes parmi les suivantes :

* + - * Les réponses correctes sont :
* La valeur du TTL indique que le paquet a traversé 2 routeurs pour atteindre sa destination
* La valeur du TTL correspond à *l’echo response* (le retour)

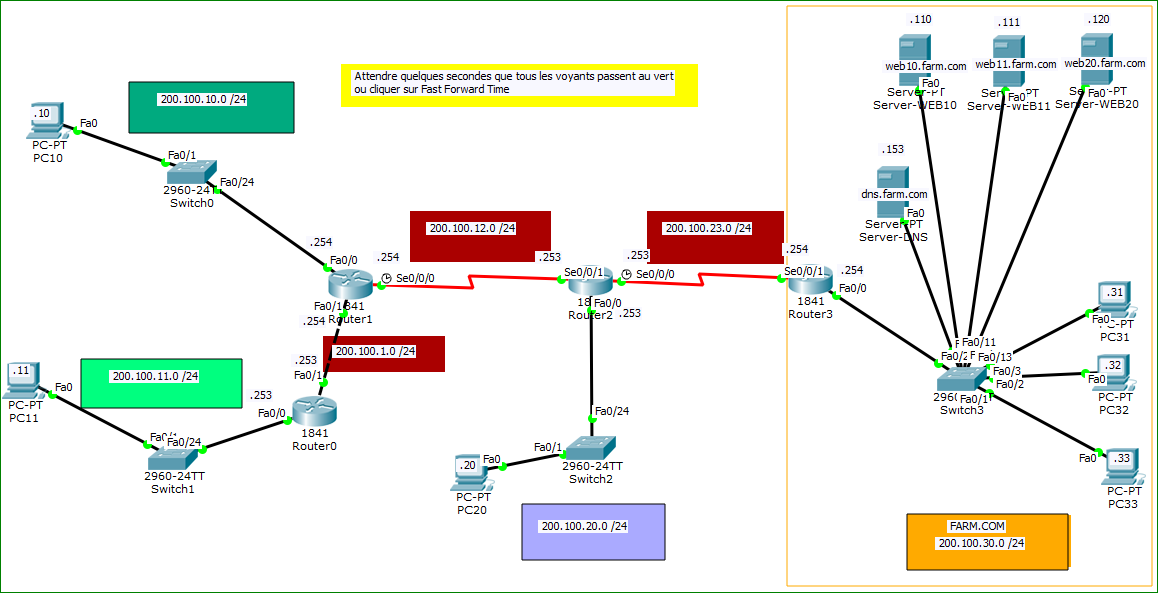
## Cas FARMHEROES

### Présentation du cas

Examinez la maquette fournie : <Bloc2_sem2_Atelier_08_routage-FARMHEROES.pka>

Des erreurs sont présentes dans la configuration des postes ou des routeurs et empêchent la communication avec le serveur WEB qui est dédié à chaque réseau, mais qui est hébergé chez FARM.COM.

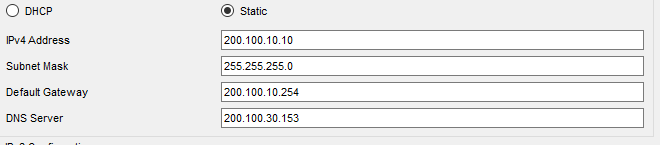
N.B. Volontairement, vous n’avez pas accès à tout le réseau de l’hébergeur FARM.COM. La configuration de Router3 est correcte.



### Répondre à la question suivante :

Lisez les instructions associées à la maquette, corrigez les erreurs, et reportez ci-dessous les 3 mots-clé attendus que vous obtiendrez lors de l’accès effectif à chaque serveur Web dédié (réalisable à partir de l’outil *Web Browser* de chaque PC), en expliquant brièvement l’erreur.

* Probléme au niveau du routeur 1 pour le PC10 :
  + - * Le paquet ne parvient pas à franchir le routeur 1. C’était un problèmes au niveau de la configuration de la passerelle par défaut, la capture ci-dessous montre la configuration correct à adopter :

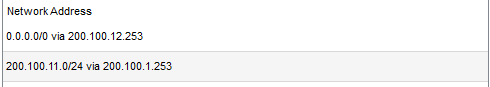


* + - * Une fois le problème résolu, voici le mot clé qui s’affiche :

Une image contenant texte

Description générée automatiquement

* Problème au niveau du Routeur 1 et 2 pour le PC11 :
  + - * Le paquet fait des aller retours entre le routeur 1 et 2.



* + - * Il fallait simplement ajouter une autre table de routage pour permettre la redirection du paquet vers le routeur 0, comme le montre la figure ci-dessus.
      * Une fois le problème résolu voici le mot clé :

Une image contenant texte

Description générée automatiquement

* Problème au niveau du routeur2 :
  + - * Le paquet ARP ne parvient pas à franchir le routeur 2.

Une image contenant texte

Description générée automatiquement

* + - * La passerelle par défaut était mal écrite (200.100.20.25). Une fois le problème résolu voici le mot clé obtenu :

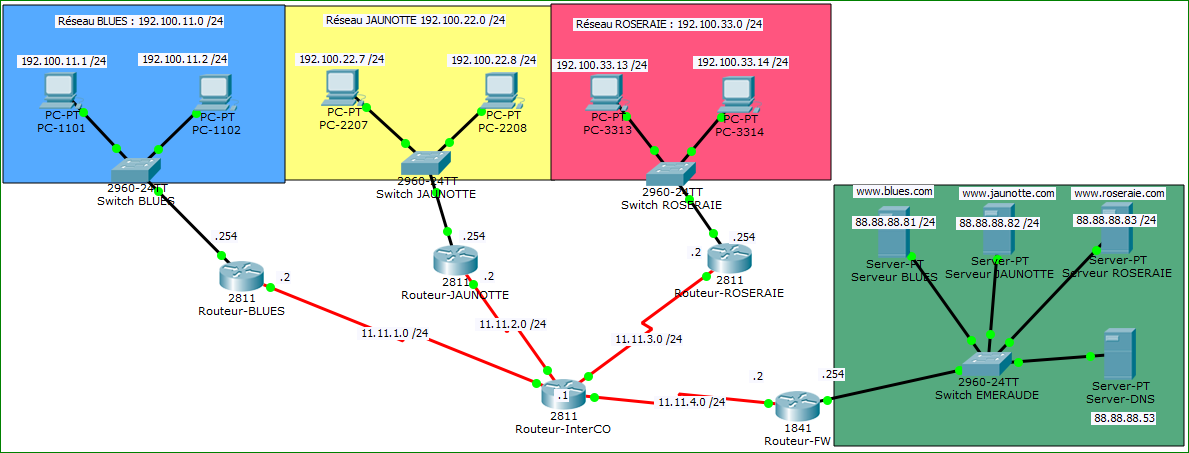
Une image contenant texte

Description générée automatiquement

## Cas ÉMERAUDE

### Présentation du cas

Étudiez la maquette proposée sous Packet Tracer : <Bloc2_sem2_Atelier_08_Routage-EMERAUDE.pka>



La communication des postes d’un réseau avec leur serveur respectif, hébergé chez la société ÉMERAUDE, ne fonctionne pas.

La cause est due à la configuration des postes ou à la configuration des routeurs auxquels vous avez accès : Routeur-BLUES, Routeur-JAUNOTTE et Routeur-ROSERAIE.

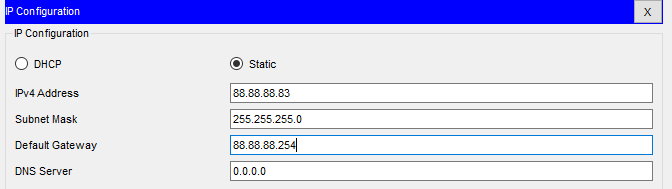
En revanche **Routeur-InterCO** et **Routeur-FW** ne peuvent pas être en cause et, de ce fait, ne sont pas accessibles.

### Trouvez et corrigez les erreurs présentées dans les 3 scénarii suivants.

* 1. Scénario 1 : la communication des postes du réseau ROSERAIE avec le serveur (www.roseraie.com) hébergé chez la société EMERAUDE ne fonctionne pas.

Corrigez l’erreur et reportez le mot secret affiché sur la page d’accueil du serveur WEB.

* Le cas roseraie :
  + - * Ici c’était un problème au niveau de la configuration du serveur, l’IPV4 était mal configurer. Voici une configuration correcte :



* + - * Une fois le problème résolu, voici le mot secret qui s’affiche :

Une image contenant texte

Description générée automatiquement

* 1. Scénario 2 : la communication des postes du réseau JAUNOTTE avec le serveur (www.jaunotte.com) hébergé chez la société ÉMERAUDE ne fonctionne pas.

Corrigez l’erreur et reportez le mot secret affiché sur la page d’accueil du serveur WEB.

* Le cas jaunotte :
  + - * Ici c’était un problème de configuration de poste, la passerelle par défaut était mal écrite(.25 au lieu de .254) . Les deux captures montrent la correction du problème :

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

* + - * Il y avait un second problème de configuration sur l’autre poste, sont adresse IP était en .4 au lieu de .7. Les deux captures ci-dessous montre la correction du problème :

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

* + - * Et enfin il fallait rajouter une IP route sur le routeur pour permettre le bon acheminement du paquet :



* + - * Une fois les trois problème corrigé, voici le mot secret qui s’affiche :



* 1. Scénario 3 : la communication des postes du réseau BLUES avec le serveur (www.blues.com) hébergé chez la société EMERAUDE ne fonctionne pas.

Corrigez l’erreur et reportez le mot secret affiché sur la page d’accueil du serveur WEB.

* Le cas BLUES :
  + - * Voici la correction du problème sur le routeur blues :



* + - * Et voici le mot secret qui devait s’afficher après la résolution de ce problème :

Une image contenant texte

Description générée automatiquement

## Conclusion :

* + - * En somme, cet atelier sur le routage a été l'occasion pour nous de tester la connectivité entre les éléments de la topologie en utilisant les protocoles IPV4 et IPV6. De plus, nous avons appris à activer le routage IPV6 en utilisant les commandes appropriées et à afficher les informations relatives au routage grâce à la commande show. Enfin, à travers différentes maquettes packet tracer comportant des problèmes, nous avons été en mesure de mettre en application nos connaissances sur le routage. En somme, cet atelier nous a permis de mieux comprendre le concept de routage et de nous familiariser avec les outils nécessaires pour configurer et résoudre des problèmes de routage.

# Sources :

* + - * <https://www.frameip.com/entete-ip/>
      * <https://www.frameip.com/entete-ipv6/>
      * <https://www.frameip.com/routage/>
      * <https://www.afrinic.net/fr/support/general-queries/how-to-develop-ipv4-addressing-plan>