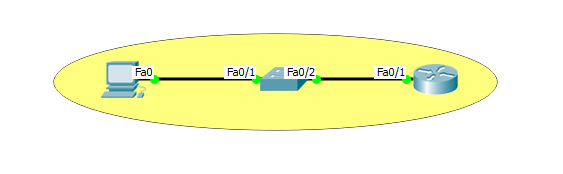
Configuration de base des équipements CISCO

# Topologie



Adresse IP de la machine cliente : 192.168.0.1 255.255.255.0

# Navigation dans les différents modes

## Le mode de configuration utilisation

Il permet d’effectuer uniquement quelques commandes de diagnostic de base ou d’information. Il ne permet aucun changement de configuration.

Il est représenté par un > à la fin du prompt.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\1-mode config sans droit.PNG

## **Le mode privilégié.**

Aussi appelé mode « enable », il permet d’accéder aux commandes qui peuvent remettre en question le fonctionnement des routeurs et commutateurs.

L’accès à ce mode peut être protéger par un mot de passe, ce qui est fortement recommandé.

Il est représenté par un # à la fin du prompt.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\2-accès mode privilège.PNG

Ou

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\2.1-accès mode privilège.PNG

Remarque :

Comme indiqué ci-dessus, les commandes peuvent être renseignées en abrégée.

## Le mode de configuration globale

Ce mode permet d’effectuer des commandes de configuration, qui affecteront le fonctionnement du routeur ou du commutateur.

Il est important de noter que les modifications sont effectives dès la validation de la commande.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\3 accès mode configuration.PNG

Ou

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\3.1 accès mode configuration.PNG

## Le sous-mode configuration

Ce mode est accessible à partir du mode de configuration. Il permet de configurer un champs particulier (interface, ligne pour l’administration de l’équipement, protocole de routage, dhcp, vlan, etc).

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\4 config interface.PNG

Ou

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\4 config interface.PNG

## Revenir au contexte précédent

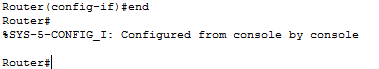
La commande « exit » permet quitter le mode en cours pour revenir au mode parent.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\5 sortie du mode config.PNG

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\6 sortie du mode config privilege.PNG

## Revenir directement mode privilège

La commande « end » permet revenir directement au mode « enable ».



La combinaison de touches « ctrl+Z » à la même fonction que la commande « end ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\7 sortie d'un mode kkconk crtl+Z.PNG

## Déconnexion

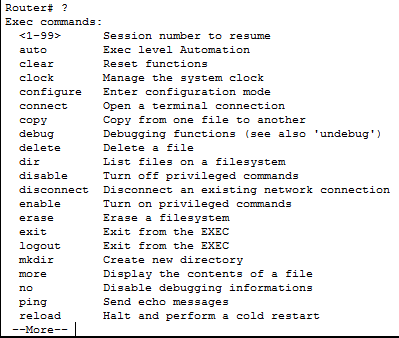
C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\8 deconnexion (du mode privilege).PNG

# Aide de la console

L’affichage des différents menu d’aide se fait à l’aide du « ? ». Les informations données par l’aide varient en fonction de la position du « ? ».

## Affichage des commandes disponibles dans le mode actuel

L’ensemble des commandes disponibles peuvent être affichées en saisissant « ? » après le prompt.



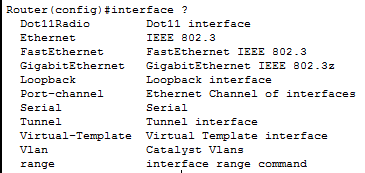
On voit donc toutes les commandes possibles dans la racine du mode privilèges.

Le C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\10 More.PNG à la fin de la liste signifie que la liste des commandes disponibles n’est pas terminée. Il y a 2 possibilités pour afficher la suite :

* Avec la touche « entrée », le déroulement de la suite de la liste se fait ligne par ligne,
* Avec la barre d’espace, le déroulement de la suite de la liste se fait page par page.

## Affichage l’aide relative à une commande

Pour afficher les options relatives à une commande, il suffit de saisir la commande puis un « ? » (séparé par un espace).

do

## Compléter d’une commande avec le « ? »

En ajoutant un « ? » à la fin d’une chaine de caractère (en cas d’oubli de la commande par exemple), l’IOS retourne la liste des commandes possibles à partir de la chaine de caractère saisie.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\9.2 affichage du complement pour une commande.PNG

Dans l’exemple ci-dessus, 3 commandes sont possibles à partir de la chaine de caractère « se ». Il ne reste plus qu’à choisir la commande désirée.

# Les différentes configurations

Il y a deux types de configuration. La configuration appelée **startup-config** et la configuration appelée **running-config**.

La configuration ***startup-config*** est la configuration mise en place au démarrage du switch (en cas de redémarrage etc…). Elle est stockée dans la NVRAM.

La configuration dite ***running-config*** est la configuration courante utilisée par le switch. Elle est stockée dans la RAM.

## Affichage de la startup-config

La commande « show » permet de visualiser des informations en fonction de l’argument que l’on aura saisi. Dans notre cas, l’argument sera « startup-config ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\13 Affichage de la config de démarrage.PNG

Dans notre exemple, aucune configuration est présente au démarrage du routeur ce qui veut donc dire que la configuration usine qui est mise en place à chaque redémarrage.

## Affichage de la running-config

Toujours avec la commande « show », en remplaçant « startup-config » par « running-config ».

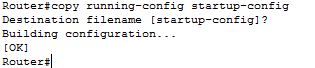
C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\14.1 Affichage de la config en cours.PNG

## Enregistrement la configuration en cours

La sauvegarde de la configuration du routeur en cours consiste à remplacer la « startup-config » par la « running-config ».

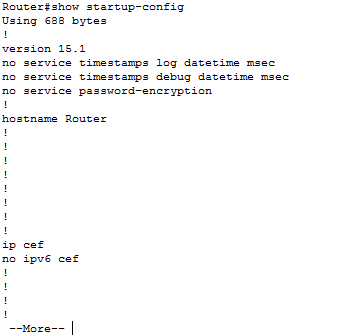
La commande ci-dessous enregistre la running-config dans la NVRAM. Elle devient donc, de fait, la startup-config.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\16 sauvegarde de la config en cours.PNG



## Vérifier le fichier startup-config

Une fois l’enregistrement de la configuration en cours effectuée, la vérification se fait via la commande « show startup-config ».



On remarque que le routeur a une configuration particulière au démarrage, contrairement au 4.1.

# Mise en place des mots de passe

Dans le but de sécuriser l’accès aux modes de configuration des routeurs, il faut définir différents mots de passe.

## Mot de passe pour l’accès au mode privilège

### « secret »

Le premier mot de passe que l’on peut mettre en place est celui qui permet l’accès au mode privilège.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\18 mot de passe accès privilège.PNG

Dans l’exemple :

* La commande est « enable secret ».
* Le mot de passe est « cisco » dans l’exemple

Pour vérifier l’activation du mot de passe, on utilise la commande « show running-config » en mode privilège.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\18.1  verification du chiffrement du mot de passe.PNG

La ligne ci-dessous montre le mot de passe chiffré, tel qu’il apparait dans la « running-config ».

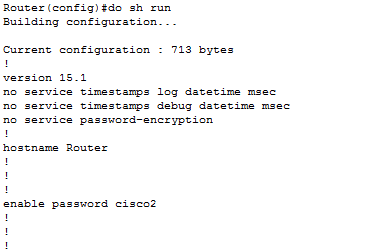
C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\18.1  verification du chirffrement du mot de passe.PNG

### « password »

Contrairement à « enable secret », la commande « enable password » crée un mot de passe non chiffré (ici, le mot de passe est « cisco2 »).

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\19 mot passe privilège non chiffré.PNG

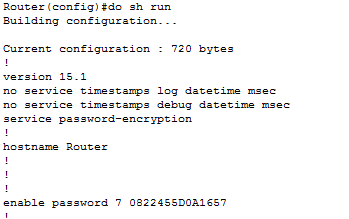
On peut voir le mot de passe en clair dans la « running-config ».



Pour chiffrer un mot de passe saisi avec la commande « enable password », il faut activer le service «password-encryption ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\19.2 chiffrement du mot de passe non chiffré.PNG

On vérifie que le mot de passe a bien été chiffré en affichant la « running-config ».



Remarques :

* Si les 2 mots de passe sont configurés, seul le mot de passe défini par la commande « enable secret » sera pris en compte,
* De fait, il est recommandé de ne plus définir les mots de passe avec la commande « enable password ».

# Mot de passe d’administration

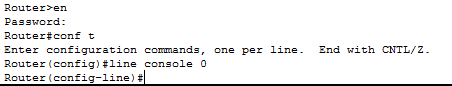
L’administration d’un équipement CISCO est possible :

* Soit en local via la ligne console (con0),
* Soit à distance via les lignes VTY (terminaux virtuels).

L’accès à ces lignes doit être protégé par un mot de passe.

## Ligne console (con0)

La sécurisation de l’accès à la ligne console se fait dans le sous mode de configuration dédié à cette ligne.



**Remarque :**

Il n’y a qu’une ligne console, elle portera toujours le numéro 0.

Les mots de passe sont mis en place à l’aide de la commande « password ». Par défaut, cette commande ne chiffre pas les mots de passe.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\27.1 mdp line console.PNG

Le mot de passe dans l’exemple est « console ». Tel qu’il a été défini, il apparaitra en clair dans la « running-config », si le service «password-encryption » n’est pas actif.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\27.2 mdp line console.PNG

La commande « login » active l’authentification (quel que soit la ligne sélectionnée). Sans cette commande, aucun mot de passe ne sera demandé à la connexion.

**Remarque :**

Il est important de saisir le mot de passe avant la commande « login ». En effet, si tel est le cas, il sera impossible de se connecter à distance.

## Lignes VTY

Les lignes VTY (terminaux virtuels) sont destinées aux connexions à distance (TELNET ou SSH).

Comme pour la ligne console, la sécurisation de l’accès à ces lignes se fait dans un sous mode de configuration dédié.

Il est possible de configurer 16 lignes, numérotées de 0 à 15.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\28 mdp line vty.PNG

Dans l’exemple, on configure l’accès à distance pour les lignes de 0 à 4.

**Remarque :**

La ligne console porte le numéro 0, ce qui implique que les lignes VTY commence à partir de 1.

On définit le mot de passe « vty ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\28.1 mdp line vty.PNG

On active l’authentification à la connexion.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\28.2 mdp line vty.PNG

## Vérification de la mise en place des mots de passe

La vérification de la mise en place des mots de passe se fait grâce à la commande « show running-config ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\29.1 verif mdp line vty.PNG

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\29.2 verif mdp line vty.PNG

On constate que les mots de passe apparaissent chiffrés, le service «password-encryption » est actif.

**Remarque :**

Il existe une 3ème ligne, la ligne auxiliaire (line aux) sur laquelle il est possible de définir un mot de passe, avec la même méthode que pour les 2 lignes présentées précédemment. Toutefois, cette ligne est de moins en moins utilisée.

## Mise en place des bannières

Les bannières permettent l’affichage de messages destinés aux différents utilisateurs du routeur.

On en distingue 2, la bannière « motd » et la bannière « login ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\22. mise en place d'une bannière.PNG

### La bannière « motd »

La bannière « motd » (Message Of The Day) définit un message qui sera affiché après le démarrage l’équipement. Elle a pour but d’informer toute personne se connectant à l’équipement d’une actualité spécifique ou ponctuelle.

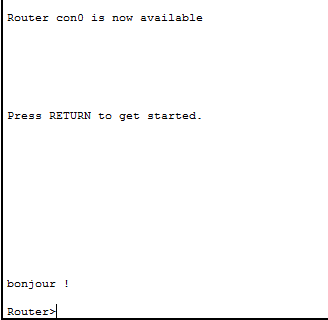
C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\22.1 mise en place d'une bannière - motd.PNG

Dans l’exemple, le message qui sera affiché est « bonjour ! ».

**Remarque :**

Lors de la saisie de la commande d’une bannière, il faut définir un caractère qui délimitera le message à afficher. Dans l’exemple ci-dessus, ce caractère est « ‘’ ».

Il est préférable d’éviter une lettre ou un chiffre. Ce choix risque de couper le message à la première occurrence de la lettre et du chiffre choisit. Le message apparaitra incomplet.



### La bannière « login »

La bannière « login » a pour but d’informer toute personne qui se connecte sur l’équipement des risques qu’elle encourt au cas où elle ne fait pas partie des personnes autorisées à s’y connecter.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\22.3 mise en place d'une bannière - login.PNG

Un exemple de message que l’on peut afficher avec une bannière « login ».

Ce message apparaîtra d’une connexion à distance.

**Remarque :**

Le message est encadré de « ‘’ » qui représente le caractère délimiteur.

# Modification de l’heure

Le réglage de l’horloge s’effectue en mode « enable » avec la commande « clock » suivi de l’argument « set ».

H:\30-11-15\Cisco\Cisco\Captures\Config de base\59 modification de l'heure..PNG

Une fois la commande et l’argument saisis, comme indiqué dans la capture, il faut indiquer l’heure avec le format affiché grâce à l’aide.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\59.1 modification de l'heure..PNG

Suivant le même principe, il faut indiquer le jour puis le mois et l’année suivant les informations affichées par l’aide.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\59.2 modification de l'heure..PNG

L’heure, la date et l’année sont définies.

**Remarque :**

Les mois sont à saisir en anglais.

# Changement du nom des équipements CISCO

Il est possible de modifier le nom de l’équipement grâce à la commande « hostname ».

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\23 changement du nom.PNG

Dans l’exemple, le nouveau « Router1 » est automatiquement pris en compte dans le prompt.

# Configuration d’une interface (routeur)

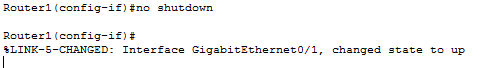
Pour communiquer avec un routeur depuis une machine cliente, il est nécessaire de renseigner au moins une interface manuellement. Cette opération se fait dans le sous mode de configuration dédié à l’interface choisie.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\24 configuration d'un interface.PNG

Une fois dans le sous mode de configuration, on renseigne l’adresse IP attribuée à l’interface, en précisant le masque sous réseau associé.

C:\Users\Administrateur.FORMATI-2M6PQGI\Desktop\Cisco\Captures\Config de base\24.1 configuration d'un interface - adressage.PNG

Il ne reste plus qu’à activer l’interface, avec la commande « no shutdown ».

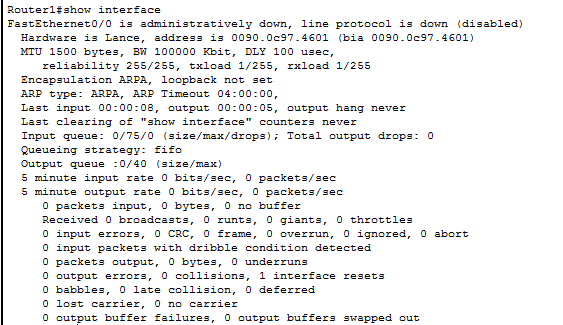


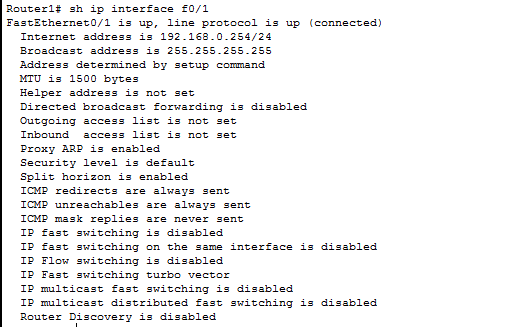
**Remarques :**

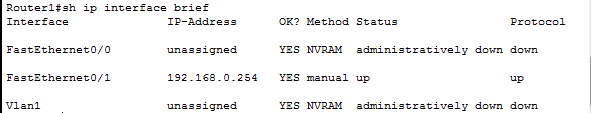
* Par défaut :
* Les interfaces sont inactives sur un routeur,
* Les interfaces sont actives sur un switch.

# Vérification de l’adressage

En modifiant les arguments associés à la commande « show », on peut visualiser les informations relatives aux interfaces. (voir cours CISCO pour les explications)

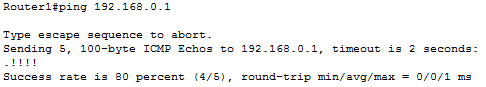






# Vérification de la connectivité

A partir de l’instant où une interface a été adressé, on peut effectuer un test de communication avec les autres machines du réseau. L’utilitaire « ping » est présent par défaut sur les équipements CISCO.



# Configuration du service DHCP sur un routeur

Les routeurs peuvent servir de DHCP dans un réseau. Ce service n’est pas actif par défaut.

## Activation du service

L’activation de ce service se fait avec la commande « ip » suivie de l’argument « dhcp pool » puis le nom que l’on souhaite attribuer à notre place.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\63 dhcp.PNG

Le nom donné au pool est « tsrit ».

Le prompt de la deuxième indique le passage dans le sous-mode de configuration de du dhcp.

## Configuration du DHCP

On définit le réseau, avec la commande « network ».

H:\30-11-15\Cisco\Cisco\Captures\Config de base\64 dhcp.PNG

On indique au routeur les adresses IP à ne distribuer. Dans notre cas, on lui indique la sienne.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\65 dhcp.PNG

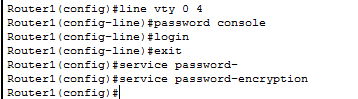
**Remarque :**

On peut indiquer une plage d’adresse IP à ne pas distribuer si cela est nécessaire. La première adresse IP représentera le début de la plage et la seconde la fin de cette dernière.

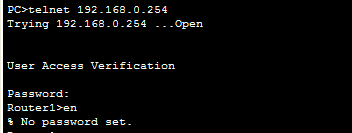
H:\30-11-15\Cisco\Cisco\Captures\Config de base\66 dhcp.PNG

# Configuration de l’accès à distance

## TELNET

Nous avons vu précédemment comment sécuriser l’accès aux lignes VTY. Pour rappel :

Par défaut, TELNET est activé. Tentons une connexion via le poste client (192.168.0.1/24).

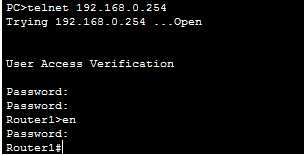


La connexion est impossible.

Il est obligatoire de définir un mot de passe pour l’accès au mode privilège.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\32 Acces telnet mdp enable.PNG

Retentons la connexion



La connexion est active.

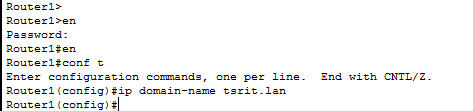
## SSH

Pour activer la connexion en SSH, il faut préalablement et obligatoirement :

* Créer un domaine,
* Générer une clé d’authentification,
* Créer un utilisateur sur le routeur,
* Mettre un mot de passe pour l’accès aux lignes VTY (vu précédemment),
* Activer le transport via le SSH.

### Créer un domaine

La création d’un domaine se fait avec la commande « ip domain-name ».

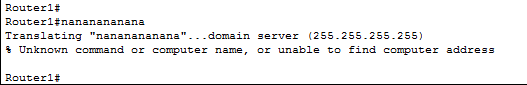


Ici on crée le domaine « tsrit.lan ».

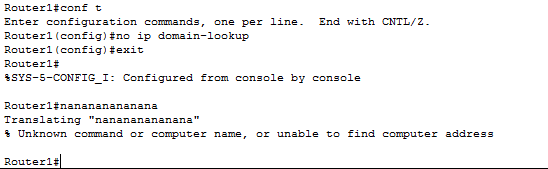
##### Astuce : Désactivation de la recherche DNS automatique.

La commande « no ip domain-lookup » permet de désactiver les requêtes DNS effectuées automatiquement par l’IOS (dans le mode privilège). L’arrêt de la recherche DNS, qui peut paraître assez longue, est utile pour éviter que les recherches DNS suite à une erreur lors de la saisie d’une commande.

Exemple :



Recherche DNS automatique active



Recherche DNS automatique désactivée. La translation a disparu.

Pour réactiver les requêtes DNS automatique, il suffit de saisir la commande sans le « no ».

### Générer une clé de chiffrement

La clé de chiffrement est générée avec la commande suivante :

H:\30-11-15\Cisco\Cisco\Captures\Config de base\37.1 crypto key.PNG

Cette commande retourne un message qu’une clé sera créée pour le domaine « tsrit.lan ». Il invite ensuite à choisir la taille de la clé comprise entre 360 et 2048 bits.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\37.2 crypto key.PNG

Par défaut, la taille de la clé est de 512 bits comme indiqué entre les crochets.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\37.3 crypto key.PNG

On laisse la valeur par défaut, et on observe ce qui se passe.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\37.4 crypto key.PNG

La clé a été créé mais elle ne peut être exportée. Il s’agit d’une clé privée.

Pour vérifier la version de SSH utilisée :

H:\30-11-15\Cisco\Cisco\Captures\Config de base\37.6 crypto key.PNG

SSHv1 présente des vulnérabilités. Activons SSH v2.

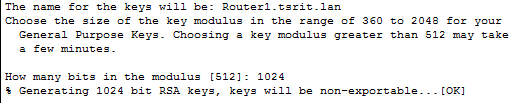
H:\30-11-15\Cisco\Cisco\Captures\Config de base\38 ssh v2.PNG

L’activation de SSH v2 nécessite une clé d’au minimum 768 bits.

**Exercice : Générer une clé de la taille adéquate.**

H:\30-11-15\Cisco\Cisco\Captures\Config de base\39 ssh v2.PNG

Une demande de confirmation de remplacement de la clé existante apparait. Répondre « yes » pour générer la nouvelle clé.



La clé de 1024 est créée.

### Création d’un utilisateur

Nous allons créer un utilisateur sur le routeur afin qu’il puisse se connecter en SSH.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\41  ssh v2.PNG

Ici on crée un utilisateur « user1 » ayant pour mot de passe « user1 ».

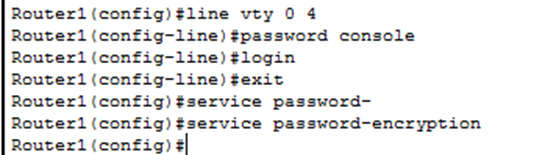
**Remarque :**

Si la taille de la clé n’est pas adéquate, le message, ci-dessous, apparait :

H:\30-11-15\Cisco\Cisco\Captures\Config de base\37.5 crypto key.PNG

### Mise en place du mot de passe pour l’accès via les lignes VTY

Pour rappel :



Après avoir défini le mot de passe, il faut indiquer au routeur qu’une authentification est nécessaire, avec la commande « login ».

H:\30-11-15\Cisco\Cisco\Captures\Config de base\46  ssh v2.PNG

L’option « local » indique au routeur où se trouve la base de données qui sera utilisé pour l’authentification (localisation de l’utilisateur créée précédemment).

### Activation du l’accès via SSH

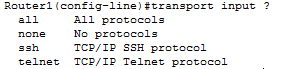
Cette opération se fait à partir du sous mode « line vty » avec la commande « transport ».

H:\30-11-15\Cisco\Cisco\Captures\Config de base\42  ssh v2.PNG

Description des options :

* input : définit le protocole qui sera utilisé pour les connexions entrantes (de l’extérieur vers le routeur)
* ouput : définit le protocole qui sera utilisé pour les connexions sortantes (du routeur vers un autre équipement).

Une fois l’option choisie, on peut définir le protocole que l’on souhaite.



Description des possibilités :

* all : active tous les protocoles,
* none : désactive tous les protocoles,
* ssh : activer le SSH,
* telnet : active Telnet.

Pour activer SSH, il suffit de saisir « ssh » à la suite de la commande.

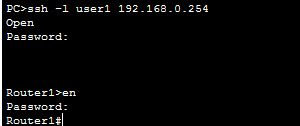
H:\30-11-15\Cisco\Cisco\Captures\Config de base\44  ssh v2.PNG

**Remarque :**

Il est possible d’activer à la fois Telnet et SSH. Dans ce cas, uniquement SSH sera utilisé.

### Connexion

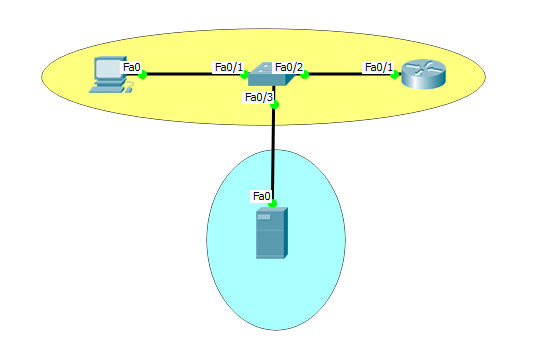
Sous packet tracer, la syntaxe de connexion est : ssh -l {utilisateur} {Adresse IP du routeur}



Une fois, la commande saisie, il suffit de renseigner le mot de passe permettant la connexion des lignes « VTY », puis le mode de passe d’accès au mode privilège.

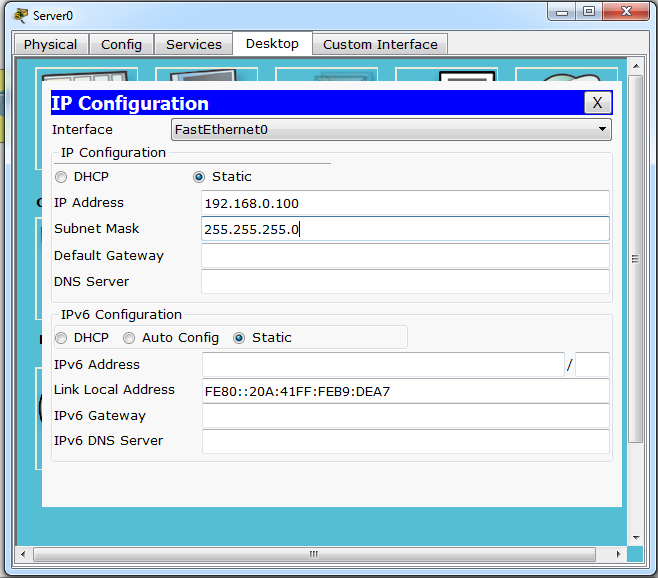
# Sauvegarde sur un serveur TFTP

Une fois notre équipement paramétré, il est important de conserver sa configuration sur un serveur TFTP. On ajoute à notre topologie un serveur TFTP.



### Adressage du serveur TFTP

Première chose à effectuer, fournir au serveur une adresse IP fixe, 192.168.0.100 255.255.255.0.

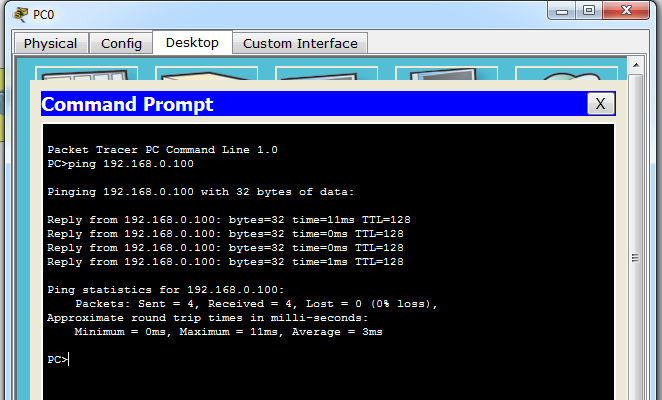


### Vérification de la communication avec le poste client

**Exercice : Effectuer un ping du poste client vers le serveur.**

Il est maintenant possible de sauvegarder notre configuration.

### Sauvegarder de la configuration

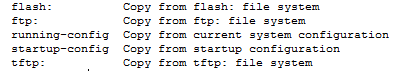
Les opérations de sauvegarde et de restauration de configuration sur un serveur TFTP utilisent la même commande « copy ». La syntaxe de la commande peut être schématiser ainsi :

Router (config)# copy {source} {destination}

Remarque :

C’est le même principe que la sauvegarde de la running-config dans la startup-config, vu précédemment.

Les sources peuvent être :



* flash : pour copier la mémoire flash (sauvegarde de l’IOS),
* ftp : pour restaurer ou importer une configuration sauvegardée ou un IOS à partir serveur FTP,
* running-config : pour sauvegarder la configuration en cours vers un serveur TFTP,
* startup-config : pour sauvegarder la configuration de démarrage vers un serveur TFTP,
* tftp : pour restaurer ou importer une configuration ou un IOS à partir d’un serveur TFTP.

Les destinations sont identiques aux sources. La liste comptera une ligne de moins en fonction de la source choisie.

Nous allons sauvegarder la configuration en cours (running-config) du routeur sur le serveur TFTP.

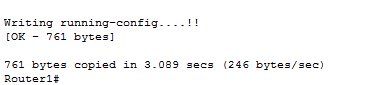
H:\30-11-15\Cisco\Cisco\Captures\Config de base\52  copy vers tftp.PNG

Après avoir saisi la commande, il faut renseigner l’adresse IP ou le nom de la machine hébergeant le serveur TFTP (dans le cas de l’utilisation d’un serveur DNS).

H:\30-11-15\Cisco\Cisco\Captures\Config de base\52.1  copy vers tftp.PNG

Il faut ensuite donner un nom à la configuration. Par défaut, elle se nomme [Router1-config].

Une fois le nom défini, il suffit d’appuyer sur entrée pour lancer l’opération de sauvegarde.



### Vérification de la sauvegarde sur le serveur TFTP

#### H:\30-11-15\Cisco\Cisco\Captures\Config de base\53 tftp sauvegarde ok.PNG

Notre sauvegarde a bien été faite sur le serveur.

# Supprimer la configuration startup-config

La suppression de startup-config se fait à partir du mode privilège avec la commande « erase ».

H:\30-11-15\Cisco\Cisco\Captures\Config de base\54 effacer la startup config.PNG

Une fois saisie, la commande demande une confirmation.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\54.1 effacer la startup config.PNG

Valeur par défaut : confirmer la suppression.

L’IOS indique que la suppression s’est bien déroulée

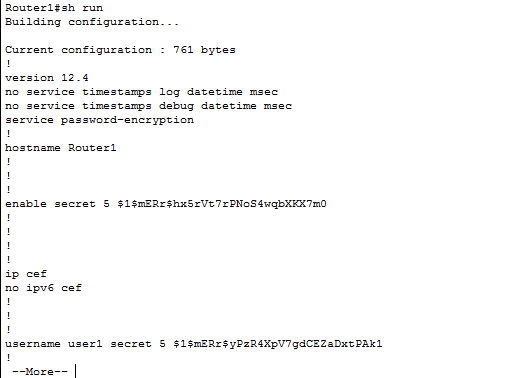
H:\30-11-15\Cisco\Cisco\Captures\Config de base\54.2 effacer la startup config.PNG

On peut le vérifier avec la commande « show startup-config ».

H:\30-11-15\Cisco\Cisco\Captures\Config de base\54.3 effacer la startup config.PNG

Il n’y a plus de startup-config.

Remarque :

Vérifions la running-config 

La running-config n’est pas modifiée. Il faut redémarrer le routeur pour que la startup-config soit appliquée.

#### Redémarrer un équipement

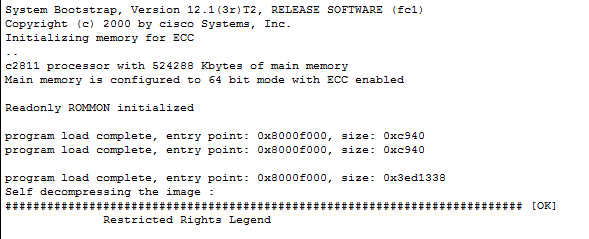
Le redémarrage se fait avec la commande « reload » en mode privilège.

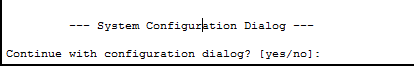
H:\30-11-15\Cisco\Cisco\Captures\Config de base\55 Reboot.PNG

Une confirmation est demandée.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\55.1 Reboot.PNG

Puis le redémarrage s’effectue après la confirmation.



A la fin du redémarrage, on entre dans le mode setup (sortie d’usine) du routeur. 

# Restaurer une configuration sauvegardée sur un serveur TFTP

La procédure de restauration est la même que la sauvegarde.

Il faut indiquer la source (TFTP ou FTP) et la destination (startup-config ou running-config), puis renseigner l’adresse IP ou le nom de la machine hébergeant la sauvegarde.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\56 restaurations.PNG

**Remarque :**

Après le redémarrage, le routeur a repris son nom par défaut « Routeur ». Le pot de passa d’accès au mode privilège a aussi disparu.

On répond aux questions posées.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\56.1 restauration.PNG

Après avoir saisi l’adresse IP, on indique à l’IOS le nom de du fichier à récupérer sur le serveur (« Source filename) et le nom du fichier de destination (ici « running-config », nom par défaut).

H:\30-11-15\Cisco\Cisco\Captures\Config de base\56.2 Restauration Source.PNG

H:\30-11-15\Cisco\Cisco\Captures\Config de base\56.2 restauration.PNG

En appuyant sur entrée, on observe un message indiquant que le processus de récupération est lancé.

H:\30-11-15\Cisco\Cisco\Captures\Config de base\56.3 restauration.PNG

Au bout d’un certain temps, un message d’erreur apparait.

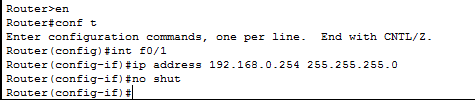
H:\30-11-15\Cisco\Cisco\Captures\Config de base\56.4 restauration.PNG

Ce message indique que la tentative de connexion au serveur à échouer. L’explication est simple.

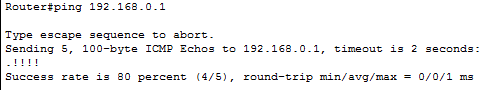
Après avoir effacé la configuration de démarrage et redémarrer le routeur, ce dernier ne peut être contacter via une machine cliente car aucune interface est adressée.

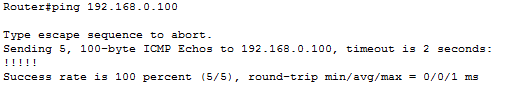
Dans tous les cas, l’administrateur doit renseigner au moins une adresse IP sur une interface pour permettre au routeur de communiquer avec les autres machines.

**Exercice : Adresser l’interface du routeur connectée au commutateur.**

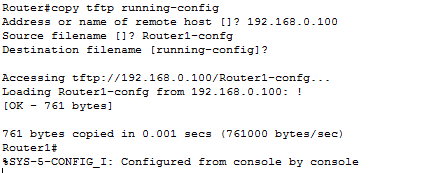
****

Par mesure de précaution, on vérifie que le routeur communique avec le serveur TFTP et la machine cliente.



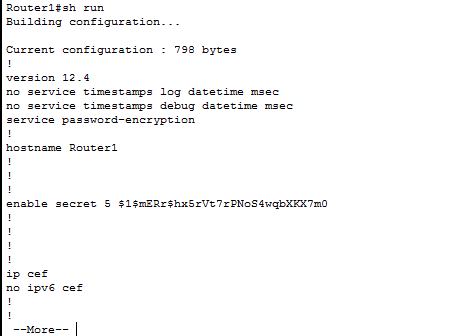


Les machines communiquent entre-elles, on peut procéder à la restauration.

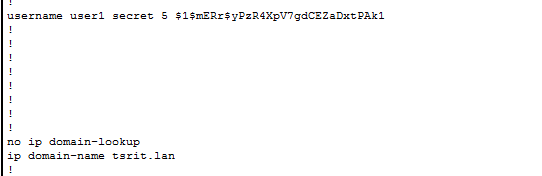


Une fois, la restauration terminée, on voit que le prompt a été modifié. Le routeur s’appelle à nouveau « Routeur1 » comme nous l’avions défini dans les configurations précédentes.

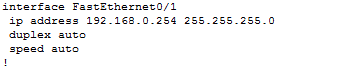
La commande « sh running-config » permet de voir la configuration qui a été appliquée.



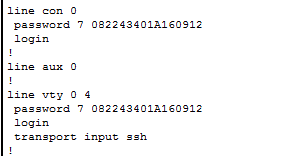
Ici, on remarque que le service « password-encryption » est actif, le nom du routeur (Router1) et le mot de passe chiffré que nous avons renseigné.



Sur cette capture de running-config, on observe l’utilisateur crée sur le routeur avec son mot de passe chiffré, que les requêtes DNS automatiques sont désactivées, et que le domaine se nomme tsrit.lan



L’interface que nous avons adressée pour restaurer la configuration.



Et pour finir, on observe que les lignes permettant l’administration du routeur avec leur mot de passe chiffrés et que le SSH est actif pour les connexions à distance.

# Mise à jour IOS ou changement d’IOS

La procédure pour mettre à jour IOS ou le remplacer est la même que pour une restauration de configuration.

Il faut préalable télécharger l’IOS à jour et le placer sur le serveur de sauvegarde, puis l’importer comme on l’a effectué avec la configuration.

**Remarque :**

Vérifier que l’IOS est compatible les modèles de l’équipement utilisé.