28/08/2024

Atelier 00 – activité 9 - Quel protocole d’administration à distance choisir ?

**Document de l’atelier :**

[Bloc2\_sem3-4\_Atelier-00-activite-1\_Inter-VLAN\_Routing Challenge.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-1_Inter-VLAN_Routing%20Challenge.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-2\_Découverte-NAT-RIP-01.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-2_Découverte-NAT-RIP-01.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-5-Configure-and-Verify-NTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-5-Configure-and-Verify-NTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-6-reconstruction-reseau.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-6-reconstruction-reseau.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut .pka](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut%20.pka)

[Bloc2\_sem3-4\_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-10-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-10-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-11-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-11-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx)

Table des matières

[1. Introduction 2](#_Toc176818008)

[2. Activité à mettre en œuvre 2](#_Toc176818009)

[1.1 Activation/désactivation des interfaces d’administration web 2](#_Toc176818010)

[1.2 Configuration du protocole ssh pour le switch 2](#_Toc176818011)

[1.1.1 Vérification de la prise en compte du protocole ssh par l’IOS 2](#_Toc176818012)

[1.1.2 Configuration du nom d’hôte et du nom de domaine, si ce n’est déjà fait. 3](#_Toc176818013)

[1.1.3 Ajout de mot de passe pour l’authentification au cas où cela aurait été oublié 4](#_Toc176818014)

[1.1.4 Affichage des lignes disponibles. 4](#_Toc176818015)

[1.1.5 Création des mots de passe et configuration de la console et des lignes virtuelles. 5](#_Toc176818016)

[1.1.6 Activation de ssh 6](#_Toc176818017)

[1.1.7 Options ajoutées au service ssh 6](#_Toc176818018)

[1.1.8 Ajout d’un compte administrateur 6](#_Toc176818019)

[1.1.9 Désactivation de telnet pour l’accès au switch 7](#_Toc176818020)

[1.1.10 Vérification de la configuration 7](#_Toc176818021)

[3. Activer l’accès à un routeur via SSH 7](#_Toc176818022)

[1.3 Prérequis 7](#_Toc176818023)

[1.4 Configuration de SSH 8](#_Toc176818024)

[4. TRAVAIL à FINALISER 10](#_Toc176818025)

# Introduction

En général, il y a le choix entre l’administration web sécurisée ou pas (protocole http ou https) et/ou l’administration en ligne de commande sécurisée ou pas (telnet ou ssh).

L’administration du switch en utilisant une interface web peut être pratique. Mais nous choisirons en priorité l’administration du switch en utilisant la ligne de commande pour les raisons suivantes :

* En cas de coupure réseau, il nous faudra intervenir directement sur le switch, donc autant être habitué à travailler en ligne de commande,
* L’interface web peut être moins stable que l’interface en ligne de commande (CLI),
* Les configurations avancées sont souvent disponibles uniquement au travers de la ligne de commande,
* Je vous laisse trouver d’autres arguments…

Pour avoir un compte rendu graphique des objets du switch, nous nous tournerons vers une solution de supervision du réseau qui allie les avantages de la ligne de commande à une présentation graphique des objets du réseau. En général, ces logiciels fonctionnent grâce au protocole SNMP.

Ainsi (revenons au sujet) les interfaces web seront désactivées.

Il nous reste à choisir entre telnet et ssh. Le second étant nettement plus sécurisé que le premier, il est préférable (quand cela est possible) d’activer uniquement ssh sur le switch.

# Activité à mettre en œuvre

## Activation/désactivation des interfaces d’administration web

Les commandes suivantes activent puis désactivent l’administration web non sécurisée et sécurisée.

2960-RG(config)#ip http server

2960-RG(config)#ip http secure-server

2960-RG(config)#no ip http server

2960-RG(config)#no ip http secure-server

## Configuration du protocole ssh pour le switch

### Vérification de la prise en compte du protocole ssh par l’IOS

Tout d’abord, il faut vérifier que l’IOS du switch supporte ssh. La mention k9 (crypto) doit figurer dans le nom de l’IOS.

La commande pour vérifier la version de l’IOS est :

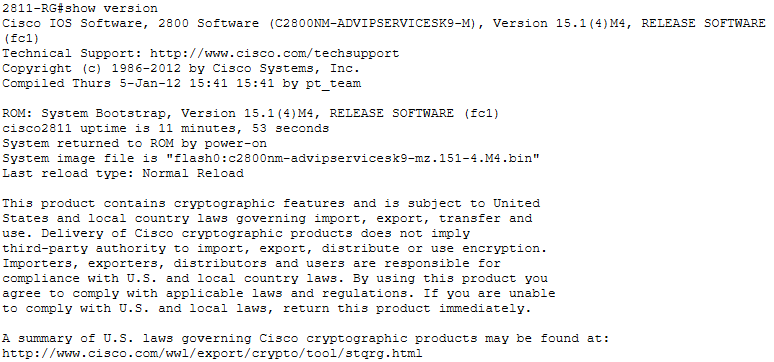
2960-RG#show version

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2010 by Cisco Systems, Inc.

Compiled Sat 07-Aug-10 23:04 by prod\_rel\_team



### Configuration du nom d’hôte et du nom de domaine, si ce n’est déjà fait.

Dans l’exemple, le nom du switch est : *2960-RG* et le domaine est *mondomaine.local*.

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

Switch(config)#hostname 2960-RG

2960-RG(config)#ip domain-name mondomaine.local

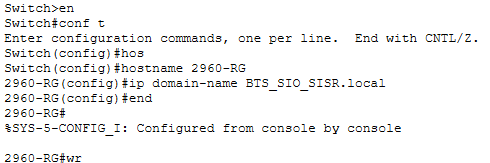
2960-RG(config)#end

2960-RG#wr

Building configuration...

[OK]

2960-RG#

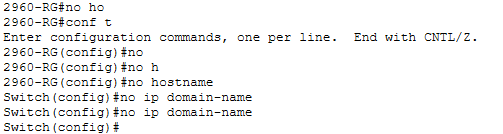


Pour supprimer le nom du commutateur et le nom de domaine, il faut saisir les commandes suivantes.

2960-RG(config)#no hostname

Switch(config)#no ip domain-name

Switch(config)#



### Ajout de mot de passe pour l’authentification au cas où cela aurait été oublié

La connexion au switch s’effectue par le port console en utilisant la ligne associée à ce port ou bien à distance en utilisant les lignes virtuelles (appelées VTY).

Par défaut, il n’y a pas de compte créé pour l’authentification.

Il faut créer au minimum un mot de passe pour l’accès aux différents terminaux (console et virtuel) et un mot de passe pour l’accès au mode privilégié (enable).

Le mode d’administration par défaut est telnet.

Par défaut, les mots de passe apparaissent en clair lors de l’affichage du fichier de configuration. Nous allons donc tout d’abord activer le service *encryption-password*, les mots de passe apparaitront alors chiffrés lorsque les commandes d’affichage de la configuration sont entrées.

Activation du service *password-encryption*

Switch(config)#service password-encryption



### Affichage des lignes disponibles.

On notera la ligne accessible par la console (CTY) et les lignes virtuelles (VTY) pour l’accès distant au switch.

2960-RG#sh line

Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int

\* 0 CTY - - - - - 0 0 0/0 -

1 VTY - - - - - 0 0 0/0 -

2 VTY - - - - - 0 0 0/0 -

3 VTY - - - - - 0 0 0/0 -

4 VTY - - - - - 0 0 0/0 -

5 VTY - - - - - 0 0 0/0 -

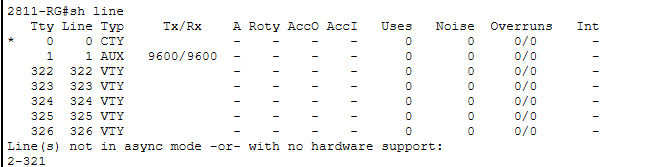
6 VTY - - - - - 0 0 0/0 -

7 VTY - - - - - 0 0 0/0 -

8 VTY - - - - - 0 0 0/0 -

9 VTY - - - - - 0 0 0/0 -

10 VTY - - - - - 0 0 0/0 –



### Création des mots de passe et configuration de la console et des lignes virtuelles.

Un mot de passe est créé pour se loguer aux différentes lignes.

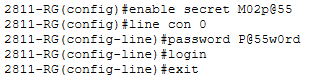
2960-RG(config)#enable secret M02p@55

2960-RG(config)#line con 0

2960-RG(config-line)#password P@55w0rd

2960-RG(config-line)#login

2960-RG(config-line)#exit



2960-RG(config)#line vty 0 15

2960-RG(config-line)#password P@55w0rd

2960-RG(config-line)#login

2960-RG(config-line)#end

2960-RG#



Il y a maintenant un mot de passe à saisir pour l’accès au switch et un mot de passe à saisir pour l’accès au mode avec privilège.

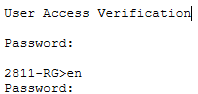
User Access Verification

Password:

2960-RG>en

Password:

2960-RG#





### Activation de ssh

RG-2960(config)#ip ssh version 2



### Options ajoutées au service ssh

- les évènements associés aux connexions ssh sont enregistrés.

- Un timeout de 60 secondes est ajouté pour les sessions ssh en cas d’inactivité.

- Nous laissons trois essais pour la connexion au switch.

clem(config)#ip ssh logging events

sur le routeur qui nous a été demande de maitre il n’est pas possible d’activer la commande :



clem(config)#ip ssh time-out 60

clem(config)#ip ssh authentication-retries 3



### Ajout d’un compte administrateur

clem (config)#service password-encryption

clem (config)#username admin password 0 P@55w0rd



### Désactivation de telnet pour l’accès au switch

clem (config)#line vty 0 15

clem (config-line)#login local

clem (config-line)#transport input ssh



### Vérification de la configuration

2960-RG#show ip ssh

SSH Enabled—version 2.0

Authentication timeout: 60 secs ; Authentication retries: 3

SSH est maintenant activé. Nous pouvons accéder au switch avec un client ssh (par exemple putty pour windows).



1. Était-ce bien utile de mettre un mot de passe pour les ports consoles et telnet ?

Mettre un mot de passe pour les ports console et Telnet pour sécuriser l'accès aux équipements réseau ce qui limite les accès non autorisés et peut protéger contre les attaques.

# Activer l’accès à un routeur via SSH

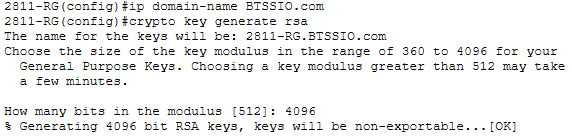
Lorsqu’on veut accéder au CLI (Command Line Interface) d’un routeur on peut soit passer par le port console, soit par telnet soit par SSH. Ici nous verrons comment configurer un routeur pour qu’il soit accessible par SSH.

## Prérequis

Il faut savoir que toutes les versions d’IOS ne supportent pas la configuration SSH. Pour que cela soit possible, il faut disposer des options de cryptographies. Pour vérifier que ces options sont disponibles, passer en mode de configuration globale et tapez la commande suivante :

Router (config)# crypto key generate rsa

Sans autre configuration le routeur devrait vous indiquer qu’il faut avoir au préalable configuré un nom de domaine. Si c’est le cas, tout va bien. Si la commande est inconnue, l’IOS ne supporte pas la cryptographie qui est nécessaire pour la génération des clés de cryptages utilisées par SSH.



## Configuration de SSH

Avant de commencer, nous partons du principe que le routeur est fonctionnel. C’est-à-dire qu’il dispose déjà d’une configuration de base lui permettant de communiquer avec les machines distantes (adresse IP définie sur une interface…).

Voici ce que nous allons faire :

* Définir un nom de domaine au routeur
* Créer un « compte » utilisateur local avec un mot de passe
* Configurer les lignes VTY pour accepter le SSH et utiliser le compte d’utilisateur local
* Générer les clés de cryptages RSA

2611XM> enable

2611XM# configure terminal

2611XM (config)# ip domain-name cisco.lab

2611XM (config)# username sshuser password sshpassword

2611XM (config)# line vty 0 4

2611XM (config-line)# transport input ssh

2611XM (config-line)# login local

2611XM (config-line)# exit

2611XM (config)# crypto key generate rsa

The name for the keys will be: 2611XM.cisco.lab

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

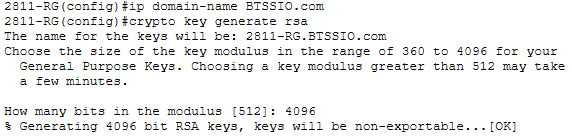
How many bits in the modulus [512]: 1024

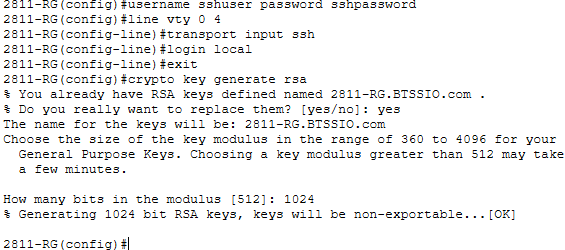
% Generating 1024 bit RSA keys, keys will be non-exportable…[OK]

\*Mar  1 03:28:34.352 : %SSH-5-ENABLED: SSH 1.99 has been enabled

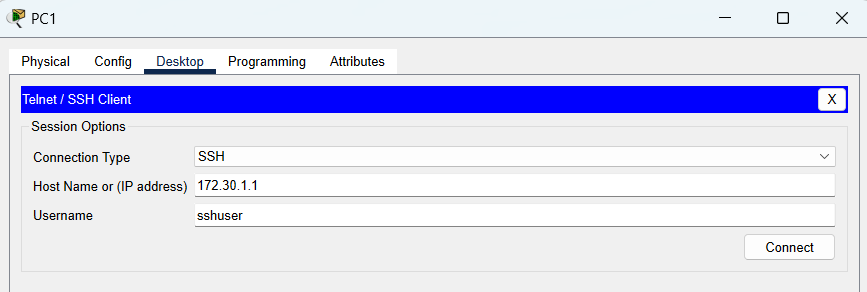
2611XM(config)#^Z

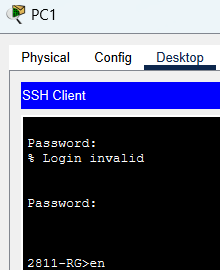
2611XM#





Et voilà, il ne reste maintenant plus qu’à se connecter au routeur en SSH en utilisant le nom d’utilisateur « sshuser » et le mot de passe « sshpassword ».







# TRAVAIL à FINALISER

Le PKT est à réaliser et montrant les modifications effectuées pour les accès administratifs.

Il devrait être de la forme suivante :

