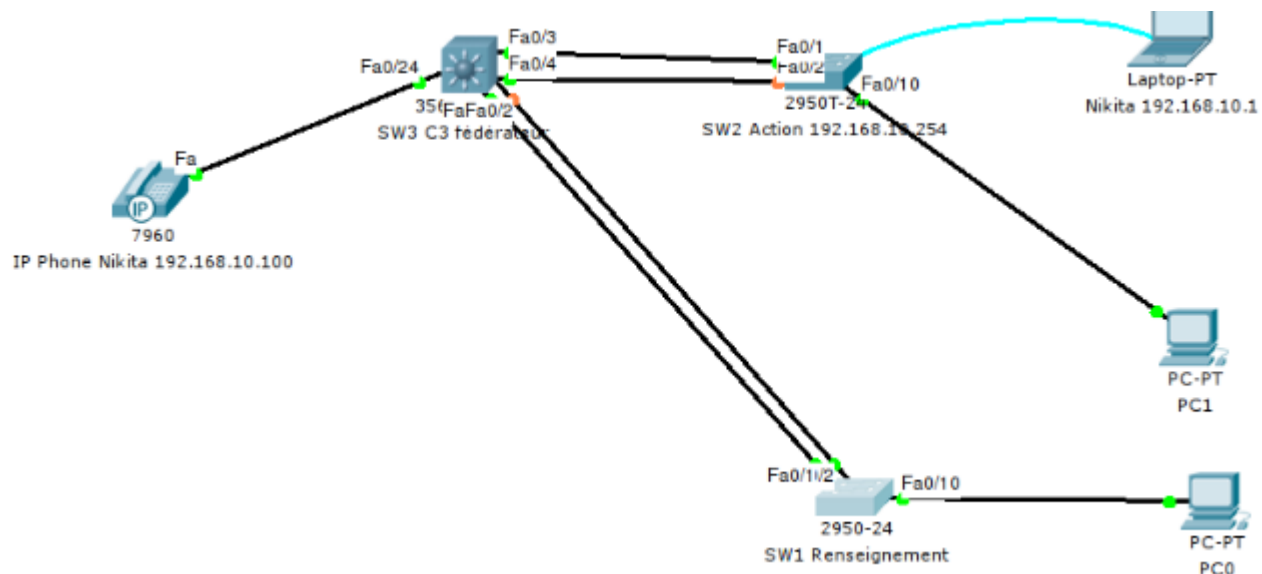


ACCEDER AU SWITCH A DISTANCE VIA LE RESEAU



QUEL PROTOCOLE D'ADMINISTRATION À DISTANCE CHOISIR?

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,

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.**

ACCES PAR TELNET

- 1 - Configurer le portable de Nikita avec l'adresse IP 192.168.10.1/24
- 2 - Faire un ping à destination du switch « Action ». Cela fonctionne-t-il ? Si non, résolvez le problème !!
- 4 - affectez l'interface du switch « Action » au VLAN 2 par les commandes :

```
Action#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Action(config)#int Fa 0/20
Action(config-if)#switchport access vlan 2

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
Action(config-if)#switchport mode access
```

- 5 - vérifiez la communication avec le ping. Réussite ? Si oui, sauvegardez la config du commutateur « Action » en mémoire flash.

- 6 - créez un ou plusieurs administrateurs autorisés à administrer le commutateur :

```
Action#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Action(config)#username nikita password passnik
```

7 - Il y a 5 lignes VTY de 0 à 4 et qui nous permettent d'effectuer 5 sessions telnet simultanées. Nous allons les configurer :

```
Action(config)#line vty 0 4
Action(config-line)#login local
Action(config-line)#
```

8 - Testez si Nikita peut ouvrir une session Telnet depuis son PC portable. Si oui, sauvegardez la configuration du commutateur. Si non, diagnostiquez !

ACCES PAR SSH (Secure SHell)

1 - Vérifier que le switch Action permet bien un accès distant via SSH. Pour cela, il faut vérifier le n° de version de l'IOS : la mention K9 doit figurer dans le nom de l'IOS. Passez la commande :

```
sh version
```

Qu'en concluez-vous ?

2 - Vous avez (normalement!!) conclu que le CISCO 2959T-24 ne supporte pas SSH (sauf mise à jour IOS).

3 - Vérifiez que le commutateur « C3 FEDERATEUR » supporte SSH. Au préalable, Nikita a connecté son notebook à C3 en mode « console ».

4 - Vous avez (normalement !!) conclu que C3 supporte SSH.

5 - Effacez la mémoire flash de C3 et relancez IOS.

6 - Donner le nom « Action » au switch 2.

7 - Donner l'adresse IP 192.168.10.253/24 associé au VLAN 2 du switch « Action ». Cette adresse va nous permettre de l'administrer à distance.

8 - Activer le service « password-encryption » pour pouvoir ensuite mettre des mots de passe chiffrés.

9 - Créer le mot de passe pour l'accès au compte privilégié (enable)

10 - Configurer un mot de passe « console »

11 - Configurez un nom de domaine pour C3 (obligatoire pour mettre en œuvre SSH) :

```
C3(config)#ip domain-name nikita.nikita
```

12 - Enregistrez la configuration de C3.

13 - Création d'une clé de chiffrement RSA longueur 1024

```
C3(config)#crypto key generate rsa
```

14 - Créez un nouvel utilisateur autorisé :

```
C3(config)# username nikita password 0 nikita
```

15 - Activez SSH sur les 5 lignes virtuelles VTY 0 à 4 :

```
C3(config)#line vty 0 4
C3(config-line)#transport input ssh
```

15 - Indiquez que vous voulez travailler avec SSH version 2 :

```
C3(config)#ip ssh ver 2
```

16 - Connectez le portable de Nikita au switch C3 avec un câble Ethernet. Le ping passe-t-il ? Si non, résolvez le problème.

17 - Tentez une connexion sécurisée SSH depuis le portable de Nikita.

From:

/ - **Les cours du BTS SIO**

Permanent link:

[/doku.php/sisr2/accesdistant](#)

Last update: **2013/12/26 18:52**

