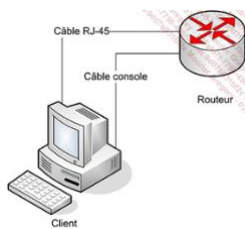


	Réseau Cisco TP n°5 Configuration de l'accès en ssh	BTS CIEL
		Semestre 1 2024_2025

Après la première configuration du routeur réalisée par câble console, le moyen le plus simple d'intervenir sur un routeur est de se connecter à l'aide du protocole Telnet. Cependant, ce protocole n'est pas sûr, les informations d'authentification étant envoyées en clair sur le réseau. Un attaquant pourrait capturer ces informations transmises au routeur et les réutiliser afin d'usurper l'identité de l'administrateur.

Pour éviter ce problème, il est possible d'utiliser le protocole SSH (*Secure SHell*) pour fournir un accès à distance sécurisé au routeur.

Voici le schéma à réaliser :



Réaliser le montage et procéder aux configurations suivantes :

Créer l'utilisateur "snir" avec le mot de passe "cisco" dans la base de comptes locale.

Configurer le protocole SSH ainsi :

- Domaine : "jouvet.local" ;
- Clé RSA de 2.048 bits ;
- SSH version 2.

Configurer une déconnexion automatique de la session SSH au bout d'une minute d'inactivité. Configurer le verrouillage de la session si 2 mots de passe incorrects sont saisis. Supprimer le mot de passe sur les terminaux VTY.

Désactiver le protocole Telnet.

Remarque : Le protocole SSH n'est pas disponible sur toutes les versions du logiciel Cisco IOS ; celui-ci doit disposer des fonctionnalités de cryptographie. Pour savoir quelle version Cisco IOS prend en charge ces fonctionnalités, saisir la commande `show version`, le nom de l'image Cisco IOS doit contenir "K9".