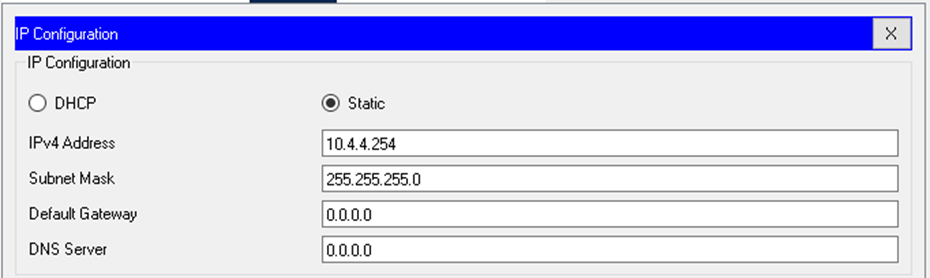
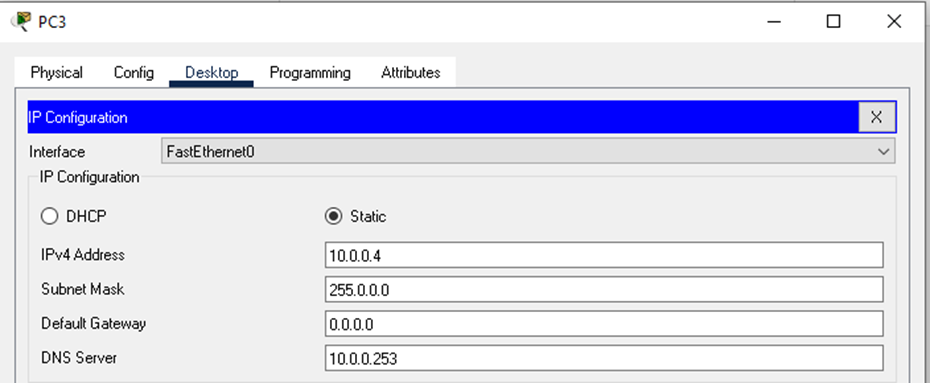
**Identifier les dysfonctionnements du réseau local**

Pour identifier les dysfonctionnements d’un réseau local, il faut regarder :

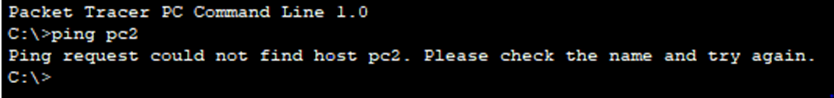
* La configuration des adresses IP, des serveurs Web
* La configuration du serveur DNS



* L’adresse de la passerelle



* Le câblage (ordinateurs, composants…)
* Vérifier la connectivité entre les PC (Par exemple, il est impossible de faire un ping avec le nom du PC -> Il faut le faire avec l’adresse IP



Exemple de dysfonctionnement sur notre TP (Switch déjà configuré) :

Les adresses IP des ordinateurs seront du type : 192.168.100.XY (X : N° du binôme, Y : au choix de 0 à 9) avec le masque par défaut 255.255.255.0.

Configurer l'adressage IP de 2 ordinateurs PC1 et PC2. 192.168.100.51 (5 = numéro du binôme et 1 comme PC1) et masque de sous-réseau par défaut

Connecter PC1 sur gi1/0/3 et PC2 sur gi1/0/2. Tester la connectivité entre les 3 éléments (les 2 ordinateurs et le commutateur). Expliquer.

Faire un ping : Cela ne fonctionne pas car nous sommes sur un vlan différent (gi1/0/2 est sur le vlan 3 et le gi1/0/3 est sur le vlan 4) Nous ne pouvons pas communiquer entre 2 VLANs différents (sauf si on configure un port en mode trunk).

Solution : -> Brancher le PC2 sur un port configuré sur le même VLAN que le PC1

Les conséquences pour les victimes d’une cyberattaque :  
- Perte de disponibilité (système d’information) : empêcher le bon fonctionnement de l’entreprise (peut affecter un site de e-commerce par exemple)

- Perte financière

- Impact sur l’image de l’entreprise : de diffuser des infos personnelles (les noms, les comptes utilisateurs, les courriels et les adresses ainsi que les historiques de navigation de ses clients). Et certaines personnes se sont suicidées suite aux révélations

- Crise pour l’entreprise : plan juridique, informatique, la réputation…