IUT de Cachan LP SARII

TP : NAT/PAT, VPN, VLAN

TP dirigé les 7 et 14 juin 2021

Anthony JUTON
Joëlle MAILLEFERT
Alexandre ‘Tsu’ MANUEL

Table des matières

1. Obligations

- Rédiger le rapport au fur et à mesure de la lecture du sujet
- Suivre les consignes
- Respecter les règles de rendu

2. Généralités

2.1 Questions

Questions	Sur place pendant le TP
Rendu Final	Jour du TP @ 12h30

2.2 La Triche

Les cas de triche seront sévèrement sanctionnés. Les tricheurs verront leur note multipliée par 0 et l'administration sera prévenue.

Tricher veut dire ne pas savoir expliquer votre rendu si on vous le demande. Vous avez en revanche le droit, et êtes même invités à travailler avec vos camarades.

Ne prenez pas le risque de rendre quelque chose que vous ne comprenez pas.

2.3 L'évaluation

Un compte-rendu est à rédiger et à envoyer par mail à la fin du TP.
Vous rédigerez le compte-rendu au fur et à mesure, en fournissant des copies d'écran commentées illustrant les résultats obtenus (symbole 🛠) et en rédigeant les réponses aux questions (symbole ✍).
Il y a 10 questions, ne trainez pas.

2.4 Prérequis

- Connaissances de base sur le fonctionnement des réseaux IPv4 et TCP/UDP :
  - Réseaux publics & privés
  - Masque de sous-réseau
  - Numéro de port TCP/UDP
- Rédaction d'un rapport
- Rendu rigoureux

2.5 Compétences à acquérir

- Configuration du NAT/PAT
- Mise en place d'un VPN « site à site » et d'un VPN « d'accès »
- Mise en place de VLAN
- Réalisation

2.6 Rendu du projet

Vous devrez envoyer votre rapport par mail **avant la fin du TP à 12h30.**

Votre mail devra être constitué comme suit :

Destinataire	`alexandre.th.manuel+lpsarii@gmail.com`
Objet	`[IUTC] [LPSARII] [TP4] Rendu de Prénom Nom`

Contenu	`Bonjour,`
	
	`Vous trouverez en pièce jointe mon rendu pour le TP de NAT/PAT, VPN et VLAN.`
	
	`[…]`
	
	`Cordialement,`
	
	`--`
	`Prénom Nom`

Pièce jointe	`nom.prenom.pdf`

Vous remplacerez :

- Prénom par votre prénom
- Nom par votre nom de famille
- […] par ce que vous voulez

Si vous en avez, remplacez les espaces dans votre prénom/nom par des tirets (-) et retirez les accents dans le nom de la pièce jointe.

**/ ! \ Les deux tirets précédant la signature sont suivis d'un espace. "-- " / ! **

Tout manquement à une de ces règles de rendu entraînera de VIOLENTES pertes de points !

Bon courage à toutes et à tous !

3. Le TP

Le but de ce TP est de mettre en œuvre trois techniques de réseau très couramment rencontrées dans le milieu professionnel :

- **La configuration du NAT/PAT** (Network Address Translation / Port Address Translation), qui permet de rediriger des ports d'une passerelle sur un service spécifique dans le LAN.
- **Les VLAN** (Virtual Local Area Network) qui permettent de créer plusieurs réseaux virtuels sur un même réseau physique.
- **Les VPN** (Virtual Private Network) qui permet de connecter de manière sécurisée des machines distantes à un réseau local.

Ethernet/IP/TCP est omniprésent dans la connexion des ordinateurs sur Internet mais aussi dans le domaine industriel où il domine très largement le marché des bus de supervision.

Ce TP se déroule dans une salle dédiée à l'étude des réseaux. Les prises Ethernet sur les tables sont reliées à une baie de brassage, puis via un switch et un routeur au réseau de l'IUT (voir la figure 1).

Chaque PC est équipé du logiciel gratuit Wireshark pour observer ce qui se passe sur la carte réseau utilisée. Voici le lien pour télécharger ce logiciel : https://wireshark.org

Nous utiliserons aussi les utilitaires *ping, tracert, arp, ipconfig…* (Accessibles via l'invité de commandes), ainsi que des utilitaires accessibles depuis un navigateur WEB.

Pour ouvrir l'invite de commande : Tapez « *cmd* » dans la barre de recherche de Windows (à ouvrir en mode administrateur pour avoir accès à toutes les commandes, clic droit sur l'icône et « *Exécuter en tant qu'administrateur »*).

Ces outils peuvent de même être installés sur un téléphone portable. L'application « *Fing – Outils réseau »* permet d'analyser un réseau efficacement depuis Android.

3.1 Configuration du NAT/PAT : Accès à un service du réseau privé depuis l'extérieur

Dans cette partie, nous allons mettre en œuvre deux procédures permettant d'accéder au réseau local privé depuis l'extérieur. Le support de test sera la fonctionnalité de serveur WEB embarqué dans l'automate. L'objectif est donc qu'un PC extérieur au réseau local qui sera ici client WEB puisse visualiser la page WEB embarquée dans l'automate. On garde le câblage de la figure 1. Cette partie de TP permettra aussi d'aborder la question de la sécurité des réseaux.

La salle est câblée pour cette partie de la manière suivante :

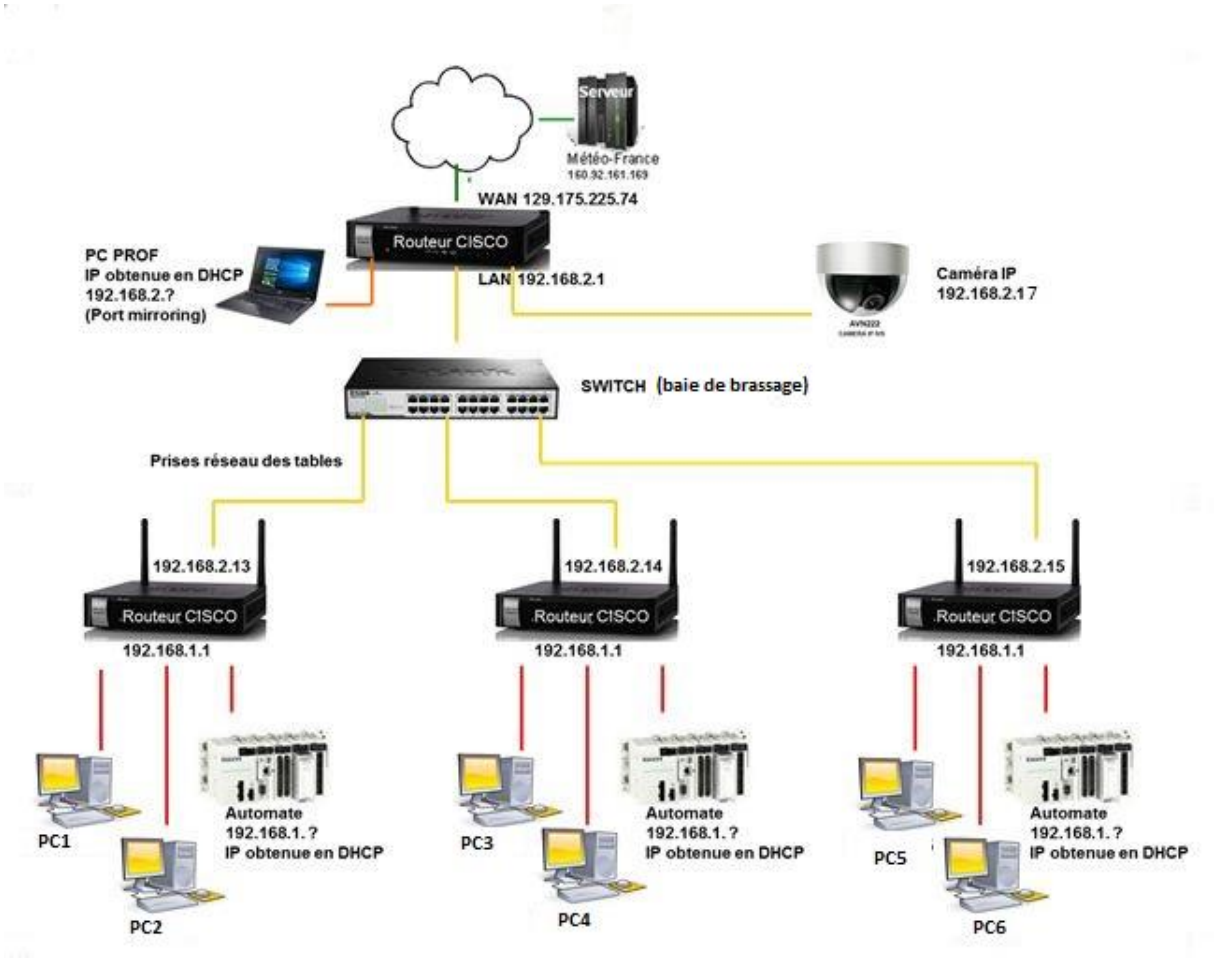

Figure 1 - Architecture du réseau pour la partie NAT/PAT

3.1.1 Supervision locale simple

Pour commencer, on teste le fonctionnement du serveur WEB embarqué dans l'automate en restant dans le réseau local.

L'adresse MAC de l'automate est indiquée près de la prise Ethernet de celui-ci. L'automate est en DHCP.

🛠 Rechercher l'adresse IP de l'automate dans la page d'administration du routeur, menu *Networking>LAN>DHCP Leased Client*.

🛠 Vérifier par un *ping* que la communication avec l'automate est possible. Ouvrir un navigateur WEB du PC local et taper cette adresse dans la barre d'adresse, vérifier que l'on visualise bien le serveur WEB embarqué dans l'automate.

✍ **Q1)** Donner l'adresse IP du PC, quel est le protocole permettant d'afficher la page web interne de l'automate ? Quel est le port utilisé par ce protocole ? **(1 point)**

✍ **Q2)** Un PC situé hors du réseau local peut-il superviser l'automate ? Pourquoi ? **(1 point)**

3.1.2 Redirection de port

Nous allons mettre en place une 1ère solution, non sécurisée, permettant l'accès à l'automate depuis le monde extérieur. Il s'agit de la redirection de port.

✍ **Q3)** Quelle est la seule adresse IP de votre réseau de table (vos PCs, vos automates, votre routeur) visible depuis les autres parties de la salle ? Pourquoi ? **(1 point)**

Pour afficher la page WEB depuis l'extérieur, il faudra taper cette IP dans la barre d'adresse du navigateur :

On configure le routeur pour qu'il redirige vers l'automate toute requête extérieure dont le numéro de port est celui du protocole http (80).

🛠 Mettre en œuvre cette solution, par une configuration du routeur (Menu *Firewall > Port forwarding* du routeur) et en testant l'accès à l'automate depuis un PC extérieur au réseau local.

✍ **Q4)** Cette connexion est-elle sécurisée ? Quel est son autre inconvénient ? **(1 point)**

3.2 Connexion VPN

Il est aussi possible de se connecter depuis l'extérieur sur un LAN, de manière sécurisée, grâce à un réseau privé virtuel (VPN). La sécurisation est faite par le cryptage des données qui circulent en dehors des réseaux concernés. Nous avons vu en cours 2 types de réseau VPN :

- Le VPN **« site to site »** qui permet d'établir une connexion cryptée entre 2 réseaux différents. On l'utilise par exemple lorsqu'une entreprise possède plusieurs sites géographiques.
- Le VPN **« d'accès »** qui permet à une machine extérieure d'accéder à un réseau de façon cryptée. On l'utilise par exemple lorsqu'une personne souhaite accéder au réseau de son entreprise à distance.

Notre routeur CISCO permet, assez facilement, d'établir ces 2 types de VPN. Les parties ci-dessous donnent la solution.

3.2.1 Connexion VPN « site à site »

🛠 Réaliser le câblage de la figure 2. On ajoute donc 3 routeurs supplémentaires dans le but d'établir 3 liaisons VPN. Les automates seront indifféremment un SCHNEIDER ou un WAGO.

🛠 Sur la figure 2 sont indiquées les adresses IP LAN et WAN des routeurs. L'adresse WAN est donnée en DHCP par le routeur de la baie de brassage. L'adresse IP LAN de chaque routeur doit être configurée via la page WEB du routeur. Réaliser cela pour les 3 nouveaux routeurs après avoir fait un « RESET » (voir l'annexe 2). Bien vérifier que chaque routeur est correctement configuré.

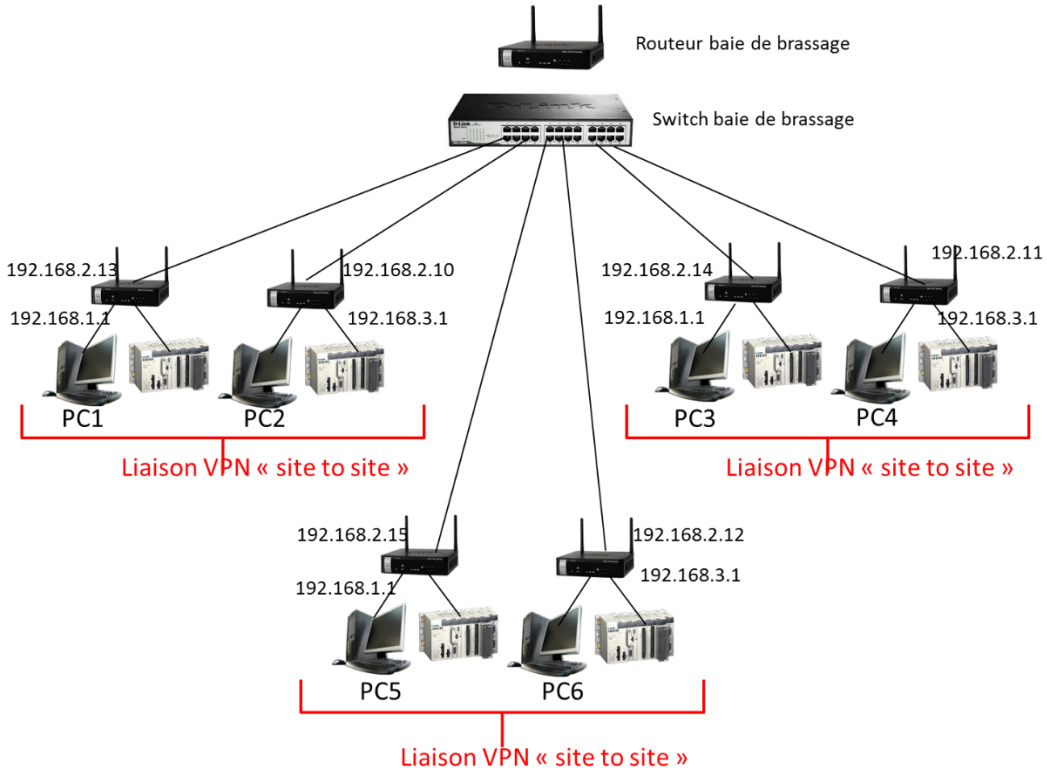

Figure 2 - Architecture du réseau pour la partie VPN site to site

🛠 Suivre ensuite la démarche ci-dessous pour configurer la liaison. Les données sont celles de liaison VPN entre les PC1 et PC2, configurée côté PC2. Il faut bien sûr configurer les 2 routeurs.

La liaison porte un nom (ici « Route1310 ») et nécessite une clé de codage (ici « iutcachan »). Cette clé est utilisée pour crypter les données lors de leur acheminement en dehors des 2 réseaux.

1- Configurer la liaison VPN (Figure 3). Ne pas oublier de sauvegarder.

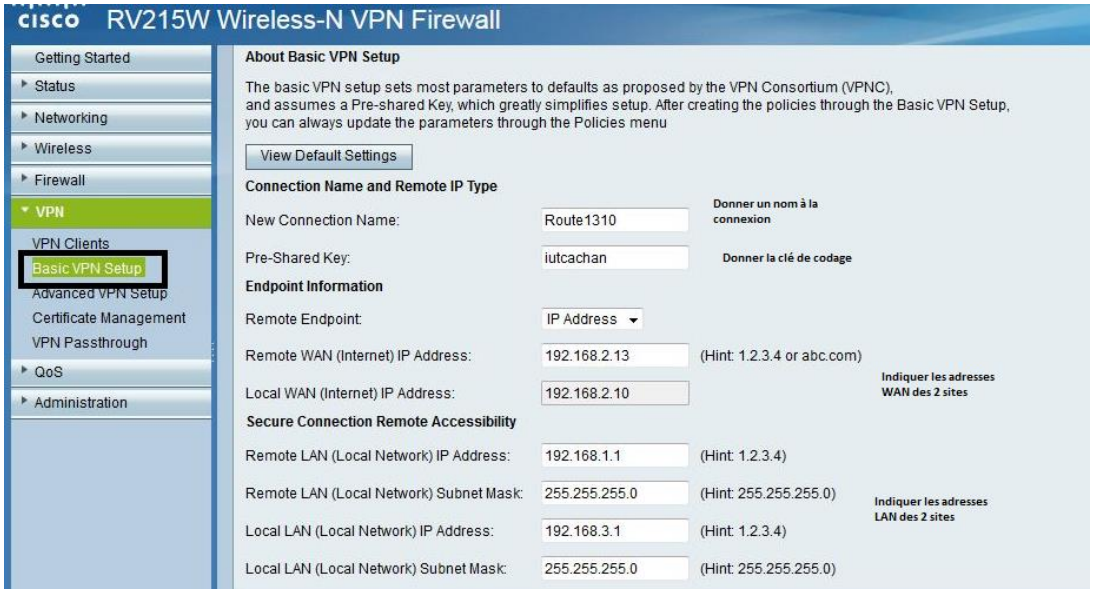

Figure 3 - Configuration de la liaison VPN

2- Lancer la connexion (Figure 4). Ne pas oublier de sauvegarder.

Figure 4 - Démarrage de la liaison VPN

🛠 Vérifier que la liaison fonctionne en faisant un *ping* par exemple du PC1 vers le PC2, ou bien du PC1 vers l'automate 2. On peut aussi visualiser les pages WEB de l'automate local et de l'automate distant.

✍ **Q5)** Faire une capture Wireshark lors du ping du PC1 vers le PC2 par exemple et montrer que les adresses IP de part et d'autre sont visibles « en clair ». **(1 point)**

✍ **Q6)** Faire un schéma représentant les équipements « virtuels » sur votre réseau, en utilisant des couleurs pour la clarté de votre explication. **(1 point)**

🛠 Pour laisser la place nette, effacer la connexion VPN des routeurs.

3.2.2 Connexion VPN « d'accès »

🛠 Réaliser le câblage de la figure 5.

🛠 Sur la figure 5, sont indiquées les adresses IP LAN et WAN des routeurs. L'adresse WAN est donnée en DHCP par le routeur de la baie de brassage. L'adresse IP LAN de chaque routeur doit être modifiée via la page WEB du routeur. Il peut y avoir plusieurs PCs de test dans la salle. Ces PCs seront utilisés pour accéder aux réseaux privés.

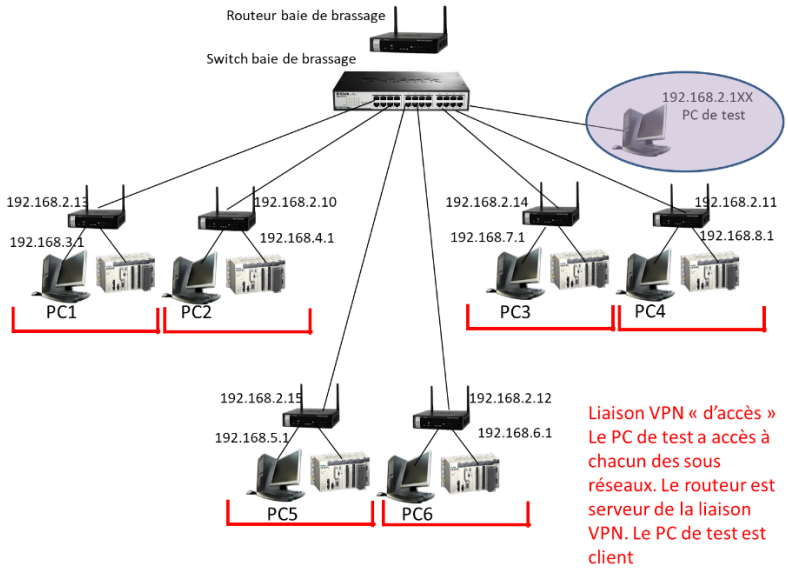

Figure 5 - Architecture du réseau pour la partie VPN d'accès

🛠 Suivre ensuite la démarche ci-dessous pour configurer le routeur du réseau auquel on souhaite accéder. Celui-ci est serveur de la liaison. Nous utilisons le protocole PPTP (Point to Point Tunneling Protocol), produit Microsoft, supporté par notre routeur.

3.2.2.1 Configuration du routeur (Figure 6):

Le nom choisi ici (« VPN_11 ») correspond au réseau d'adresse 2.11 Il peut être modifié.

Les clients sont les machines qui se connectent au réseau privé de l'extérieur.

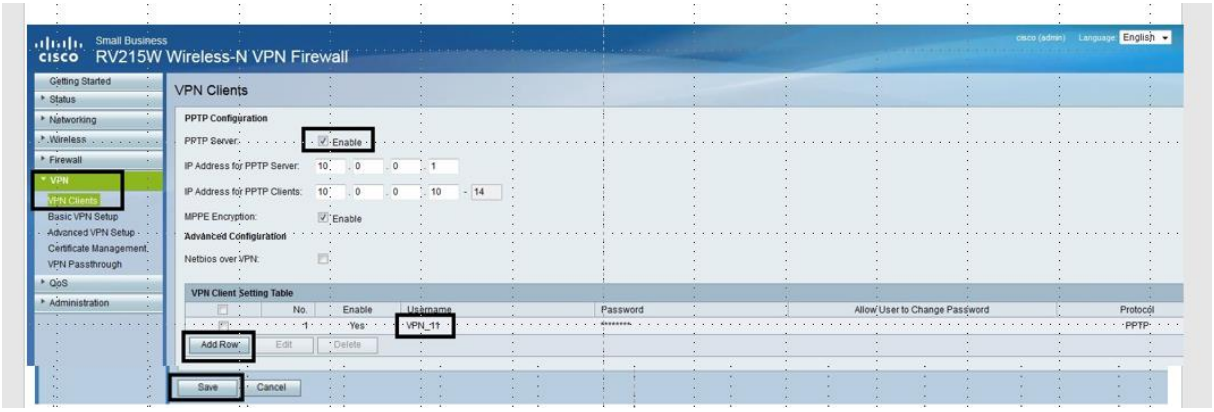

Figure 6 - Configuration du routeur / serveur (1)

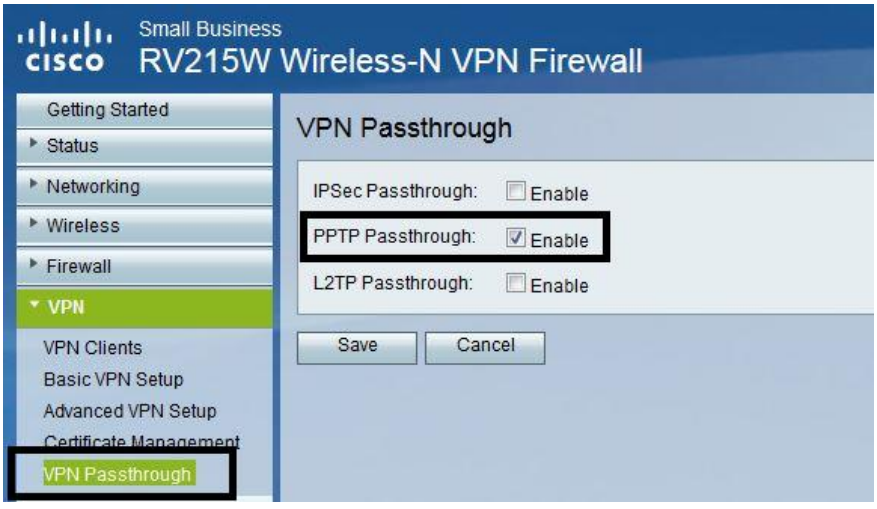

Figure 7 - Configuration du routeur /serveur (2)

On peut vérifier l'état de la connexion (Figure 8) :

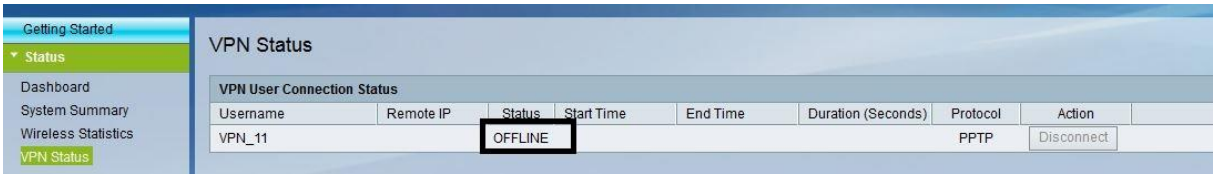

Figure 8 - Etat de la connexion VPN

A ce stade, aucune machine ne s'est encore connectée via le VPN.

3.2.2.2 Configuration du PC client (Figures 9 à 15): (Windows 10 ou 7)

Dans le panneau de configuration, on ouvre la rubrique « Réseau et Internet » puis « Ethernet » puis « Centre Réseau et Partage » . On crée une nouvelle connexion.

Figure 9 - Configuration du client (1)

Figure 10 - Configuration du client (2)

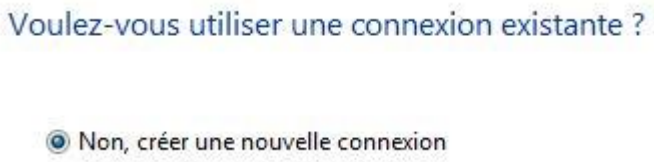

Figure 11 - Configuration du client (3)

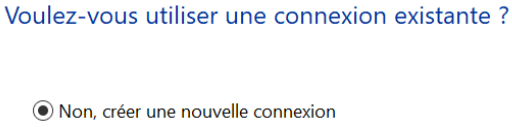

Figure 12 - Configuration du client (4)

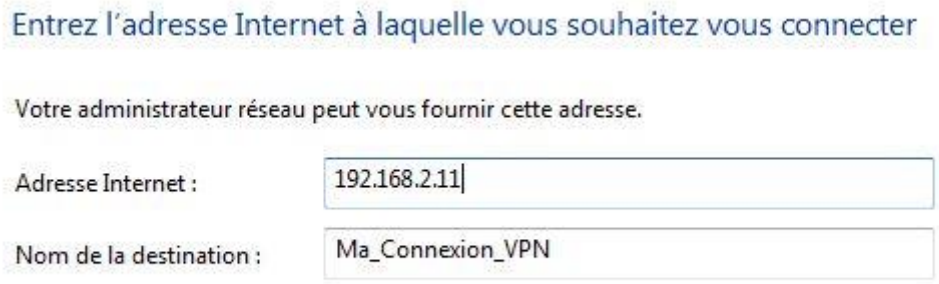

Figure 13 - Configuration du client (5)

Figure 14 - Configuration du client (6)

Figure 15 - Configuration du client (7)

🛠 Via la commande *ipconfig /all* faite avec le PC client, montrer que la connexion VPN existe, et indiquer l'adresse IP virtuelle de la machine (celle pour laquelle elle est reconnue dans le réseau distant).

🛠 On doit voir maintenant, dans le panneau de configuration du serveur que la connexion est établie (Figure 16)

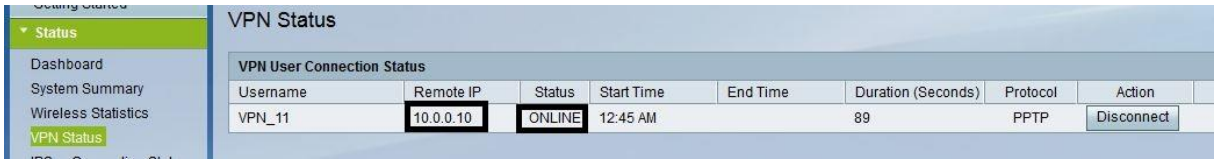

Figure 16 - Connexion VPN établie

✍ **Q7)** Lancer simultanément une capture Wireshark sur le PC client et sur le PC du réseau distant à l'occasion d'un ping de celui-ci depuis le client. Montrer notamment le cryptage des données côté WAN du routeur. **(1 point)**

✍ **Q8)** Faire un schéma représentant les équipements « virtuels » sur votre réseau, en utilisant des couleurs pour la clarté de votre explication. **(1 point)**

3.3 Configuration d'un VLAN

Faire un RESET des routeurs et revenir au câblage de la figure 1 (avec 3 routeurs seulement)

🛠 Dans l'onglet Networking > LAN > VLAN Membership, créer un second VLAN de numéro 3 par exemple. Attribuer 2 ports pour chacun des VLANs, en mode Untagged. Le mode Tagged est réservé pour les machines gérant en interne les VLANs (les téléphones VoIP par exemple). Le VLAN 1 est celui

de l'administration du réseau par exemple et le VLAN 3 celui du contrôle d'accès. Noter la possibilité de faire dialoguer ou non les VLANs entre eux. Bloquer cette possibilité pour l'instant.

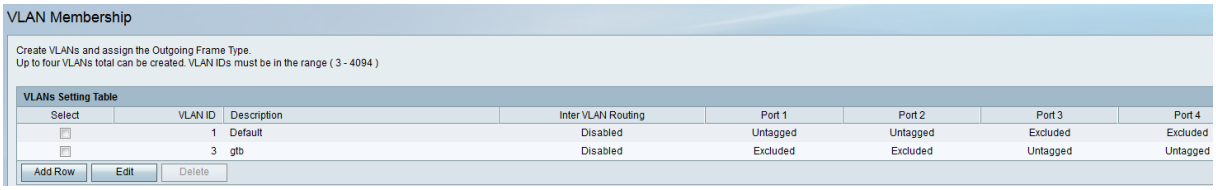

Figure 17 - Configuration du VLAN

Dans LAN Configuration, régler le DHCP pour chacun des VLANs et dans Wireless, attribuer un réseau Wifi par VLAN (voir Figure 18)

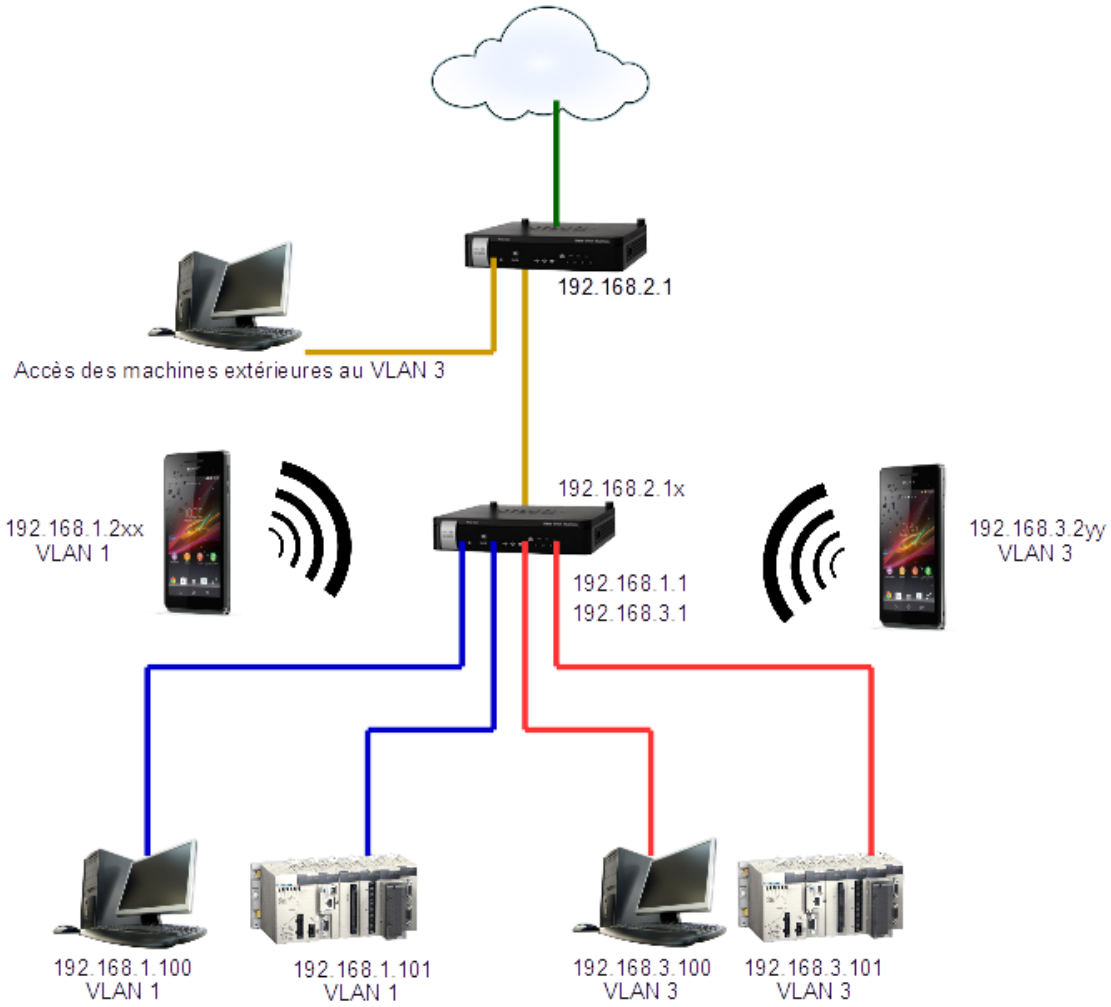

Figure 18 - Architecture du réseau pour la partie VLAN

✍ **Q9)** Expliquer quelle machine a accès au serveur web de l'automate 1.101 et quelle machine a accès à l'automate 3.101. **(1 point)**

✍ **Q10)** Vérifier qu'un équipement WIFI, informé des clés des deux réseaux WIFI, peut choisir d'accéder au VLAN1 ou au VLAN3. L'application FING par exemple permet de scruter les membres du réseau d'un téléphone. **(1 point).**

4. Annexe : réinitialisation du routeur

Si le routeur de votre table a un comportement étrange, s'il ne reconnaît pas le login et le mot de passe, c'est certainement qu'il a été configuré de mauvaise manière. Il faut le réinitialiser. Pour cela, suivre la procédure suivante :

Figure 19 - Photographie du routeur

1. A l'aide d'une pointe de stylo ou d'un tournevis fin, enfoncer le bouton RESET de la face arrière du routeur pendant plus de 10s.

2. Eteindre et rallumer le routeur.

3. L'adresse LAN du routeur est alors 192.168.1.1 et le login/mdp cisco/cisco. Pour bien fonctionner en TP, laisser la carte réseau WAN en DHCP (rubrique Networking/WAN/WAN Configuration). On accède à la page de configuration depuis le LAN par un navigateur web : http://192.198.1.1, login cisco et pwd cisco).

4. Par défaut, le pare-feu du routeur bloque les requêtes entrantes WAN, notamment les *ping*, Il faut donc désactiver cette fonction du pare-feu, dans la rubrique *Firewall>BasicSettings (*Figure 20)

Figure 20 - Configuration du pare-feu du routeur