# TD n° 5 : Configuration d'un pare-feu

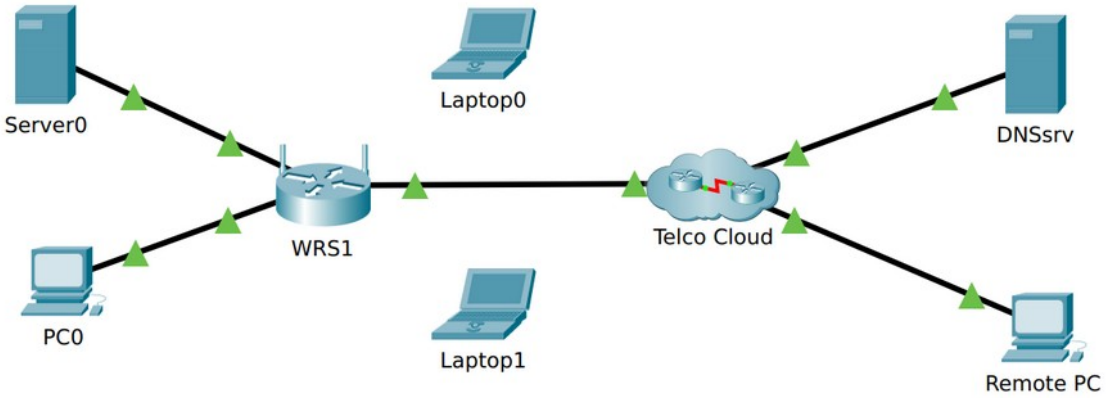
*Rappel : ce TD doit faire l'objet d'un Compte Rendu électronique à déposer sur GitLab avant le début de séance suivante, à l'attention de l'enseignant responsable de votre groupe.*

L'objectif de ce TD est de sécuriser les accès sur un routeur sans fil de type WRT300N, au fonctionnement proche d'une « box » domestique. Nous allons étudier les différentes possibilités offertes : le filtrage par adresse MAC, la configuration d'une zone démilitarisée (DMZ) ou le transfert de port (*Single Port Forwarding*).

## Partie 1 : mise en place du réseau

Le WRT300N comprend un point d'accès Wifi, un commutateur 4 ports Ethernet (interface « LAN ») et un port « routeur » vers Internet.

1. Ouvrir avec Packet Tracer le fichier **`R3.06_TD5.pkt`** correspondant à la topologie suivante :




2. Depuis le navigateur web de **`PC0`**, se connecter à la page de configuration du routeur WRS1, à l'adresse **`192.168.0.1`**
   Utiliser **`admin`** pour le nom d'utilisateur et le mot de passe.

3. Accéder aux paramètres sans fil pour déterminer le **SSID** et la phrase de passe pour la connexion à **`WRS1`** :

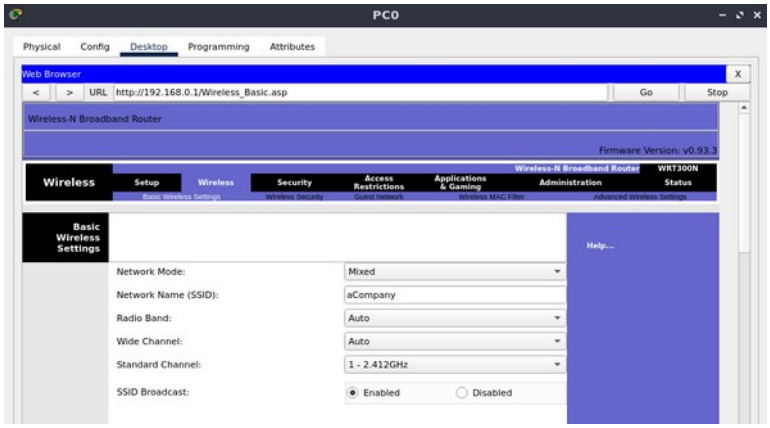



*Figure 1: Onglet 'Wireless' de l'interface du routeur Wifi*

4. Connecter l'ordinateur **`Laptop0`** au réseau sans fil de **`WRS1`** avec ces paramètres de sécurité : Onglet ***Desktop*** > ***PC Wireless*** : appuyer sur ***Refresh*** dans l'onglet ***Connect*** pour faire apparaître les réseaux disponibles …
5. Fermer la fenêtre ***PC Wireless*** et cliquer sur ***Command Prompt***.
6. **Vérifier la configuration IP et MAC** de **`Laptop0`** (à vous de trouver la commande !)


**À quelle adresse réseau cela correspond-il ?**
**Laptop0 peut-il se connecter à Server0 ? Pourquoi ?**

7. Connecter de la même manière **`Laptop1`** au wifi.

# Partie 2 : filtrage MAC et connectivité avec l'extérieur

1. Sur la page de configuration de **`WRS1`**, activer le filtrage MAC pour le wifi.
2. Saisir l'adresse MAC de **`Laptop0`** dans le champ ***MAC01*** (attention au format demandé !). **Valider la modification** en cliquant sur **[SaveSettings]**
3. **Tester la connectivité** en envoyant un ***`ping`*** vers **`192.168.0.1`** à partir de **`Laptop0`** et de **`Laptop1`**.

**Les deux ordinateurs portables ont-ils pu se connecter au wifi de WRS1 ?**
**Peut-on les associer au point d'accès ?**

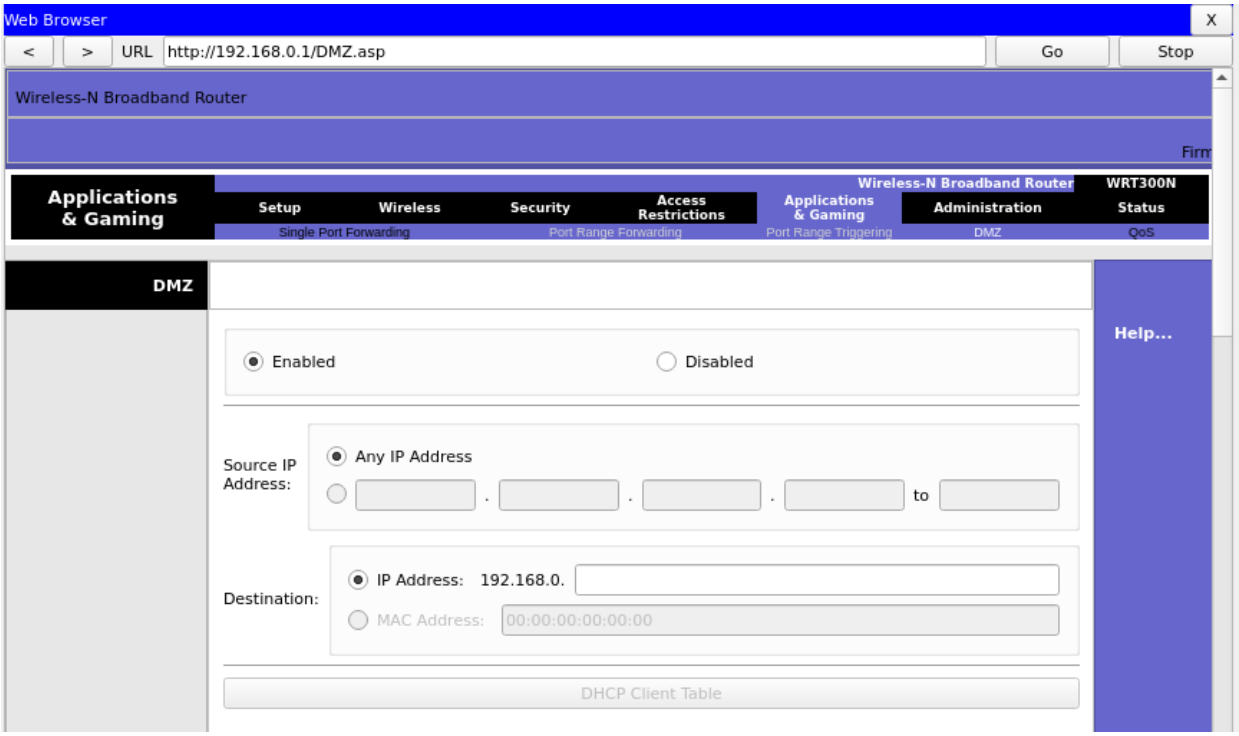
4. Toujours dans le ***Command Prompt*** sur **`Laptop0`, en mode Simulation**, tester la connectivité avec **`Remote PC`** : réitérer la commande jusqu'à obtenir une réponse positive. **Observer les paquets** de type **`ARP`** et **`ICMP`** et l'enchaînement des échanges pendant que le réseau converge.
5. Sur **`Remote PC`**, demander l'affichage de la page d'accueil du site http://www.acompany.com/ : que se passe-t-il ?
6. Vérifier l'adresse du serveur en tapant la commande **`nslookup acompany.com`**

**Pourquoi la demande de page Web du `Remote PC` vers `Serveur0` n'aboutit-elle pas ?**

# Partie 3 : configurer la DMZ

Une zone démilitarisée (DMZ) est une zone où une partie du réseau de l'entreprise est exposée à un réseau externe non fiable, tel qu'Internet.

1. Revenir sur la page de configuration du routeur avec **`PC0`**.
2. Naviguer vers ***Application & Gaming > DMZ***.




3. Cliquer sur ***Enabled***.
4. On veut que **`Server0`** soit accessible via la **DMZ** : compléter en conséquence la configuration ! **Valider la modification** en cliquant sur **[SaveSettings]**
5. **En mode simulation, tester l'accès à http://www.acompany.com/** depuis **`Remote PC`**.

## Est-ce que la demande aboutit cette fois ?

## Qu'observe-t-on dans les paquets IP au passage de WRS1 ?

6. Tester l'accès par ftp : **`ftp acompany.com`** (utilisateur/mdp : cisco/cisco)

## Est-ce que l'accès FTP fonctionne ?

Une fois l'affichage obtenu, **désactiver la DMZ** : nous allons observer une autre technique !

# Partie 4 : configurer le transfert de port

Le transfert de port (*Port Forwarding*) est une technique particulière de NAT, qui est utilisée dans de nombreuses applications : consoles ou serveurs de jeu vidéo, protection contre les attaques externes (DDOS par exemple), accès distant à des caméras IP ou d'autres équipements internes …

Cette technique vient compléter (ou remplacer) le mode DMZ : le transfert d'un seul port (Single Port Forwarding) permet de n'exposer qu'une seule application (serveur) en n'autorisant les connexions externes seulement vers le port TCP/UDP correspondant.

1. À nouveau sur la page de configuration du routeur avec **`PC0`**, naviguer vers ***Application & Gaming > Single Port Forwarding***
2. Activer le transfert de port pour le protocole **HTTP** à destination de **`Server0`** ; **valider la modification** en cliquant sur **[SaveSettings]**.
3. Tester l'accès à la page d'accueil du site http://www.acompany.com/ depuis **`Remote PC`**.
4. Tester l'accès par ftp : **`ftp acompany.com`**

### Est-ce que l'accès HTTP fonctionne ?

### Est-ce que le FTP fonctionne ? Pourquoi ?

5. Pour confirmer, essayer l'accès FTP depuis **`PC0`** ...