

Systeme & Réseau TD

**INSA** INSTITUT NATIONAL  
DES SCIENCES  
APPLIQUÉES  
ROUEN

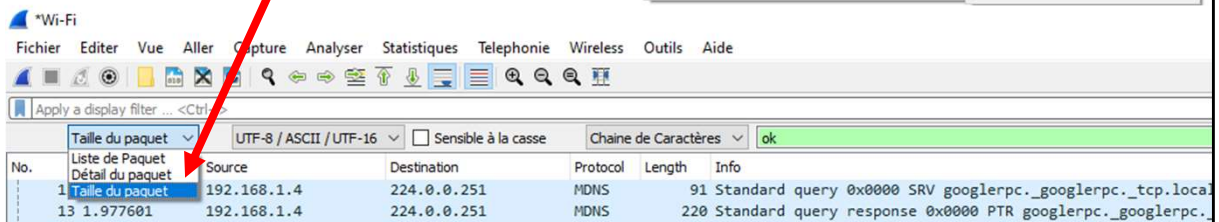
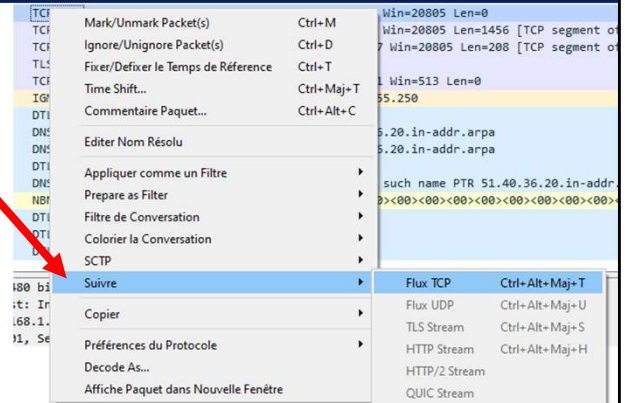


[www.wooclap.com/KFOQIR](http://www.wooclap.com/KFOQIR)

# Suivre un flux avec Wireshark

Astuce Wireshark 1 : sur une trame, utiliser clic droit / suivre / flux tcp pour suivre toute la conversation

Astuce Wireshark 2 : pour rechercher une chaine dans toute le dialogue, Choisir Détail du paquet



# Exercice de recherche

Recherche d'informations  
sur un ensemble de  
protocoles



Application  
+  
Présentation  
+  
Session

Transport

Réseau




Liaison  
de données

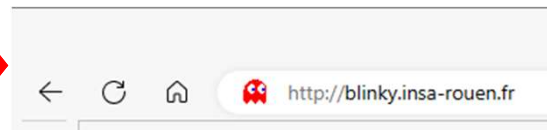
Physique



## Analyse : Préparation VERSION

5



- Ouvrir un navigateur Web (Firefox par exemple) 
- Lancer une nouvelle capture Wireshark 
- Sans utiliser un moteur de recherche , utiliser le navigateur pour afficher le site  
**<http://blinky.insa-rouen.fr> !!** 
- Stopper la capture Wireshark
- Indiquer que vous êtes prêt dans Wooclap



wooclap



**Lancer « au rythme du participant... »**

- 1) Quelle est l'adresse IP du site blinky.insa-rouen.fr 
- 2) Quel protocole (nom + protocole de transport + port) est à l'origine de cette conversion ?
- 3) Par quoi débute le dialogue avec le serveur hébergeant blinky.insa-rouen.fr ?
- 4) Quel(s) protocole(s) + port(s) sont utilisés durant ce dialogue ?
- Répondre aux questions Wooclap à votre rythme 

#### Astuces Wireshark :

- Ctrl+F permet de chercher une chaîne de caractères
- Un clic droit sur une trame permet de suivre un flux



L'adresse IP de blinky.insa-rouen.fr est le 172.29.8.9

La conversion s'est effectuée avec le protocole DNS, utilisant le protocole de transport UDP sur le port 53.

Dans Wireshark, on peut retrouver la première trame du DNS avec CTRL+F 'chaîne de caractère' + 'insa-rouen'.

Le dialogue avec le serveur web peut être filtré en utilisant le menu conversation, et en retrouvant le dialogue entre votre IPv4 et celle du serveur, ensuite un clic droit permet de transformer cette ligne en filtre qui n'affichera que le dialogue avec le serveur Web.

Le dialogue débute par une connexion CTP en 3 étapes nommée '3 way handshake'. Ensuite le dialogue se fait d'abord en protocole HTTP, sur le protocole de transport TCP et vers le port 80.

## Elément de correction TD ( questions 1 et 2)

En cherchant le mot blinky dans les paquets envoyés il est possible de trouver une première trame qui fait référence au protocole DNS.

Il utilise le protocole de transport UDP avec en destination le port 53

The image shows a Wireshark packet capture of a DNS query. The packet list on the left shows a packet at time 11.921440 from source 192.168.1.24 to destination 192.168.1.254, identified as a DNS packet. The packet details pane on the right shows the structure of the packet. The 'User Datagram Protocol' section is highlighted in green, showing 'Src Port: 56955' and 'Dst Port: 53'. The 'Domain Name System (query)' section is highlighted in yellow, showing 'Transaction ID: 0xe138', 'Flags: 0x0100 Standard query', 'Questions: 1', and the query details for 'blinky.insa-rouen.fr: type A, class IN'. The packet bytes pane on the right shows the raw data of the packet.

La zone en vert correspond à la couche de transport

La zone jaune correspond à la partie 'dialogue DNS' de notre trame

**ATTENTION** : Les captures d'écrans affichées sur les pages de correction n'ont pas été réalisées à l'INSA et vont afficher des adresses IP différentes du TD

La réponse n'est pas affichée ici mais dans la trame de réponse du DNS et donnera l'adresse IP 172.29.8.9 pour l'hôte blinky.insa-rouen.fr

Attention, lors du TD il y a eu parfois confusion, les adresses IP qui s'affichent sur la trame capturée, que cela soit lors de la question (comme ici) ou lors de la trame de réponse du serveur DNS sont les adresses du demandeur et du serveur DNS, en aucun cas l'adresse recherchée.

L'adresse se retrouve dans la partie DNS de la trame, ici avec le fond jaune.



## Elément de correction TD ( question 3)

La zone jaune

Début de dialogue avec le serveur Web en TCP

Début de la consultation de la page Web en HTTP

Sur cette capture Wireshark de consultation de la page Web du TD,  
le PC client utilise l'adresse IP 192.168.1.22 et le serveur est en 192.168.1.24

J'utilise un filtre Wireshark pour ne conserver à l'écran que le dialogue entre les deux hôtes

ip.addr==192.168.1.22 && ip.addr==192.168.1.24

La première ligne de dialogue trouvée utilise le protocole de transport TCP.  
Aucune couche supérieure n'est visible ! Il n'y a donc aucune application (Niveau 7) d'impliquée.

Le dialogue visible dure sur 3 échanges, il ne nomme le 'Three Way Handshake'

Trame 19, le client demande une connexion **[SYN]** au serveur sur son port 80 à partir de son port 54516

Trame 20, le serveur répond sur le port indiqué trame 19, avec un accusé de réception de la demande **[ACK]**

tout en demandant lui aussi une demande de connexion TCP **[SYN]** au client pour assurer les échanges de données.

Trame 21, le client accepte la demande de connexion du serveur **[ACK]**

## Elément de correction TD ( question 4)

No.	Time	Source	Destination	Protocol	Length	Info
22	1.56...	192.168.1.22	192.168.1.24	HTTP	419	GET / HTTP/1.1
23	1.57...	192.168.1.24	192.168.1.22	HTTP	613	HTTP/1.1 200 OK

> Frame 22: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface wlo1, id 0

> Ethernet II, Src: IntelCor\_42:09:3c (2c:db:07:42:09:3c), Dst: IntelCor\_3a:ac:0f (4c:1d:96:3a:ac:0f)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.24

> Transmission Control Protocol, Src Port: 54516, Dst Port: 80, Seq: 1, Ack: 1, Len: 365

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: 192.168.1.24\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/112.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n

Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

[Full request URI: <http://192.168.1.24/>]

[HTTP request 1/2]

[Response in frame: 23]

[Next request in frame: 28]

La zone jaune

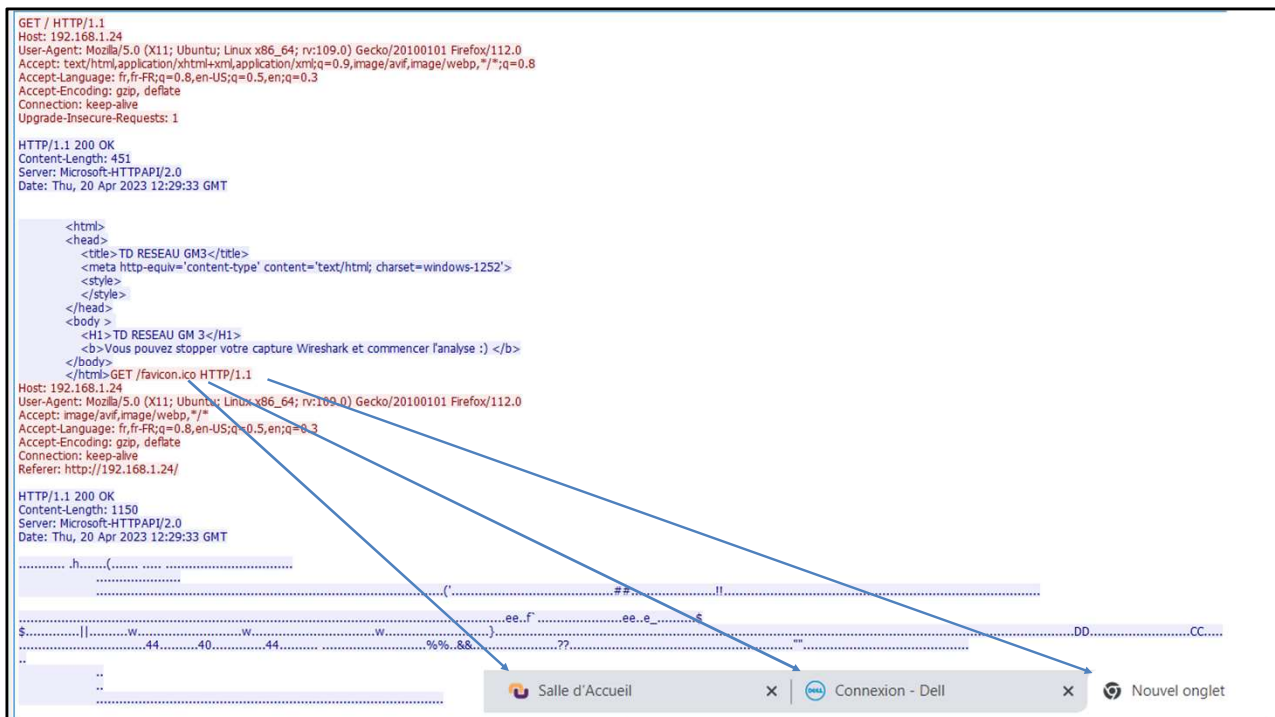
Début de dialogue avec le serveur Web en TCP

Début de la consultation de la page Web en HTTP

A partir de la trame 22 commence le dialogue HTTP : HyperText Transfert Protocol  
La commande envoyée par le Firefox est un GET / HTTP/1.1 qui peut se comprendre par 'Je souhaite obtenir la page web du dossier racine (/)'

Le protocole de transport utilisé est bien sur TCP avec les ports vus précédemment.  
Si l'on affiche le contenu de la demande HTTP, des éléments qui auraient du appartenir à la couche 'session' (Connection keep alive par exemple) et 'présentation' (accept language fr ...) sont visibles mais noyés dans la couche 7 application.

Trame 23, le serveur répond avec le code 200 OK.



Avec Wireshark, il est possible de SUIVRE un dialogue, voici ce qui s'affiche avec un clic droit sur la trame 22 en choisissant SUIVRE puis FLUX HTTP

En rouge, ce qui vient du PC client et en bleu du serveur Web.

A noter : la page web, en général contenue dans un fichier texte, s'affiche après le dialogue lié au protocole HTTP (de HTTP/1/1 200 OK à la ligne date) elle débute par le texte <html> et se termine par la ligne </html>

Les navigateurs demandent automatiquement si une icone nommée favicon.ico est disponible pour illustrer la page web dans le navigateur (demande en rouge avec les flèches)

# Utilisation de service

Interroger le DNS

Application  
+  
Présentation  
+  
Session

Transport

Réseau

Liaison  
de données

Physique

## Utilisation du DNS

13

L'analyse permet de trouver le protocole DNS (Domain Name System)

L'outil en ligne de commande **nslookup** permet d'interroger un serveur DNS

- Pour voir le serveur DNS utilisé par la carte réseau :  
Linux : saisir **resolvectl status**  
Windows : saisir **IPCONFIG /ALL**
- Saisir **nslookup**, le serveur DNS par défaut est affiché
- Saisir **moodle.insa-rouen.fr** et analyser le résultat



Sous Linux il est aussi possible d'utiliser la commande **dig** pour interroger les DNS.

## Utilisation du DNS

Exemple de résultat effectué lors du TD connecté au 'TdREseauGm3':

nslookup	
Serveur par défaut : dlinkrouter.tdgm	Indication du serveur DNS par défaut (ici notre 'box')
Address: 192.168.4.254	Adresse IP du serveur DNS
> moodle.insa-rouen.fr	<a href="#">Informations sur la demande</a>
Serveur : dlinkrouter.tdgm	le serveur dns se nomme dlinkrouter du domaine tdgm
Address: 192.168.4.254	Il ne fait autorité que pour les demandes en .tdgm
	<a href="#">Informations sur la réponse</a>
Réponse ne faisant pas autorité :	Indique que le DNS à sous traité la demande a un autre DNS
Nom : moodle-2018.insa-rouen.fr	Nom réel de la demande (l'enregistrement A)
Address: 193.49.10.217	Adresse IP de la demande
Aliases: moodle.insa-rouen.fr	Indique l'utilisation d'un CNAME DNS

Notre 'box' regroupant un ensemble de fonctions, elle fait aussi office de serveur DNS.

L'adresse IP 192.168.4.254 se retrouve tout au long des TD mais dans le cadre d'une infrastructure plus importante les services (DHCP, DNS par exemple) seraient hébergés sur des serveurs distincts.

Le domaine DNS de notre box se nomme tdgm et la box porte le nom dlinkrouter, son FQDN est dlinkrouter.tdgm. Ce serveur DNS ne fait autorité que pour les hôtes de ce domaine.

Nous n'avons pas utilisé cette possibilité lors des TD car nous avons utilisé les adresses IP directement.

## Utilisation du DNS autorité pour insa-rouen.fr

### Interrogation d'un autre serveur DNS

```
> server 194.254.19.131
```

```
Serveur par défaut : ns.insa-rouen.fr
```

```
Address: 194.254.19.131
```

La commande server permet de changer de serveur DNS

ns.insa-rouen.fr est le serveur principal de l'établissement

Le serveur se nomme ns dans le domaine insa-rouen.fr

```
> moodle.insa-rouen.fr
```

```
Serveur : ns.insa-rouen.fr
```

```
Address: 194.254.19.131
```

[Informations sur la demande](#)

```
Nom : moodle-2018.insa-rouen.fr
```

```
Address: 193.49.10.217
```

```
Aliases: moodle.insa-rouen.fr
```

[Informations sur la réponse](#)

Nom réel de la demande (l'enregistrement A)

Adresse IP de la demande

Indique l'utilisation d'un CNAME DNS

# Exercice de curiosité

Mon PC est-il bavard ?



Application  
+  
Présentation  
+  
Session

Transport

Réseau

Liaison  
de données

Physique



## Les demandes invisibles



Objectif : chercher des requêtes DNS non demandés par l'utilisateur

Pour que cette analyse soit pertinente, votre PC ne doit pas avoir d'autre activités

- Fermer votre navigateur WEB 
- Avec Wireshark, saisir le filtre d'affichage DNS et faire une nouvelle capture 
- Ouvrir votre navigateur Web et attendre que la page vide s'affiche 
- Il y a-t-il eu des requêtes DNS ? 

Vous pouvez réaliser cette expérience chez vous, en fermant le maximum d'applications ouvertes, en général vous pouvez voir que des requêtes DNS multiples

## Test sur le site www.tf1.fr

Liste des demandes dns effectuées lors de la connexion à la page web www.tf1.fr

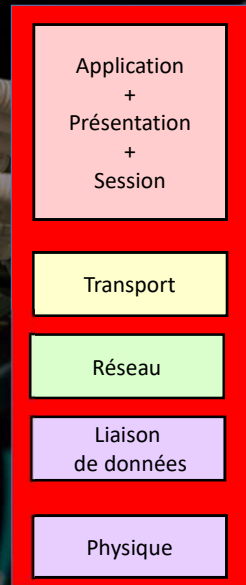
Sans surprise, facebook et google sont utilisés

dns.qry.type == 1 && !(dns.flags.response == 1)									
No.	Time	Source	Destini	Protocol	Length	Info			
30	9.3...	17...	19...	DNS	70	Standard query 0xa343 A www.tf1.fr			
43	9.3...	17...	19...	DNS	70	Standard query 0x2d25 A www.tf1.fr			
...	9.4...	17...	19...	DNS	78	Standard query 0x1544 A cdns.eu1.gigya.com			
...	9.4...	17...	19...	DNS	73	Standard query 0x57a3 A api.ipify.org			
...	9.4...	17...	19...	DNS	78	Standard query 0x0ad3 A ariane.abtasty.com			
...	9.4...	17...	19...	DNS	86	Standard query 0xc19a A s3-eu-west-1.amazonaws.com			
...	9.4...	17...	19...	DNS	75	Standard query 0x9958 A try.abtasty.com			
...	9.5...	17...	19...	DNS	80	Standard query 0x53c8 A cdn.tagcommander.com			
...	9.5...	17...	19...	DNS	80	Standard query 0xe474 A connect.facebook.net			
...	9.5...	17...	19...	DNS	76	Standard query 0x1b11 A www.facebook.com			
...	9.5...	17...	19...	DNS	86	Standard query 0x4976 A privacy.trustcommander.net			
...	9.5...	17...	19...	DNS	73	Standard query 0xa780 A photos.tf1.fr			
...	9.5...	17...	19...	DNS	78	Standard query 0xb824 A apps.identrust.com			
...	9.6...	17...	19...	DNS	82	Standard query 0xeb59 A cdn.trustcommander.net			
...	9.6...	17...	19...	DNS	85	Standard query 0x6c5d A dcinfos-cache.abtasty.com			
...	9.6...	17...	19...	DNS	73	Standard query 0xd17b A compte.tf1.fr			
...	9.6...	17...	19...	DNS	74	Standard query 0x429d A w.usabilla.com			
...	9.7...	17...	19...	DNS	91	Standard query 0x7533 A content-autofill.googleapis.com			
...	10...	17...	19...	DNS	86	Standard query 0xbf3c A static.adsafeprotected.com			
...	10...	17...	19...	DNS	78	Standard query 0x9482 A cdns.eu1.gigya.com			
...	10...	17...	19...	DNS	73	Standard query 0x3861 A via.batch.com			
...	10...	17...	19...	DNS	87	Standard query 0x8281 A safebrowsing.googleapis.com			
...	10...	17...	19...	DNS	77	Standard query 0x6e46 A js.sentry-cdn.com			
...	10...	17...	19...	DNS	77	Standard query 0x1975 A cdn.facil-iti.app			
...	10...	17...	19...	DNS	74	Standard query 0x6e17 A prof.estat.com			
...	11...	17...	19...	DNS	75	Standard query 0x90c9 A apis.google.com			
...	11...	17...	19...	DNS	77	Standard query 0xbefb A logs1169.xiti.com			
...	11...	17...	19...	DNS	72	Standard query 0x1cf8 A ws.batch.com			

Pour ce test, j'ouvre la page web du site www.tf1.fr et je n'affiche que les demandes DNS (dns.qry.type == 1) et je n'affiche pas les réponses (dns.flags.response == 1)

# Serveurs & Nat

Comment traverser ?



# Héberger un serveur derrière un routeur



Comment héberger un serveur sur un réseau privé avec du NAT ?

- Le serveur possède une IP privé non routable sur Internet
- Le routeur possède un firewall bloquant toute communication entrante

## ■ LES ÉTAPES DU TD :

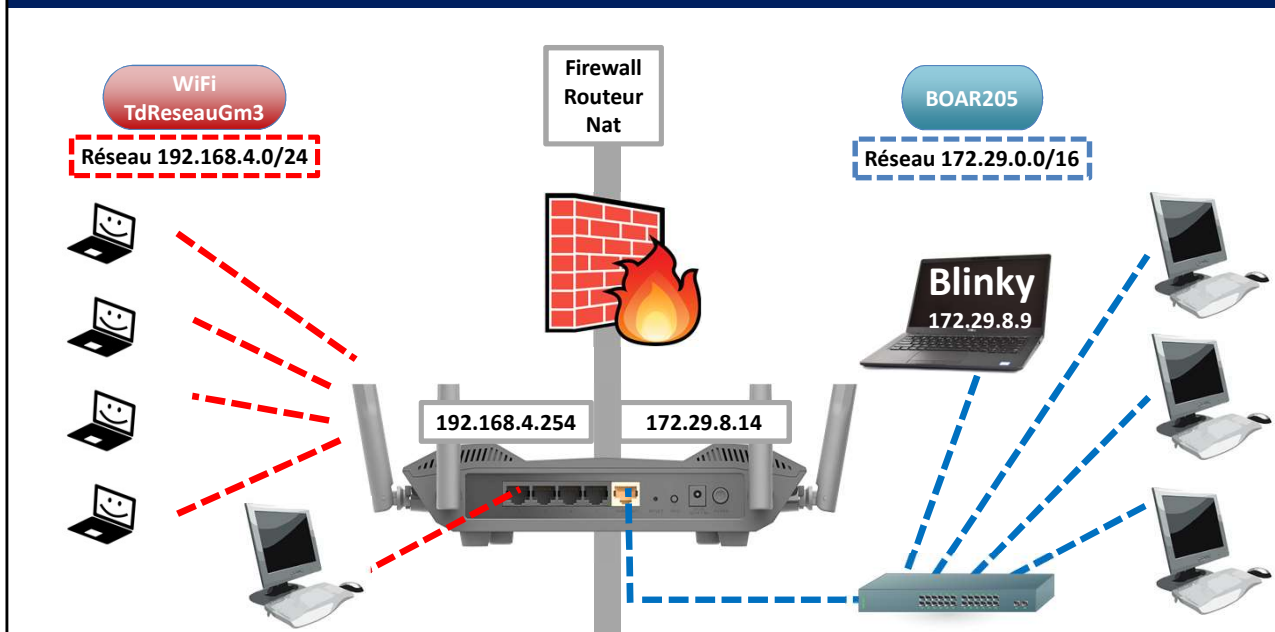
1. Proposer un serveur sur votre portable
2. Un nmap depuis l'extérieur montre les ports ouverts (démon de mon PC)
3. Ouverture du ou des ports
4. Nouveau nmap et test de connexion depuis un des PC de la salle

L'objectif est ici de montrer qu'un serveur accessible dans notre réseau local est indisponible une fois hors de ce réseau (côté Internet).

Les ports ouverts sur le serveur ne le sont pas sur le routeur.

Il faut ajouter une règle dans le routeur qui est la seule IP visible de l'Internet.

# Héberger un serveur derrière un routeur avec NAT



Pour les besoins du TD, notre boîtier utilise deux réseaux IPv4 privés.  
Pour une box 'familiale' le côté côté WAN utilise une adresse IP Publique.

Configuration TD :

- Les PC portables utilisent le WiFi 'TdReseauGm3'  
Les adresses réseaux sont en 192.168.4.0/24  
Un PC relié par un câble utiliserait le commutateur intégré, sur le même réseau.  
La passerelle utilise l'adresse 192.168.4.254
- Le PC de la salle de TD utilise le réseau pédagogique de l'INSA  
Les adresses réseaux sont en 172.29.0.0/16  
La passerelle est en 172.29.0.3  
Le PC utilisé lors de l'exercice précédent se nomme blinky.insa-rouen.fr  
(172.29.8.9)

## Installation rapide d'un serveur Web

Les informations de cette page sont disponibles  
sur le site : <http://192.168.4.21/>

Sur votre UBUNTU :

- `sudo apt update`
- `sudo apt install apache2`
- Le serveur Web est accessible, vous pouvez consulter la page par défaut sur le <http://127.0.0.1>
- La page web source est `/var/www/html/index.html`
- Il faut se donner les droits pour la modifier (chown)
- Modifier la page permet de la reconnaître, sinon nous avons tous la même

## Contrôle du bon fonctionnement

Quels ports sont ouverts en écoute sur votre PC ?

- Sous Linux : **netstat -nat**
- Sous Windows : **netstat -n -a -p tcp**
- Notes :
  - L'option -n conserve l'affichage de l'adresse IP
  - a affiche toutes les connexions
  - t affiche les connexions TCP (-p tcp sous Windows)
- Que donne en comparaison un nmap sur votre PC ?
- Demander à un autre utilisateur de se connecter sur votre serveur Web en utilisant votre adresse IP
- La connexion est elle bonne ?
- Pouvez-vous vous connecter à votre serveur Web depuis un des PC de la salle BOAR205 ?

L'objectif est ici de montrer qu'un serveur accessible dans notre réseau local est indisponible une fois hors de ce réseau (coté Internet).

Les ports ouverts sur le serveur ne le sont pas sur le routeur.

Il faut ajouter une règle dans le routeur qui est la seule IP visible de l'Internet.

## Configuration Firewall (Uncomplicated FireWall)

Sur votre UBUNTU :

- Par défaut le firewall est inactif `sudo ufw status` → Etat : inactif  
Le serveur Web est accessible
- Activer le pare-feu : `sudo ufw enable`  
Le serveur web est il encore accessible depuis un autre poste ?
- Autoriser Apache dans le firewall `sudo ufw allow Apache`  
Faire un `sudo ufw status` pour voir l'impact depuis l'autre poste
- Les fichiers de configuration sont visibles dans le dossier `/etc/ufw`  
(fichiers .rules)

On montre ici l'impact du firewall intégré au système d'exploitation



## Héberger un serveur derrière un routeur

The image displays three screenshots of a router's configuration interface, specifically the 'Create New Rule' section.

- Virtual Server:** This window shows a rule named 'HTTP'. The Local IP is set to '192.168.4.200'. The Protocol is 'TCP'. The External Port is '80' and the Internal Port is also '80'. The Schedule is set to 'Always Enable'.
- Port Forwarding:** This window shows a rule named 'MonServeurWeb'. The Local IP is '192.168.4.200'. The TCP Port is '80'. The Schedule is set to 'Always Enable'.
- Firewall:** This window shows a rule named 'JusteInsa'. The Source IP Address Range is 'WAN' (193.49.0.0-193.49.254.254). The Destination IP Address Range is 'LAN' (192.168.4.200). The Protocol & Port Range is 'TCP' (80-443). The Schedule is set to 'Always Enable'.

To the right of the screenshots, there is a list of three examples of configurations:

- Port Forwarding:** redirection de port simple
- Virtual Server:** redirection avec possibilité de changement du port de destination
- Firewall:** Restriction d'accès en fonction de l'IP entrante et sur certains ports seulement.

Attention, les écrans affichés ici concerne l'interface de configuration du routeur DLINK utilisé en TD et peuvent varier suivant le matériel utilisé.

### Le plus simple: **Port Forwarding**

La zone **Name** est une simple zone de texte utilisée ici pour indiquer qu'il s'agit d'un serveur Web.

La zone **Local Ip** est automatiquement remplie par la liste déroulante de droite (computer Name) qui affiche les PC du réseau.

Le **TCP Port** est le numéro de port à rediriger, ici le 80.

**Le port 80 du routeur sera redirigé sur le port 80 du 182.168.4.200**

Le mode **Virtual Server** reprend les même réglages mais permet de dissocier le port externe (du routeur) de l'interne (notre serveur).

Ainsi, si notre serveur web est en écoute sur le port 8080, un port non standard, son accès sera transparent pour les utilisateurs (voir le cas du téléphone de l'exercice vu précédemment)

Le **firewall** est une autre fonction importante de nos 'box'.

L'exemple affiché permet de restreindre l'accès au serveur Web configuré dans le Port

forwarding a une plage d'adresse IP publique appartenant à l'INSA

**Protocol & Port Range** : Les ports TCP 80 à 443 de l'adresse 192.168.4.200 sont ouverts pour toutes machines possédant une adresse IP en 193.49.0.0 à 193.49.254.254

Dans cette configuration, les PC pédagogiques de l'INSA sont exclus puisqu'ils utilisent une adresse en 194.254.19.x

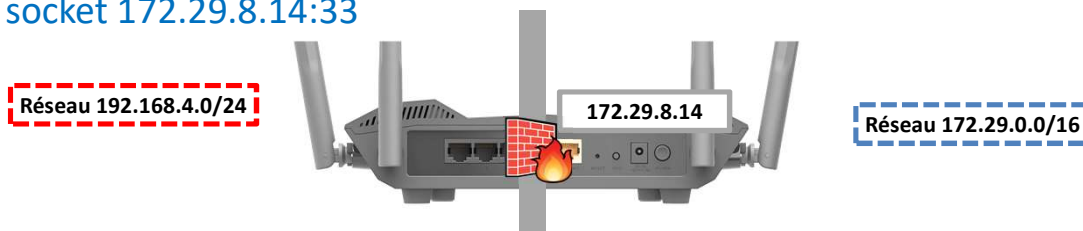
Il est possible d'ajouter une plage horaire pour tous les réglages (Schedule).

## Configuration redirection de ports

Votre site Web n'est pas visible pour les postes hors de votre réseau local

Démo : nmap / modification firewall / nmap

- Indiquez moi votre adresse IP et votre serveur sera accessible sur l'adresse IP de notre boîtier TdReseauGm3 côté WAN
- Le socket ouvert sera 'IP du boîtier': 'adresse de votre hôte'  
Par exemple, pour le PC d'adresse 192.168.4.33, la page sera visible sur le socket 172.29.8.14:33



Nous n'avons pas eu le temps de faire cette opération.

Lors du TD, seul un serveur web était accessible du réseau pédagogique (des PC de la salle) vers le réseau Wifi de notre TD.

Pour afficher la page Web depuis les PC de la salle de cours, il faut aller sur le site <http://172.29.8.14>. La fonction utilisée par notre box 'DLINK' pour réaliser cette ouverture était le port forwarding.

Seul défaut, un seul serveur est accessible par cette méthode, tous les serveurs web étant en écoute sur le même port 80.

Pour rendre accessibles les autres serveurs Web, il faut ouvrir d'autres ports sur notre 'box' avec la fonction 'virtual server' qui permet de changer le port d'entrée et de sortie. Ce qui permet, par exemple, d'ouvrir le port 81 de l'adresse 172.29.8.14 et de la rediriger vers une adresse interne, par exemple 192.168.4.120 et le port 80.

Pour afficher depuis le réseau des PC de la salle de cours, il faut aller sur le site, il faut aller sur le site <http://172.29.8.14:81>, on spécifie à la fois l'adresse IP et le port à consulter.

FIN DU TD 4

